PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INSTITUTO DE TRÁNSITO DE BOYACÁ

Oficina de Planeación y Sistemas

VIGENCIA 2025 – V8
15/01/2025

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA APROBACIÓN
1	Procedimiento emitido en Versión 1 para prueba.	30-07-2018
2	Actualización	28-01-2019
3	Actualización	15-01-2020
4	Actualización	28-01-2021
5	Actualización	14-01-2022
6	Actualización	27-01-2023
7	Actualización	25-01-2024
8	Actualización	15-01-2025

CONTENIDO

1. INTRODUCCIÓN 3
2. ALCANCE 3
3. OBJETIVO 3
3.1. Objetivo General: 3
3.2. Objetivos Específicos: 3
4. DEFINICIONES 3
5. JUSTIFICACION 4
6.1. Políticas de seguridad de información 6
6.2. Levantamiento de inventarios de activos de información 6
6.3. Elaboración de matriz de riesgos 6
6.4. Plan de tratamiento de riesgos 7
6.5. Plan de socialización 7
6.6. Modelo de Seguridad y privacidad de la información 7
7. PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 7
8. ACTIVIDADES VIGENCIA 2025: 8
8.1. Socializar boletines informativos o recomendaciones de seguridad 10
8.2. Proveedores Críticos 10
8.3. Riesgos de activos críticos 10
8.4. Respaldo de información 10
8.5. Control de direcciones IP 10
8.6. Control de Navegación y administración de la red 10
9. ROLES Y RESPONSABILIDADES 11
9.1. Gerente 11
9.2. Nivel directivo – Subgerentes, asesores, directores y jefe de oficinas 11
9.3. Líder de seguridad y privacidad de la información – Jefe de oficina asesora de Planeación y Sistemas 11
9.4. Oficial de tecnología – Profesional Especializado 11
9.5. Funcionarios y contratistas 12

1. INTRODUCCIÓN

Reconociendo la importancia de la información y apoyados en su significado, como el conjunto organizado de datos generados, obtenidos, transformados o controlados que constituyen un mensaje sin importar el medio en que se contenga (digital y no digital); nace la necesidad de definir normativas y buenas prácticas para su tratamiento general dentro de la entidad.

Mediante este plan se indicarán las medidas que implementará el Instituto de Transito de Boyacá - ITBOY, para garantizar la seguridad y privacidad de la información que se maneja, según lo establecido en el decreto 1008 del 14 de junio 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.

2. ALCANCE

El Plan de Seguridad y Privacidad de la Información que se generará mediante este plan se aplicará para todo activo de información integrado en los procesos de la entidad, los cuales incluyen: funcionarios, contratistas, sistemas de información, equipo de cómputo, servidores y todo lo que se incluya en el inventario de activos de información del modelo en la entidad.

3. OBJETIVO

3.1. Objetivo General:

Identificar y ejecutar actividades orientadas a fortalecer el aseguramiento de los servicios de TI y la información que se procesa, genera y custodia, y para preservar la confidencialidad, integridad y disponibilidad de la información del Instituto de Tránsito de Boyacá - ITBOY.

3.2. Objetivos Específicos:

- Fortalecer el aseguramiento de los servicios de TI y la información suministrada o relacionada con los usuarios de Instituto de Tránsito de Boyacá, mediante la medición de la Implementación del Modelo de Seguridad y Privacidad de la Información.
- Fomentar en los procesos de la Entidad, la gestión de riesgos de seguridad de la información, con base en los activos previamente identificados y las acciones para mitigar el riesgo.
- Ejecutar actividades en el marco de una metodología de gestión de la seguridad, para establecer un modelo de madurez aplicable y repetible.
- Definir y socializar políticas, lineamientos, buenas prácticas y recomendaciones para establecer cultura en Seguridad de la Información en la Entidad.
- Crear las políticas y procedimientos en materia de seguridad y privacidad de la información.
- Mejorar los tiempos y la calidad de respuesta en los procesos de la entidad.
- Generar una cultura de seguridad y privacidad de la información en los funcionarios, contratistas y ciudadanos.
- Minimizar los riesgos asociados con los activos de información.

4. DEFINICIONES

Confidencialidad: Propiedad que impide la divulgación de información a personas o sistemas no autorizados.

Disponibilidad: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Integridad: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.

Seguridad: Protección de los activos de información, contra amenazas que garanticen la continuidad del negocio, minimizando el riesgo y maximizando las oportunidades de la unidad

No repudio: capacidad de demostrar o probar la participación de las partes (origen y destino, emisor y receptor, remitente y destinatario), mediante su identificación, en una comunicación o en la realización de una determinada acción.

5. JUSTIFICACION

El Instituto de Transito de Boyacá requiere la implementación del Plan de Seguridad y privacidad de la Información a fin de dar cumplimiento a la normatividad vigente que obliga el adecuado tratamiento de la información manejada por la Entidad en términos de confidencialidad, integridad y disponibilidad. Entre otras se citan:

- **Ley 1437 de 2011, Capítulo IV**, "*utilización de medios electrónicos en el procedimiento administrativo*". *"Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos.*"

- **Ley 1581 de 2012**) Principio de seguridad: *"La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*"

- **Ley 1581 de 2012, Artículo 17, ítem d**: "*Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*"

- **Ley 1712 de 2014**, "*principio de transparencia*": "*Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley.*"

- **Ley 1712 de 2014, artículo 7**: "*Disponibilidad de la información "En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a*

disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."

- **Ley 1712 de 2014** -Título III "*Excepciones acceso a la información*" "*Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito.*"

- **Decreto 2573 de 2014**: "*Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea…*" donde se encuentra como componente el modelo de Seguridad y Privacidad de la Información.

- **Decreto 1413 de 2017**, artículo 2.2.17.6.6, "*Seguridad de la información.*" "*Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.*"

- **Decreto 1413 de 2007**, artículo 2.2.17.6.1, "*responsable y encargado del Tratamiento*: "Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen."

- **Artículo 2.2.17.6.3**, "*Responsabilidad demostrada*"."*Los operadores de servicios ciudadanos digitales deberán adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deben crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales.*"

- **Decreto 1413 de 2007**, artículo 2.2.17.6.5, "*Privacidad por diseño y por defecto*":*"Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales que son adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy Impact Assessment (PIA), cuyo objetivo se dirige a que la protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador"*

- **Decreto 1413 de 2017**, artículo 2.2.17.5.10, "*Derechos de los usuarios de los servicios ciudadanos digitales*":

  a) *Registrarse de manera gratuita eligiendo al operador de servicios ciudadanos digitales de su preferencia entre aquellos que estén vinculados por el articulador.*
  b) *Aceptar, actualizar y revocarlas autorizaciones para recibir información, comunicaciones y notificaciones electrónicas desde las entidades públicas a su elección a través de los servicios ciudadanos digitales.*
  c) *Hacer uso responsable de los servicios ciudadanos digitales a los cuáles se registre.*
  d) *Interponer peticiones, quejas, reclamos y solicitudes de información en relación con la prestación*

a los servicios ciudadanos digitales.

e) *Elegir y cambiar libremente el operador de servicios ciudadanos digitales.*
f) *Solicitar en cualquier momento, y a través de cualquiera de los medios de atención al usuario, su retiro de la plataforma de servicios en· cuyo caso podrá descargar su información a un medio de almacenamiento propio.*

- **Decreto 1413 de 2017**, artículo 2.2.17.2.1.1 "*Descripción de los servicios ciudadanos digitales, 1.5 servicio de interoperabilidad: Cualquier desarrollo en el marco de los servicios ciudadanos digitales especiales deberá hacer uso de o estar soportado en los servicios ciudadanos digitales básicas cuando lo requieran."*

- **Decreto 612 de 2018, artículo** 1. *"Integración de planes institucionales y estratégico. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web."*

- **Conpes 3854 de 2016, objetivo** general "*Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país*".

Por lo anterior, el Instituto de Transito de Boyacá debe emprender acciones orientadas a la protección de la información que gestiona, realizando la identificación y tratamiento de riesgos de la información de los activos críticos que la soportan, de manera que se establecen y realiza el seguimiento a dichas acciones en el marco del plan de acción y del Sistema Integrado de Gestión.

6. ANTECEDENTES

6.1. Políticas de seguridad de información

Por medio del Manual "Políticas de Seguridad Informática" MN-GET-01, en su versión 4 de fecha 28 de mayo 2019 firmada y aprobado, se adoptan las políticas de Seguridad de la Información aplicables a funcionarios, usuarios y terceros que accedan a la información del Instituto, se pretende proteger la información de amenazas, garantizando la continuidad, así como minimizar los posibles daños y maximizar el rendimiento de las inversiones y las oportunidades de negocio. Es importante subrayar que la seguridad de la información no es sinónimo de seguridad informática. La seguridad de la información efectivamente incluye aspectos técnicos, pero se extiende también al ámbito de la organización y contempla aspectos que son estrictamente jurídicos.

6.2. Levantamiento de inventarios de activos de información

En el año 2018, en el marco del Sistema Integrado de Gestión y el Subsistema de Gestión de Seguridad de la Información, los 12 procesos de la Entidad realizaron el levantamiento de los activos de información con base en el procedimiento de "Análisis de activos de información". Este insumo permitió, dar cumplimiento a lo establecido en la Ley 1712 de 2014.

6.3. Elaboración de matriz de riesgos

Teniendo en cuenta las actividades ejecutadas en periodos anteriores, el proceso de Gestión Tecnológica generó la matriz de riesgos de seguridad de la información, con un total de 20 riesgos Identificados, conforme a la Metodología de Administración Gestión de Riesgos de la Entidad, lo que permitirá durante la vigencia 2024 gestionar los riesgos identificados por proceso.

6.4. Plan de tratamiento de riesgos

Considerando la definición de riesgo como la amenaza latente de que ocurra un evento, que afecte de manera significativa a la organización, las consecuencias que atentan contra el buen nombre y la operatividad de la misma, se debe entonces tomar acciones que reduzcan la posibilidad de ocurrencia.

Para la vigencia 2024 el ITBOY implementará los controles requeridos para el tratamiento de los riesgos identificados en busca de cumplir con los estándares establecidos en la norma ISO/IEC 27002:2005, como guía de buenas prácticas, lo cual permitirá mitigar los riesgos, amenazas y vulnerabilidades del proceso de Gestión Tecnológica existentes en el ITBOY.

6.5. Plan de socialización

El proceso de Gestión Tecnológica realizara durante la vigencia 2024 un plan de sensibilización, mediante el cual se generaron boletines informativos enviados masivamente y de forma articulada con el proceso de Comunicaciones.

6.6. Modelo de Seguridad y privacidad de la información

El proceso de Gestión Tecnológica durante el segundo semestre de la vigencia 2024 realizará mediciones de la evaluación de la implementación del Modelo de Seguridad y Privacidad de la Información de acuerdo a la metodología establecida por el MinTIC – MSPI.

7. PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Proteger la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.
- Proteger 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.
- Proteger su información de las amenazas originadas por parte del personal.
- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementará control de acceso a la información, sistemas y recursos de red.
- Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- Garantizar 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.
- Garantizar la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
- Definir, implementar, operar y mejorar de forma continua un modelo de seguridad y privacidad de la información, soportado en lineamientos claros alineados a las necesidades de las partes interesadas, y a los requerimientos regulatorios que le aplican a su naturaleza.

8. ACTIVIDADES VIGENCIA 2025:

A continuación, se describen las actividades que se ejecutarán junto con los respectivos entregables, en aras de cumplir con los objetivos propuestos:

FASE	ACTIVIDAD	ENTREGABLE/RESULTADO
FASE DE DIAGNÓSTICO	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad.	Documento del diagnóstico.
	Identificar el nivel de madurez de seguridad y privacidad de la información en la entidad	
	Identificar vulnerabilidades que sirvan como insumo para la fase de planificación.	
FASE DE PLANIFICACIÓN	Identificar el alcance y objetivos de seguridad y privacidad de la información	Documento con la política de seguridad de la información.
	Política de seguridad y privacidad de la información	
	Roles y responsabilidades de seguridad y privacidad de la información.	
	Políticas de seguridad y privacidad de la información	Manual con las políticas y procedimientos de seguridad y privacidad de la información.
	Procedimientos de seguridad de la información	
	Inventario de activos de información	Documento con la metodología para identificación, clasificación y valoración de activos de información
		Matriz con la identificación, valoración y clasificación de activos de información

	Identificación, valoración y tratamiento de riesgo	Documento con el plan de tratamiento de riesgos
		Documento con la declaración de aplicabilidad
		Matriz de riesgos
	Plan de comunicaciones	Documento con el plan de comunicación, sensibilización y capacitación para la entidad
FASE DE IMPLEMENTACIÓN	Planificación y control operacional	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección
	Implementación del plan de tratamiento de riesgos	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso
	Indicadores de gestión	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información
FASE DE EVALUACIÓN DE DESEMPEÑO	Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección
	Plan de ejecución de auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección
FASE DE MEJORA CONTINUA	Plan de mejora continua	Documento con el plan de mejoramiento
		Documento con el plan de comunicación de resultados

El proceso de Gestión Tecnológica proyecta las actividades en el marco del Plan de Acción – Modelo Integrado de planeación y Gestión, teniendo en cuenta los procedimientos documentados e implementados en el Instituto de Transito de Boyacá:

PD-GET-01 ADMINISTRACION DE SERVICIOS ANTIVIRUS
PD-GET-02 ADMINISTRACION RECURSOS ALMACENAMIENTO
PD-GET-03 ADMINISTRACION USUARIOS Y RED
PD-GET-04 COPIAS DE SEGURIDAD
PD-GET-05 MANTENIMIENTO PREVENTIVO Y CORRECTIVO
PD-GET-06 ADMINISTRACION DEL CANAL DE COMUNICACIONES INTERNET
PD-GET-07 ADMINISTRACION DE CLAVES DE ACCESO

PD-GET-08 MODIFICACION DE REGISTRO A TRAVES DE ACCESOS REMOTOS
PD-GET-09 PRUEBAS ADECUACIONES A LOS SISTEMAS DE INFORMACION
PD-GET-10 ADMINISTRACION DE LA PAGINA WEB INSTITUCIONAL

A continuación, se relacionan las actividades a realizar de forma articulada con el plan de acción Institucional.

8.1. Socializar boletines informativos o recomendaciones de seguridad

Para que la información sobre Seguridad de la Información llegue a todos los procesos de la Entidad, se hace necesario contar con la ayuda del demás proceso del SIG, los cuales deben replicar los tips, noticias, boletines y buenas prácticas de seguridad de la información.

8.2. Proveedores Críticos

El objetivo de la actividad de identificación de proveedores críticos es tener el inventario de los terceros que proporcionan o soportan servicios necesarios para la operación del Instituto de Transito de Boyacá, para la identificación del inventario se requiere que todos los procesos se involucren en esta actividad.

8.3. Riesgos de activos críticos

Los riesgos de seguridad de información son asociados a los activos críticos de información definidos y categorizados por cada proceso de la Entidad, con base en la metodología de generación de inventario de activos de información establecido en el marco del Sistema Integrado de Gestión, conforme a la Metodología de Administración Gestión de Riesgos del Instituto de Transito de Boyacá.

8.4. Respaldo de información

Para proteger la información almacenada en los equipos de cómputo, los usuarios deberán realizar el respaldo de la información, en los servicios dispuestos por el proceso de Gestión Tecnológica, adicional a esto deben resguardarse los documentos que hacen parte de registro automotor y proceso tanto contravencional como coactivo en servidores dispuestos como repositorio en la nube y en físico en el cuarto donde se encuentra la granja de servidores

8.5. Control de direcciones IP

Todo equipo de Cómputo que se conecte a la red del Instituto de tránsito de Boyacá, debe incluirse dentro del rango de direcciones de IP fijas establecidas por la oficina de sistemas quién controlará y habilitara el direccionamiento requerido de acuerdo a las normas establecidas por la Organización de Internacional de telecomunicaciones, según las cuales se ajustan al principio de direccionamiento Privado Clase C para IPV4.

8.6. Control de Navegación y administración de la red

Todos los equipos que hacen parte de la plataforma tecnológica del Instituto deben ser incluidos en el

servidor de Dominio, este recurso, permite el monitoreo, control de navegación, control de máquinas, control de entorno, entre otras, las políticas de seguridad del sistema son tomadas por los nuevos equipos generando uniformidad en los lineamentos, y control total de los equipos desde el área de sistemas.

9. ROLES Y RESPONSABILIDADES

Los funcionarios y contratistas del Instituto de Transito de Boyacá que deberán asumir siguientes roles y responsabilidades, donde se garantice la implementación, revisión y mejora continua del Modelo de Seguridad y Privacidad de la Información al interior de la Entidad.

9.1. Gerente

- Aprobar y verificar del cumplimiento de las políticas y procedimientos de seguridad y privacidad de la información.
- Hacer que los miembros del comité directivo sean conscientes de la criticidad de los activos de información para el desarrollo de los procesos de la Entidad.
- Divulgar las responsabilidades de seguridad y privacidad de la información de la entidad con base en los lineamientos del MSPI

9.2. Nivel directivo – Subgerentes, asesores, directores y jefe de oficinas

- Liderar y apoyar de mejora continua para la aplicación del MSPI al interior de la dependencia a cargo.
- Alineación de los objetivos de la dependencia para que su cumplimiento este apoyado por el MSPI.
- Asignar y verificar el cumplimiento de las funciones y responsabilidades de seguridad y privacidad de la información para los roles definidos en la dependencia a cargo.
- Proveer los recursos necesarios para la implementación del MSPI al interior de la dependencia a cargo.
- Apoyar la capacitación y entrenamiento requerido para que los funcionarios y contratistas de la dependencia a cargo que cumplan con el MSPI.
- Aplicar el proceso disciplinario ante los incidentes de seguridad y privacidad de la información originada por un funcionario o contratista de la dependencia a cargo.

9.3. Líder de seguridad y privacidad de la información – Jefe de oficina asesora de Planeación y Sistemas

- Liderar y apoyar la mejora continua para la aplicación del MSPI al interior del Instituto.
- Asignar dentro de su equipo de trabajo quien servirá como oficial de seguridad y privacidad de la información.
- Apoyar las actividades relacionadas con el MSPI.

9.4. Oficial de tecnología – Profesional Especializado

- Apoyar en definir y actualizar el inventario de los activos de información.
- Realizar análisis de riesgos de seguridad y privacidad de la información con base en lo establecido en el MSPI.
- Apoyar en definir del plan de tratamiento de los riesgos de seguridad y privacidad de la información.
- Velar por la ejecución del plan de tratamiento de los riesgos de seguridad y privacidad de la información.
- Definir, actualizar y difundir las políticas, procedimientos y formatos del MSPI.
- Definir y generar las métricas de seguridad y privacidad de la información establecida en el MSPI.
- Propender una cultura de seguridad y privacidad de la información al interior de la entidad.

9.5. Funcionarios y contratistas

Todos los funcionarios y contratistas vinculados a la Alcaldía tendrán la responsabilidad de velar por la confidencialidad, integridad, disponibilidad y privacidad de la información que maneje, así mismo debe reportar los incidentes de seguridad, eventos sospechosos o un mal uso de los recursos que identifique.

El incumplimiento a la política general 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 y privacidad de la información se refiere.

En Tunja a los quince (15) días del mes de enero de 2025.

NIDIA CAROLINA PUENTES AGUILAR
Gerente Instituto de Transito de Boyacá

Elaborado por:
Richard Hernan Ayala Joya
Profesional Especializado
INSTITUTO DE TRANSITO DE BOYACA
2025

Revisado por:
William Rene Higuera Morales
Jefe Oficina Asesora Planeación y Sistemas
INSTITUTO DE TRANSITO DE BOYACA
2025