



TRÁNSITO DE
SOLEDAD

GRAN PACTO SOCIAL POR SOLEDAD



Manual de Políticas de Seguridad y Privacidad de la Información IMTTRASOL



ALCALDÍA DE
SOLEDAD
GRAN PACTO SOCIAL POR SOLEDAD

www.transitsoledad.gov.co



**Director Instituto Municipal de Tránsito y Transporte de Soledad
IMTTRASOL**

Abogado JESÚS MONTENEGRO TERNERA

Jefe Oficina de Sistema y Telecomunicaciones

Ingeniero RAMSÉS RAÚL ESCORCIA

Contratistas Oficina de Sistema y Telecomunicaciones

Ingeniero ALEXANDER MENDOZA

Ingeniero OSCAR LOZANO

Manual de Políticas de Seguridad y Privacidad de la Información

Instituto Municipal de Tránsito y Transporte de Soledad

IMTTRASOL

jefesistemas@transitsoledad.gov.co

Versión 1.0

2020-2023



TABLA DE CONTENIDO

Contenido	
INTRODUCCION	05
1 OBJETIVOS.....	06
1.1 Objetivo General.....	06
1.2 Objetivo Específicos.....	07
2 ALCANCE DEL DOCUMENTO.....	07
3. DEFINICIONES.....	07
4. MARCO NORMATIVO.....	11
5. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	08
6. POLITICAS ESPECIFICAS DE MANEJO DE LA INFORMACION.....	15
6.1. Política de Seguridad de los Recursos Humanos.....	15
6.2. Política de Gestión De Activos.....	15
6.3. Política de Control De Acceso.....	17
6.4. Política de Criptografía.....	17
6.5. Política de Privacidad	17
6.6. Política de Seguridad Física y del Entorno	18
6.7. Política de Seguridad de las Operaciones.....	18
6.8. Política de Seguridad de las Comunicaciones.....	19
6.9. Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas.....	20
6.10. Política de Seguridad para Relación con Proveedores.....	21
6.11. Política de Gestión de Incidentes de Seguridad de La Información.....	21
6.12. Política de la Continuidad de la Operación de los Servicios.....	21
6.13. Política de Cumplimiento.....	21
6.14. Política de Seguridad de la Información en la Gestión de Proyectos.....	22
6.15. Política de Seguridad de la Sede Electrónica.....	22



7. RESPONSABILIDADES DE COLABORADORES FRENTE AL USO DE SERVICIOS TECNOLÓGICOS.....	23
7.1. Política de Seguridad Digital.....	23
7.2. Política de Revisión.....	29
BIBLIOGRAFÍA.....	





INTRODUCCION

El Instituto Municipal de Tránsito y Transporte de Soledad, reconoce la importancia de la información que gestiona, debido a que es uno de los activos más significativos para su funcionamiento y que ésta puede ser de naturaleza legal, estratégica, financiera, operativa y en algunos casos corresponder a datos personales de servidores públicos, contratistas y grupos de valor.

De igual manera, es consciente de las amenazas que enfrenta la información y de las consecuencias a las que se expone el Instituto Municipal de Tránsito y Transporte de Soledad cuando no cuente con las medidas de seguridad y protección adecuadas. En ese sentido, IMTRASOL debe tener una visión general de los riesgos de seguridad digital que pueden afectar la seguridad y privacidad de la información, donde se podrán establecer controles y medidas efectivos, viables y transversales con el propósito de realizar el aseguramiento de la disponibilidad, integridad y confidencialidad tanto de la información del negocio como de los datos de los servidores públicos, contratistas y partes interesadas.

Es indispensable que el Instituto Municipal de Tránsito y Transporte de Soledad realice una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riesgos de seguridad digital que puedan afectar la información de la entidad, con el propósito de implementar medidas y controles efectivos que permitan estar preparados ante situaciones en las que se vea comprometida tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

Teniendo en cuenta lo anterior, el presente Manual tiene como finalidad de establecer los principios orientadores en seguridad que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad, continuidad, autenticidad y no repudio de la información del Instituto Municipal de Tránsito y Transporte de Soledad, así como dar lineamientos para la aplicación de mecanismos que eviten la vulneración de la seguridad y privacidad de la información, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información – SGSI.



1. OBJETIVOS

1.1. Objetivo General:

Establecer los lineamientos necesarios a implementar para el cumplimiento de la Política de Seguridad y privacidad de la información en el Instituto Municipal de Tránsito y Transporte de Soledad IMTRASOL, contempladas en el Modelo de Seguridad y Privacidad de la Información y alineadas con la Política de Seguridad Digital.

1.2. Objetivos Específicos:

- Definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del Instituto Municipal de Tránsito y Transporte de Soledad.
- Proteger la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte del Instituto.
- Definir las responsabilidades frente a la seguridad de la información las cuales serán compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos.
- Implementar diferentes controles tanto de acceso a la información, sistemas y recursos de red.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del Instituto Municipal de Tránsito y Transporte de Soledad.



2. ALCANCE DEL DOCUMENTO

Los lineamientos contenidos en el presente manual son aplicables a todos los niveles del Instituto Municipal de Tránsito y Transporte de Soledad, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del IMTRASOL compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación.

De igual manera esta política aplica a toda la información creada, procesada o utilizada por el Instituto Municipal de Tránsito y Transporte de Soledad, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

3. DEFINICIONES

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.

Activo crítico: Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectarán el cumplimiento de los objetivos estratégicos de la entidad.

Administración de Riesgos: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

Análisis de Impacto al Negocio (BIA): Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Características de la Información: las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.



Centro de cableado: El centro de cableado es el lugar donde se ubican los recursos de comunicación de tecnologías de información, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos).

Cifrado: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Control: Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Confiabilidad de la Información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Código malicioso: Es un código informático que crea brechas de seguridad para dañar un sistema informático.

Custodio: Es una parte designada de la entidad, un cargo o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación y borrado.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables. Debe entonces entenderse el “dato personal” como una información relacionada con una persona natural (persona individualmente considerada).

Dato personal público: Toda información personal que es de conocimiento libre y abierto para el público en general.

Dato personal privado: Toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general.



Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general.

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Datacenter: Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Dispositivos móviles: Equipo celular smartphone, equipos portátiles, tablets, o cualquiera cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.

Evento: Es el suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

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.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.



Impacto: Resultado de un incidente de seguridad de la información.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad.

Mesa de Servicios: Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de Servicios que la Oficina de Sistemas y Comunicaciones recolecta las necesidades que tienen dependencias en cuanto a los recursos tecnológicos.

No repudio: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.

Partes interesadas: Persona u organización que puede afectar o ser afectada o percibirse a sí misma como afectada por una decisión o actividad.

Plan de Continuidad de Negocio: Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.

Propietario de la información (titular): Es la unidad organizacional o proceso donde se crean los activos de información.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso.

Terceros: Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad.

VPN: Red virtual privada por sus siglas en inglés Virtual Private Network.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.



4. MARCO NORMATIVO

A continuación, se relaciona la normatividad que soporta el diseño y ejecución del Manual con las Políticas de Seguridad y Privacidad de la Información del Instituto Municipal de Tránsito y Transporte de Soledad, el cual se encuentra fundamentado en el marco legal y las políticas establecidas para el uso de las tecnologías de la información y la seguridad digital en las entidades públicas del Estado.

Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).

Ley 527 de 1999. Por 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, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 594 de 2000. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas.

Ley 962 de 2005. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos Administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones.

Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.



Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

Ley 1978 de 2019. Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones.

Decreto 1747 de 2000. Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con: “Las entidades de certificación, los certificados y las firmas digitales”.

Decreto 19 de 2012. Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.

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 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

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

Decreto 1078 de 2015. Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y las comunicaciones – Título 9 – Capítulo I.

Decreto 415 de 2016. Por el cual se adiciona el Decreto Único Reglamentario del Sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

Decreto 1499 de 2017. Modifica el decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública

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.

Conpes 3854 de 2016. Política Nacional de Seguridad Digital.

Conpes 3920 de 2018. Política Nacional de Explotación de Datos.



5. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección del Instituto Municipal de Tránsito y Transporte de Soledad “IMTTRASOL”, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el Instituto Municipal de Tránsito y Transporte de Soledad, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del Instituto Municipal de Tránsito y Transporte de Soledad.
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del Instituto Municipal de Tránsito y Transporte de Soledad y la ciudadanía en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de Instituto Municipal de Tránsito y Transporte de Soledad:



- El Instituto Municipal de Tránsito y Transporte de Soledad ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- El Instituto Municipal de Tránsito y Transporte de Soledad protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- El Instituto Municipal de Tránsito y Transporte de Soledad protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- El Instituto Municipal de Tránsito y Transporte de Soledad protegerá su información de las amenazas originadas por parte del personal.
- El Instituto Municipal de Tránsito y Transporte de Soledad protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- El Instituto Municipal de Tránsito y Transporte de Soledad controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- El Instituto Municipal de Tránsito y Transporte de Soledad implementará control de acceso a la información, sistemas y recursos de red.
- El Instituto Municipal de Tránsito y Transporte de Soledad garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- El Instituto Municipal de Tránsito y Transporte de Soledad garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- El Instituto Municipal de Tránsito y Transporte de Soledad garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- El Instituto Municipal de Tránsito y Transporte de Soledad garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad de la Información.



6. POLITICAS ESPECIFICAS DE MANEJO DE LA INFORMACION

6.1. POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS.

La Oficina de Talento Humano del Instituto Municipal de Tránsito y Transporte de Soledad debe desplegar esfuerzos para generar conciencia y apropiación en los servidores públicos de la entidad, sobre sus responsabilidades en el marco de la Política de Seguridad y Privacidad de la Información del IMTTRASOL, 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 la Oficina Jurídica incluirá en las minutas de los contratos y convenios, cualquiera que sea su naturaleza o modalidad, cláusulas y obligaciones frente al cumplimiento de la Política de Seguridad y Privacidad de la Información del IMTTRASOL, 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. obligaciones y las del Instituto Municipal de Tránsito y transporte de Soledad, compartan, utilicen, recolecten, procesen, intercambie o consulte su información.

6.2. POLÍTICA DE GESTIÓN DE ACTIVOS.

La Oficina de Sistemas y Comunicaciones del Instituto Municipal de Tránsito y Transporte de Soledad, 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 siguientes literales que serán consolidados y publicados en el proceso de apoyo a la Gestión Documental.

- a. **Inventario de Activos:** Los activos del del Instituto Municipal de Tránsito y Transporte de Soledad deben ser identificados, clasificados valorados y controlados para garantizar su uso, protección y recuperación ante desastres. Por tal motivo, La Oficina de Sistemas y Comunicaciones, diseñará una metodología con los lineamientos necesarios para llevar el inventario de los activos de información, discriminados por procesos y dependencias, 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 Oficina de Sistemas y Comunicaciones.



- c. **Archivos de Gestión:** La Oficina Financiera 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 Instituto Municipal de Tránsito y Transporte de Soledad.
- d. **Clasificación de la Información:** La Oficina Financiera deberá establecer una metodología para la clasificación y rotulado de la información del Instituto Municipal de Tránsito y Transporte de Soledad, en el marco de la Ley 594 de 2000 (Ley General de Archivos), la Ley 1712 de 2014, reglamentada por el Título 1 de la Parte 1 del Libro 2 del Decreto 1081 de 2015 y el Decreto 1080 de 2015 y demás normatividad que reglamente la clasificación de información de las entidades públicas del país. Así mismo la Oficina de Sistemas y Comunicaciones implementará una herramienta informática que permita rotular la información digital y la Oficina Financiera mecanismos para rotular la información física, de acuerdo con la metodología establecida.
- e. **Firma de documentos:** Las firmas de documentos que produzca en el Instituto Municipal de Tránsito y Transporte de Soledad será válida en cualquiera de los siguientes métodos, garantizando la confiabilidad, integridad, autenticidad y disponibilidad de la información de los documentos expedidos por los servidores públicos y contratistas en el marco de sus funciones y competencias:
- I. En físico con firma autógrafa mecánica.
 - II. Con firma digital de persona natural asignadas por la Oficina de Sistemas y comunicaciones según lo dispuesto por la Ley 527 de 1999.
 - III. Con firma electrónica, de acuerdo con lo dispuesto en el Decreto 2364 de 2012 y el Decreto 287 de 2020, para lo cual la Oficina de Sistemas y Comunicaciones deberá adquirir o Implementar un aplicativo integrado con el sistema de gestión documental que contenga como mínimo lo siguiente:
 1. Control seguro de acceso y uso al aplicativo, sincronizado con el directorio activo, garantizando que solo personal vinculado pueda hacer uso del mecanismo de firma electrónica.
 2. Múltiples controles para la autenticación y firma del documento electrónico, garantizando que el firmante es quien dice ser.
 3. 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 servidor o contratista que firma.
 4. Identificador único provisto por el sistema que permita la verificación de la veracidad del documento.



5. Fecha de creación y finalización de la firma provisto por el servidor y sincronizado con la hora legal colombiana de acuerdo con lo establecido en el numeral 4 del artículo 6 del Decreto 4175 de 2011.
6. Estado del trámite de firma.
7. Firma digital de persona jurídica del Instituto Municipal de Tránsito y Transporte de Soledad según sea el caso.
8. En ningún caso se debe utilizar firmas facsímil. salvo en aquellos que se autorice, indicando para que fin y porqué medios podrá ser utilizada.

6.3. POLÍTICA DE CONTROL DE ACCESO.

Los propietarios de los activos de información, teniendo en cuenta el tipo de activo, deberán adoptar las medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías e infraestructura física (instalaciones y oficinas) establecidas, 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 del Instituto Municipal de Tránsito y Transporte de Soledad.

6.4. POLÍTICA DE CRIPTOGRAFÍA.

La Oficina de Sistemas y Comunicaciones dispondrá de herramientas que permitan el cifrado de la Información clasificada y reservada para proteger su confidencialidad, integridad y disponibilidad. El cifrado de la información se realizará por solicitud de los usuarios o de manera general cuando así lo requiera el Instituto Municipal de Tránsito y Transporte de Soledad.

6.5. POLÍTICA DE PRIVACIDAD.

El Instituto Municipal de Tránsito y Transporte de Soledad deberá disponer, a través de la Oficina de Sistemas y Comunicaciones, de los controles necesarios para la protección de la información de los servidores públicos, contratistas y partes interesadas externas en los términos de la Ley 1581 de 2012 y sus decretos reglamentarios, así como la política de tratamiento de datos personales del IMTTRASOL.

La Oficina de Sistemas y Comunicaciones, deberá diseñar un formato de autorización y uso de datos personales, así como su tratamiento, en lo que respecta al uso de datos semiprivados privados y sensibles; dicho formato debe ser claro y detallado en lo referente a la recolección de la información de los servidores públicos y contratistas del IMTTRASOL; así mismo, deberá ser firmado por todos los servidores públicos y contratistas como parte de sus obligaciones.



La Oficina de Sistemas y Comunicaciones, diseñarán y actualizará los formatos de autorización, por parte de los ciudadanos, de la captación y uso de imágenes, videos o cualquier medio audiovisual, de conformidad con lo dispuesto en las normas vigentes sobre protección de datos personales, en especial la Ley 1581 de 2012 y el Decreto 1074 de 2015, así como su autorización libre, expresa e inequívoca al IMTRASOL o a quien este autorice o encargue, para el uso del recurso audiovisual en el marco del cumplimiento de su misión. Los formatos deberán prever la opción en que el ciudadano sea menor de edad y se deberá establecer un procedimiento para el caso en que el ciudadano no autorice dicho tratamiento.

6.6. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO.

El Instituto Municipal de Tránsito y Transporte de Soledad, a través de la Oficina de Sistemas y Comunicaciones, 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 designadas 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.

La Oficina Financiera en coordinación con la Oficina de Sistemas y Comunicaciones, deberá garantizar la protección de los datos, semiprivados, privados y sensible recolectados de los servidores públicos, contratistas y visitantes, en lo que refiere el artículo 10 de la presente resolución y establecer mecanismos alternativos para quienes no autorizan el tratamiento de sus datos.

Todos los servidores públicos contratistas y visitantes que se encuentren en las instalaciones físicas del Instituto Municipal de Tránsito y Transporte de Soledad debe estar debidamente identificados con un carné, documento o distintivo que acredite su tipo de vinculación, dichos elementos deben portarse en un lugar visible.

Los visitantes de las instalaciones del Instituto Municipal de Tránsito y Transporte de Soledad siempre deben permanecer acompañados por un colaborador de la entidad, ambos debidamente identificados.

El personal de empresas o entidades que desempeñe funciones de forma permanente en las instalaciones del Instituto Municipal de Tránsito y Transporte de Soledad, 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.

6.7. POLÍTICA DE SEGURIDAD DE LAS OPERACIONES.

La Oficina de Sistemas y Comunicaciones será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación.



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 un comité de control de cambios, para que los cambios efectuados 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 en el marco de la operación del Instituto Municipal de Tránsito y Transporte de Soledad.

La Oficina de Sistemas y Comunicaciones deberá realizar y mantener copias de seguridad de la información de la entidad en medio digital y velará que ésta sea reportada, con el objetivo de recuperarla en caso de cualquier tipo de falla. La Oficina de Sistemas y efectuará las copias respectivas, de acuerdo con el esquema definido previamente, en un procedimiento que enmarque la gestión de las copias de seguridad de la Información digital, sistemas de Información, bases de datos y demás recursos tecnológicos de la entidad.

Dicho procedimiento se hará bajo la dirección de la Oficina de Sistemas y Comunicaciones, 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.

En el evento que alguna dependencia haga uso de una plataforma tecnológica fuera de las instalaciones físicas y en el marco de las funciones misionales u operacionales del Instituto Municipal de Tránsito y Transporte de Soledad, deberá cumplir con lo establecido en la presente política y los lineamientos dispuestos por la Oficina de Sistemas y Comunicaciones.

6.8. POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES.

La Oficina de Sistemas y Comunicaciones 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 del Instituto Municipal de Tránsito y Transporte de Soledad.

La Oficina Asesora de Planeación establecerá 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 servicio web (web service) o de cualquier otro medio tecnológico, el intercambio deberá realizarse con los controles criptográficos definidos en el artículo 9º de esta Resolución y será coordinado por la Oficina de Sistemas y Comunicaciones con los mecanismos establecidos para tal fin.



Como parte de sus términos y condiciones iniciales de trabajo, funciones u obligaciones todos los servidores públicos o contratistas del Instituto Municipal de Tránsito y Transporte de Soledad, sin importar su nivel jerárquico firmarán un acuerdo o compromiso de confidencialidad y no divulgación, que será elaborado por la Oficina de Talento Humano y la Oficina Jurídica con el apoyo de la Oficina de Sistemas y Comunicaciones, según el tipo de vinculación, en lo que respecta a la información de del Instituto Municipal de Tránsito y Transporte de Soledad.

Dicho documento original será conservado y archivado en forma segura en la historia laboral de los servidores públicos y en la carpeta de los procesos contractuales para el caso de los contratistas.

En el caso de persona jurídica proveedora de servicios para el Instituto Municipal de Tránsito y Transporte de Soledad, en la respectiva carpeta del contrato deberá reposar el acuerdo o compromiso de confidencialidad y no divulgación debidamente suscrita por el representante legal.

6.9. POLÍTICA DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

La Oficina de Sistemas y Comunicaciones garantizará porque el desarrollo interno y externo de los sistemas de información, cumplan con los requerimientos de seguridad adecuados para la protección de la información del Instituto Municipal de Tránsito y Transporte de Soledad, 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 Oficina de Sistemas y Comunicaciones es la única dependencia de la entidad con la capacidad de adquirir, desarrollar e implementa soluciones tecnológicas para el Instituto Municipal de Tránsito y Transporte de Soledad, así como de 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 Instituto.

En consecuencia, cualquier software que opere en el Instituto Municipal de Tránsito y Transporte de Soledad deberá contar con la autorización de la Oficina de Sistemas y Comunicaciones 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 o realice mantenimientos a sistemas de información dentro del desarrollo misional u operacional del Instituto Municipal de Tránsito y Transporte de Soledad, deberá cumplir con lo establecido en la presente política y deberá solicitar acompañamiento de la Oficina de sistemas y Comunicaciones.



6.10. POLÍTICA DE SEGURIDAD PARA RELACIÓN CON PROVEEDORES.

El Instituto Municipal de Tránsito y Transporte de Soledad a través de la Oficina Financiera, 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 del 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 en conjunto con la Oficina Financiera sean los responsables de aplicar las políticas y procedimientos de seguridad de la información durante la ejecución de los contratos, estos lineamientos deberán ser comunicados a los proveedores.

6.11. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

El Instituto Municipal de Tránsito y Transporte de Soledad, a través de la Oficina de Sistemas y Comunicaciones, promoverá entre los servidores públicos y contratistas de la entidad, el reporte y seguimiento de incidentes relacionados con la seguridad 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.

Solo la Dirección del Instituto Municipal de Tránsito y Transporte de Soledad está autorizado para reportar Incidentes de seguridad ante las autoridades de defensa nacional Policía, Fiscalía y de control; así mismo, es el único canal de comunicación autorizados para hacer pronunciamientos oficiales ante en entidades externas, medios de comunicación o la ciudadanía. La delegación de esta potestad se podrá ser formal, por media de acto administrativo.

6.12. POLÍTICA DE LA CONTINUIDAD DE LA OPERACIÓN DE LOS SERVICIOS.

El Instituto Municipal de Tránsito y Transporte de Soledad dispondrá los planes necesarios para la continuidad de la operación de los servicios, los cuales serán operados por los líderes de los procesos. La Oficina de Sistemas y Comunicaciones, la Oficina Asesora de Planeación y la Oficina Financiera liderarán conjuntamente la elaboración del Análisis de Impacto del Negocio y del Plan de Continuidad de la Operación de los Servicios.

6.13. POLÍTICA DE CUMPLIMIENTO.

El Instituto Municipal de Tránsito y Transporte de Soledad, a través de la Oficina de Sistemas y Comunicaciones 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 nacional, para lo cual dispondrá una Matriz de Requisitos Legales para su control y seguimiento.



6.14. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.

La Oficina 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.

6.15. POLÍTICA DE SEGURIDAD DE LA SEDE ELECTRÓNICA.

La Oficina de Sistemas y Comunicaciones será la encargada de la administración y gestión de la sede electrónica del Instituto Municipal de Tránsito y Transporte de Soledad, 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 de IMTRASOL, se deberán identificar fácilmente y de manera clara, los canales digitales oficiales de recepción de solicitudes, peticiones y de información, estos canales deben contar con los mecanismos de cifrado de información.

El Instituto Municipal de Tránsito y Transporte de Soledad a través del proceso de Gestión Documental, 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 de seguridad, privacidad de la información, seguridad digital, continuidad de la operación de los servicios y demás lineamientos de los que trata esta resolución.

La Oficina Financiera, junto con la Oficina de Sistemas y Comunicaciones, deberán 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.



7. RESPONSABILIDADES DE LOS COLABORADORES FRENTE AL USO DE LOS SERVICIOS TECNOLÓGICOS

7.1. POLÍTICA DE SEGURIDAD DIGITAL.

Todos los colaboradores que hagan uso de los recursos tecnológicos del Instituto Municipal de Tránsito y Transporte de Soledad tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable; entendiéndose que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación de los servicios y por ende, el cumplimiento 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 servidores públicos y contratistas del Instituto Municipal de Tránsito y Transporte de Soledad, 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 Oficina de Sistemas y Comunicaciones, que cuenta con el dominio @transitsoledad.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 Oficina de Sistemas y Comunicaciones 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. Se prohíbe el envío de correos masivos internos o externos, con excepción de los enviados por los despachos de las Oficinas del Instituto Municipal de Tránsito y Transporte de Soledad, Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.



VII. Todo mensaje de correo electrónico enviado por el Instituto Municipal de Tránsito y Transporte de Soledad median e plataformas externas deberá hacerse con la cuenta de la entidad y utilizando el dominio @transitsoledad.gov.co, con el fin de que no sea 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 servicios 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 inmediatamente reportado a la Oficina de Sistemas y Comunicaciones a través de la mesa de servicios 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, .pi, 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 del Instituto Municipal de Tránsito y Transporte de Soledad a otras entidades o ciudadanos sin la debida autorización del despacho del IMTRASOL.

XIII. El cifrado de los mensajes de correo electrónico institucional será necesario siempre que la información transmitida sea catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la ley.

XIV. El correo electrónico institucional en sus mensajes debe contener una sentencia de confidencialidad, que será diseñada por la Oficina de Sistemas y Comunicaciones, dicha sentencia debe reflejarse en todos los buzones con dominio @transitsoledad.gov.co.

XV. Está expresamente prohibido distribuir copiar o reenviar información del Instituto Municipal de Tránsito y Transporte de Soledad y las Comunicaciones a través de correos personales o sitios web diferentes a los autorizados en el marco de las funciones obligaciones contractuales.

XVI. Cuando un servidor público o contratista cesa en sus funciones o Culmina la ejecución de contrato con el Instituto Municipal de Tránsito y Transporte de Soledad, no se le entregará copia de los buzones de correo institucionales a su cargo, salvo autorización expresa del director, por



orden judicial, por solicitud de la Oficina de Control Interno Disciplinario como parte de un proceso de investigación.

El Instituto Municipal de Tránsito y Transporte de Soledad a través de la Oficina de Sistemas y Comunicaciones se reserva el derecho de monitorear los accesos y el uso de los buzones de los correos institucionales de todos sus servidores 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 servidores y accesos a sistemas de información de la entidad o de terceros operados en la misma, previa solicitud expresa del supervisor del contrato, jefe Inmediato, jefe oficina control interno disciplinarlo, Oficina de Talento Humano a la Oficina de Sistemas y Comunicaciones. Para ello, al inicio de la relación laboral o contractual se deberá comunicar a los funcionarios y contratistas que el Instituto Municipal de Tránsito y Transporte de Soledad realiza el referido monitoreo.

- b. **Del uso de Internet:** La Oficina de Sistemas y Comunicaciones establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía, funciones u obligaciones. Será responsabilidad de los funcionarios y contratistas las siguientes, entre otras:
- I. Los servicios a los que un determinado usuario pueda acceder en internet dependerán del rol o funciones que desempeña en el Instituto Municipal de Tránsito y Transporte de Soledad 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 con a 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 del Instituto Municipal de Tránsito y Transporte de Soledad.
 - IV. Abstenerse de enviar y descarga 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 Instituto Municipal de Tránsito y Transporte de Soledad a través de la Oficina de Sistemas y Comunicaciones 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 de cualquier otro uso ajeno a los fines de la Entidad.



- c. **Del uso de los recursos tecnológicos:** Los recursos tecnológicos del Instituto Municipal de Tránsito y Transporte de Soledad son herramientas de apoyo a las labores y responsabilidades de los servidores 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 servidor público 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 por la Oficina de Sistemas y Comunicaciones, salvo que medie solicitud formal de los Directivos, jefes de Oficina a través de la Mesa de Servicios.
 - II. Sólo está permitido el uso de software licenciado por la entidad y aquel que, sin requerir licencia sea expresamente autorizado por la Oficina de Sistemas y Comunicaciones.
 - III. En caso de que el servidor público o contratista deba hacer uso de equipos ajenos al Instituto Municipal de Tránsito y Transporte de Soledad, éstos deberán cumplir con la legalidad del Software instalado, sistema operativo y antivirus licenciado, actualizado y solo podrá conectarse a la red del IMTRASOL una vez esté avalado por la Oficina de Sistemas y Comunicaciones.
 - IV. Los servidores públicos y contratistas deberán realizar y mantener las copias de seguridad de su información y entregarla a la entidad 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 servidores públicos y contratistas deberán utilizar las herramientas tecnológicas que proporcione la Oficina de Sistemas y Comunicaciones para gestionar la información digital del Instituto Municipal de Tránsito y Transporte de Soledad.
 - 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 por la Oficina de Sistemas.
 - 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 Oficina de Sistemas y Comunicaciones.



X. La Oficina de Sistemas y Comunicaciones 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 Oficina de Sistemas y Comunicaciones, 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 a la Oficina de Sistemas y Comunicaciones por el servidor público o contratista a quien se le hubiere asignado; en caso de que el equipo de cómputo sea propiedad del Instituto Municipal de Tránsito y Transporte de Soledad, deberá reportarse a la Oficina Financiera 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 Oficina de Sistemas y Comunicaciones a través de la Mesa de Servicios, 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 a la Oficina de Sistemas y Comunicaciones, a través de la Mesa de Servicios, siguiendo el procedimiento establecido.

XV. La Oficina de Sistemas y Comunicaciones es la única dependencia autorizada para la administración del software del Instituto, 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 Oficina de Sistemas y Comunicaciones.

XVII. La conexión a la red wifi institucional para servidores públicos y contratistas deberá ser administrada desde la Oficina de Sistemas y Comunicaciones mediante un SSID (Service Set Identifier) único; la autenticación deberá ser con usuario y contraseña de directorio activo.

XVIII. La conexión a la red institucional para visitantes deberá tener un SSID y contraseñas administradas por la Oficina de Sistemas y Comunicaciones las contraseñas deberán cambiarse periódicamente.

XIX. La red Wifi para servidores públicos y contratistas estará disponible para sus equipos personales, teniendo en cuenta las capacidades técnicas, contractuales y lineamientos de seguridad establecidos por la Oficina de Sistemas y Comunicaciones.



XX. Los equipos deben quedar apagados cada vez que el servidor público 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, siempre y cuando no vaya a realizar actividades vía remota.

XXI. Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la entidad debe acogerse a las políticas de seguridad.

XXII. Las herramientas corporativas instaladas en los dispositivos móviles personales serán gestionadas por la Oficina de Sistemas y Comunicaciones con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de la entidad, garantizando el cumplimiento del artículo 10 de la presente resolución.

d. **Del uso de los sistemas o herramientas de Información:** Todos los servidores públicos y contratistas del Instituto Municipal de Tránsito y Transporte de Soledad 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 servido es públicos y contratistas no debe revelarlas a terceros, ni utilizar claves ajenas.

II. Todo servidor público y contratista es responsable del cambio periódico de su clave de acceso a los sistemas de información o recursos informáticos.

III. Todo servidor público y contratista es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.

IV. En ausencia del servidor público o contratista, el acceso a la estación de trabajo le será bloqueada con una solicitud a la Oficina de Sistemas y Comunicaciones 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 Oficina de Talento Humano debe reportar de inmediato, cualquier tipo de novedad de servidores públicos, a su vez los supervisores de contrato deben reportar oportunamente todas las novedades del contratista.

V. Cuando un servidor público o contratista cesa sus funciones o culmina la ejecución del contrato con el Instituto Municipal de Tránsito y Transporte de Soledad 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 servidor público o contratista cesa sus funciones o culmina la ejecución de contrato con el Instituto Municipal de Tránsito y Transporte de Soledad el jefe inmediato o supervisor es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual, de acuerdo con la normativa vigente.



VII. Cuando un servidor público o contratista cesa sus funciones o culmina la ejecución del contrato con el Instituto Municipal de Tránsito y Transporte de Soledad deberá tramitar el paz y salvo, de acuerdo con el procedimiento establecido por la entidad.

VIII. Todos los servidores públicos 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.

7.2. POLITICA DE REVISION

La Política de Seguridad y Privacidad de la Información del Instituto Municipal de Tránsito y Transporte de Soledad, será revisada anualmente o antes, si existiesen modificaciones que así lo requieran, para que sea siempre oportuna, suficiente y eficaz. Este proceso será liderado por la Oficina de Sistemas y Comunicaciones.

La Oficina de Control Interno, debe realizar de manera periódica auditorías internas para comprobar el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información en cuanto a los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información.

Los líderes de los procesos deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas

Es un deber de los servidores públicos contratistas y terceros del Instituto Municipal de Tránsito y Transporte de Soledad, conocer esta Política y realizar todos los actos conducentes para su cumplimiento, implementación y mantenimiento.



BIBLIOGRAFÍA

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Manual Operativo del Modelo Integrado de Planeación y Gestión. 2019.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Manual De Gobierno Digital. 2018.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. G.ES.05 Diseño e implementación de una estrategia de seguridad de la información. 2019.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI. 2019.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad de la información. 2016.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía Metodológica de Pruebas de Efectividad. 2016.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía Elaboración de la política general de seguridad y privacidad de la información. 2016.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía Procedimientos De Seguridad De La Información. 2016.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía Roles y Responsabilidades. 2016.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía para la Gestión y Clasificación de Activos de Información. 2016.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía de Referencia sobre Gestión Documental. 2016.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Manual de Políticas de Seguridad y Privacidad de la información. 2021.

ALCALDIA MUNICIPAL DE SOLEDAD. Plan de Desarrollo Municipal “El Gran Pacto Social por Soledad”. 2020.

INSTITUTO MUNICIPAL DE TRANSITO Y TRANSPORTE DE SOLEDAD. Resolución No. 003 D.T. enero 04 de 2021 Adopción del plan anual de adquisición de bienes y servicios para la vigencia fiscal 2021.



CONTROL DE VERSIONES

TITULO	MANUAL DE POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMTRASOL
PROCESOS	Gestión Tecnologías de la Información

VERSIÓN	FECHA DE APROBACIÓN	REFERENCIA DE CAMBIO
V 1.0	18-11-2021	Versión Inicial

ENCARGADOS DE LA REVISIÓN DEL DOCUMENTO

NOMBRE	ORGANIZACIÓN	CARGO	FECHA
Ingeniero RAMSÉS ESCORCIA MAYA	Instituto Municipal de Tránsito y Transporte de Soledad	Jefe Oficina de Sistemas y Telecomunicaciones	18-11-2021

ENCARGADO DE ELABORACIÓN

NOMBRE	ORGANIZACIÓN	CARGO	FECHA
Ingeniero ALEXANDER MENDOZA	Instituto Municipal de Tránsito y Transporte de Soledad	Contratista Oficina de Sistemas y Telecomunicaciones	18-11-2021
Ingeniero OSCAR LOZANO	Instituto Municipal de Tránsito y Transporte de Soledad	Contratista Oficina de Sistemas y Telecomunicaciones	18-11-2021