REPUBLICA DE COLOMBIA
DEPARTAMENTO DE LA GUAJIRA
MUNICIPIO DE ALBANIA
INSTITUTO DE TRANSITO Y TRANSPORTE
NIT: 900.221.828 – 4

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE INFORMACION DEL INSTITUTO MUNICIPAL DE TRANSITO Y TRANSPORTE DEL MUNICIPIO DE ALBANIA– LA GUAJIRA

HASSLER DANIEL QUINTANA DIAZ
Director

Enero de 2025

1. INTRODUCCION

El Instituto Municipal de Tránsito y Transporte del Municipio de Albania – INSTRANS – reconoce que la información es uno de sus activos más importantes para el cumplimiento de su misión institucional. La seguridad y privacidad de los datos que gestiona la entidad son fundamentales para garantizar la confianza de los ciudadanos, la continuidad del servicio y el cumplimiento de las obligaciones legales.

Con base en lo anterior, y en cumplimiento del **Decreto 1078 de 2015** y los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC –, la entidad adopta el presente **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información**, como parte integral de su Modelo de Seguridad y Privacidad de la Información (MSPI).

Este plan busca identificar, valorar, mitigar y monitorear los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional, a través de medidas de control adecuadas, responsables definidos, cronogramas de ejecución y un esquema de seguimiento.

La implementación de este plan hace parte de la estrategia institucional de mejora continua, de conformidad con las mejores prácticas internacionales (como la norma ISO/IEC 27001:2013 e ISO 31000:2018) y con el enfoque preventivo del ciclo PHVA (Planear – Hacer – Verificar – Actuar).

Este documento se constituye en una guía técnica y operativa para proteger los activos de información del INSTRANS, alineado con su estructura organizacional, recursos disponibles y compromiso institucional con la seguridad digital y la protección de datos personales.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer las acciones necesarias para identificar, analizar, evaluar, tratar y controlar los riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información en el Instituto Municipal de Tránsito y Transporte de Albania – INSTRANS –, en el marco de su Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).

2.2 OBJETIVOS ESPECIFICOS

- Identificar los activos de información críticos de la entidad y sus vulnerabilidades.
- Evaluar los riesgos asociados al tratamiento de la información institucional y personal.
- Determinar los controles técnicos, administrativos y físicos necesarios para mitigar los riesgos identificados.
- Asignar responsables institucionales para la implementación y seguimiento de las medidas de tratamiento.
- Establecer cronogramas y recursos necesarios para la ejecución del plan.
- Cumplir con los lineamientos del Ministerio TIC y la normativa vigente en materia de seguridad y protección de datos.
- Fomentar una cultura organizacional orientada a la gestión del riesgo digital y al uso responsable de la información.

3. MARCO NORMATIVO

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto Municipal de Tránsito y Transporte de Albania – INSTRANS –, se fundamenta en el siguiente marco normativo y técnico:

3.1 Normativa nacional

- **Decreto 1078 de 2015**: Compila la normativa del sector TIC y establece las políticas de gobierno digital y seguridad de la información para las entidades públicas.
- **Ley 1581 de 2012**: Establece disposiciones generales para la protección de datos personales en Colombia.
- **Ley 1273 de 2009**: Modifica el Código Penal para incluir delitos informáticos y protección de la información.
- **Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional)**.
- **Decreto 1377 de 2013**: Reglamenta parcialmente la Ley 1581 de 2012, en especial para la recolección y tratamiento de datos personales.
- **Circular 01 de 2016 – MinTIC**: Define lineamientos generales para el Modelo de Seguridad y Privacidad de la Información (MSPI).
- **Guía de Implementación del MSPI – Versión 3.02 del Ministerio TIC**: Documento técnico que orienta el diseño e implementación de controles para la protección de los activos de información en entidades públicas.

3.2 Estándares internacionales de referencia

- **ISO/IEC 27001:2013**: Norma internacional para sistemas de gestión de seguridad de la información (SGSI), sobre los principios de confidencialidad, integridad y disponibilidad.
- **ISO 31000:2018**: Directrices sobre la gestión del riesgo, aplicable a todo tipo de organizaciones.

- **ISO/IEC 27005:2018**: Directriz específica para la gestión del riesgo dentro de un SGSI.

Este marco normativo proporciona el respaldo legal y técnico necesario para implementar, monitorear y mejorar las medidas de seguridad de la información, conforme al principio de debida diligencia y responsabilidad institucional.

4. METODOLOGÍA Y ENFOQUE

El Instituto Municipal de Tránsito y Transporte de Albania – INSTRANS – ha adoptado un enfoque preventivo y estructurado para la gestión de riesgos en seguridad y privacidad de la información, siguiendo los lineamientos del **Modelo de Seguridad y Privacidad de la Información (MSPI)** del Ministerio TIC y las recomendaciones de la norma **ISO 27005**.

Este enfoque permite identificar y reducir los riesgos que puedan afectar la **confidencialidad, integridad y disponibilidad** de los activos de información institucional, mediante una gestión planificada, documentada y con mejora continua.

4.1 Ciclo de gestión adoptado: PHVA

Se utiliza el ciclo de mejora continua PHVA (Planear – Hacer – Verificar – Actuar) para asegurar el desarrollo progresivo del sistema de gestión:

- **Planear (P)**: Identificación, análisis y evaluación de riesgos.
- **Hacer (H)**: Implementación de controles y medidas de tratamiento.
- **Verificar (V)**: Seguimiento y verificación de la efectividad de las medidas.
- **Actuar (A)**: Ajuste de acciones y retroalimentación al plan.

4.2 Etapas del tratamiento de riesgos

1. **Identificación de activos**: Clasificación de la información, responsables, sistemas y procesos asociados.
2. **Valoración del riesgo**: Evaluación del impacto y la probabilidad de ocurrencia.
3. **Análisis de brechas**: Determinación de vulnerabilidades y controles actuales.
4. **Definición de controles**: Técnicos, administrativos y físicos.
5. **Asignación de responsables**: Según roles institucionales.
6. **Cronograma y recursos**: Definición de tiempos, recursos humanos y técnicos.
7. **Seguimiento y mejora**: Indicadores, reportes y ajustes al plan.

4.3 Roles institucionales

- **Director del INSTRANS**: Responsable principal del cumplimiento y seguimiento del plan.
- **Responsables de proceso**: Apoyan en la identificación de activos y riesgos asociados.
- **Usuarios de sistemas de información**: Cumplen con las políticas internas y reportan incidentes o vulnerabilidades.

Este enfoque permite al INSTRANS abordar los riesgos de forma estructurada, sistemática y con una visión de mejora continua.

5. ACTIVIDADES ESTRATÉGICAS

El Instituto Municipal de Tránsito y Transporte de Albania – INSTRANS – desarrollará una serie de actividades estratégicas que permiten estructurar y ejecutar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de manera eficaz. Estas acciones están alineadas con el Modelo de Seguridad y Privacidad de la Información (MSPI), adoptado por el Ministerio TIC.

A continuación, se describen las principales actividades:

5.1 Diagnóstico inicial

- Identificación de la situación actual de la entidad en materia de seguridad de la información.
- Revisión de políticas, procedimientos y controles existentes.
- Identificación de brechas frente a los requisitos del MSPI.

5.2 Inventario y valoración de activos

- Elaboración de un inventario de activos de información (físicos, digitales, humanos, tecnológicos).
- Clasificación según criticidad: confidencialidad, integridad y disponibilidad.
- Asignación de responsables para cada activo.

5.3 Análisis de riesgos

- Evaluación del impacto y la probabilidad de ocurrencia de cada riesgo.
- Priorización de los riesgos con base en su nivel (alto, medio, bajo).
- Documentación de vulnerabilidades asociadas.

5.4 Definición del plan de tratamiento

- Selección de controles y medidas específicas para mitigar, aceptar, transferir o evitar cada riesgo.
- Inclusión de políticas, procedimientos y configuraciones técnicas.

5.5 Socialización y sensibilización

- Divulgación del plan entre funcionarios, contratistas y partes interesadas.
- Campañas internas de cultura organizacional en seguridad de la información.

- Capacitaciones sobre uso seguro de la información y protección de datos personales.

5.6 Control y seguimiento

- Establecimiento de indicadores para medir el cumplimiento del plan.
- Reportes periódicos de avance.
- Evaluación de efectividad de los controles implementados.
- Ajustes al plan según los resultados y cambios en el entorno.

Estas actividades garantizan un enfoque integral, preventivo y participativo, permitiendo una gestión efectiva de los riesgos que puedan comprometer los activos de información del INSTRANS.

6. Cumplimiento de Implementación por Dominios

Para asegurar la correcta protección de los activos de información del Instituto Municipal de Tránsito y Transporte de Albania – INSTRANS –, se han definido **dominios de implementación** que agrupan controles y acciones específicas. Estos dominios están alineados con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO/IEC 27001:2013.

El cumplimiento por dominios permite organizar la ejecución del plan y hacer seguimiento al avance de cada componente de seguridad.

6.1 Dominios de cumplimiento y acciones asociadas

DOMINIO	ACCIÓN ESTRATÉGICA
1. Política de seguridad	Actualización y publicación de la política institucional de seguridad.
2. Organización de la seguridad	Asignación de responsabilidades, funciones y roles.

3. Gestión de activos	Inventario, clasificación y valoración de activos de información.
4. Seguridad relacionada con el personal	Sensibilización, capacitación y compromisos de confidencialidad.
5. Control de accesos	Implementación de contraseñas seguras, perfiles y permisos controlados.
6. Seguridad física y del entorno	Control de acceso físico a oficinas y servidores.
7. Seguridad en la operación	Procedimientos para el uso seguro de equipos y sistemas.
8. Seguridad en las comunicaciones	Protección de la información en tránsito (correo, red, dispositivos).
9. Adquisición, desarrollo y mantenimiento	Verificación de seguridad en sistemas nuevos o actualizados.
10. Gestión de incidentes de seguridad	Establecimiento de un protocolo para reporte y atención de incidentes.
11. Cumplimiento normativo	Alineación con Ley 1581 de 2012, Ley 1273 de 2009 y normas internas.
12. Relación con terceros	Revisión de contratos con proveedores que procesen o accedan a información.

6.2 Plazos de implementación

El cumplimiento de cada dominio se realizará progresivamente entre los meses de **febrero a junio de 2025**, de acuerdo con el cronograma definido en este plan y los recursos disponibles en la entidad.

7. CRONOGRAMA DE IMPLEMENTACIÓN

El siguiente cronograma establece la programación de actividades para la implementación del Plan de Tratamiento de Riesgos de Seguridad y

Privacidad de la Información del INSTRANS, entre los meses de febrero y junio de 2025. Las fechas pueden ajustarse de acuerdo con la disponibilidad de recursos y las necesidades institucionales.

#	Actividad	Febrero	Marzo	Abril	Mayo	Junio
1	Diagnóstico de seguridad de la información	5 al 16 feb				
2	Revisión de normatividad y lineamientos MinTIC	12 al 23 feb				
3	Inventario y clasificación de activos de información	26 feb – 8 mar	11 al 22 mar			
4	Valoración y análisis de riesgos		25 al 29 mar	1 al 12 abr		
5	Definición del plan de tratamiento de riesgos			15 al 26 abr		
6	Socialización del plan con servidores públicos			29 abr – 3 may	6 al 17 may	
7	Implementación de controles definidos				20 al 31 may	3 al 14 jun
8	Seguimiento y evaluación del plan				20 al 31 may	3 al 21 jun
9	Ajustes y retroalimentación del proceso					24 al 28 jun

Observaciones:

- Las fechas son tentativas y pueden ajustarse según la disponibilidad institucional.
- Cada actividad puede superponerse con otra si se considera necesario para avanzar en paralelo.
- Las semanas están pensadas con márgenes razonables para validación interna y participación de todos los involucrados.

8. SEGUIMIENTO Y EVALUACIÓN

El seguimiento y evaluación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información permitirá verificar su avance, eficacia y cumplimiento, además de identificar oportunidades de mejora y ajustes necesarios durante su ejecución.

El proceso de seguimiento será liderado por el **Director del INSTRANS**, quien tendrá la responsabilidad de supervisar el cumplimiento de cada una de las actividades programadas y de coordinar los reportes de avance con los funcionarios responsables.

8.1 Estrategia de seguimiento

- **Frecuencia**: Se realizará un seguimiento **quincenal**, con base en el cronograma establecido.
- **Medios**: Se emplearán informes de avance, listas de chequeo y reuniones periódicas.
- **Instrumentos**: Registro de ejecución de actividades, actas de socialización, y formatos de control.

8.2 Evaluación del cumplimiento

- Al finalizar el ciclo de implementación (junio de 2025), se elaborará un **informe final de ejecución**, que incluirá:
    - Actividades completadas.
    - Grado de cumplimiento por dominio.
    - Efectividad de los controles aplicados.
    - Recomendaciones para futuras actualizaciones.

- Este informe será evaluado por la **Secretaría General o la instancia de control institucional designada**, para verificar la conformidad con los objetivos del plan y con la normatividad vigente.

9. ENTREGABLES

Como resultado de la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el Instituto Municipal de Tránsito y Transporte de Albania – INSTRANS – generará los siguientes entregables:

1. **Plan de tratamiento de riesgos**
   Documento principal que describe los riesgos identificados, las acciones de mitigación y los responsables de su ejecución.
2. **Política de Seguridad de la Información**
   Declaración formal que establece los principios y compromisos institucionales para proteger la información.
3. **Análisis de recursos tecnológicos**
   Evaluación de los equipos, sistemas y herramientas tecnológicas disponibles y necesarias para implementar los controles definidos.
4. **Matriz de identificación del riesgo**
   Registro estructurado de los activos de información, amenazas, vulnerabilidades y responsables.
5. **Análisis del riesgo**
   Evaluación del impacto y la probabilidad de ocurrencia de los riesgos detectados.
6. **Valoración del riesgo**
   Clasificación de los riesgos por nivel (alto, medio o bajo) y priorización de su tratamiento según el impacto institucional