ALCALDÍA DE MANIZALES
Secretaría de Servicios Administrativos

MANUAL DE OPERACIÓN DE LAS POLÍTICAS DE MIPG

DIMENSIÓN GESTIÓN CON VALORES PARA RESULTADOS

POLÍTICA DE SEGURIDAD DIGITAL 2025

INTRODUCCION

La Alcaldía de Manizales, mediante el Decreto 0419 del 5 de septiembre de 2023, implementó el Modelo Integrado de Planeación y Gestión en la entidad con el fin de orientar, fortalecer, articular, alinear y dirigir la gestión institucional mejorando la interacción de la entidad y la ciudadanía.

Este proceso ha permitido agilizar su implementación en la entidad, el cual consiste en procesos como el ciclo PHVA, incluyendo con esto la mejora continua; es así como se estableció la responsabilidad para la implementación, desarrollo, y control y mejora del esquema operativo de MIPG, dejando la estructura de las políticas, y líneas de acción.

Cada política será trabajada a través de mesas técnicas, con planes de trabajo anuales. Estas mesas tendrán que reunirse periódicamente con carácter obligatorio, deberán reportar los avances, de las actividades al Comité de Desempeño Institucional con el fin de que se tomen las decisiones, atendiendo la implementación y operación del modelo.

Finalmente, la Unidad de Transparencia y Gobierno Abierto, adscrita a la Secretaría de Servicios Administrativos, como Líder de MIPG, desarrolló conjuntamente con los funcionarios enlaces de cada dependencia la compilación y expedición de este Manual, buscando con ello promover la gestión y eficiencia de la entidad manteniendo su vigencia.

El Manual Operativo, que presentamos se ha desarrollado de acuerdo con el Modelo Integrado de Planeación y Gestión, describiendo los diferentes mecanismos a través de los cuales se deben dinamizar cada una de las 19 políticas, en el marco del direccionamiento y la planeación estratégica de la Alcaldía de Manizales, con la siguiente estructura:

- Objetivo general
- Objetivos específicos
- Marco Legal
- Definiciones
- Líneas de acción
- Responsables
- Seguimiento

Este manual, podrá ser consultado en la sede electrónica de la Alcaldía de Manizales en el botón de transparencia y acceso a la información pública, así mismo, debe ser objeto de socialización a los funcionarios de la administración municipal con el fin de que en sus actuaciones administrativas estén inmersas los lineamientos descritos en este documento.

7. OPERACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

7.1 Objetivo General

Identificar, gestionar y mitigar los riesgos de seguridad digital que puedan afectar la confianza de los ciudadanos y la calidad de datos que se gestionan por ambas partes.

7.2 Objetivos Específicos

- Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y el MinTIC para el Tratamiento de Riesgos de Seguridad Digital.
- Actualizar el Modelo de Privacidad y Seguridad de la Información y aplicar los lineamientos allí establecidos para garantizar un entorno de confianza digital de manera articulada con la política de Gobierno Digital.
- Promover en los usuarios internos y externos el uso y comportamiento responsable, en el entorno digital, de forma que no afecten la seguridad de los activos digitales de la Entidad.
- Establecer los mecanismos de aseguramiento físico, digital y de cultura organizacional, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la Información de la Administración Municipal.

7.3 Marco Legal

NORMA	DESCRIPCION
Ley 23 1982	Sobre Derechos de Autor.
Ley 80 1993	Por la cual se expide el Estatuto General de Contratación de la Administración PÚBLICA.
Ley 1341 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 1581 2012	Por el cual se dictan disposiciones generales para la protección de datos personales. HABEAS DATA.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Modificado en el artículo 2.2.9.1.1.3., incluye la seguridad de la información entre los principios de las Políticas de Gobierno Digital y Seguridad Digital; de igual manera, en el artículo 2.2.9.1.2.1. se establece que las Políticas de Gobierno Digital y Seguridad Digital ÚLTIMA FECHA DE ACTUALIZACIÓN: 22 DE AGOSTO DE 2023.
Decreto 1414 de 2017	A través del cual se modificó la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones, asignando a la Dirección de Gobierno Digital, antes "Dirección de Gobierno en Línea".
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Directiva presidencial de 2019	Simplificación de la interacción digital entre los ciudadanos y el estado.
Decreto 2106 de 2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
CONPES 3995 de 2020	Política nacional de confianza y seguridad digital.
Resolución 2893 2020	Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPAs y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado Colombiano, y se dictan otras disposiciones.
Resolución 1519 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

Decreto 338 2022	Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 767 de 2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 88 de 2022	Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los articulas 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.
Resolución 460 de 2022	Por lo cual se expide el plan nacional de infraestructura de datos y su hoja de ruta en el desarrollo de la política de Gobierno Digital y se dictan los lineamientos generales para su implementación.
Decreto 1263 2022	Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública.
Ley 2294 2023	Por la cual se expide el Plan Nacional de Desarrollo 2022-2026 "Colombia Potencia Mundial de la Vida" establece en su artículo 43 las medidas que implementará el Ministerio de las Tecnologías de la Información y las comunicaciones entre las que se encuentra el Fortalecimiento del Gobierno digital para tener una relación eficiente entre el Estado y el ciudadano, que lo acerque y le solucione sus necesidades, a través del uso de datos y de tecnologías digitales para mejorar la calidad de vida.

7.4 Definiciones

Amenaza cibernética: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (Documento CONPES 3854)

Ataque cibernético: Acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio. (Documento Modelo Nacional Riesgo de Seguridad Digital)

Ciberdefensa: Es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. (Documento CONPES 3854).

Ciberespionaje: Es el acto o práctica de obtener secretos sin el permiso del dueño de la información (personal, sensible, propietaria o de naturaleza clasificada) para ventaja personal, económica, política o militar en el Ciberespacio, a través del uso de técnicas malintencionadas. (Documento CONPES 3854).

Ciberterrorismo: Es el uso del Ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado trayendo. (Documento CONPES 3854).

Cibercrimen (delito cibernético): Conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio. (Documento CONPES 3854).

Ciberlavado: Es el uso del Ciberespacio, en cualquiera de sus formas, para dar apariencia de legalidad a bienes obtenidos ilícitamente o para ocultar dicha ilicitud ante las autoridades.

Ciberseguridad: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio. (Documento CONPES 3854).

Entorno digital: Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

Entorno digital abierto: Entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica.

Gestión de riesgos de seguridad digital: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades.

Incidente digital: Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos.

Infraestructura crítica cibernética nacional: Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (Documento CONPES 3854).

Riesgo: Es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.

Riesgo de seguridad digital: Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital.

Resiliencia: Es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (Documento CONPES 3854).

Seguridad de la información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua, con miras a preservar la confidencialidad, integridad, y disponibilidad de la información (ISO/IEC 27000).

Seguridad digital o ciberseguridad: Conjunto de medidas de "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (Documento CONPES 3854).

7.5. Controles y políticas

7.5.1 Controles Organizacionales

7.5.1.1 Política de Gestión de Activos

La Oficina de Bienes y Servicios de la Alcaldía de Manizales con el acompañamiento permanente de la Unidad de Gestión Tecnológica, establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración, rotulado y buen uso de los activos de información, con el objetivo de garantizar su protección. Dichos lineamientos se impartirán teniendo en cuenta los siguiente literales:

a. **Inventario de Activos**: Los activos de la Alcaldía de Manizales deben ser identificados, clasificados, valorados y controlados para garantizar su uso, protección y recuperación ante desastres. Por tal motivo, se diseñará una metodología con los lineamientos necesarios para llevar el inventario de los activos de información, discriminado por procesos y dependencia, tipo, nivel de criticidad, clasificación, ubicación, responsable, custodio, y demás atributos que la entidad defina.

b. **Protección**: Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de su función se encargarán de proteger la información, así como de mantener y actualizar el inventario de activos de información relacionados con sus servicios (información física o digital, software, hardware y recurso humano), bajo los parámetros que establezca la Unidad de Gestión Tecnológica.

c. **Archivos de Gestión**: La Secretaría Administrativa deberá implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo con las Tablas de Retención Documental y Tablas de Control de Acceso, con el fin de proteger y conservar la confidencialidad,

integridad y disponibilidad de la información física del Ministerio de Tecnologías de la Información y las Comunicaciones.

d. Clasificación de la Información: La Secretaría de Servicios Administrativos implementará mecanismos para rotular la información física, de acuerdo con la metodología establecida.

e. Firma de documentos: Las firmas de documentos que produzca la Alcaldía de Manizales, serán válidas en cualquiera de los siguientes métodos, garantizando la confiabilidad, integridad, autenticidad y disponibilidad de la información y de los documentos expedidos por los empleados públicos y contratistas en el marco de sus funciones y obligaciones, respectivamente:

a. En físico con firma autógrafa mecánica.

b. Con firma digital de persona natural asignada por la Secretaría de Servicios Administrativos según lo dispuesto por la Ley 527 de 1999.

c. Con firma electrónica, de acuerdo con lo dispuesto en el Decreto 1074 de 2015 y el Decreto 1287 de 2020 "Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.", para lo cual se deberá adquirir o implementar un aplicativo integrado con el sistema de gestión documental que contenga como mínimo lo siguiente:

i. Control seguro de acceso y uso de aplicativo, sincronizado con el directorio activo, garantizando que solo personal vinculado como empleados públicos y contratistas de prestación de servicios profesionales o de apoyo a la gestión pueda hacer uso del mecanismo de firma electrónica.

ii. Múltiples controles para la autenticación y firma del documento electrónico, garantizando que el firmante es quien dice ser.

iii. El sistema debe solicitar la firma digitalizada o escaneada y quedar estampada en el documento junto con el nombre completo, cargo, correo electrónico institucional del funcionario o contratista que firma.

iv. Identificador único provisto por el sistema que permita la verificación de la veracidad del documento.

v. Fecha de creación y finalización de la firma, información que debe ser provista por el servidor y estar sincronizada con la hora legal colombiana de acuerdo con lo establecido en el numeral 14 del artículo 6 del Decreto 4175 de 2011.

vi. Estado del trámite de firma.

vii. Firma digital de persona jurídica de la Alcaldía de Manizales, según sea el caso.

viii. Las firmas facsímil, solo podrán ser autorizadas por Resolución expedida por la Alcaldía de Manizales, en la que señale para que fin y porqué medios podrá ser utilizada.

7.5.1.2 Política de control de acceso

Los propietarios de los activos de información, teniendo en cuenta el tipo de activo, deberán establecer medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías (*on premise* o en nube) e infraestructura física (instalaciones y oficinas), todo esto con el fin de mitigar riesgos asociados al acceso a la información, infraestructura tecnológica e infraestructura física de personal no autorizado y así propender por salvaguardar la integridad, disponibilidad y confidencialidad de la información de la Alcaldía de Manizales.

7.5.1.3 Política de Seguridad para Relación con Proveedores

La Alcaldía de Manizales, establecerá en el manual de contratación, las disposiciones necesarias para asegurar que la información que se genere, custodie, procese, comparta, utilice, recolecte, intercambie o a la que se tenga acceso con ocasión de un contrato, se utilice dentro del marco de la seguridad y privacidad de la información por parte de los proveedores. En el mismo sentido y a través del seguimiento a la ejecución, se garantizará que los supervisores de los contratos, convenios o acuerdos sean los responsables de aplicar las políticas y procedimientos de seguridad de la información durante la ejecución de los mismos. Estos lineamientos deberán ser comunicados a los proveedores y terceros a través de los canales dispuestos por la Alcaldía.

Tratándose de relaciones contractuales de la Alcaldía de Manizales, estas disposiciones deberán ser incorporadas en los términos, minutas o acuerdos con los que se relacionen estos, a efectos de garantizar su implementación.

7.5.1.4 Política de Gestión de Incidentes de Seguridad y Privacidad de la Información

La Alcaldía de Manizales, a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, promoverá entre los empleados públicos y contratistas, el reporte y seguimiento de incidentes relacionados con la seguridad y privacidad de la información y sus medios. Así mismo, asignará responsables para el tratamiento de los mismos, quienes investigarán y solucionarán los incidentes reportados, de acuerdo a su sana crítica.

El Alcalde de Manizales o su delegado son los únicos autorizados para reportar incidentes de seguridad y privacidad ante las autoridades de defensa nacional, policía, fiscalía y de control. En esta medida, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía. La delegación de esta potestad podrá ser formal, por medio de acto administrativo, en los términos de la Ley 489 de 1998, o cualquiera que la modifique, adicione, subrogue o derogue.

7.5.1.5 Política de la Continuidad de la Operación de los Servicios

La Alcaldía de Manizales dispondrá los planes necesarios para la continuidad de la operación de los servicios, los cuales serán operados por los líderes de los procesos. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces y la Secretaría de Planeación liderarán conjuntamente la elaboración del Análisis de Impacto del Negocio (BIA) y del Plan de Continuidad de la Operación de los Servicios (BCP).

El Plan de Continuidad de los Servicios de la Alcaldía de Manizales, contendrá el Plan de Continuidad de Tecnologías y los Planes de Emergencia y Contingencia, así como cualquier estrategia orientada a la continuidad de la prestación del servicio de la Alcaldía.

La Unidad de Gestión Tecnológica de la Alcaldía de Manizales, liderará, implementará y actualizará el Plan de Continuidad de las TIC (Plan de Recuperación ante Desastres Tecnológicos) alineado a su vez con el BIA y el BCP. Este plan incluirá escenarios de falla, estrategias de recuperación, roles y responsabilidades, plan de comunicación, pruebas y demás atributos que la entidad defina, lo cual permita propender por la disponibilidad y el acceso a los sistemas, datos y aplicaciones de información críticos en caso de interrupciones o eventos disruptivos.

7.5.1.6 Política Legal y Cumplimiento

La Alcaldía de Manizales, a través del Oficial de Seguridad y Privacidad de la Información, o quien haga sus veces, velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad y privacidad de la información, de acuerdo con lo establecido por el gobierno nacional, entre ellos los referentes a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública, para lo cual dispondrá una Matriz de Requisitos Legales para su control y seguimiento.

Los funcionarios, contratistas y colaboradores que ejecuten actividades de adquisición o licenciamiento de software tienen el deber de seguir los lineamientos de compra pública e incluir dentro de los estudios previos y pliegos de condiciones, los términos mediante los cuales se acreditará que la forma del licenciamiento, la forma en la que se ejercerán derechos morales y patrimoniales de autor, el número máximo de usuarios o recursos, la forma de instalación y los procedimientos para mantener las condiciones de licencia adecuadas, desechar o transferir software a otros. Igualmente, se establecerá y comunicará la Política de Tratamiento de Datos Personales.

7.5.1.7 Política de Privacidad

La Alcaldía de Manizales deberá disponer, a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, de los controles necesarios para la protección de la información personal de los empleados públicos, contratistas y partes interesadas externas, en los términos del artículo 15 de la Constitución política, regulado por la Ley 1581 de 2012 y sus decretos reglamentarios.

Podrán emplearse técnicas de enmascaramiento para proteger la confidencialidad de datos personales, caso en el cual podrá acudirse a herramientas de pseudoanonimización o anonimización dispuestas por la Unidad de Gestión Tecnológica.

7.5.1.8 Política de Protección de la Información

Para propender por la confidencialidad, integridad y disponibilidad de todos los activos de información se adoptarán estándares y buenas prácticas en protección de información. Los funcionarios, contratistas y colaboradores deben identificar y catalogar los activos de información según su nivel de sensibilidad y adoptar los controles y medidas de protección aplicables al tratamiento que requiera conforme a la sana critica.

A efectos de acuerdos o convenios, se considerará como información confidencial todo dato, documento, material, conocimiento o cualquier otra información que atienda a los presupuestos del artículo 18 y 19 de la Ley 1712 de 2014 y que sea revelada al Receptor

durante el curso de su relación laboral, contractual o de cualquier índole, exceptuando aquella que sea de dominio público acorde con el principio de máxima publicidad. La obligación de confidencialidad permanecerá en vigor en los términos previstos por la ley, independientemente de la razón de dicha terminación.

Se facilitarán acuerdos y/o cláusulas de confidencialidad que serán suscritos por los servidores públicos, contratistas, proveedores, entidades y ciudadanos que por diferentes razones requieran conocer, transferir o intercambiar información restringida y/o confidencial.

7.5.1.9 Política de Seguridad de la Información en la gestión de proyectos

La Secretaría de Planeación deberá incluir los requerimientos y consideraciones en materia de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, en la metodología de gestión de proyectos de la entidad, garantizando que se implementen en las fases iniciales de los proyectos, en el mismo sentido, la Oficina de Control Interno deberá incluir dentro de su plan de auditorías la revisión de su cumplimiento e implementación.

La Secretaría jurídica debe velar porque en todos los estudios previos de los proyectos o contratos a celebrar por la Alcaldía de Manizales, se incluyan los requerimientos y consideraciones referentes a Política Institucional de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios que se están contratando.

7.5.2 Controles De Personas

7.5.2.1 Política de Seguridad de los Recursos Humanos

La Unidad de Gestión Humana, aplicará los lineamientos dados por la norma vigente y los procedimientos internos en los procesos de selección, vinculación y retiro del personal, realizando las verificaciones necesarias para confirmar la veracidad de la información suministrada por la persona candidata a emplear, a su vez, debe desplegar esfuerzos para generar conciencia y apropiación en los empleados públicos de la entidad, sobre sus responsabilidades en el marco de la Política Institucional de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios en el Ministerio/Fondo Único de TIC, con el fin de reducir los riesgos, el mal uso de las instalaciones y recursos tecnológicos y así asegurar la confidencialidad, integridad y disponibilidad de la información.

Con el mismo fin, incluirá en las minutas de los contratos y convenios, cualquiera que sea su naturaleza o modalidad, cláusulas y obligaciones en relación con el cumplimiento de la Política Institucional de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios, las cuales deberán ser divulgadas a través de los supervisores de los contratos, a proveedores, a operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y obligaciones, compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

La Oficina de Formación y Capacitación deberá fomentar la participación de los empleados públicos de la entidad en las convocatorias para el fortalecimiento de capacidades en Seguridad digital realizadas por el Gobierno Nacional u organismos internacionales.

7.5.3 Controles Físicos

7.5.3.1 Política de Seguridad Física y del Entorno

La Alcaldía de Manizales, a través de la Secretaría de Servicios Administrativos, con el apoyo del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, debe adoptar medidas para la protección del perímetro de seguridad de sus instalaciones físicas para controlar el acceso y permanencia del personal en las oficinas, instalaciones y áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones), con el fin de mitigar los riesgos, amenazas externas, ambientales y evitar afectación a la confidencialidad, integridad y disponibilidad de la información de la entidad.

Se deberá garantizar la protección de los datos, semiprivados, privados y sensibles recolectados de los empleados públicos, contratistas y visitantes, y establecer mecanismos alternativos para quienes no autorizan el tratamiento de sus datos.

Todos los empleados públicos, contratistas, proveedores y visitantes que se encuentren en las instalaciones físicas de la Alcaldía de Manizales deben estar debidamente identificados mediante un carné, documento o distintivo que acredite su tipo de vinculación. En el caso de utilizar un carné, este debe portarse en un lugar visible.

El personal de empresas, cooperativas o entidades que desempeñe funciones de forma permanente en las instalaciones del Ministerio de Tecnologías de la Información y las Comunicaciones, deben estar identificados con carné y chalecos o distintivos de la empresa o entidad y portar el carné de la Administradora de Riesgos Laborales (ARL).

7.5.4 Controles tecnológicos

7.5.4.1 Política de Seguridad de las Operaciones

La Unidad de Gestión Tecnológica será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación de la Entidad. Así mismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información e implantará el control de cambios, para asegurar que los cambios realizados sobre los recursos tecnológicos y sistemas de información en ambientes de producción sean controlados y debidamente autorizados, así mismo implementará mecanismos para controlar la información en los ambientes de desarrollo y prueba. De igual manera, proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la entidad, al igual que desarrollará mecanismos de contingencias y recuperación ante desastres con el fin de propender por la disponibilidad de los servicios de TI.

La Unidad de Gestión Tecnológica deberá realizar y mantener las copias de seguridad de acuerdo con el procedimiento **PSI-SAM-002: Gestión de las copias de seguridad**, en los servidores que contienen los sistemas de información internos. Además, los proveedores serán responsables de realizar las copias de seguridad y las pruebas de recuperación de los sistemas de información desarrollados para la entidad.

El Oficial de Seguridad y Privacidad de la Información, o quien haga sus veces, velará porque estas copias sean reportadas por el responsable, con el objetivo de poder recuperarlas en caso de cualquier tipo de falla.

El diseño de este procedimiento se hará bajo la dirección de la Unidad de Gestión Tecnológica, con el apoyo de los líderes de proceso y deberá estar alineado con la gestión documental de la entidad, con el fin de determinar la información a respaldar, la periodicidad, los tiempos de retención, recuperación, restauración y los mecanismos para generar el menor impacto en la prestación del servicio durante el tiempo de la indisponibilidad de la información.

En el evento que alguna dependencia opere una plataforma tecnológica fuera de las instalaciones físicas y en el marco de las funciones misionales u operacionales, deberá cumplir con lo establecido en la presente política y los lineamientos dispuestos por el Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, para tal fin.

7.5.4.2 Política de Seguridad del Sistema y de la Red

La Unidad de Gestión Tecnológica establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios tecnológicos que dependen de ellas; así mismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información, con el fin de detectar comportamientos anómalos y tomar las medidas apropiadas para evaluar posibles eventos o incidentes de seguridad y privacidad de la información.

Se establecerán mecanismos estratégicos para que el intercambio de información con las partes interesadas internas o externas, se realice asegurando su integridad. En el evento que los acuerdos de intercambio de información requieran del desarrollo de servicios web (*web service*) o de cualquier otro medio tecnológico, el intercambio deberá realizarse con los controles criptográficos establecidos para tal fin.

Como parte de sus términos y condiciones iniciales de trabajo de todos los empleados públicos, sin importar su nivel jerárquico, o los contratistas según el caso, firmarán un acuerdo o compromiso de confidencialidad y no divulgación, según el tipo de vinculación. Dicho documento original será conservado y archivado en la historia laboral de los empleados públicos y en la carpeta de los procesos contractuales para el caso de los contratistas.

En el caso de persona jurídica proveedora de servicios, en la carpeta del contrato deberá reposar el acuerdo o compromiso de confidencialidad y no divulgación, debidamente suscrito.

7.5.4.3 Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas

La Unidad de Gestión Tecnológica velará porque los desarrollos internos y externos de los sistemas de información, cumplan con los requerimientos de seguridad adecuados para la protección de la información, para lo cual, establecerá una metodología que detalle los requerimientos de seguridad para el desarrollo, pruebas, puesta en producción y mantenimiento de los sistemas de información.

En el marco del Plan Estratégico de Tecnologías de la Información (PETI), la Unidad de Gestión Tecnológica es la única dependencia de la entidad con la capacidad de adquirir, conforme con su ficha de inversión, desarrollar e implementar soluciones tecnológicas, así como avalar la adquisición y recepción de software de cualquier tipo en el marco de convenios y contratos con terceros, conforme a los requerimientos de las dependencias, con

el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en el Ministerio.

En consecuencia, cualquier software que opere deberá contar con la autorización de la Unidad de Gestión Tecnológica y deberá reportarse y entregarse cumpliendo con los lineamientos técnicos y presupuestales de dicha oficina, con el fin de salvaguardar la información, brindar el soporte y demás procesos técnicos que permitan su recuperación en caso de algún incidente o siniestro.

En caso de que alguna dependencia adquiera, desarrolle o realice mantenimientos a sistemas de información dentro del desarrollo misional u operacional, deberá cumplir con lo establecido en la presente política.

7.5.4.4 Política de Servicios en la nube

La Unidad de Gestión Tecnológica será la encargada de mantener la seguridad y privacidad de la información y los servicios de procesamiento de información en plataformas de computación en la nube que son utilizados por la Entidad, garantizando su continuidad, cumpliendo los niveles de servicio requeridos aplicando las políticas y lineamientos definidos. Los contratos o convenios que impliquen el aprovisionamiento de servicios en la nube deberán incluir obligaciones para la prestación de servicios tecnológicos y aprovisionamiento de infraestructura, de cara a la mitigación de posibles riesgos.

El uso de los servicios de computación en la nube dispuestos en la Entidad debe ser exclusivo para el cumplimiento de las funciones u obligaciones encomendadas, no está autorizado el uso de servicios de computación en la nube para fines personales.

7.5.5 Políticas Especificas

7.5.5.1 Política de seguridad de la sede electrónica

La Unidad de Gestión Tecnológica será la encargada de administración y gestión de la sede electrónica, en donde se deberán integrar todos los portales, sitios web, plataformas, ventanillas únicas, aplicaciones y soluciones existentes. Para la operación de la sede electrónica se deberá definir e implementar, en concordancia con las dependencias responsables de trámites, procesos y procedimientos dirigidos a los ciudadanos, las medidas jurídicas, organizativas y técnicas que garanticen la calidad, seguridad, privacidad, disponibilidad, integridad, confidencialidad, accesibilidad, neutralidad e interoperabilidad de la información y de los servicios.

En la sede electrónica se deberán identificar fácilmente y de manera clara, los canales digitales oficiales de recepción de solicitudes, peticiones y de información.

A través del proceso de Gestión Documental, se deberá disponer de un sistema de gestión documental electrónica y de archivo digital, asegurando la conformación de expedientes electrónicos con características de integridad, disponibilidad y autenticidad de la información.

La emisión, recepción y gestión de comunicaciones oficiales, a través de los diversos canales electrónicos, deberá asegurar un adecuado tratamiento archivístico, estar debidamente alineado con la gestión documental electrónica y de archivo digital e igualmente deberá contar con todas las consideraciones en materia seguridad, privacidad de la información, seguridad digital, continuidad de la operación de los servicios y demás lineamientos de los que trata esta resolución.

La Secretaría de Servicios Administrativos deberá establecer las estrategias que permitan el tratamiento adecuado de los documentos electrónicos y garantizar la confidencialidad, integridad, disponibilidad y acceso a largo plazo conforme a los principios y procesos archivísticos definidos por el Archivo General de la Nación.

7.5.6 Responsabilidades De Los Colaboradores Frente Al Uso De Los Servicios Tecnológicos.

7.5.6.1 Política de Seguridad Digital

Todos los empleados públicos o contratistas que hagan uso de los recursos tecnológicos de la Alcaldía de Manizales tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable; entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación de los servicios y por ende, el cumplimento de la misión institucional. Para ello, deben acatar las siguientes disposiciones:

a. **Del uso del correo electrónico.** El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los empleados públicos y contratistas de la Alcaldía, cuyo uso se facilitará en los siguientes términos:

i. El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la entidad es el asignado por la Unidad de Gestión Tecnológica, que cuenta con el dominio @manizales.gov.co, el cual

cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.

ii. El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional, en consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro ajeno a los propósitos de la entidad.

iii. En cumplimiento de la iniciativa institucional del uso aceptable del papel y la eficiencia administrativa, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la ley lo permita.

iv. Los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones), la cual establece la validez de los mensajes de datos.

v. La Unidad de Gestión Tecnológica implementará herramientas tecnológicas que prevengan la pérdida o fuga de información de carácter reservada o clasificada, de conformidad con la Ley 1712 de 2014.

vi. Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.

vii. Todo mensaje de correo electrónico enviado mediante plataformas externas deberá hacerse con la cuenta de la entidad y utilizando el dominio @manizales.gov.co, con el fin de que no sean catalogados como spam o suplantación de correo.

viii. Para apoyar la gestión de correo electrónico de directivos, el titular debe solicitar a la mesa de ayuda la delegación del buzón correspondiente, relacionando los colaboradores que podrán escribir o responder *en nombre del* titular, con el fin de mitigar la suplantación.

ix. Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser reportado a través de la Mesa de Ayuda como incidente de seguridad, según el procedimiento establecido, y deberán acatarse las indicaciones recibidas para su tratamiento, lo anterior, debido a que puede contener virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, o explícitas

referencias no relacionadas con la misión de la entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos). Está expresamente prohibido el envío y reenvío de mensajes en cadena.

x. La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o cualquier otra ajena a los fines de la entidad.

xi. Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y que atenten contra la integridad moral de las personas o instituciones.

xii. Está expresamente prohibido distribuir información oficial de carácter clasificada o reservada a otras entidades o ciudadanos sin la debida autorización.

xiii. Está expresamente prohibido distribuir, copiar o reenviar información de la Alcaldía de Manizales a través de correos personales o sitios web diferentes a los autorizados en el marco de las funciones u obligaciones contractuales.

xiv. El municipio de Manizales se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional de todos sus empleados públicos o contratistas. Además, podrá realizar copias de seguridad del correo electrónico en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información de la entidad o de terceros operados en la misma, previa solicitud expresa del nominador, ordenador del gasto, supervisor del contrato, jefe inmediato, Control Interno Disciplinario o Unidad de Gestión Humana. Para ello, al inicio de la relación laboral o contractual se deberá comunicar a los funcionarios y contratistas que se realiza el referido monitoreo.

b. **Del uso de Internet:** La Unidad de Gestión Tecnológica, en conjunto con el Oficial de la Seguridad de la Información o quien haga sus veces, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones. Será responsabilidad de los colaboradores lo siguiente:

i. Los servicios a los que un determinado usuario pueda acceder en internet dependerán del rol, funciones u obligaciones que desempeñe y para las cuales

esté formal y expresamente autorizado por su jefe o supervisor y solo se utilizará para fines laborales.

ii. Abstenerse de enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.

iii. Abstenerse de acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por la política de navegación.

iv. Abstenerse de enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.

v. Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso.

El municipio de Manizales se reserva el derecho de monitorear los accesos y el uso del servicio de Internet, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines de la Entidad.

c. **Del uso de los recursos tecnológicos:** Los recursos tecnológicos son herramientas de apoyo a las labores, responsabilidades y obligaciones de los empleados públicos y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

i. Los bienes de cómputo que provea la entidad se emplearán de manera exclusiva y bajo la completa responsabilidad del funcionario o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por tanto, no pueden ser utilizados con fines personales o por terceros no autorizados.

ii. Sólo está permitido el uso de software licenciado por la entidad y aquel que, sin requerir licencia, sea expresamente autorizado por la UNIDAD DE GESTIÓN TECNOLÓGICA.

iii. En caso de que el funcionario o contratista deba hacer uso de equipos ajenos a la entidad, éstos deberán cumplir con la legalidad del software instalado, sistema operativo y antivirus licenciado, actualizado y solo podrá conectarse a la red una vez esté avalado por la UNIDAD DE GESTIÓN TECNOLÓGICA.

iv. Los empleados públicos y contratistas deberán realizar y mantener las copias de seguridad de su información y entregarla a su jefe inmediato al finalizar la vinculación.

v. Está expresamente prohibido el almacenamiento en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional o que atenten contra los derechos de autor o propiedad intelectual de los mismos.

vi. Los empleados públicos y contratistas deberán utilizar las herramientas tecnológicas que proporcione la UNIDAD DE GESTIÓN TECNOLÓGICA para gestionar la información digital.

vii. No está permitido ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a daño parcial o total y por ende, a la pérdida de la integridad de ésta.

viii. No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos autorizados expresamente.

ix. Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar o reparar sus componentes, son las designadas para tal labor por la Unidad de Gestión Tecnológica.

x. La UNIDAD DE GESTIÓN TECNOLÓGICA realizará control y monitoreo sobre los dispositivos de almacenamiento externos como USB, CD-ROM, DVD, Discos Duros externos, entre otros, con el fin de prevenir o detectar fuga de información clasificada y reservada.

xi. La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la Unidad de Gestión Tecnológica, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes de la Entidad.

xii. La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá ser informada de inmediato por el funcionario o contratista a quien se le hubiere asignado; en caso de que el equipo de cómputo sea suministrado por la Alcaldía de Manizales, deberá reportarse siguiendo los procedimientos establecidos para este tipo de siniestros, sin perjuicio de las acciones penales y disciplinarias que requiera adelantar según sea el caso.

xiii. La pérdida de información deberá ser informada con detalle a la UNIDAD DE GESTIÓN TECNOLÓGICA, a través de la Mesa de Ayuda, como incidente de seguridad.

xiv. Todo incidente de seguridad que comprometa la confidencialidad, integridad o disponibilidad de la información física o digital deberá ser reportado a la mayor brevedad, siguiendo el procedimiento establecido.

xv. La UNIDAD DE GESTIÓN TECNOLÓGICA es la única dependencia autorizada para la administración del software del Ministerio de TIC, el cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales.

xvi. Todo acceso a la red de la entidad, mediante elementos o recursos tecnológicos no institucionales, deberá ser informado, autorizado y controlado por la UNIDAD DE GESTIÓN TECNOLÓGICA.

xvii. La conexión a la red wifi institucional para empleados públicos y contratistas deberá ser administrada mediante un SSID (Service Set Identifier) único y con la debida autenticación.

xviii. La conexión a la red institucional para visitantes deberá tener un SSID y contraseñas administradas por la UNIDAD DE GESTIÓN TECNOLÓGICA.

xix. La red wifi para empleados públicos y contratistas estará disponible para sus equipos personales, teniendo en cuenta las capacidades técnicas, contractuales y lineamientos de seguridad establecidos.

xx. Los equipos deben quedar apagados cada vez que el funcionario o contratista no se encuentre en la oficina o durante la noche, esto, con el fin de proteger la seguridad y distribuir bien los recursos de la entidad.

xxi. Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la entidad debe acogerse a las políticas de "Trae tu propio dispositivo", que se establezcan.

xxii. Las herramientas corporativas instaladas en los dispositivos móviles personales serán gestionadas por la Unidad de Gestión Tecnológica con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de la entidad.

d. **Del uso de los sistemas, herramientas de información y Sistemas de almacenamiento institucionales:** Todos los empleados públicos y contratistas son responsables de la protección de la información a la que acceden y procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:

i. Las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los empleados públicos y contratistas no deben revelarlas a terceros, ni utilizar claves ajenas.

ii. Todo funcionario o contratista es responsable del cambio periódico de su clave de acceso a los sistemas de información o recursos informáticos.

iii. Todo funcionario o contratista es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.

iv. En ausencia del funcionario o contratista, el acceso a la estación de trabajo le será bloqueada con una solicitud a la Unidad de Gestión Tecnológica a través de la Mesa de Servicios, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. La Unidad de Gestión Humana debe reportar de inmediato, cualquier tipo de novedad de los empleados públicos, a su vez los supervisores de contrato deben reportar dichas novedades.

v. Cuando un funcionario o contratista cesa sus funciones o culmina la ejecución del contrato, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información que estos ostenten será almacenada en los repositorios de la entidad.

vi. Cuando un funcionario o contratista cesa sus funciones o culmina la ejecución de su contrato, el jefe inmediato o supervisor será el encargado de la custodia de los activos de información. Esto incluye la cesión de derechos de propiedad intelectual

de acuerdo con la normativa vigente. Además, el funcionario no podrá llevarse información institucional, garantizando así la protección y cuidado de la información de la entidad.

vii. Cuando un funcionario o contratista cesa sus funciones o culmina la ejecución del contrato deberá tramitar el paz y salvo, de acuerdo con el procedimiento establecido por la entidad.

viii. Todos los empleados públicos, funcionarios y contratistas de la entidad deben dar estricto cumplimiento a lo estipulado en la Ley 23 de 1982 "Sobre derechos de autor", la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia.

ix. Todos los funcionarios públicos, contratistas, colaboradores y terceros de la entidad deben realizar el uso consciente de los sistemas de almacenamiento dispuestos por la Unidad de Gestión Tecnológica, de esta manera son responsables de la información allí almacenada la cual debe ser estrictamente institucional y relacionada con sus actividades, obligaciones y funciones encomendadas asegurando su clasificación y los niveles de control de acceso requeridos para salvaguardar su integridad, disponibilidad y confidencialidad.

x. Cuando un funcionario o contratista cesa sus funciones o culmina la ejecución de contrato, no podrá llevarse información institucional.

xi. La creación de copias de seguridad de los equipos de cómputo de funcionarios o contratistas solo podrá ser solicitada por el jefe inmediato o supervisor del contrato. Este deberá custodiar la información, garantizando la operabilidad de la entidad. La Unidad de Gestión Tecnológica conservará las copias de seguridad por el tiempo establecido en las políticas de la entidad.

7.6. Responsabilidades de la Operación de la Política

La responsabilidad de la implementación, desarrollo, control y mejora de la Política de Seguridad Digital y su marco de referencia se encuentra a cargo de los siguientes servidores públicos:

Responsable Institucional de la Política de Seguridad Digital: es el representante legal, responsable de coordinar, hacer seguimiento y verificar la implementación de la Política de Seguridad Digital.

Responsable de orientar la implementación de la Política de Seguridad Digital: es el Comité Institucional de Gestión y Desempeño, de que trata el artículo 2.2.22.3.8 del Decreto 1083 de 2015. Esta instancia será la responsable de orientar la implementación de la política de Seguridad Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión.

Responsable de liderar la implementación la Política de Seguridad Digital: La Secretaría de Servicios Administrativos es la encargada de coordinar, orientar y promover la articulación de los actores institucionales para la óptima implementación de las Políticas.

Los líderes de proceso dentro del rol que les corresponde deben liderar, impulsar, apoyar, evaluar y hacer seguimiento al cumplimiento en concordancia con sus competencias y nivel de responsabilidad, así como generar las recomendaciones de mejoramiento pertinentes.

Los servidores públicos que tienen a su cargo cada plan, programa, proyecto o estrategia, son los responsables de realizar el seguimiento y la evaluación de los resultados institucionales, y definir las acciones de corrección o prevención de riesgos.

Los servidores públicos de la entidad que no se encuentren inmersos en los roles anteriores y los terceros vinculados con ella, son responsables de aplicar lo establecido en el Modelo Integrado de Planeación y Gestión y su marco de referencia, en el desarrollo de sus funciones u obligaciones a su cargo.

POLITICA	SECRETARIAS LIDER	LIDER TEMATICO	GESTOR
Seguridad Digital	Servicios Administrativos con el apoyo de TIC y Competitividad, Movilidad, Hacienda, Salud, Planeación y Educación	Líder de Proyecto – Unidad de Gestión Tecnológica	Profesional Especializado Unidad Administrativa de Planeación y Control Para la Movilidad. Profesional Especializado Unidad de Planeación Estratégica. Profesional Especializado de Unidad de Fomento Empresarial. Profesional Universitario Unidad de TIC. Profesional Universitario Estadística – Salud. Profesional Universitario - Líder Cobertura y sistemas de información. Líder de Proyecto – Unidad de Gestión Tecnológica. Profesional Universitario – Unidad de Gestión Tecnológica.

7.7. Seguimiento de la Operación de la Política

Se crea la Mesa Técnica de Transformación Digital para que sea la instancia encargada de la actualización de la política y el desarrollo de las actividades derivadas de la misma.

Secretarías que componen la mesa técnica:

- Secretaría de Servicios Administrativos
- Secretaría de TIC y Competitividad
- Secretaría de Educación
- Secretaría de Salud Pública
- Secretaría de Planeación
- Secretaría de Hacienda
- Secretaría de Movilidad

Dentro del seguimiento a la operación, la identificación de activos tecnológicos es fundamental para que una entidad pueda comprender cuáles son los recursos, datos e información críticos para su operación y, así, protegerlos de manera adecuada.

Una vez que se han identificado estos activos, es necesario evaluar los riesgos que podrían afectarlos. Esto implica analizar las amenazas potenciales, establecer la matriz de riesgos, las acciones de mitigación y el manejo de los mismos, de igual manera cuantificar y determinar el impacto y las vulnerabilidades que podrían ser explotadas.

Una vez que se han identificado los riesgos, es fundamental implementar acciones de mitigación. Estas acciones pueden incluir la aplicación de medidas de seguridad técnicas, como firewalls, sistemas de detección de intrusiones y actualizaciones regulares de software, así como la implementación de políticas y procedimientos para concientizar a los funcionarios y contratistas sobre las mejores prácticas de seguridad.

De igual forma, es importante tener un plan de respuesta a incidentes en su lugar para abordar rápidamente cualquier problema de seguridad que pueda surgir.

7.8 Aprobación Del Documento

Aprobación del documento		
Etapa	**Nombres y apellidos**	**Cargos**
Elaboró	Adriana Marcela Ospina	Técnica Operativa
Revisó	Rafael Antonio Tejada Quintero	Líder de Proyecto Unidad de Gestión Tecnológica
Aprobó	Miembros con voto	Comité de Gestión y Desempeño Institucional

7.9 Control De Cambios

Fecha	Versión	Descripción del cambio
23 noviembre 2023	01	Inicial
16 enero 2025	02	Actualización de controles y políticas