MANUAL DE POLÍTICAS DEL MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ALCALDÍA DE PITALITO

TABLA DE CONTENIDO

1. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

1.1 Objetivo del MSPI

Establecer las normas, políticas y recomendaciones inherentes a la seguridad y privacidad de la información y al uso de los recursos tecnológicos del Municipio de Pitalito - Huila con el ánimo de preservar los activos de información en óptimos niveles de integridad, privacidad y confidencialidad.

1.2 Determinación del Alcance del MSPI

Este manual debe aplicarse para servir a la alta dirección en la protección de los activos, la protección de la infraestructura tecnológica que soporta la operación de la Entidad y gestión de los riesgos de seguridad y privacidad de información. Las políticas aquí enmarcadas deben ser cumplidas por todo el personal de la Entidad sus funcionarios, contratistas, terceros y la ciudadanía en general que acceda a la información de la Alcaldía de Pitalito- Huila.

2. NORMATIVIDAD Y OTROS DOCUMENTOS EXTERNOS

- Constitución Política de Colombia, artículo 15, consagra que *"todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas (...)"*; artículo 209 establece que *"(...) la administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley (...)"*; así mismo, en el artículo 269 Impone a las autoridades de las entidades públicas la obligación de "(...) *diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control Interno* (...)".

- Ley 23 de 1982 "Sobre Derechos de Autor". Congreso de la República.

- Decreto 2693 de 2012 "Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones". Ministerio de Tecnologías de la Información y las comunicaciones.

- Decreto 1377 DE 2013 "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".

- Decreto 2573 de 2014, "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".

- Decreto 103 de 2015, "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".

- Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3., incluye la seguridad de la Información entre los principios de la Política de Gobierno Digital; de igual manera, en el artículo 2.2.9.1.2.1. se establece que la Política de Gobierno Digital se desarrollará a través de componentes y habilitadores transversales, y respecto de estos últimos indica que son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

- Decreto 1083 de 2015, artículo 2.2.22.2.1 tal como fue sustituido por el Decreto 1499 de 2017, regula las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

- CONPES 3854 de 2016 establece la Política Nacional de Seguridad Digital en la República de Colombia.

- Decreto 1499 de 2017, "Por medio del cual modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector de Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015", adoptó el Modelo Integrado de Planeación y Gestión - MIPG, definiéndolo en su artículo 2.2.22.3.2 como "(...) un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio".

- NORMA TÉCNICA COLOMBIANA NTC – ISO/IEC- 27001 (2013). Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.

- MANUAL GOBIERNO EN LÍNEA 3.1. Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la

Estrategia de Gobierno en Línea; Formato Política SGSI - Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea. Ver 2014-06-12

- Manual Modelo de Seguridad y Privacidad de la Información - Ministerio de Tecnologías de la Información y las Comunicaciones. Versión 3.0.2 del 29 de julio de 2016.

- Manual de Gobierno Digital - Ministerio de Tecnologías de la Información y las Comunicaciones. - Versión 7 abril de 2019.

- Documento Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Ministerio de Tecnologías de la Información y las Comunicaciones - Guía riesgos 2018.

3. DEFINICIONES

Activo: Todo lo que tiene valor para la Entidad. Hay varios tipos de activos entre los que se incluyen:

- Información
- Software, como un programa de cómputo.
- Físico, como un computador
- Servicios
- Personas, sus calificaciones, habilidades y experiencia

Almacenamiento en la Nube: Del inglés cloud storage, es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet. Esos lugares de Internet son aplicaciones o servicios que almacenan o guardan esos archivos.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.
Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Clave: Contraseña, clave o password es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. A aquellos que

desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso. En ocasiones clave y contraseña se usan indistintamente. (Asimismo llamado PIN - Personal Identificación Number).

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, de otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencial: Significa que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados.

Correo Electrónico Institucional: Es el servicio basado en el intercambio de información a través de la red y el cual es provisto por La Estrategia de Gobierno Digital, para los funcionarios, contratistas y practicantes autorizados para su acceso de la entidad. El propósito principal es compartir información de forma rápida, sencilla y segura. El sistema de correo electrónico puede ser utilizado para el intercambio de información, administración de libreta de direcciones, manejo de contactos, administración de agenda y el envío y recepción de documentos, relacionados con las responsabilidades institucionales.

Disponibilidad de la información: La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

Estrategia de Gobierno en Línea: Estrategia definida por el Gobierno Nacional que busca apoyar y homologar los contenidos y servicios ofrecidos por cada una de las entidades públicas para el cumplimiento de los objetivos de un Estado más eficiente, transparente y participativo, donde se presten servicios más eficientes a los ciudadanos a través del aprovechamiento de las tecnologías de información.

Extranet: Herramienta del sistema de gestión documental y ventanilla única del municipio de Pitalito, con el cual se ha edificado la organización, manejo, accesibilidad y trazabilidad de los procesos de comunicación interna y externa que desarrolla el Ente Territorial en cada uno de los procesos de interacción con la comunidad y para sí misma, que permiten tener certeza respeto a todos los procesos de atención al ciudadano contribuyendo a la satisfacción de los múltiples intereses comunitarios.

Hardware: Conjunto de los componentes que integran la parte material de una computadora.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento los cuales deben ser exactos.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

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 semi-privado 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.

Internet: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

Legalidad: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que

el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

Memoria USB: La memoria USB (Universal Serial Bus) es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información. Se le denomina también lápiz de memoria, lápiz USB o memoria externa, siendo innecesaria la voz inglesa pen drive o pendrive.

Política: Declaración general de principios que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías, las políticas deben ser pocas (es decir un número pequeño), deben ser apoyadas y aprobadas por las directivas de la Institución y deben ofrecer direccionamientos a toda la Entidad o a un conjunto importante de dependencias. Por definición, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.

Puntos de entrada y salida USB: Cualquier dispositivo (distinto de la memoria RAM) que intercambie datos con el sistema lo hace a través de un "puerto", por esto se denominan también puertos de E/S ("I/O ports"). Desde el punto de vista del software, un puerto es una interfaz con ciertas características; se trata por tanto de una abstracción (no nos referimos al enchufe con el que se conecta físicamente un dispositivo al sistema), aunque desde el punto de vista del hardware, esta abstracción se corresponde con un dispositivo físico capaz de intercambiar información (E/S) con el bus de datos.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
Seguridad de la información: Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información.

Servicio: Es el conjunto de acciones o actividades de carácter misional diseñadas para incrementar la satisfacción del usuario, dándole valor agregado a las funciones de la entidad.

SGSI: Sistema de Gestión de Seguridad de la Información: Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. En el contexto, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Sistemas de Información: Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Habitualmente el término se usa de manera errónea como sinónimo de sistema de información informático, en parte porque en la mayoría de los casos los recursos materiales de un sistema de información están constituidos casi en su totalidad por sistemas informáticos. Estrictamente hablando, un sistema de información no tiene por qué disponer de dichos recursos (aunque en la práctica esto no suela ocurrir). Se podría decir entonces que los sistemas de información informáticos son una subclase o un subconjunto de los sistemas de información en general.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Tecnología de la información y las Comunicaciones TIC: Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.

Usuario: En el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de la Alcaldía de Pitalito-Huila, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la Entidad y a quienes se les otorga un nombre de usuario y una clave de acceso.

Virus: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tardo tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

4. LIDERAZGO

4.1 Roles y Responsabilidades del Sistema de Gestión de Seguridad de la Información

Secretaría de Planeación

- Coordinar, implementar, gestionar y cumplir con la Seguridad y Privacidad de la Información, acorde con las necesidades de la Entidad y los recursos disponibles.

Líder de Seguridad de la Información

- Diseñar y presentar para aprobación, políticas, normas y procedimientos que fortalezcan la seguridad de la información, y someterlos a decisión del Comité Institucional de Gestión y Desempeño.
- Implementar y difundir al interior de la Entidad, del Modelo de Seguridad y Privacidad de la Información.
- Velar por el cumplimiento y actualización de la política general de seguridad y privacidad de la información y sus políticas específicas.
- Velar por la implementación de los controles de seguridad y privacidad de la información.
- Gestionar y analizar periódicamente los riesgos de seguridad existentes y proponer soluciones que fortalezcan la seguridad y privacidad de la información en la Entidad.
- Gestionar los incidentes de seguridad y recomendar acciones preventivas y correctivas para evitar afectaciones al interior de la Entidad.
- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.

- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Alcaldía de Pitalito-Huila.

- Promover la difusión y sensibilización de la seguridad y privacidad de la información dentro de la entidad.

- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.

- Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.

- Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.

- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité Institucional de Gestión y Desempeño en caso de ser necesario.

- Trabajar de manera integrada con el grupo o áreas asignadas.

- Asegurar la calidad de los entregables y del proyecto en su totalidad.

- Velar por el mantenimiento de la documentación del proyecto, su custodia y protección.

- Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.

- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.

Usuario

- Toda persona que tenga acceso a la información de la Alcaldía municipal de Pitalito-Huila, sin importar su forma de vinculación con la entidad, quienes deben conocer y cumplir, ésta y todas las políticas y buenas prácticas de Seguridad y Privacidad de la Información.

Grupo de Apoyo a la Seguridad (Técnico Administrativo – Oficina Gestión TIC)

- Desarrollar, mantener y administrar operativa y técnicamente la seguridad de la información conforme con las políticas de seguridad adoptadas por la Alcaldía Municipal de Pitalito, Huila.

- Materializar las medidas de largo, mediano y corto plazo que permitan el desarrollo efectivo, estratégico y armónico de las políticas planteadas.

Secretaría General

- Notificar a todo el personal de la Alcaldía Municipal de Pitalito - Huila, sin importar su forma de vinculación con la entidad, las obligaciones respecto del cumplimiento de la Política de Seguridad y Privacidad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan de la misma.

- Responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los Compromisos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comité del Modelo Institucional de Planeación y Gestión - MIPG.

- La Secretaría General por medio del área de Talento Humano y el supervisor del contrato, deberán velar por que los funcionarios, contratistas, terceros, aprendices, practicantes y demás partes interesadas de la Entidad, reciban entrenamiento y actualización periódica en materia de Seguridad de la Información.

- La Secretaria General por medio del área de Talento Humano, deberá incorporar la aplicación de las políticas de seguridad de la información en su plan de capacitación institucional, y velar por la correcta inducción de los funcionarios nuevos en materia de seguridad de la información.

Control Interno Administrativo

- Practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información.

- Informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

Organización para la seguridad de la información

La Alcaldía Municipal de Pitalito - Huila garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Modelo de Seguridad y Privacidad de la Información, del cual hace parte integral la presente política, por medio del Comité Institucional de Gestión y Desempeño.

Comité Institucional de Gestión y Desempeño

La Alcaldía de Pitalito, Huila, a través del Comité Institucional de Gestión y Desempeño-MIPG, tendrá las funciones relacionadas a continuación y que son requeridas para la implementación y gestión del Modelo de Seguridad y Privacidad de la Información (MSPI):

- Asesorar al Alcalde municipal, en temas de seguridad de la información coordinadamente con el Líder de Seguridad de la Información.

- Realizar seguimiento a los incidentes de seguridad, presentados por el líder de Seguridad y establecer en conjunto las acciones preventivas y correctivas para evitar afectaciones al interior de la Entidad.

- Realizar acompañamiento a las actividades de planeación, implementación, seguimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información.
- Realizar un proceso continuo de revisión y aprobación de las políticas de seguridad y privacidad de la Información con el fin de mantenerlas actualizadas, vigentes y operativas para asegurar su permanencia y apropiación por parte de todos los colaboradores.

- Realizar seguimiento a las revisiones periódicas del MSPI, presentadas por el líder de Seguridad (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes en conjunto.

5. POLÍTICAS

5.1 Política de Dispositivos Móviles

La Entidad establece las condiciones para el uso seguro de los dispositivos móviles (portátiles, teléfonos, inteligentes, tabletas, entre otros) institucionales que hagan uso de servicios de la Entidad, para lo cual se establecen las siguientes directrices:

- Establecer contraseñas de acceso robustas, cifrar la información almacenada, mantener el dispositivo móvil con el sistema operativo siempre actualizado y con un antivirus activo.

- Los funcionarios y contratistas no están autorizados a cambiar la configuración, ni la instalación/desinstalación de las aplicaciones móviles de los dispositivos móviles institucionales que se les entregue como recurso para la ejecución de sus obligaciones o funciones.

- Es responsabilidad del servidor públicos al que se le asignó el dispositivo móvil evitar la instalación de programas desde fuentes desconocidas, evitar el uso de redes inalámbricas públicas, y mantener desactivadas las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

- Los servidores públicos deben evitar conectar los dispositivos móviles institucionales a puertos USB de computadores públicos, hoteles o cafés internet, terminales, y demás sitios de acceso público.

- Los servidores públicos y contratistas deben notificar los dispositivos móviles institucionales con sospecha de infección por malware al personal técnico responsable de la Entidad para el proceso de análisis, evaluación y tratamiento.

- Los dispositivos móviles que son autorizados para salir de las instalaciones por la Entidad deben ser protegidos mediante el uso e implementación de los controles apropiados como: cifrado de información, políticas de restricción en la ejecución de aplicaciones y de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN, entre otros.

- Todos los dispositivos móviles propiedad de la Entidad pueden ser monitoreados y sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.

- Evitar almacenar información de la Entidad que no sea estrictamente necesaria para el desarrollo del trabajo en el dispositivo móvil.

- Cifrar la información confidencial y eliminarla del dispositivo móvil una vez se haga la actividad que corresponda de acuerdo al desarrollo del trabajo.

- Mantener el registro actualizado de los dispositivos móviles de la Entidad asignados a los colaboradores, así como el registro de la instalación del software y hardware requerido por el colaborador.

- Para los dispositivos móviles asignados por la Entidad, se debe notificar al personal técnico responsable la sospecha de infección por virus u otro software malicioso del equipo.

- Evitar la exposición del dispositivo móvil a altas temperaturas.

- Al utilizar el dispositivo móvil en lugares públicos se recomienda mantenerlo siempre vigilado, utilizar guaya de seguridad y en caso de robo o pérdida del equipo notificar a los jefes de las áreas responsables para la realización del debido proceso.

- Desactivar en los dispositivos móviles la búsqueda de redes wifi y de dispositivos vía Bluetooth cuando no sea necesario.

5.2 Política de Teletrabajo

La Entidad brinda los lineamientos de seguridad digital para la protección de la información a la que se tiene acceso, se procesa o almacena en lugares en los que se realiza teletrabajos, y se hace uso de los recursos tecnológicos y activos de información autorizados por la Entidad para el desarrollo de las actividades de Teletrabajo, para lo cual se establecen las siguientes directrices:

- Toda información gestionada por la Entidad, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales con esta.

- La Entidad establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos y contratistas de la entidad, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.

- La Entidad establece el proceso de implementación de teletrabajo, de acuerdo con la normativa y los lineamientos exigidos, con el fin de proteger la información.

- La Entidad revisa la seguridad física y del entorno del sitio donde se va a realizar teletrabajo, con el fin de proteger la confidencialidad, integridad y disponibilidad.
- Al utilizar el dispositivo móvil en lugares públicos se recomienda mantenerlo siempre vigilado, utilizar guaya de seguridad y en caso de robo o pérdida del equipo notificar a los jefes de las áreas responsables para la realización del debido proceso.

- En los lugares que se realiza teletrabajo se debe aplicar las mismas políticas de uso de los activos de información, aplicación de contraseñas, bloqueo de sesión y demás que se relacionen, y en caso sospechar de un evento o incidente de seguridad, informar inmediatamente al área responsable.

5.3 Políticas de Seguridad de los Recursos Humanos

La Entidad establece directrices para asegurarse que los colaborares y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad de la información, para lo cual se establecen las siguientes directrices:

- El área que realice la contratación de personal en la Entidad debe realizar las verificaciones de los antecedentes (procuraduría, contraloría, policía) de los candidatos al cargo, la formación académica, experiencia y demás información que se requiera, de acuerdo a las leyes, reglamentos de la Entidad y ética pertinente.

- Todo servidor público y contratista debe recibir inducción y procesos periódicos de sensibilización en seguridad y privacidad de la información en la Entidad.

- La Entidad establece directrices para asegurar que los servidores públicos y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad y privacidad de la información.

- Los acuerdos contractuales entre la Entidad y los servidores públicos o contratistas deben especificar el cumplimiento a los lineamientos de seguridad y privacidad de la información establecidos en la Entidad.
- Todos los funcionarios y contratistas deben firmar un acuerdo de confidencialidad y no divulgación, donde se especifiquen la responsabilidad con el acceso y gestión de la información confidencial, de datos personales, derechos de autor, entre otra que tenga implicaciones legales.

- Se debe especificar en los contratos las sanciones que conlleva el uso indebido de la información de la Entidad y Comunicar a los funcionarios y contratistas las obligaciones que deben cumplir con la información de la Entidad al finalizar el contrato o relación laboral.

- El proceso de Talento Humano y el proceso de contratación cuando gestionan las actividades de desvinculación, licencias, vacaciones o cambio de labores de los servidores públicos y contratistas debe llevar a cabo los procedimientos y ejecutar los controles establecidos para tal fin, así mismo, los directores, jefes, supervisores de contrato o líderes deben informar la desvinculación o cambio de labores de acuerdo con los procedimientos, está información debe ser entregada oportunamente al proceso de TIC.

- La Entidad debe incorporar los roles y responsabilidades en seguridad y privacidad de la información dentro de las funciones y obligaciones contractuales de los funcionarios y Terceros.

- El incumplimiento o la violación de las políticas de seguridad de la información de la Entidad, por parte de toda persona que tenga acceso a la información de la Alcaldía municipal de Pitalito-Huila, sin importar su forma de vinculación con la entidad, se les aplicará lo establecido en el proceso de investigaciones disciplinarias.

5.4 Políticas de Gestión de Activos

La Entidad debe desarrollar estrategias de trabajo para optimizar el uso de los recursos de seguridad, establecer los métodos de identificación clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades y manteniendo mecanismos acordes para el control de riesgos de la información, para lo cual se establecen las siguientes directrices:

- Cada activo de información de la Entidad debe tener un responsable que debe velar por su seguridad. Los propietarios de la información deben garantizar que todos los activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y requerimientos legales de retención.

- La Entidad debe establecer los niveles de clasificación de la información de acuerdo a la normatividad Legal Colombiana y brindar protección a la información de acuerdo con su importancia para la organización.

- Es responsabilidad del líder de proceso, jefe de área o Director, la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos.

- Todos los activos de información deben contar con un responsable, que asegure la protección de la información y los datos que son almacenados en cada uno de ellos.

- Se deber solicitar autorización para retirar los medios de la Entidad (USB, portátiles, discos duros etc.) y se debería llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría.

- Los servidores públicos y contratistas deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la Entidad.

- Se debe almacenar la información en la nube o CD autorizada por la Entidad y realizar la configuración técnica que se requiera para obtener la trazabilidad de con quien se comparte la información, fechas y demás datos de interés.

5.5 Políticas de Gestión de Medios de Almacenamiento

La Entidad debe disponer de diferentes mecanismos de almacenamiento para propender por la disponibilidad de la información y el establecimiento de medidas para el control de riesgos de la información. Es importante tener en cuenta que almacenar la información en un sitio centralizado evita duplicidades y problemas de versiones, evita pérdidas de documentos, centraliza las copias de seguridad y facilita compartir información para realizar trabajo colaborativo, para lo cual se establecen las siguientes directrices:

5.5.1 Almacenamiento en la Red

- Para que los funcionarios puedan compartir información única y exclusivamente laboral, se dispone de servidores de almacenamiento en red.

- Los controles de acceso a esta información son definidos por el área solicitante de la creación del recurso compartido en la red (carpeta) y el responsable de sistemas, con el objetivo de limitar quién puede acceder, a dónde y los permisos autorizados (lectura, escritura o lectura y escritura)

- Se debe establecer los criterios de almacenamiento corporativos (qué se puede almacenar, quién tiene acceso y cuándo se elimina la información).

- Se debe Establecer e implementar reglas de acceso que permitan llevar un control de quién tiene acceso y a qué discos/directorios.
- Se debe definir un plan de copias de seguridad en el que se detalla la información a guardar, cada cuanto tiempo se va a realizar, donde se va a almacenar y el tiempo de conservación de la misma.

- Se debe proponer una estructura para el almacenamiento clasificado, es decir crear carpetas organizadas según la política de clasificación de la información para que el personal almacene la documentación donde corresponde.

- Se debe realizar auditorías de servidores, que comprenda la revisión periódica del estado de los servidores: uso actual, capacidad, registros, estadísticas de uso, etc.

- Se debe cifrar la información crítica almacenada en los servidores.

5.5.2 Almacenamiento en la Nube

- Se debe informar a los funcionarios cuales son los servicios de almacenamiento cloud permitidos.

- Se debe informar a los funcionarios los pasos a seguir para un adecuado borrado de la información contenida en los repositorios en la nube.

5.5.3 Almacenamiento en Dispositivos Extraíbles

- Para los dispositivos de almacenamiento extraíble (memorias USB, discos duros portátiles, tarjetas de memoria, CD, etc.) que guarden información de la Entidad, deben aplicarse medidas de seguridad, puesto que son susceptibles al robo, manipulación, extravío e infección por virus.

- La Entidad no autoriza el uso de dispositivos de almacenamiento extraíble para el almacenamiento de información de trabajo. En caso que sea estrictamente necesario realizar tal acción, se debe solicitar autorización por parte del jefe del área, además, se debe guardar los activos con clave o cifrado.

- Se deben bloquear los puertos USB a todos los equipos de cómputo de la Entidad.

- Si se necesita almacenar información sensible o confidencial en dispositivos externos corporativos, estos deben estar debidamente protegidos por parte del usuario responsable del guardado de esta información, el cual se debe almacenar en lugares seguros y si ocurre algún incidente (robo, pérdida, infección del dispositivo, etc.) debe informar inmediatamente al personal encargado de la gestión de incidentes.

5.5.4 Almacenamiento en Equipos de Trabajo

- A los funcionarios de la Entidad y algunos contratistas se les asigna como herramienta equipos informáticos: ordenadores, tabletas, teléfonos móviles, etc., para el desempeño de sus funciones. Por lo anterior la Entidad debe establecer las directrices para el almacenamiento de manera local en los equipos.

- Se puede guardar información de la Entidad en el disco local del equipo de cómputo asignado, cuando sea estrictamente necesario y no se cuente con otro medio de almacenamiento autorizado ya sean nube o en los servidores de la red.

- La información que se guarda en los discos locales de los equipos de cómputo de los dispositivos móviles no cuentan con respaldo de información. Para respaldar la información y mantener su conservación por un tiempo determinado por la Entidad, se debe transferir a los servidores o nube autorizada.

5.6 Políticas de Seguridad Física y del Entorno

La Entidad debe prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización, para lo cual se establecen las siguientes directrices:

- Las oficinas administrativas, áreas de procesamiento de información, equipos tecnológicos y de soporte, información de medios físicos entre otros, son base para el cumplimiento de los objetivos de la Entidad, por tanto, se deben establecer y mantener controles para resguardar la seguridad de las instalaciones y ambientes de trabajo, el acceso a las áreas, y demás que procesen información.

- Los equipos de cómputo que pasen a un estado de retiro o se requieran para la reutilización deberán cumplir los siguientes lineamientos: a) Al momento de retirar un equipo en la organización (almacén), el proceso de TIC realiza una copia de respaldo de la información almacenada en este activo. b. El proceso de TIC realiza el proceso de borrado seguro de la información almacenada en los equipos que van a ser cedidos o reutilizados en la organización.

- Los servidores públicos y contratistas, garantizan que no se disponga información de la Entidad en los escritorios de los equipos y que esta no estará almacenada y fácilmente copiada o accedida por alguien sin autorización desde un computador desatendido.

- Para todos los usuarios de las aplicaciones y sistemas de información de la Entidad, es obligatorio que las sesiones sean cerradas al finalizar las actividades y no se deben dejar abiertas o desatendidas.

- Todos los visitantes, sin excepción, deben portar la tarjeta de identificación de visitante o escarapela en un lugar visible mientras permanezcan en un lugar dentro de las instalaciones de la Entidad.

- Las áreas dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles adecuados para la protección de la información.

5.7 Políticas de Controles Criptográficos

La Entidad debe asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la integridad y el no repudio de la información, para lo cual se establecen las siguientes directrices:

- Se deben utilizar técnicas criptográficas y cifrado como son: Para la transferencia o almacenamiento de información sensible o pública reservada, se debe cifrar asignando clave para abrir el archivo.

- Los discos duros internos, externos y memorias USB utilizados por las diferentes áreas o procesos de la Entidad, están cifrados mediante algoritmos de cifrado simétrico. El personal de cada proceso es quien debe solicitar el cifrado de la información que esté clasificada como crítica o sensible por la Entidad.

- La Entidad asegura el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la integridad y el no repudio de la información. Por lo cual establece técnicas criptográficas y cifrado como son: Cifrado de la información cuando se requiere trasferir o almacenar información sensible o crítica, uso de protocolos seguros para las redes Wifi, uso de protocolo HTTPS con un nivel de cifrado actualizado.

- El acceso remoto a la red y los sistemas de información de la Entidad desde una red externa, será a través de conexiones seguras.

- Se debe contar con buenas prácticas para la gestión de llaves.

5.8 Políticas de Seguridad en las Operaciones

La Entidad debe propender por que las operaciones Tecnológicas se gesten de forma correctas y se brinde seguridad a las instalaciones de procesamiento de información, se brinde protección contra código malicioso, gestión de vulnerabilidades, respaldo de información entre otros, que son necesarios para asegurar la correcta operación de los procesos técnicos y la protección de la información, para lo cual se establecen las siguientes directrices:

- La Entidad garantiza que las operaciones Tecnológicas se gesten de forma correctas y se brinde seguridad a las instalaciones de procesamiento de información.

- Los cambios en la Entidad deben ser tratados a través, de un procedimiento establecido de gestión de cambios con el fin de minimizar los riesgos de alteración de los sistemas de información.

- Según la clasificación de la información establecida por la Entidad, se deben establecer las medidas de respaldo de la información a través de mecanismos como cintas, discos de almacenamiento o en la nube.

- Los responsables de TIC definen anualmente un cronograma de pruebas de restauración que permita validar la integridad y disponibilidad de la información almacenada, garantizando la confiabilidad del proceso ejecutado para copias de respaldo.

- El proceso de TIC es el encargado de aplicar las actualizaciones, controles o remediaciones derivadas de la ejecución de pruebas periódicas de análisis de vulnerabilidades.

- Se debe Realizar un listado del software existente autorizado en la Entidad y diseñarle el plan de actualización y aplicación de parches de seguridad, para esto se debe tener en cuenta la revisión de características y los requisitos de las actualizaciones y parches del fabricante antes de instalarlos.

- Se deben implementar mecanismos y procedimientos para deshacer los cambios sufridos tras ejecutar una actualización en caso de no resultar conveniente.

5.9 Políticas de Seguridad de las Comunicaciones

La Entidad debe asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de soporte, para lo cual se establecen las siguientes directrices:

- Se debe implementar tecnología aplicada a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red como por ejemplo un firewall de seguridad perimetral.

- El Proceso de TIC realiza el bloqueo a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso institucional, mediante el uso de servidor proxy, firewall o control que mejor se ajuste a la necesidad.

- El proceso de TIC implementa y mantiene la separación de las redes virtuales para garantizar la confidencialidad de la información en la red de telecomunicaciones de la Entidad.

- Se debe aplicar un método para gestionar la seguridad de las redes dividiéndola en dominios de red separados, por ejemplo: Red de dominio de acceso público y red de dominio de computador de escritorio, dominio de servidor), junto con unidades organizacionales (por ejemplo, recursos humanos, finanzas, mercadeo) o alguna combinación (por ejemplo, un dominio de servidor que se conecta a múltiples unidades organizacionales). La separación se puede hacer usando diferentes redes físicas o diferentes redes lógicas (por ejemplo, redes privadas virtuales).

- Se debe evitar dejar mensajes que contengan información confidencial, en las máquinas contestadoras, ya que éstos pueden ser escuchados por personas no autorizadas, o almacenados incorrectamente como resultado de una marcación incorrecta.

- La transferencia de información deberá realizarse protegiendo la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la clasificación del activo tipo información involucrada.
- La Entidad asegura la protección de las redes y la transferencia de información. Para dar cumplimiento se deben firmar acuerdos de confidencialidad y de no divulgación entre la Entidad y entidades externas con las cuales se intercambie información e implementar controles de seguridad al monitoreo de la red.

5.10 Políticas de Adquisición, Desarrollo y Mantenimiento de Sistemas

La Entidad debe propender porque la Seguridad de la Información sea parte integral de los sistemas de información dentro ciclo de vida de desarrollo de los sistemas de información y en la adquisición de aquellos que presten servicios a la Entidad, para lo cual se establecen las siguientes directrices:

- Se debe establecer el procedimiento de desarrollo seguro de software, la revisión técnica y de seguridad de las aplicaciones para detectar vulnerabilidades antes de salir a producción y la aplicación del procedimiento gestión de cambios.

- La Entidad garantiza que los sistemas de información estén asociados a lineamientos, procesos, buenas prácticas y demás requisitos que sirvan para regular los desarrollos de software internos en un ambiente controlado, así mismo se identifican y gestionan los posibles riesgos referentes a seguridad de la información durante todo el ciclo de vida del software.

- La Entidad asegura que se diseñe e implemente los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.

- La Entidad debe establecer controles técnicos para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información que son públicos mediante herramientas de seguridad perimetral de proveedores o de forma local.

- La Entidad cuenta con un ambiente de desarrollo y de pruebas seguro o, en su defecto, exige al proveedor mediante los contratos, que éste cuente con los controles de seguridad de la información sobre los ambientes.

- Los datos de pruebas que se utilicen durante todo el ciclo de vida de los sistemas de información deben ser seleccionados, utilizados y eliminados de forma segura.

- La Entidad debe establecer una metodología de desarrollo seguro de software.

5.11 Políticas de Relación con Proveedores

La Entidad debe controlar que toda relación con proveedores, y en particular aquellos que tienen acceso a la información, está suficientemente protegida, para lo cual se establecen las siguientes directrices:

- Para proveedores críticos de tecnología, así como de procesos misionales, la Entidad exige que cuente con planes de continuidad de negocio y recuperación de desastres definidos e implementados, de modo que el proveedor contratado pueda responder ante eventuales escenarios que afecten el suministro de servicios o productos a la Entidad.

- La protección de la información, debe contemplarse antes, durante y a la finalización del servicio. Para dar este cumplimiento se deben establecer cláusulas contractuales en materia de seguridad y privacidad de la información y determinar que controles de seguridad son de obligatorio cumplimiento en las relaciones con los proveedores de servicios tecnológicos.

- Cualquier cambio que se realice con algún proveedor crítico de TIC o de los procesos misionales, debe aplicarse mediante el procedimiento de gestión de cambios establecido en la Entidad.

- La Entidad realiza revisiones periódicas al cumplimiento de las Políticas de Seguridad y Privacidad de la Información a los Proveedores.

- La protección de la información, debe contemplarse antes, durante y a la finalización del servicio. Para dar este cumplimiento se deben establecer cláusulas contractuales en materia de seguridad y privacidad de la información y determinar que controles de seguridad son de obligatorio cumplimiento en las relaciones los proveedores de servicios tecnológicos.

5.12 Políticas de Gestión de Incidentes de Seguridad

La Entidad debe asegurarse que todos los funcionarios conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información, para lo cual se establecen las siguientes directrices:

- Se debe establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

- Todos los servidores públicos y contratistas deben conocer el método de reporte de eventos e incidentes de seguridad de la información.

- En la gestión del incidente y cuando sea necesario obtener evidencia de un incidente, siempre se debe garantizar el cumplimiento de los requisitos legales aplicables o comunicar a un ente competente para que realice el debido proceso.

- La Entidad establece y ejecuta procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.

- La Entidad debe establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

- La Entidad debe establecer y poner a disposición de los funcionarios el formato o mecanismos de reporte de eventos e incidentes de seguridad y privacidad de la información.

- La Entidad debe contar con una bitácora de los incidentes de seguridad de la información reportados y atendidos y el establecimiento de indicadores relacionados a la gestión de los incidentes de seguridad y privacidad de la información.

5.13 Políticas de Cumplimiento

La Entidad gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente, para lo cual se establecen las siguientes directrices:

- Se debe analizar los requisitos legales aplicables a la información, incluyendo los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de

registros y los delitos informáticos y brindar los lineamientos que permitan dar cumplimiento a la normatividad legal.

- La Entidad asegura el conocimiento y cumplimiento de las obligaciones legales en materia de seguridad de la información. Por lo anterior, garantiza el cumplimiento de los derechos de propiedad intelectual de terceros controlando la adquisición y uso del software en la Entidad. Debe determinar las responsabilidades para gestionar la protección de datos personales.

- La Entidad, debe asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.

6. APOYO O SOPORTE

6.1 Toma de Conciencia

La Secretaría General por medio del área de Talento Humano y el supervisor del contrato, Brindaran lineamientos para que toda la entidad, sus funcionarios, contratistas, practicantes y en general cualquier persona que tenga acceso a información oficial, a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la Institución, sin importar el tipo de vinculación con la Alcaldía Municipal de Pitalito-Huila, reciban la educación, actualización periódica en materia de seguridad de la información, formación en toma de conciencia adecuada, y actualizaciones sobre las políticas y procedimientos.

También se incorporará la aplicación de las políticas de seguridad de la información en su plan de capacitación institucional, y se velará por la correcta inducción de los funcionarios nuevos en materia de seguridad de la información.

6.2 Comunicación

La Entidad deberá establecer los canales accesibles para la comunicación permanente de todas las políticas, procedimientos u otros documentos que hagan parte del Modelo de Seguridad y Privacidad de la Información (MSPI), algunos canales accesibles y formales para la comunicación son:

Correo Electrónico Institucional, Extranet, comunicación impresa, charlas y capacitaciones.

El presente manual de políticas de Seguridad y Privacidad de la Información, será comunicado a todas las partes interesadas de la Entidad, a través de las tecnologías de la información y medios físicos de ser necesario.

Todas las políticas, procedimientos y demás documentos relacionados con la seguridad y privacidad de la información serán publicados en la página web de la alcaldía de Pitalito, Huila https://alcaldiapitalito.gov.co/.

7. EVALUACIÓN DEL DESEMPEÑO

7.1 Seguimiento, Medición, Análisis y Evaluación

La Entidad, debe asegurar que la seguridad y privacidad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales, para lo cual se establecen las siguientes directrices:

Seguimiento de tareas, actividades o acciones asignadas en reuniones Comité Institucional de Gestión y Desempeño, donde se traten los temas de seguridad y privacidad de la información y auditoria interna del último ciclo, para revisar y evaluar el cumplimiento de la política y demás normas de seguridad y privacidad de la información.

Analizar propuestas o acciones correctivas y de mejora al MSPI por parte de los servidores públicos y contratistas y documentar los resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos

Revisión y actualización anual en caso de que aplique de la política general, la revisión de las políticas específicas de seguridad, de objetivos de Seguridad de la Información (su contenido y cumplimiento en los diferentes procesos) por medio de planes de acción.

7.2 Revisión por la Dirección

La Alcaldía Municipal de Pitalito - Huila garantiza el apoyo al proceso de revisión, del Modelo de Seguridad y Privacidad de la Información, del cual hace parte integral la presente política, por medio del Comité Institucional de Gestión y Desempeño.

8. CONTROL DE CAMBIOS

No	Fecha de aprobación	Ítem alterado	Motivo del cambio	Realizado por
1	10-12-2020	N.A	Creación del manual	Jaime Andrés Murcia Losada- Apoyo Profesional Gestión TIC

9. APROBACIONES

	REVISÓ	APROBÓ
NOMBRE	Harvey Oswald Carmona Granados	Comité Institucional de Gestión y Desempeño - Acta 09 del 10 de diciembre de 2020.
CARGO	Secretario de Planeación	