TABLA DE CONTENIDO

1. OBJETIVOS 2
2. RESPONSABLES. 3
3. DEFINICIONES. 6
4. MARCO NORMATIVO 11
5. RECURSOS 13
6. GENERALIDADES. 14
   6.1 POLÍTICAS ESPECÍFICAS DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN. 14
   6.1.1 ORGANIZACIÓN DE LA INFORMACIÓN. 14
   6.1.2 GESTIÓN DE ACTIVOS. 17
   6.1.3 DISPOSITIVOS MÓVILES. 19
   6.1.4 POLÍTICA DE CONTROL DE ACCESO. 22
   6.1.5 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES. 26
   6.1.6 INTEGRIDAD DE LA INFORMACIÓN. 30
   6.1.7 DISPONIBILIDAD Y CONTINUIDAD DEL SERVICIO E INFORMACIÓN. 31
   6.1.8 CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN. 33
   6.1.9 POLÍTICA DE ESCRITORIOS Y PANTALLA LIMPIA. 35
7. CONTROL DE DOCUMENTOS. 37
8. ANEXOS. 37

Elaborado por:	Aprobado por:	Registrado SIG:
ORIGINAL FIRMADO	ORIGINAL FIRMADO	ORIGINAL FIRMADO
	Jennifer Lorena Suarez Bermúdez Subdirectora General	
	ORIGINAL FIRMADO	
José Antonio Palma Bacca. Profesional Universitario CPS	**Luis Carlos Londoño Vargas** Director General	**Rafael Andrés Melo C**. Coordinador de Calidad

1. OBJETIVOS

OBJETIVO GENERAL

Establecer las Políticas específicas de Controles de Seguridad y Privacidad de la Información que regulan la seguridad de la información en el Instituto de Turismo del Meta, proteger los activos de información, con base en los criterios de Confidencialidad, Integridad y Disponibilidad, mediante la implementación de controles en los procesos del Instituto de manera coordinada con las partes interesadas, presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros.

OBJETIVOS ESPECÍFICOS.

Los objetivos para las políticas específicas son:

- **Política de Organización De La Seguridad De La Información:** Establecer como máxima autoridad del Sistema de Gestión de Seguridad de la Información al Comité de Desempeño Institucional, establecer la mesa de seguridad de la información, definir los roles y responsabilidades de la seguridad de la información.

- **Política de Gestión de Activos:** Establecer las directrices mediante los cuales se indica a los funcionarios, contratistas y terceras partes involucradas los límites y procedimientos frente a la identificación, uso, administración y responsabilidad de los activos de Información.

- **Política de Dispositivos Móviles**: Especificar las condiciones para el uso de los dispositivos móviles institucionales o personales que acceden a información del Instituto de Turismo del Meta, y velar por el uso responsable de estos por parte del personal, reducir el riesgo de pérdida, daño o divulgación de la información pública, clasificada o reservada por el uso de dispositivos móviles.

- **Política de Control de Acceso**: Garantizar que la información, las áreas de procesamiento de información, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información del Instituto de Turismo del Meta estén debidamente registrados, protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.

- **Política de Tratamiento de Datos Personales:** Garantizar la protección de los datos personales o de cualquier otro tipo de información que sea utilizada o repose en sus

bases de datos y archivos del Instituto de Turismo del Meta, garantizando el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se hubiera recogido sobre ellas en bases de datos o archivos.

- **Política De Integridad de la Información:** Establecer los lineamientos definidos por el Instituto para garantizar el manejo íntegro e integral de la información tanto interna como externa, conocida o administrada por funcionarios, contratistas o terceras partes involucradas en los procesos organizacionales del Instituto de Turismo del Meta.

- **Política de Disponibilidad:** Asegurar que los servicios TIC estén disponibles y funcionen correctamente siempre que los funcionarios, contratistas y Usuarios externos del Instituto de Turismo del Meta deseen hacer uso de ellos.

- **Política De Capacitación Y Sensibilización en seguridad de la información:** Establecer los parámetros necesarios para fortalecer en los servidores públicos y contratistas del Instituto de Turismo del Meta, y personal provisto por terceras partes, una cultura organizacional capacitada, informada y comprometida con la seguridad de la información bajo los criterios del SGSI del Instituto.

- **Política De Escritorios Y Pantalla Limpias:** Establecer los lineamientos que deberán acatar los usuarios y partes interesadas del Instituto de Turismo del Meta en pro de prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral, mediante lineamientos que sean aplicados por los colaboradores a los que se les haya otorgado permiso de acceso a la documentación, sistemas de información, bases de datos, equipos informáticos o servicios de TI.

2. RESPONSABLES.

A continuación, se detallan los roles y responsabilidades frente a las políticas específicas de seguridad de la información:

COMITÉ DE DESEMPEÑO INSTITUCIONAL.

- Implementar al interior del Instituto la política de Seguridad digital y la gestión de la Seguridad de la Información.
- Responsable de liderar y vigilar el establecimiento, implementación, mantenimiento y mejora continua del SGSI conforme a la norma NTC-ISO-IEC 27001

- Desarrollar el proceso de gestión del riesgo en la seguridad de la información que sea adecuado para la institución.
- Definir las funciones y las responsabilidades, en cuanto a seguridad de la información, de todas las partes, tanto internas como externas, de la institución.
- Revisar, validar y aprobar las políticas, manuales, planes, procedimientos, formatos y demás documentos que soporten la implementación y mejoramiento continuo del SGSI.

RESPONSABLE DEL DIRECCIONAMIENTO ESTRATÉGICO / DIRECCIÓN GENERAL

- Es el representante legal del Instituto de Turismo del Meta y responsable principal de la aplicación del sistema de Gestión de Seguridad de la Información.
- Asegurar los recursos para la implementación y aplicación del SGSI
- Asegurar que se establezca la política de seguridad de la información y los objetivos de seguridad de la información, compatibles con la estrategia de la organización.
- Comunicar y promover la toma de conciencia en cuanto a la importancia de una gestión de seguridad de la información eficaz conforme con los requisitos del sistema de gestión de seguridad de la información.
- Revisar, aprobar y hacer seguimiento a la implementación y mejora continua del SGSI.
- Dirigir y apoyar a las personas, para contribuir a la eficacia del sistema de gestión de seguridad de la información.

SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA. / SUBDIRECCIÓN GENERAL.

- Rendición de Cuentas al coordinador Nacional de Seguridad Nacional, sobre la implementación de la política de Seguridad de la Información (Seguridad Digital).
- Asignar los rubros y recursos necesarios para la implementación y mejora continua del SGSI.
- Garantizar la integridad y disponibilidad de los bienes y recursos necesarios para la operación y continuidad de los procesos del Instituto.
- Garantizar la integridad, disponibilidad y confidencialidad de la información financiera del Instituto.
- Articulación de esfuerzos, recursos, metodologías y estrategias del Instituto.

LÍDERES DE PROCESOS.

- Conocer y velar por la aplicación de las políticas, objetivos, manuales y procedimientos de seguridad de la información (seguridad digital) en cada uno de los procesos.

- Garantizar los recursos necesarios para la aplicación de los controles definidos por el SGSI para la seguridad de la información en sus respectivos procesos, cuando se requieran, y dichos controles deben ser aplicados a cargo de sus dependencias.
- Incluir en el plan institucional de capacitación el plan de capacitación, socialización y sensibilización del SGSI, y velar por su aplicación al interior del Instituto.
- Asegurar la integración de los requisitos del SGSI en los procesos del Instituto.
- Integrar y aplicar las políticas, manuales, formatos y procedimientos de seguridad digital y seguridad de la información al ciclo de vida de los programas y proyectos, y a los demás procesos de planeación.

RESPONSABLE DE LA CONTINUIDAD / SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA – GESTOR DE TIC.

- Velar por la continuidad de la seguridad de la información.
- Realizar la planificación de la continuidad de la seguridad de la información.
- Asegurar la Implementación de la continuidad de la seguridad de la información.
- Verificar, revisar y evaluar la continuidad de la seguridad de la información.
- Mantener una alta disponibilidad de las instalaciones de procesamiento de información.
- Realizar control de acceso a áreas restringidas de administración de equipos de información y comunicaciones.
- Definir y aplicar los perímetros de seguridad física necesarios.
- Definir e implementar gestión de Teletrabajo.

RESPONSABLE DE SI - GESTOR DEL SGSI

- Dirigir la definición de la política de seguridad de la información (Seguridad Digital)
- Dirigir la definición del alcance, exclusiones y objetivos del SGSI.
- Acompañar la definición de la seguridad física y del entorno para el Instituto.
- Acompañar la formulación de los procedimientos operacionales y responsabilidades necesarios para el Instituto en cuanto a seguridad de la información.
- Acompañar la formulación del plan de Capacitación, socialización y sensibilización de la seguridad de la información.
- Acompañar la definición del Plan de seguimiento, evaluación y análisis del MSPI.
- Planificar y definir los requisitos de seguridad de los sistemas de información.

RESPONSABLE DE LA GESTIÓN DOCUMENTAL / SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA.

- Garantizar la disponibilidad, integridad y confidencialidad de la información en la gestión de los archivos físicos de gestión y general del Instituto.
- Garantizar la disponibilidad, integridad y confidencialidad de la información en la gestión de los documentos electrónicos del Instituto.
- Garantizar la aplicación correcta de la gestión de cambios en la documentación del SGSI y del SIG en general.

3. DEFINICIONES.

- **Pantalla limpia:** Protección de los equipos de cómputo, tabletas, portátiles u otros dispositivos mediante un bloqueo de pantalla o desconexión cuando no está en uso.
- **Escritorio limpio:** Protección de los papeles y dispositivos removibles de almacenamiento de información, almacenados y manipulados en puestos de trabajo, de accesos no autorizados, pérdida o daño de la información.
- **Acceso físico**: Significa ingresar a las áreas de misión crítica o instalaciones en general de un sitio del Instituto.
- **Acceso lógico:** En general, el acceso lógico es un acceso en red, por ejemplo: acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos. La mayoría de los accesos lógicos se relacionan con algún tipo de información.
- **Acceso:** En relación con la seguridad de la información se refiere a la identificación, autenticación y autorización de un usuario a los sistemas, recursos y áreas de la Superintendencia de Subsidio Familiar en un momento dado.
- **Área segura:** Espacio físico donde se almacena o procesa información crítica del Instituto.
- **Autorización:** Es el permiso o consentimiento que da el titular de los datos para el tratamiento específico de estos, acorde con las funciones del Instituto.
- **Aviso de Privacidad:** Comunicación verbal o escrita generada por el responsable, dirigida al Titular de los Datos, para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las Políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.
- **Base de datos personales:** Conjunto organizado de datos de carácter personal, creados, almacenados, organizados, tratados y con acceso manual o a través de programas de ordenador o software.

- **Base de Datos:** Conjunto organizado de Datos Personales que sean objeto de tratamiento.
- **Biométrico:** Sistema de información de control de acceso de funcionarios, que permite registrar los ingresos y salidas de los funcionarios mediante un control de identificación por huella digital, con algunas excepciones con contraseña asignada a cada funcionario.
- **Dato personal:** Es la información que identifica a una persona o que pueda asociarse y la haga identificable; estos datos pueden ser numéricos, alfabéticos, gráficos, visuales, biométricos, o de cualquier otro tipo.
- **Dato Privado:** Aquel que por su naturaleza íntima o reservada sólo es relevante para el Titular.
- **Dato Semiprivado:** Es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial.
- **Dato personal público:** Es la información personal que la Constitución y las normas han determinado como públicos y que para su recolección y tratamiento no requiere de autorización del titular de la información y los cuales pueden ser ofrecidos u obtenidos sin reserva alguna.
- **Dato personal semiprivado:** Son datos que no tienen naturaleza íntima ni pública, cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. Para su tratamiento se requiere la autorización expresa del titular de la información. (Ej. Dato financiero y crediticio).
- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Dato sensible:** Información que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos, entre otros, la captura de imagen fija o en movimiento, huellas digitales, fotografías, iris, reconocimiento de voz, facial o de palma de mano, etc.
- **Documento Electrónico:** Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares.

- **Encargado del tratamiento**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.
- **Habeas Data:** Derecho fundamental que le asiste a toda persona para conocer, actualizar, rectificar y/o cancelar la información y datos personales que se hayan recolectado en bases de datos públicas o privadas, acorde con lo dispuesto en la ley y demás normas que le apliquen.
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.
- **Información Pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.
- **Lugar seguro:** Es aquel que protege el activo de información de acceso de personas no autorizadas, que su contenido no sea alterado y que el activo pueda ser recuperado por las personas autorizadas de manera oportuna (algunos ejemplos son: Cajón seguro con llave, oficina con llave, etc.)
- **Medio Extraíble:** Dispositivo que permite almacenar o transportar información como memorias USB, tarjetas de memoria, cintas magnéticas, CD, DVD, discos duros externos.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **Personal:** Es aquella persona que tiene una relación con el Instituto de Turismo del Meta directa o a través de un tercero, bajo cualquier tipo de vinculación Planta, carrera administrativa, contratistas, etc.
- **Principio de Acceso y Circulación Restringida**: El Tratamiento de datos personales sólo podrá realizarse por las personas autorizadas por el Titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la ley.
- **Principio de Confidencialidad:** Todas las personas que en el Instituto de Turismo del Meta, administren, manejen, actualicen o tengan acceso a informaciones de cualquier tipo que se encuentre en Bases de Datos, están obligadas a garantizar la reserva de

la información, por lo que se comprometen a conservar y mantener de manera estrictamente confidencial y no revelar a terceros, toda la información que llegaren a conocer en la ejecución y ejercicio de sus funciones; salvo cuando se trate de actividades autorizadas expresamente por la ley de protección de datos.

- **Principio de Finalidad:** El Tratamiento obedecerá a una finalidad legítima de acuerdo con la Constitución Política de Colombia, las leyes aplicables y demás normas que las desarrollen. El Titular será informado de manera clara, suficiente y previa acerca de la finalidad de la información suministrada.
- **Principio de Legalidad**: El tratamiento de datos es una actividad reglada, la cual deberá estar sujeta a las disposiciones legales vigentes y aplicables que rigen la materia. El Tratamiento se ejercerá únicamente con el consentimiento previo, expreso e informado del Titular. Los Datos Personales que sean recolectados sin el mencionado consentimiento estarán autorizados por la Ley o por la implementación de mecanismos eficientes de comunicación, sin perjuicio de la solicitud de supresión de los Datos Personales que eventualmente pueda ser elevada por el Titular y que proceda por no mediar una obligación legal o contractual que lo impida.
- **Principio de Seguridad:** La información sujeta a tratamiento por el Instituto de Turismo del Meta, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- **Principio de Transparencia**: En el Tratamiento de Datos Personales se garantiza el derecho del Titular a obtener en cualquier momento y sin restricciones, información acerca de la existencia de datos que le concierne.
- **Principio de Veracidad o Calidad:** La información sujeta a Tratamiento de datos personales debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- **Principios aplicables al tratamiento de datos personales**: Para efectos de garantizar la protección de datos personales, se aplicarán de manera armónica e integral los siguientes principios, a la luz de los cuales se deberá realizar a recolección, manejo, uso, tratamiento, almacenamiento, transferencia y transmisión de datos personales:
- **Propietario de la base de datos:** El Instituto de Turismo del Meta es el propietario de la base de datos personales que por su misión ha organizado por medio de la información que recolecta a través de sus sistemas de información y tiene bajo su responsabilidad el tratamiento, gestión y resguardo de estas.
- **Puesto de trabajo:** Área dispuesta por el Instituto de Turismo del Meta para que cada funcionario o contratista de prestación de servicios pueda llevar a cabo sus actividades. Tales como oficinas, escritorios entre otros.

- **Reclamo:** Solicitud del Titular del dato o de las personas autorizadas por éste o por la Ley para corregir, actualizar o suprimir sus datos personales o para revocar la autorización en los casos establecidos en la Ley.
- **Responsable de la base de datos:** Es la persona o funcionario que tiene bajo su resguardo las bases de datos personales al interior del Instituto de Turismo del Meta.
- **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y lo el tratamiento de los datos.
- **RGDPC o Régimen General de Protección de Datos Personales Colombiano**: es el conjunto de normas que regula el Tratamiento de Datos Personales en el territorio colombiano tales como, el artículo 15 de la Constitución Política colombiana; la ley 1266 de 2008, la Ley 1581 de 2012; el Decreto 1377 de 2013; el Decreto 1074 de 2015; el Decreto 886 de 2014; y las demás normas que las modifiquen o adicionen.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Titular**: Persona natural o jurídica cuyos datos personales sean objeto de tratamiento.
- **Transferencia de datos:** Se da cuando el responsable o encargado directo del tratamiento de datos personales, ubicado en Colombia, envía o entrega la información o los datos personales a otra persona o entidad pública o privada que a su vez es responsable del tratamiento de los datos el cual puede encontrarse dentro o fuera del país.
- **Transferencia**: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del responsable.
- **Tratamiento de datos**: Se define como la manipulación o conjunto de operaciones y procedimientos técnicos de carácter manual o automatizado, que se realiza sobre datos personales, tales como: recolección, grabación, almacenamiento, conservación, uso, análisis, circulación, modificación, bloqueo, cancelación, y transferencia, entre otros.
- **Tratamiento**: Es cualquier operación o conjunto de operaciones sobre Datos Personales, tales como la recolección, administración, almacenamiento, uso, circulación, transmisión, transferencia o supresión.
- **Usuario:** Es la persona natural o jurídica que tiene interés en el uso de la información de carácter personal.

4. MARCO NORMATIVO

MARCO LEGAL

- Constitución Política de Colombia. Artículo 15.
- **Ley 44 de 1993:** "Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor)".
- **Ley 527 de 1999**: "Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones".
- **Ley 594 de 2000:** "Por medio de la cual se expide la Ley General de Archivos".
- **Ley 850 de 2003:** "Por medio de la cual se reglamentan las veedurías ciudadanas".
- **Ley 1266 de 2008:** "Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".
- **Ley 1273 de 2009**: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- **Ley 1341 de 2009**: "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC, se crea la agencia Nacional de espectro y se dictan otras disposiciones".
- **Ley 1437 de 2011:** "Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo".
- **Ley 1474 de 2011**: "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública".
- **Ley 1581 de 2012:** "Por la cual se dictan disposiciones generales para la protección de datos personales".
- **Ley 1712 de 2014**: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1915 de 2018: Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos".
- **Ley 1952 de 2019:** "Por medio de la cual se expide el código general disciplinario".
- **Decreto 2609 de 2012:** "Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
- **Decreto 0884 del 2012:** "Por el cual se reglamenta parcialmente la Ley 1221 del 2008".

- **Decreto 1377 de 2013**: "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".
- **Decreto 886 de 2014**: "Por el cual se reglamenta el Registro Nacional de Bases de Datos".
- **Decreto 103 de 2015:** "Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".
- **Decreto 1074 de 2015**: "Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26".
- **Decreto 1078 de 2015**: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- **Decreto 1080 de 2015:** "Por medio del cual se expide el Decreto Reglamentario del Sector Cultura".
- **Decreto 1081 de 2015:** "Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia".
- **Resolución 512 de 2019**: "Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información".
- **CONPES 3701 de 2011**. "Lineamientos de Política para Ciberseguridad y Ciberdefensa".
- **CONPES 3854 de 2016**. Política Nacional de Seguridad digital.

REQUISITOS TÉCNICOS:

- **Decreto 2269 de 1993**. "El Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, es el organismo nacional de normalización"
- **NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001: "TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI**)", Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).
- **GTC ISO IEC 27002** Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para Controles de Seguridad de la Información
- **NTC ISO IEC 27005** Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.
- **TC ISO 19011** Directrices para la Auditoría de los Sistemas de Gestión.
- **MSPI**: Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

5. RECURSOS

La alta dirección debe garantizar todos los recursos necesarios para la aplicación y cumplimiento de las políticas específicas de seguridad y privacidad de la información en el Instituto de Turismo del Meta.

TALENTO HUMANO

La aplicación de estas Políticas específicas compromete a los servidores públicos del proceso Administrativo y Financiero y Direccionamiento Estratégico, de acuerdo al rol que este realice en el presente procedimiento.

MAQUINARIA Y TECNOLOGÍA

Equipos de cómputo, impresora y software básicos. Muebles archivadores con capacidad suficiente para almacenar los documentos del sistema. Conexión y acceso a Internet.

MATERIALES O LOGÍSTICOS

Papelería, espacios, mobiliario, sonido, elementos de oficina.

METODOLÓGICOS

Normas técnicas y legales aplicables.

MEDIO AMBIENTE

Oficina con muebles suficientes con temperatura e iluminación adecuada.

6. GENERALIDADES.

6.1 POLÍTICAS ESPECÍFICAS DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN.

Las presentes políticas específicas de controles de seguridad de la información son aplicables a todos los funcionarios(as), contratistas y terceros del Instituto de Turismo del Meta, sin excepción, en donde cada uno de los cuales cumple un rol en la administración de la seguridad de la información. Todos los funcionarios, contratistas y terceros del Instituto son responsables de mantener un ambiente seguro para la información.

Las **POLÍTICAS ESPECÍFICAS DE CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** serán revisadas una vez al año, con el fin de asegurar su eficiencia y efectividad, de igual manera será actualizada en caso que se requiera

El Instituto de Turismo del Meta debe establecer un **PLAN DE MEJORAMIENTO ANUAL** para el fortalecimiento del Sistema de Gestión de seguridad de la Información (SGSI).

Se considerará en el **PLAN ANUAL DE ADQUISICIONES** los recursos necesarios para el cumplimiento en la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información, con el objetivo de asignar los recursos necesarios para el fortalecimiento en la implementación de la infraestructura tecnológica requerida para la seguridad de la Información en el **INSTITUTO DE TURISMO DEL META.**

6.1.1 POLITICA DE ORGANIZACIÓN DE LA INFORMACIÓN.

- **Comité de Desempeño Institucional.**

El Instituto de Turismo del Meta define como máxima autoridad del Sistema de Gestión de Seguridad de la Información al Comité de Desempeño Institucional quien es responsable de la orientación estratégica para la administración de los activos de información, la sostenibilidad y mejora del sistema Integrado de Gestión del Instituto de Turismo del Meta.

- **Mesa de Seguridad de la Información**

a) Conformación:

Esta política además tiene como finalidad establecer la **Mesa de Seguridad de la Información,** integrada por:

- Subdirección General - Administrativa y financiera o su delegado.
- Profesional a cargo del Proceso de Gestión de las TIC´S.
- Profesional a cargo del Proceso del Sistema Integrado de Gestión.
- Funcionario a cargo del Proceso de Gestión Documental.
- Profesional a cargo del Sistema de Gestión de Seguridad de la Información.

La Mesa de Seguridad de la Información determina las estrategias para el desarrollo del Sistema de Gestión de Seguridad de la Información, garantizando que se cumplan los lineamientos y los objetivos establecidos.

Esta mesa de Seguridad de la Información podrá ser conformada por funcionarios y/o contratistas del Instituto de Turismo del Meta.

b) Funciones:

Los miembros de Mesa de Seguridad de la Información deben:

- Monitorear el cumplimiento de las políticas de seguridad definidas, revisar y hacer seguimiento a la implementación y mejora continua del SGSI.
- Estudiar y realizar propuesta para la asignación de los recursos necesarios para el cumplimiento de las metas establecidas del SGSI.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de la información del SGC frente a posibles amenazas, sean internas o externas.
- Verificar el inventario de activos de la Información.
- Estudiar y conceptuar los casos especiales de seguridad presentados en la institución, para recomendar las acciones pertinentes y apoyar la toma de decisiones.
- Revisar los diagnósticos del estado de seguridad de la información.
- Acompañar e impulsar el desarrollo de proyectos de seguridad de la información.
- La **Mesa de Seguridad de la Información** se reunirá mínimo una vez cada tres meses, previa convocatoria por parte de la Subdirección General - Administrativa y financiera o su delegado, adicionalmente podrán ser citados a participar a sesiones extraordinarias de trabajo cuando las circunstancias lo ameriten, en especial frente al montaje, implementación y mantenimiento del sistema de gestión de seguridad de la información y/o incidentes de seguridad.
- Promover la difusión y sensibilización de la seguridad de la información en el SIG.
- Realizar una revisión inicial a las políticas como mínimo una vez al año o cuando se produzca un cambio relevante en la operación que implique realizar ajustes de los cambios en el entorno físico, tecnológico y/o de las necesidades de la operación.
- Revisar la definición y actualización de la "**MATRIZ DE ROLES Y RESPONSABILIDADES",** respecto a la Seguridad y privacidad de la Información.

- Revisar la definición y actualización de la "**MATRIZ DOFA – CONTEXTO INSTITUCIONAL",** respecto a la Seguridad y privacidad de la Información.
- Presentar ante el Comité de Desempeño institucional las propuestas, sugerencias y comentarios frente a las políticas, manuales, procedimientos y formatos del SGSI del Instituto departamental para su estudio y aprobación, en el marco de un proceso de mejora continua.
- Revisar, monitorear la matriz de riesgos de seguridad y privacidad de la información y su tratamiento, en el marco de un proceso de mejoramiento continuo en la aplicación de controles.

➢ **Contacto con autoridades y grupos de interés**

- El Instituto de Turismo del Meta debe mantener contacto con las autoridades y grupos de interés para estar al corriente en cambios de normativa del gobierno electrónico en Colombia e identificar las tendencias en Seguridad de la Información.
- El Instituto de Turismo del Meta debe mantener un directorio actualizado para el contacto con autoridades y grupos de interés especial, formato: **"CONTACTO CON LAS AUTORIDADES"**, formato: **"CONTACTO CON LOS GRUPOS DE INTERÉS ESPECIAL."**
- Las autoridades corresponden a las entidades competentes en caso de que se presentara un incidente de cualquier índole que pusiera en riesgo la confidencialidad, integridad y disponibilidad de la información, en caso de requerirse el llamado a las autoridades mencionadas, sólo podrán hacerlo los funcionarios encargados.
- Se debe mantener contacto permanente con las Universidades, los grupos de investigación, entidades del gobierno, proveedores de tecnología que trabajan en pro de mantener actualizado a las personas que se desarrollan dentro del ámbito de la tecnología, para de esta manera mantenerse al tanto en amenazas, incidentes y soluciones.

➢ **Revisión independiente en seguridad de la información:**

- El Instituto de Turismo del Meta debe implementar y ejecutar un **PLAN INTERNO DE AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN.**
- Este plan debe estar enfocado hacia la revisión de todos los requerimientos (políticas y procedimientos) de seguridad de la información, los resultados deben generar un programa de seguridad, que incluya como mínimo: acciones a realizar, tablas de tiempo y responsables.
- El plan debe ser aprobado por el Comité de Desempeño Institucional previa revisión de la Mesa de Seguridad de la Información

6.1.2 POLITICA DE GESTIÓN DE ACTIVOS.

El Instituto de Turismo del Meta debe definir, dar a conocer a todos los involucrados de la organización, aplicar, monitorear, controlar, actualizar y mejorar periódicamente el **"PROCEDIMIENTO PARA LA GESTIÓN DE ACTIVOS DE INFORMACIÓN"**, junto con el formato **"MATRIZ DE GESTIÓN DE ACTIVOS DE INFORMACIÓN"**, en el que se considere lo siguiente:

- **Identificación de Activos**

- El Instituto de Turismo del Meta, debe realizar la identificación y/o actualización del inventario de Activos de Información una vez al año o en su defecto cuando se requiera por cambios normativos y/o administrativos.
- Considerar en la estructura del formato de la "**MATRIZ DE GESTIÓN DE ACTIVOS DE INFORMACIÓN",** como mínimo: un identificador del activo de información; el proceso responsable; trazabilidad con las tablas de retención documental o la gestión documental del Instituto; el nombre del activo; su descripción corta; idioma; tipo; medio de conservación; formato; si está disponible y/o publicada; su frecuencia de actualización.
- Cada funcionario o contratista debe ser responsable de realizar la actualización del inventario de los activos de información a su cargo, por lo menos una vez al año, en la herramienta definida por el Instituto de Turismo del Meta.
- La designación del responsable de coordinar la actualización de la matriz de Gestión de Activos de la información debe ser específica y explícita en el "**PROCEDIMIENTO PARA LA GESTIÓN DE ACTIVOS DE INFORMACIÓN"**.

- **Clasificación de Activos:**

- Definir en el "**PROCEDIMIENTO PARA LA GESTIÓN DE ACTIVOS DE INFORMACIÓN"** los criterios de clasificación de los activos de información de acuerdo a la criticidad, sensibilidad y reserva de la misma.
- Considerar las leyes y normatividades actuales y aplicables al Instituto, como son: Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015, entre otras que puedan aplicar de acuerdo a la naturaleza del Instituto, así como también los lineamientos establecidos por los gobiernos nacional y departamental aplicables a el Instituto.
- Considerar en la estructura del formato de la Matriz de Gestión de Activos de Información, como mínimo: la clasificación según disponibilidad, integridad y confidencialidad; quién es el propietario, el custodio y el usuario; fecha de ingreso y

salida; y su índice de información clasificada y reservada; de conformidad con los requisitos y lineamientos de la norma ISO27001 y demás normatividad aplicable.

- Cada responsable (designado por el líder del proceso) debe realizar el proceso de actualización de la clasificación de los activos de información a su cargo, por lo menos una vez al año, en la herramienta definida por la institución, o en su defecto cuando se requiera por cambios normativos y/o administrativos.
- Cualquier involucrado en los procesos organizacionales del Instituto debe informar al responsable de un respectivo activo de información o al responsable del SGSI, cualquier falencia en su tratamiento con el fin de adoptar las medidas pertinentes para la seguridad y privacidad de la información.

➢ **Etiquetado de la Información:**

- Los activos de información del Instituto deben estar clasificados y rotulados conforme a las tablas de retención documental, considerando tiempos de permanencia en su ciclo de vida y los lineamientos del proceso de gestión documental.
- Los documentos clasificados serán manejados, preparados, copiados y entregados sólo al personal autorizado.
- Se establecerán acuerdos periódicos con el líder del proceso de Gestión documental para revisiones de seguridad en la producción y copiado.

➢ **Devolución de los Activos:**

- Determinar el **FORMATO ÚNICO DE INVENTARIO DOCUMENTAL FUID**, mediante el cual se genera obligatoriedad para que los funcionarios, contratistas y/o terceros realicen la adecuada administración de la información al igual que la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con el Instituto.
- Dar a conocer a toda la organización el formato definido para este fin, y garantizar su aplicación.
- Determinar el responsable de la recepción y aprobación de la devolución de los activos de información, para cada proceso, mediante el formato definido por el Instituto.

➢ **Gestión de medios removibles:**

- La información confidencial crítica para el Instituto no puede ser extraída en medios removibles de uso personal sin previa autorización del propietario de la misma.
- El líder de cada proceso es responsable de emitir las autorizaciones para el uso de medios removibles.

- Las personas que tienen autorización para el uso medios de almacenamiento extraíbles deben comprometerse y cumplir con la **"DECLARACIÓN DE CONFIDENCIALIDAD"** firmada al momento de su vinculación.
- La información crítica o sensible del Instituto que se encuentra almacenada en un medio removible cuya vida útil es menor al tiempo de retención de la información establecida por el Instituto de Turismo del Meta, deberá respaldarse en otro medio para evitar la pérdida de información.

➢ **Disposición de los activos:**

- El Instituto de Turismo del Meta debe definir, dar a conocer y aplicar el procedimiento de **"DISPOSICIÓN DE LOS ACTIVOS FÍSICOS DOCUMENTALES DE INFORMACIÓN"** del proceso de Gestión documental mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o reúso cuando ya no se requieren los activos.
- Para la disposición final de los equipos de procesamiento y/o almacenamiento de información se debe dar cumplimiento al **"PROCEDIMIENTO PARA EL MANTENIMIENTO PREVENTIVO Y/O CORRECTIVO DE LA INFRAESTRUCTURA TECNOLÓGICA".**
- El líder del proceso o a quien este designe, debe emitir las correspondientes autorizaciones para la disposición de los medios removibles como activos de procesamiento y/o almacenamiento de información, en el formato de **"MANTENIMIENTO, SOPORTE Y CONCEPTO TECNICO DE TI".**

6.1.3 POLITICA DE DISPOSITIVOS MÓVILES.

La Dirección General del Instituto De Turismo Del Meta, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de la **POLÍTICA DE DISPOSITIVOS MÓVILES** buscando las mejores prácticas, teniendo en cuenta que los controles que se adopten para el uso de computadores portátiles, tabletas y demás dispositivos Móviles, protejan la información almacenada o procesada en estos dispositivos y el acceso a servicios de TI desde los mismos.

El Instituto de Turismo del Meta pone a disposición de algunos miembros del personal dispositivos móviles institucionales para facilitar el desempeño de sus labores y propende porque dichos funcionarios hagan un uso responsable de ellos.

Con el objetivo de dar cumplimiento y garantizar buenas prácticas de seguridad de la información, todos los involucrados en el alcance deben cumplir las siguientes directrices:

- Los documentos electrónicos que producen los funcionarios o contratistas en el ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales, según el caso, deben guardarse en la carpeta de almacenamiento en red dispuesta por el Instituto.
- El personal encargado de realizar las auditorías internas o externas que se realicen al Sistema de Gestión de Seguridad de la Información – SGSI del Instituto de Turismo del Meta, podrá realizar la verificación de las configuraciones de seguridad de los equipos móviles y su cumplimiento con los lineamientos de esta política.
- El profesional del proceso de Gestión de las TIC´S debe verificar que los equipos personales de los Servidores Públicos, contratistas o terceros del Instituto de Turismo del Meta que se conecten a la red de datos del Instituto cumplan con todos los requisitos o controles para autenticarse.
- En cualquier momento el profesional del Proceso de Gestión de las TIC´S podrá hacer revisión del cumplimiento de la presente política directamente en los dispositivos móviles.

➢ **Seguridad para el uso de dispositivos móviles privados**

Se debe considerar la seguridad para el uso de dispositivos móviles privados que accedan y procesen información del Instituto de Turismo del Meta.

- Los dispositivos móviles personales de contratistas o funcionarios que requieran tener acceso a los servicios de la red de datos del Instituto de Turismo del Meta deben solicitar autorización al supervisor de su contrato o jefe inmediato mediante un correo electrónico aceptando el cumplimiento de la política de dispositivos móviles.
- El supervisor de contrato o jefe inmediato debe comunicar mediante correo electrónico al profesional de apoyo encargado del proceso TIC "sistemas@turismometa.gov.co" la respectiva autorización de uso indicando la marca, número de serial del dispositivo y el nombre del contratista o funcionario a cargo.
- Todo equipo móvil como portátil, Tablet, disco duro externo que sea autorizado su uso por el Instituto de Turismo del Meta, se debe registrar en el formato **"FORMATO DE REGISTRO DE EQUIPOS MÓVILES AUTORIZADOS".**
- Los dispositivos móviles autorizados deberán tener instalado y configurado un software de antivirus y sistema operativo actualizado.
- Los dispositivos deben tener configurado un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 6 puntos de contacto, o huella digital.
- Configurar el bloqueo de pantalla para un mínimo de 5 minutos de inactividad.

- Configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos de forma remota, en caso de ser requerido.
- Utilizar en los dispositivos móviles únicamente redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.
- El usuario del dispositivo móvil autorizado debe mantener las configuraciones mínimas requeridas, antes mencionadas, mientras se encuentre conectado a la red del Instituto de Turismo del Meta.

➢ **Seguridad para dispositivos móviles del Instituto**

El Instituto de turismo del Meta debe considerar la seguridad de la información para los dispositivos móviles que hacen parte de su inventario tecnológico, y velar por el cumplimiento de los siguientes lineamientos y recomendaciones:

- Está prohibido almacenar información personal en los dispositivos móviles asignados por el Instituto de Turismo del Meta.
- Está prohibido realizar instalación de software de aplicaciones no autorizadas por el profesional de apoyo encargado del proceso TIC.
- Está prohibido cambiar la configuración, desinstalar software, formatear o restaurar de fábrica los equipos de cómputo.
- Utilizar los equipos móviles asignados por el Instituto de Turismo del Meta exclusivamente para desempeñar las funciones asignadas al cargo o las obligaciones contractuales pactadas.
- El funcionario al cual se le asigna el equipo móvil es responsable por su seguridad y correcta operación dentro de la red interna y en lugares públicos.
- Definir, socializar y aplicar el **"PROCEDIMIENTO DE AUTORIZACIÓN FORMAL DE SALIDA DE DISPOSITIVOS DE LAS INSTALACIONES"**, donde se especifique, entre otras cosas, que el uso de los equipos portátiles de propiedad del Instituto De Turismo Del Meta, fuera de las instalaciones, únicamente se permitirá a usuarios autorizados mediante el formato **"ORDEN DE SALIDA DE ELEMENTOS"**, la cual debe tener el visto bueno del jefe inmediato con firma autorizada para este fin.
- En caso de pérdida o robo de un dispositivo móvil de propiedad del Instituto de Turismo del Meta, los Servidores Públicos, tendrán que realizar la respectiva denuncia ante la entidad competente, luego debe dar aviso inmediato y por correo electrónico al profesional de apoyo encargado del proceso TIC "sistemas@turismometa.gov.co" con copia a la subdirección administrativa y financiera "subdireccionfinanciera@turismometa.gov.co" del Instituto de Turismo del Meta, quienes deben realizar las acciones necesarias para la protección de la información.

6.1.4 POLÍTICA DE CONTROL DE ACCESO.

Todos los funcionarios y contratistas del Instituto de Turismo del Meta, deben tener acceso sólo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de la institución. La asignación de privilegios y acceso a los activos de información (correo electrónico institucional, software, aplicaciones, carpetas compartidas, impresoras, etc.), áreas de trabajo, áreas de procesamiento de información y demás instalaciones del Instituto, deben estar basados en las necesidades de las áreas y aprobados por el supervisor o jefe Inmediato.

- **Control de Acceso Lógico**

Para dar cumplimiento al control de acceso lógico a la información, todos los involucrados en el alcance deberán:

a) Requisitos del Instituto para el control de acceso.

- El Líder de proceso o supervisor del contrato deberá autorizar y solicitar por correo electrónico al profesional de apoyo encargado del proceso TIC al email: sistemas@turismometa.gov.co, los permisos que corresponde a cada perfil que puede acceder a los recursos de la plataforma tecnológica, servicios de red y sistemas de información.
- El profesional de apoyo encargado del proceso TIC debe llevar un formato de **REGISTRO DE CONTROL DE ACCESOS** actualizado donde se relacionen los funcionarios y/o contratista con los respectivos perfiles y/o permisos autorizados por los, líder de proceso o supervisor del contrato, para el acceso a los diferentes recursos de la plataforma tecnológica del Instituto.
- Los funcionarios, contratistas y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos del Instituto de Turismo del Meta, deben contar con la **"DECLARACIÓN DE CONFIDENCIALIDAD"** firmado previamente en su proceso de vinculación.
- Asegurar que las redes inalámbricas del Instituto cuenten con métodos de autenticación que evite accesos no autorizados.
- Establecer mecanismos que garanticen el control de acceso a la red inalámbrica del Instituto.
- Para los eventos que se realicen en el Instituto de Turismo del Meta se debe generar clave de red Wifi, el cual debe expirar una vez finalizado el evento, limitando el acceso al recurso de información del Instituto.
- Garantizar que para el ingreso a los servicios tecnológicos del Instituto las contraseñas no sean visibles en texto claro.

b) Gestión de acceso de usuarios.

El profesional de apoyo encargado del proceso TIC del Instituto de Turismo del Meta debe:

- Velar por que los servicios tecnológicos estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.
- El profesional del proceso de Gestión de TIC´S deberá establecer los tipos de usuarios en la red y los recursos tecnológicos e informáticos dispuestos por el Instituto de Turismo del Meta.

  - Usuario Administrador.
  - Usuario funcionario.
  - Usuario Contratista.

Nota: El profesional de apoyo encargado del proceso TIC deberá documentar los privilegios de acceso de cada uno de los roles de usuario establecidos.

- Definir, socializar y aplicar el "**PROCEDIMIENTO DE CONTROL DE ACCESO LÓGICO"** que contemple la creación, actualización, activación e inactivación de cuentas de usuario.
- Asignar un nombre de usuario y contraseña para conceder el acceso a los recursos de red y sistemas de información del Instituto de Turismo del Meta.
- Definir el mecanismo que garantice el cambio de contraseña a los usuarios para el acceso a los servicios de red.
- Definir el mecanismo que garantice el cambio de contraseña a los usuarios para los sistemas de información a los que hayan sido autorizados, según su perfil y rol.
- Otorgar a los usuarios, los accesos solicitados y autorizados por el jefe inmediato o supervisor del contrato.
- Por defecto los usuarios creados no tienen permisos de administrador, sólo se otorgan los privilegios para la administración de recursos tecnológicos, servicios de red, sistemas operativos y sistemas de información a aquellos usuarios que estén autorizados explícitamente para este fin.
- La contraseña para la autenticación se debe suministrar a los usuarios de manera segura, y el sistema debe solicitar el cambio inmediato de la misma al ingresar.
- El profesional de apoyo encargado del proceso TIC debe establecer controles para que los usuarios finales de los servicios tecnológicos no tengan instalado en sus equipos de cómputo software o herramientas que permitan la obtención de privilegios no autorizados.

c) Responsabilidades del director general, subdirectores y supervisores:

- Autorizar y solicitar por escrito al correo electrónico institucional del proceso de Gestión de TIC al email sistemas@turismometa.gov.co los permisos para el acceso a los recursos tecnológicos y sistemas de información habilitados para el desarrollo de las funciones del personal a cargo.
- Una vez finalizada la gestión de servicios prestados por terceras partes para el Instituto, el supervisor de contrato debe garantizar que los accesos queden cerrados al finalizar el proceso o contrato, informando por correo electrónico al profesional de apoyo encargado del proceso TIC al email: sistemas@turismometa.gov.co la relación del personal a los que se deben deshabilitar los permisos de acceso a los recursos tecnológicos y sistemas de información asignados.
- Antes de autorizar la finalización del contrato se debe validar vía correo electrónico la confirmación de la cancelación de las credenciales y permisos de acceso a los recursos tecnológicos del Instituto.
- Se deberá verificar periódicamente las novedades de personal y validar la eliminación, reasignación o bloqueo de las cuentas de acceso de los recursos tecnológicos y
- sistemas de información.

d) Uso de contraseñas y responsabilidades de los usuarios.

- Las contraseñas deben poseer algún grado de complejidad y no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por tanto: Debe cambiarse obligatoriamente cada vez que el sistema lo requiera de lo contrario la contraseña caducará y obligará su cambio (Aplica para las plataformas y/o aplicaciones que así lo permitan).
- El Instituto de Turismo del Meta define como regla general para el uso de contraseñas de acceso, con los requisitos de complejidad mínimos establecidos en cada servicio, aplicación, equipo o dispositivo de la plataforma tecnológica.
- La contraseña no debe ser visible en la pantalla, al momento de ser ingresada.
- La contraseña no se debe registrar en papel, correo electrónico, archivos digitales a menos que se puedan almacenar de forma segura.
- Los administradores de los servicios tecnológicos deben cumplir con los lineamientos de contraseñas seguras indicadas.
- Los administradores de los servicios tecnológicos o Sistema de Información deben de entregar de manera adecuada las credenciales de acceso.
- El usuario y la contraseña asignados para el acceso a los diferentes servicios tecnológicos, es personal e intransferible. Cualquier actividad que se realice con el usuario y clave será responsabilidad del servidor público y/o contratista al cual le fue asignado.

- No utilizar la opción de almacenar contraseñas en Internet.
- No se debe habilitar la opción – "recordar clave en este equipo", que ofrecen los programas.

➢ **Control de Acceso Físico**

Para la seguridad y control de acceso a las áreas de trabajo, procesamiento y almacenamiento de información del Instituto de Turismo del Meta, los funcionarios, contratistas, colaboradores y terceras partes deberán aplicar y dar cumplimiento a los siguientes lineamientos, directrices y recomendaciones:

- Identificar al personal que requiere acceso a las instalaciones del Instituto, autorizar y registrar su ingreso a través del formato **"INGRESO Y SALIDA DE PERSONAL, VEHÍCULOS Y EQUIPOS TECNOLÓGICOS"**, la autorización de ingreso está a cargo del director general y/o Subdirección administrativa y financiera.
- El porte del carnet de identificación en un lugar visible es de uso obligatorio dentro de las instalaciones del Instituto y será requerido por el personal de seguridad para ingreso al Instituto de Turismo del Meta.
- Está prohibido prestar el carnet de identificación, se considera como suplantación de identidad por parte de la persona que lo usa sin ser la persona autorizada.
- El denuncio de pérdida del carnet de identificación debe ser reportado a la subdirección administrativa y financiera por medio de correo electrónico.
- Contar con mecanismos de control de acceso para las áreas seguras (centro de cómputo, administración de infraestructura tecnológica, oficinas de almacén, archivo, tesorería y las demás consideradas por la mesa técnica de seguridad de la información); tales como puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, personal de vigilancia, entre otras.
- Las puertas de acceso al centro de cómputo, administración de infraestructura tecnológica, y centros de cableado u otras áreas que alberguen información crítica, deberán permanecer siempre cerradas y aseguradas.
- Aprobar de manera previa las solicitudes de acceso de terceros al centro de cómputo, administración de infraestructura tecnológica, o a los centros de cableado, además se deberá acompañar permanentemente a los visitantes durante su estancia en las áreas mencionadas.
- La subdirección Administrativa y financiera deberá autorizar e informar por correo electrónico al profesional de apoyo encargado del proceso TIC al email: sistemas@turismometa.gov.co, los permisos que corresponden para acceder a las instalaciones físicas y recursos físicos de la plataforma tecnológica, servicios de red y sistemas de información.

- Se deberá registrar el ingreso de los visitantes al centro de cómputo en un formato de registro **DE INGRESO DE VISITANTE AL CENTRO DE CÓMPUTO**, conforme a las autorizaciones emitidas como respuesta a las solicitudes realizadas vía correo electrónico.
- Implementar controles de acceso físico al centro de cómputo y/o cableado para evitar la manipulación no autorizada.
- Bloquear de manera inmediata los privilegios de acceso físico a las instalaciones tan pronto el personal termine su vinculación contractual.
- Solicitar la devolución del carnet institucional tan pronto el personal termine su vinculación contractual.
- Todo ingreso a las instalaciones del Instituto de Turismo del Meta de contratistas o visitantes para los fines de semana deberá ser solicitado previamente a la Subdirección Administrativa y Financiera, indicando el motivo del requerimiento, en caso de ser autorizado se informará vía correo electrónico a la empresa de vigilancia de las instalaciones del Instituto de Turismo del Meta para el ingreso del personal.
- El personal de vigilancia del Instituto, deberá revisar todo bolso o paquetes del personal al ingresar o salir de las instalaciones.
- No se permite el ingreso de armas a las instalaciones del Instituto, salvo para el personal expresamente autorizado.
- Todo vehículo que ingrese a las instalaciones del Instituto de Turismo del Meta será objeto de revisión por parte del personal de vigilancia, quien además registrará sus datos en el formato **"INGRESO Y SALIDA DE PERSONAL, VEHÍCULOS Y EQUIPOS TECNOLÓGICOS".**
- Los vehículos de los funcionarios, contratistas y/o visitantes que ingresen a el Instituto deberán ser registrados y autorizados por la subgerencia administrativa y financiera del Instituto de Turismo del Meta en el Formato **"INGRESO Y SALIDA DE PERSONAL, VEHÍCULOS Y EQUIPOS TECNOLÓGICOS".**

6.1.5 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES.

- Esta política aplicará a todos los funcionarios, contratistas, terceros, clientes, distribuidores, proveedores o contratistas que realicen tratamiento de datos personales en el desarrollo de su relación comercial o laboral con el Instituto de Turismo del Meta, o a quienes se haya encargado una labor general o específica, a partir de la cual se derive un tratamiento particular de datos personales, esta política le aplicará a los terceros con quienes el Instituto de Turismo del Meta haya suscrito un contrato de transmisión o transferencia de Datos Personales o entregue información para el desarrollo de actividades particulares.
- El Instituto de Turismo del Meta establece controles, instalando las medidas técnicas y organizativas necesarias para evitar la pérdida, mal uso, alteración, acceso no

autorizado y robo de los datos facilitados por los usuarios, en cumplimiento de la Ley Estatutaria 1581 de 2012, Decreto 1377 de 2013 y demás normativa vigente en el tema. El Instituto, bajo ninguna circunstancia utilizará la información recopilada para otra acción diferente a su misionalidad y al objeto de recolección, previa autorización informada del titular de los datos a excepción de los terceros autorizados por el titular o por la ley.

- El Instituto de Turismo del Meta, conserva la información de sus usuarios; esta información ha sido recolectada en el desarrollo de sus funciones públicas, en el momento que el ciudadano ha realizado cualquier solicitud al Instituto, ha participado de eventos o reuniones, caracterización de usuarios, caracterización de la gestión de formalización y gestión turística.

➢ **Las finalidades del tratamiento de datos son las siguientes:**

Los datos personales son objeto de tratamiento por parte del Instituto de Turismo del Meta - IT con las siguientes finalidades:

- Para el fortalecimiento de las relaciones con los ciudadanos, mediante el envío de información relevante, la atención de queja y reclamos (PQR´s) y la invitación a eventos entre otros.
- Para la atención de requerimientos judiciales administrativos y el cumplimiento de mandatos judiciales o legales.
- Para eventualmente contactar, vía correo electrónico, o por cualquier otro medio, a personas naturales con quienes se tiene o se ha tenido relación, con el objetivo de articulación y/o promoción Institucional.
- Consultas de antecedentes, verificación de información de las certificaciones y experiencias laborales y/o académicas.
- Verificación de pagos de seguridad social, reportes a la DIAN y Contraloría
- Para actualizar el directorio de oferta turística del Departamento del Meta.
- Para realizar análisis estadísticos.
- Para caracterizar e identificar toda la cadena de valor de los sectores turístico del Departamento del Meta.
- En el desarrollo de las actividades propias del Instituto de Turismo del Meta - ITM.

- **Datos personales**

Entiéndase como datos personales los siguientes tipos de datos:

- **De Identificación:** Nombre, apellido, tipo de identificación, número de identificación, fecha y lugar de expedición, nombre, estado civil, sexo, firma, nacionalidad, datos de familia, firma electrónica, otros documentos de identificación, lugar y fecha de nacimiento, edad, huella, ADN, iris, Geometría facial o corporal, fotografías, vídeos, fórmula dactiloscópica, voz, etc.
- **De Ubicación:** como los relacionados con la actividad comercial o privada de las personas como dirección, teléfono, correo electrónico, etc.
- **De contenido socioeconómico:** como estrato, propiedad de la vivienda, Datos financieros, crediticios y/o de carácter económico de las personas, Datos patrimoniales como bienes muebles e inmuebles, ingresos, egresos, inversiones, historia laboral, experiencia laboral, cargo, fechas de ingreso y retiro, anotaciones, nivel educativo, capacitación y/o historial académico de la persona, etc.

- **Responsabilidades de los funcionarios y contratistas del Instituto**

Es responsabilidad de funcionarios y contratistas garantizar la protección de los datos personales que se obtengan del ejercicio misional de los usuarios y ciudadanía en general.

- **Manejo de datos personales para ingreso a el Instituto**

El Instituto de Turismo del Meta, como responsable del tratamiento de los datos personales de las personas naturales que ingresan al Instituto, solicitará la autorización al usuario para el tratamiento, recolección, almacenamiento, gestión y eliminación de sus datos personales.

- **Formato de autorización para el tratamiento de datos personales**

Para efectos del tratamiento de los Datos Personales recolectados, El Instituto de Turismo del Meta como responsable de los datos personales obtenidos a través de sus distintos canales de atención, solicitará a todas las personas su autorización para que, de manera libre, previa, expresa y voluntaria permitan continuar con su tratamiento para ser agregados en sus bases de datos y que sean necesarios para la adecuada prestación de sus servicios.

La subdirección Administrativa y Financiera definirá los casos en los que se debe solicitar al propietario de la información la lectura, diligenciamiento y firma del formato "**AUTORIZACIÓN DE TRATAMIENTO DE DATOS PERSONALES".**

- **Formatos para solicitud y registro de información de carácter personal.**

Todos los formatos que requieran el registro de la información de carácter personal, antes mencionada, debe incluir el consentimiento por parte del propietario, con el siguiente texto predeterminado:

"**Nota:** El Instituto de Turismo del Meta, en cumpliendo de lo previsto en la ley 1581 de 2012, es responsable del tratamiento de los datos personales suministrados, por lo anterior, de manera voluntaria, previa, explicita, informada e inequívoca, autorizó al Instituto de Turismo del Meta – ITM, para tratar mis datos personales de acuerdo con su política de tratamiento de Datos personales publicada en la página web www.turismometa.gov.co.

- **Derechos Del Titular De La Información**

- Conocer, actualizar, suprimir, revocar y rectificar sus datos personales frente al Instituto de Turismo del Meta. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
- Ser informado con relación al uso que el Instituto de Turismo del Meta les ha dado a sus datos personales.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

- **Deberes del responsable del tratamiento de los datos personales**

El responsable del Tratamiento ha sido definido por la Ley 1581 de 2012 como la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros decida sobre la base de datos y/o el tratamiento de los datos.

Son deberes de los responsables del Tratamiento y, por consiguiente, del Instituto de Turismo del Meta los establecidos en el artículo 17 de la Ley 1581 de 2012:

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Solicitar y conservar, en las condiciones previstas en la citada ley, copia de la respectiva autorización otorgada por el Titular.
- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, aplicando las políticas específicas de controles de seguridad.
- Actualizar la información, comunicando de forma oportuna al responsable del Tratamiento de los Datos personales, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.
- Informar a solicitud del Titular sobre el uso dado a sus datos.
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio

6.1.6 POLITICA DE INTEGRIDAD DE LA INFORMACIÓN.

- Toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.
- El proceso de contratación debe incluir una **"Cláusula de integridad de la información"** en los contratos, convenios y/o acuerdos que se suscriban con terceros, que establezca el compromiso de administración y manejo integro e integral de la información interna y externa.
- Se debe establecer la vigencia de los compromisos de funcionarios, contratistas y terceras partes contratadas, frente a la integridad de la información.
- El profesional a cargo del Proceso de Gestión de las TIC debe asegurar que las plataformas, aplicaciones y demás recursos informáticos, utilizados por el Instituto de Turismo del Meta, deben tener la capacidad de llevar el registro de eventos, para realizar seguimiento a los accesos realizados por los usuarios a la información del Instituto, con el objeto de minimizar el riesgo de pérdida de integridad de la información.
- Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información, el profesional responsable del Proceso de Gestión de las TIC deberá documentar y realizar las acciones tendientes a su solución.
- Todo funcionario y/o contratista que utilice los equipos de cómputo y los servicios informáticos disponibles, tiene la responsabilidad de velar por la integridad de la información bajo su custodia.

- El profesional responsable del Proceso de Gestión de las TIC debe fortalecer la seguridad de las redes de datos del Instituto de Turismo del Meta, con el fin de mitigar las vulnerabilidades frente a posibles intromisiones de terceros no autorizados a la información crítica del Instituto y que pongan en riesgo su integridad.
- Se debe garantizar la separación de deberes frente a responsabilidad de los diferentes activos de información, y comunicarlo a toda la organización, con el fin de poder identificar quiénes son los responsables y tienen la autorización para alterarlos o modificarlos.
- Funcionarios y contratistas con acceso a los recursos tecnológicos del Instituto deben aplicar y dar cumplimiento a las políticas de control de acceso, con el fin de reducir posibles intromisiones por personas no autorizadas a los activos de información que estén bajo su responsabilidad.
- Velar por el cumplimiento de la política general y las políticas específicas de seguridad y privacidad de la información establecidas, comunicadas e implementadas por el Instituto de Turismo del Meta, las cuales buscan contribuir a la preservación de la integridad de información y en general a la seguridad de la información crítica para el Instituto.

6.1.7 POLITICA DE DISPONIBILIDAD Y CONTINUIDAD DEL SERVICIO E INFORMACIÓN.

El Instituto de Turismo del Meta deberá contar con un **"PLAN DE CONTINUIDAD DE SERVICIOS TI Y RECUPERACIÓN DE DESASTRES"** con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales del Instituto, ante el evento de un incidente de seguridad de la información o catástrofes.

- **Funciones y responsabilidades para gestión de la continuidad:**

- El profesional responsable de TI, es el responsable de establecer y mantener actualizado el **"PLAN DE CONTINUIDAD DE SERVICIOS TI Y RECUPERACIÓN DE DESASTRES"** conforme la norma ISO/IEC 22301:2012, identificando estándares, normas, directivas en la materia, documentarlas y publicarlas como lineamiento transversal para todos los procesos del Instituto de Turismo del Meta.
- El profesional de apoyo encargado del proceso TIC es el encargado de gestionar riesgos de Tecnologías de Información, y ejecutar el plan de continuidad y recuperación ante desastres.
- La oficina de Control Interno tiene la responsabilidad de hacer seguimiento en el cumplimiento de las políticas y plan de continuidad y recuperación; así mismo, de hacer seguimiento a la gestión de riesgos.

- La alta Dirección es responsable de aprobar el plan de continuidad de servicios TI y recuperación ante desastres.

➢ **Directrices para la Continuidad**

- Se debe elaborar, revisar y aprobar el **"PLAN DE CONTINUIDAD DE SERVICIOS TI Y RECUPERACIÓN DE DESASTRES"** y realizar mejoras de forma periódica o ante cambios significativos tales como procesos, tecnología o estructura organizativa; para lo cual deberán participar activamente en dicha revisión los procesos identificados como críticos.
- La estrategia de continuidad de servicios de Tecnologías de Información y recuperación ante desastres del Instituto de Turismo del Meta deberá diseñar e implementar actividades de prevención y de recuperación que ofrezcan las garantías necesarias para el restablecimiento de las operaciones de la Institución después de un desastre.
- Los propietarios y administradores de la información en cada una de los procesos deben identificar, clasificar y priorizar la información crítica de sus procesos utilizando el formato suministrado por el proceso de Gestión de TIC´S.
- Los propietarios y administradores de los sistemas de información deben identificar y priorizar aplicaciones de software, que se encuentren operando en cada una de las estaciones de trabajo.
- Se debe establecer el tiempo aceptable para recuperar los datos que tiene el Instituto en caso de una interrupción o desastre, y garantizar una recuperación eficaz.
- Se debe establecer el tiempo para retornar a las actividades normales después de la interrupción o desastre, y garantizar que los procesos críticos son recuperados dentro de los márgenes de tiempo requeridos en el Plan.
- Se debe contar con equipos servidores alternos que permitan tener disponibles versiones de sistema operativo, plataformas de base de datos, de servicios Web y configuraciones necesarias que estén compatibles y sincronizadas con los servidores principales.
- Se debe disponer de energía eléctrica a través de Sistemas de Alimentación Ininterrumpida y plantas eléctricas para suministrar energía a los equipos de cómputo, principalmente a equipos servidores, ante fallas en la línea principal de suministro del servicio de energía.
- Se debe garantizar la divulgación, socialización y concientización de las políticas y del **"PLAN DE CONTINUIDAD DE SERVICIOS TI Y RECUPERACIÓN DE DESASTRES".**

- **Directrices para la Recuperación de Desastres.**

- Se debe contar con una ubicación física desde la cual el plan de recuperación de desastres pueda ser ejecutado; es decir, un centro de procesamiento alterno con capacidad para el respaldo de las operaciones críticas del Instituto.
- Se deberá establecer un **"PROCEDIMIENTO DE VERIFICACIÓN DEL DESASTRE Y DE EVALUACIÓN DE DAÑOS"**. Una vez que la evaluación se ha hecho, los responsables deberán activar al personal apropiado para realizar las actividades de soporte y recuperación.
- Se debe realizar **copia de seguridad (Backup)** de acuerdo al **PROCEDIMIENTO DE COPIAS DE SEGURIDAD** de las aplicaciones, bases de datos y archivos alojados en servidores, con el propósito de salvaguardar la información. Estas se deben realizar periódicamente por el proceso de gestión de las TIC, de acuerdo a las indicaciones establecidas en el plan de continuidad y se deberán almacenar en un sitio alterno fuera del edificio donde se encuentra en centro de procesamiento principal.
- Se debe realizar copias de seguridad (Backup) de la información más relevante almacenada en los equipos de cómputo en cada uno de los procesos, esta debe ser ejecutada por el profesional de apoyo encargado del proceso TIC del Instituto de Turismo del Meta, de acuerdo a la periodicidad definida.
- Se debe almacenar copias de seguridad de archivos relevantes de las dependencias, organizadas en archivos electrónicos de documentos, incluyendo sus metadatos a través de Tablas de Retención Documental (TRD) y preservar los documentos según se indique en la TRD de cada dependencia.
- Se debe etiquetar los medios de almacenamiento con el propósito de identificar las características de las copias de seguridad, de acuerdo a las indicaciones definidas en el **"PLAN DE CONTINUIDAD DE SERVICIOS TI Y RECUPERACIÓN DE DESASTRES".**
- Los proveedores de Sistemas de Tecnología de Información deben tener capacidad para brindar soporte a requerimientos que se deriven después del desastre. El Instituto de Turismo del Meta debe solicitar que estos compromisos queden incluidos en dentro de las condiciones del servicio.

6.1.8 POLITICA DE CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

Esta política establece los lineamientos para la integrar al **"PLAN DE CAPACITACIÓN INSTITUCIONAL"**, la temática relacionada con la capacitación, sensibilización y comunicación de la seguridad de la información, para así asegurar que este, que los funcionarios y/o contratistas del Instituto de Turismo del Meta conozcan, apliquen y se

apropien del SGSI, buscando que cada uno cumpla con sus roles y responsabilidades ante la seguridad y privacidad de la información.

Requerimientos:

- El Instituto de Turismo del Meta debe planificar, ejecutar, monitorear y actualizar un **Plan de capacitación Institucional** que integre las actividades de Capacitación, Comunicación y Sensibilización del SGSI, con temas relacionados con la seguridad y privacidad de la información.
- La alta dirección debe garantizar los recursos suficientes y necesarios para la correcta ejecución de las actividades de Capacitación, Comunicación y Sensibilización del SGSI incluidos en el plan de capacitación Institucional.
- El Plan de Capacitación Institucional debe definir las temáticas de la seguridad de la información a abordar en las jornadas de capacitación.
- El **Plan de capacitación Institucional** deben ser comunicado asertivamente a toda la organización.
- Los funcionarios y contratistas, involucrados en los procesos organizacionales, deben ser capacitados en cuanto al conocimiento y apropiación del SGSI del Instituto.
- Los funcionarios y/o contratistas que ingresen a el Instituto deben participar en una jornada de inducción frente al SGSI del Instituto y sus compromisos y responsabilidades frente al mismo.
- Todos los funcionarios, contratistas y terceras partes interesadas deben ser sensibilizadas frente a las políticas, objetivos y alcance del SGSI, así como de la importancia de su aplicación y cumplimiento para la seguridad y protección de los activos de información del Instituto.
- El profesional responsable del sistema de Gestión de Seguridad de la Información debe establecer procesos de métrica que permitan una revisión periódica para el mejoramiento en la implementación del SGSI en el Instituto de Turismo del Meta.
- El Instituto de Turismo del Meta, a través del profesional responsable del sistema de Gestión de Seguridad de la Información y con el acompañamiento del equipo de comunicaciones debe generar piezas gráficas de sensibilización frente al SGSI, políticas, objetivos, alcance, importancia y aplicación.
- El Instituto de Turismo del Meta, a través del profesional responsable del Sistema de Gestión de Seguridad de la Información debe desarrollar actividades lúdicas esporádicas que permitan sensibilizar a funcionarios y contratistas involucrados en los diferentes procesos organizacionales, frente al SGSI, políticas, objetivos, alcance, importancia y aplicación.
- El Instituto de Turismo del Meta a través de la Mesa Técnica de Seguridad de la Información deberá evaluar anualmente el **PLAN DE CAPACITACIÓN INSTITUCIONAL** en cuanto lo referente al desarrollo del SGSI y recomendar al Comité

de Desempeño Institucional las mejoras al mismo para la aprobación en su siguiente vigencia.

6.1.9 POLÍTICA DE ESCRITORIOS Y PANTALLA LIMPIA.

Se debe adoptar por parte de los funcionarios y/o contratistas del Instituto de Turismo del Meta una política de escritorios y pantalla limpia para evitar el acceso no autorizado, pérdida, robo o daño de la información que se encuentre en los puestos de trabajo, equipos de cómputo, impresoras, escáneres y medios de almacenamiento estando o no en uso, durante y fuera del horario laboral. Los usuarios y partes interesadas deberán acatar e implementar los siguientes lineamientos, recomendaciones y buenas prácticas:

- **Escritorios limpios**

- Los puestos de trabajo deben permanecer limpios, ordenados y libres de archivos o información institucional que pueda ser objeto de consulta, copiado, eliminación por personal no autorizado.
- Se debe evitar el consumo de alimentos o bebidas en áreas de trabajo donde se encuentre ubicada la información institucional en papel, equipos de cómputo, dispositivos electrónicos o cualquier medio de almacenamiento que pueda llegar a ser afectado por el derrame de líquidos o residuos de alimentos.
- Es responsabilidad del personal que se ausente temporalmente de su puesto de trabajo que los escritorios deben permanecer despejados y libres de documentos físicos y/o medios extraíbles que contengan información pública clasificada o pública reservada, estos se deberán guardar en un lugar seguro y bajo llave en gabinete u otro mueble de seguridad dispuesto para la seguridad y almacenamiento de la información.
- Los gabinetes, cajones y archivadores que contengan documentos y/o medios extraíbles con información pública, pública clasificada o pública reservada deben quedar cerrados bajo llave durante la hora de almuerzo y al finalizar la jornada laboral.
- Los documentos electrónicos que producen los funcionarios o contratistas en el ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales, según el caso, deben guardarse en el sistema de almacenamiento dispuesto por el Instituto.
- Al finalizar la jornada de trabajo, los funcionarios o contratistas deberán guardar en un lugar seguro los documentos y medios que contengan información pública de uso interno, pública clasificada o pública reservada.

➢ **Pantallas limpias**

- La pantalla de computador (escritorio) debe estar libre de archivos o enlaces de acceso a archivos, estos deben ubicarse en las debidas carpetas de almacenamiento.
- El equipo de cómputo siempre tendrá configurado un fondo de pantalla y un protector de pantalla predefinido por el proceso de gestión de las TIC.
- Es responsabilidad del funcionario y/o contratista siempre que se ausente de su puesto de trabajo, bloquear o cerrar las sesiones de sus equipos de cómputo con solicitud de contraseña reingreso.
- La pantalla del computador (escritorio) no debe contener ningún tipo de archivo, salvo los accesos directos a las aplicaciones necesarias para que los funcionarios o contratistas ejerzan sus funciones o cumplan sus obligaciones contractuales.
- El responsable del proceso gestión de las TIC, implementará un mecanismo de bloqueo de sesión al transcurrir un tiempo de inactividad predeterminado por el Instituto.
- Una vez termine su jornada laboral, debe apagar el equipo de cómputo, exceptuando los casos en que los equipos se encuentran en proceso de actualización y para los usuarios del proceso de gestión de las TIC que por sus funciones deben permanecer atentos a cualquier situación o anomalía que se presente en los sistemas de información, y los demás equipos que su funcionalidad operacional deben permanecer encendidos.
- El profesional de apoyo encargado del proceso TIC implementará un mecanismo para apagar los equipos que se encuentren encendido en horario no laboral.

➢ **Equipos de reproducción de información**

- Los equipos de reproducción de información (impresoras, fotocopiadoras, escáneres, etc.), deben permanecer limpios de documentos, cualquier documentación con información pública clasificada o pública reservada se debe retirar inmediatamente del equipo y ser puesta en un lugar seguro.
- Todo documento que contenga información clasificada como confidencial no podrá ser reciclado; y deberá ser destruido de tal manera que se impida la reconstrucción de dicha información.
- Todos los equipos de cómputo y dispositivos de impresión y digitalización deben apagarse cuando no estén en uso.

7 CONTROL DE DOCUMENTOS.

VERSIÓN No.	FECHA	DESCRIPCIÓN MODIFICACIONES
1	21/07/2021	Creación del Manual, Primera versión

8 ANEXOS.

N/A