PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**INSPECCIÓN DE TRÁNSITO Y TRANSPORTE**

**DE BARRANCABERMEJA**

### Datos de Contacto:

|  |  |
| --- | --- |
| **Empresa** | INSPECCIÓN DE TRÁNSITO Y TRANSPORTE DE BARRANCABERMEJA |
| **NIT** | 890270948 - 3 |
| **Representante Legal** | Debison Gomez Martínez |
| **Documento****preparado por** | Zaida Milena González CárdenasCarlos Eduardo Amado Noguera |
| **Conmutador** | +57 6228685 |
| **Correo Notificaciones****Judiciales** | notificacionesjudiciales@aguasdebarrancabermeja.gov.co |
| **Correo contacto y****PQRD** | https://consorciostb.com/pqrs/ |
| **Sitio Web** | www.transitobarrancabermeja.gov.co |
| **Horario de Atención****al Público** | lunes a Jueves 7:00 am a 11:30 pm y de 2:00 pm a 5:00pm y Viernes de 7:00 am a 04:00 pm y 2:00 pm a 4:00pm |
| **Dirección** | Carrera 2 No. 50 - 25 Barrancabermeja - Colombia |

**INTRODUCCIÓN**

El departamento administrativo de la función pública establece que todos los entes nacionales y territoriales deben contar con un el plan de tratamiento de riesgos de seguridad y privacidad de la información. En este plan de sebe establecer un método lógico y sistemático para la administración, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con la seguridad y privacidad de la información, que permitan minimizar la perdida de información como principal activo de la organización.

Actualmente cualquier organización o empresa gestiona sus actividades a través de herramientas tecnológicas como sistema de información están expuestas a los riesgos asociados con la privacidad y seguridad de la información; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, el presente plan tiene como objetivo orientar y facilitar la implementación y desarrollo de una forma eficaz, eficiente y efectiva de la gestión de los riesgos asociados con la seguridad y privacidad de la información, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y generar los lineamientos para su adecuada gestión.

## OBJETIVOS

* 1. ***Objetivo general***

Definir los riesgos de seguridad y privacidad de la información contemplando: Identificación de activos de información, amenazas, vulnerabilidades, riesgos y controles, los niveles aceptables y tratamiento de riesgo en la empresa Inspección de Tránsito y transporte de Barrancabermeja.

## Objetivos específicos

* Realizar un análisis y valoración de los riesgos de seguridad de la información sobre el Desarrollo y/o actualización del inventario de activos de información.
* Definir metodología para la gestión de los riesgos de seguridad y privacidad de la información.
* Elaborar procedimientos gestión de Riesgos de seguridad de la información sobre medidas de protección que contribuyan al correcto tratamiento de los riesgos a través de una adecuada selección y relación de controles.

# Alcance

El Análisis de Riesgos de Seguridad y Privacidad de la Información provee los mecanismos necesarios para identificar, analizar, evaluar y tratar de manera adecuada los riesgos asociados a los activos de información de la Empresa Inspección de Tránsito y transporte de Barrancabermeja.

# Ámbito de Aplicación

El presente Plan aplica para el Sistema SIOT WEB de la Empresa Inspección de Tránsito y transporte de Barrancabermeja.

# Definiciones

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

* **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
* **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
* **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación
* **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
* **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
* **Causa:** medios, circunstancias y/o agentes que generan riesgos.
* **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
* **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
* **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
* **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
* **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
* **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
* **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
* **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
* **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
* **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
* **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
* **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
* **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
* **Mapa de riesgos:** documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
* **Materialización del riesgo:** ocurrencia del riesgo identificado
* **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
* **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
* **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
* **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
* **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.
* **Riesgo de corrupción:** posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
* **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
* **Riesgo institucional**: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:
	+ Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
	+ Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
	+ Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
	+ Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.
* **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
* **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

# Contexto de Seguridad y Privacidad de la Información

La información de la Inspección de Tránsito y transporte de Barrancabermeja sin importar el tipo, es crucial para el desarrollo de su objeto misional, su correcto desempeño dentro de la política pública y su relación con el ciudadano, es por ello que debe ser protegida de cualquier posibilidad de ocurrencia de eventos de riesgo de seguridad de la información y que pudiese significar un impacto indeseado generando una consecuencia negativa para el normal progreso de las actividades de la entidad. De acuerdo con lo anterior y tomando como referencia el Modelo de Seguridad y Privacidad de la información del MINTIC.

# Riesgos de Seguridad y Privacidad de la Información

### Definición del Riesgo

De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la “Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias”. De igual manera el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información.

De acuerdo con lo anterior y en el marco de la Política Nacional de Seguridad Digital, la estrategia de administración de riesgos para el flujo de la información en los procesos de la Empresa Inspección de Tránsito y transporte de Barrancabermeja, busca diseñar una metodología ágil enfocada en la identificación, gestión y tratamiento de los Riesgos de Seguridad y Privacidad de la Información:



### Riesgos de Seguridad Digital

Riesgos que resultan de la combinación de amenazas y vulnerabilidades en el ambiente digital y dado su naturaleza dinámica incluye también aspectos relacionados con el entorno físico. En la tipificación de dichos riesgos, se encuentran los siguientes:

**Fuga o Pérdida de la Información**: Información que hace que esta llegue a personas no autorizadas, sobre la que su responsable pierde el control o el estado que genera una condición irreparable en el tratamiento y procesamiento de la Información. Ocurre cuando un sistema de información o proceso diseñado para restringir el acceso sólo a sujetos autorizados revela parte de la información que procesa o transmite debido a errores en la ejecución de los procedimientos de tratamiento, las personas o diseño de los Sistemas de Información.

**Pérdida de la Confidencialidad**: Violación o incidente a la propiedad de la información que impide su divulgación a individuos, entidades o procesos no autorizados.

**Pérdida de la Integridad**: Pérdida de la propiedad de mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

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

### Riesgos de Privacidad

Riesgos que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos. Como riesgo tipificado se cuenta con lo siguiente:

**Inadecuado Tratamiento de Datos Personales**: Uso no adecuado de la información que identifica a las personas, lo que repercute en una violación de los derechos constitucionales

### Metodología de Valoración del Activo y Análisis de Riesgos de Seguridad de la Información

La Empresa Inspección de Tránsito y transporte de Barrancabermeja utiliza una metodología para valorar los riesgos de la Seguridad de la Información, basado en el Sistema de Gestión de Riesgos. La Matriz de Valoración de Activos y Análisis de Riesgos de Seguridad de la Información, contribuyen al Sistema Integrado de Gestión abarcando los siguientes aspectos:

Se identifican los activos de información en el flujo de cada proceso, con el objetivo de valorarlos e identificar los riesgos de seguridad y privacidad de la información asociada a los factores.

### Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Con base en el resultado del análisis de riesgos de seguridad y privacidad de la información y con el fin de gestionar el riesgo residual, se proponen acciones de mejora los cuales pueden estar en marcha por medio de planes de acción o de tratamiento con la finalidad de que la información siempre conserve las características de confidencialidad, integridad y disponibilidad de la misma, desarrollándose como un proceso de seleccionar e implementar medidas para modificar el nivel de riesgo.

El Plan de Tratamiento de Riesgos de Seguridad de la Información se integra al presente Plan Metodológica y a la Matriz de Valoración de Activos y Análisis de Riesgos de Seguridad de la Información, contribuyendo al fortalecimiento de los mecanismos de Gestión de Riesgos del Sistema de la Empresa Inspección de Tránsito y transporte de Barrancabermeja.

### Establecimiento del contexto.

###  Consideraciones generales

**Entrada:** Toda la información de la Organización

**Acción:** El contexto para la gestión de riesgos de seguridad de la información debería ser establecida:

* + - Criterios Básicos
			* Criterios de Evaluación de Riesgos
			* Criterios de Impacto
			* Criterios de Aceptación de Riesgos
		- Alcance y Limites
		- Organización de gestión de Riesgos de seguridad de la información
			* Cargos: Responsable y Administrador del proceso de gestión de riesgos
			* Roles y responsabilidades
			* Nivel de reporte
			* Registros

**Salida: Criterios** Básicos, alcance, límites y organización para proceso de gestión de riesgos de seguridad**. Asignación de recursos:** Técnicos.

### Análisis de Riesgos Identificación de Riesgos

* **Identificación de Activos**
	+ **Entrada:** Alcance y límites para la gestión de riesgos de TI, lista de componentes con propietarios, ubicación, función
	+ **Acción:** Los activos deberían ser identificados dentro del alcance establecido:
		- Activo
		- Propietario
		- Custodio

Existen varios tipos de activos:

* + - Software
		- Hardware
		- Documentos electrónicos y físicos
		- Personas
		- Procesos

**Salida:** Lista de activos de Información con propietarios

**Asignación de Recursos:** Técnicos

### Identificación de Amenazas

* + **Entrada:** Información de amenazas obtenidas de revisión de incidentes, propietarios de activos, usuarios y otras fuentes.
	+ **Acción:** Amenazas y sus fuentes deben ser identificadas
	+ **Salida:** Una lista de amenazas con la identificación de tipo de amenaza y fuente

**Asignación de recursos:** Técnicos

### Identificación de controles existentes

* + **Entrada:** Documentación de controles, plan de implementación de tratamiento de riesgos
	+ **Acción:** Los controles existentes y planificados deberían ser identificadas
	+ **Salida:** Una lista de controles existentes y planificados, su estado de Implementación y uso

**Asignación de Recursos:** Técnicos

### Cronograma

