TRÁNSITO DEL ATLÁNTICO

# Plan de tratamiento de riesgos de seguridad y privacidad de la información (PTRSPI) del Instituto de Tránsito del Atlántico para la vigencia 2025 – 2028

## Dimensión del MIPG: Información y Comunicación.

## Oficina asesora de planeación

## Departamento de Sistemas

**Enero 2025**

TRÁNSITO DEL ATLÁNTICO

# Contenido

# 1. Objetivos

## 1.1. Objetivo general

Establecer un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PTRSPI que permita establecer la hoja de ruta a seguir tanto para la minimización de los riesgos de pérdida de activos de la información en el Instituto de Transito del Atlántico como también, para las acciones por ejecutar ante cualquier catástrofe tecnológica que ocurra.

## 1.2. Objetivos específicos

- ✓ Plantear modelos de reportes para su posterior uso en cada incidencia presentada en el Instituto de Transito del Atlántico – ITA.
- ✓ Gestionar los eventos de seguridad de la información con el propósito de que sean detectados y tratados eficientemente, en particular, definir si es necesario o no clasificarlos como incidentes de Seguridad de la Información.
- ✓ Determinar el alcance del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PTRSPI.
- ✓ Definir los principales activos a proteger en el Instituto de Transito del Atlántico.
- ✓ Identificar las principales amenazas que afectan los activos del Instituto.
- ✓ Proponer acciones que minimicen los riesgos a los que está expuesto cada activo del Instituto.
- ✓ Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el PTRSPI.
- ✓ Definir el esquema de capacitación del talento humano del Instituto.

## 2. Alcance

Este Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PTRSPI, debe tener un alcance totalmente integral que abarque el cien por ciento de los aspectos relevantes relacionados con la gestión de los Riesgos en Seguridad y Privacidad de la Información del Instituto de Tránsito del Atlántico, en el marco de lo establecido en las normatividades del Estado Colombiano que rigen estas directrices.

Todo esto deberá ir de la mano con el total compromiso de los altos mandos del Instituto de acompañar las actividades de implementación del PTRSPI y, las posteriores de seguimiento, evaluación y control.

También, se deberá designar funciones de liderazgo que apoyen y asesoren el proceso de diseño e implementación del Plan y, trabajar en la capacitación del talento humano del Instituto en lo referente a las acciones de mitigación de incidentes planteadas en el PTRSPI.

## 3. Marco normativo

- ✓ **Resolución 500 de 2021:** referente a la seguridad digital y MSPI.
- ✓ **Resolución 1519 de 2020:** que define los estándares y directrices para publicar la información y los requisitos de acceso a la información pública, accesibilidad web, seguridad digital y datos abiertos.
- ✓ **Ley 1712 de 2014:** por la cual se crea la ley de transparencia y del derecho al acceso a la información pública nacional y se dictan otras disposiciones.
- ✓ **Ley 1581 de 2012:** por la cual se dictan las disposiciones generales para la protección de datos personales.
- ✓ **Ley 1273 de 2009:** por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado “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 527 de 1999:** referente al comercio electrónico y firmas digitales.
- ✓ **Norma ISO 27001:** referente a la gestión de seguridad de la información.
- ✓ **Norma ISO 27701:** referente a la gestión de privacidad de la información.

## 4. Algunas definiciones propias de la información

- ✓ **Fuentes de información:** hace referencia a la identificación de los recursos de información del Instituto, como son: las bases de datos, los sistemas de información, las aplicaciones y las redes informáticas.
- ✓ **Clasificación de la información:** se puede clasificar la información del Instituto según su grado de sensibilidad y el de la necesidad de protección, teniendo en cuenta en todo momento el potencial impacto que pueda tener en caso de que se presente alguna vulneración.

## 5. Gestión del riesgo

### 5.1. Importancia de la Gestión del Riesgo

En el ámbito empresarial global actual la prioridad número se centra en asegurar, proteger y salvaguardar los activos de información, estos representan una parte importante tanto en la toma de decisiones, como en garantizar la supervivencia de los negocios, sin desconocer todo el caos que ha significado el incremento exponencial en la implementación de diversos Sistemas de Información y nuevas tecnologías como apoyo a diversos procesos, que a su vez generan gran cantidad de datos e información diariamente, volviendo complejo la gestión de estos.

El Instituto de Transito del Atlántico ajustado a los lineamientos marcados por el Gobierno Nacional en la Ley de Transparencia 1712 de 2014 y en la Política de Gobierno Digital, que impulsan actividades dentro de las entidades públicas que se ciñen a modelos y estándares que buscan brindar seguridad a la información, dando cumplimiento a lo definido en el Decreto 1078 de 2015.

Los riesgos causados por desastres naturales, los inherentes relacionados con procesos de manejos inadecuados en el tratamiento de la información, los que son producto del desconocimiento de normas, políticas de seguridad y el no cumplimiento de estas; suelen ser los de mayor impacto en las entidades.

Por todo lo expuesto anteriormente, las entidades del Estado Colombiano están obligadas a trabajar en el diseño e implementación de planes que permitan gestionar y/o mitigar los posibles riesgos que puedan afectar sistemas, tecnologías de información y/o activos informáticos con que cuenten, en muchos casos el objetivo es afectar la confidencialidad, disponibilidad e integridad de la información.

En conclusión, considerando el estado tecnológico actual del Instituto y las razones revisadas anteriormente, debemos trabajar en reducir al máximo el impacto y/o riesgos que puedan presentarse, para esto, debemos diseñar un plan que incentive la aplicación de las normas y políticas de seguridad que nos permitan asegurar una buena gestión de los incidentes que puedan presentarse y la continuidad en la prestación de los servicios de la entidad.

### 5.2. Definición de gestión del riesgo

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como: “la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización”.

### 5.3. Identificación del riesgo

- ✓ **Riesgo Estratégico:** se asocia con la forma en que se administra el Instituto. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
- ✓ **Riesgos de Imagen:** están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
- ✓ **Riesgos Operativos:** comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.
- ✓ **Riesgos Financieros:** se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
- ✓ **Riesgos de Cumplimiento:** se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.
- ✓ **Riesgos de Tecnología:** están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y, el cumplimiento de la misión.

### 5.4. Situaciones no deseadas

- ✓ Hurto de información durante el cumplimiento de las funciones laborales, por intromisión, incendio en las instalaciones de la empresa, por desastres naturales o de manera intencional.
- ✓ Hurto de equipos de cómputo o de redes.

- ✓ Alteración de claves o información.
- ✓ Baja Cobertura del Internet.
- ✓ Daños físicos en equipos de cómputo.
- ✓ Atrasos en la entrega de información.
- ✓ Atrasos en asistencia técnica.
- ✓ Ciberataques.
- ✓ Fraude de datos.

## 6. Origen del plan de gestión

Es necesario crear un plan de tratamiento de riesgos de seguridad y privacidad de la información que permita proteger los activos de información teniendo una orientación estratégica para el desarrollo de una cultura de carácter preventivo, es decir, si comprendemos el concepto de riesgo y su contexto, debemos planear acciones que reduzcan el impacto en la entidad si se logran materializar.

### 6.1. Propósitos del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PTRSPI

- ✓ Desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo del riesgo con mayor objetividad.
- ✓ Dar soporte al modelo de seguridad de la información al interior de la entidad.
- ✓ Preparación de un plan de respuesta a incidentes.
- ✓ Descripción de los requisitos de seguridad de la información para un producto, un servicio o un mecanismo.
- ✓ Alcances, límites y organización de los procesos de tratamiento de riesgos de seguridad y privacidad de la información.
- ✓ Fortalecimiento de los diversos componentes que integran los sistemas de información en la entidad.
- ✓ Capacitar y/o concientizar a los usuarios de los peligros existentes con el tratamiento de la información.
- ✓ Conformidad legal y evidencias de la debida diligencia.

## 7. Análisis de vulnerabilidades

### 7.1. Descripción de vulnerabilidades

Las vulnerabilidades en seguridad pueden definirse como debilidades o fallos en los sistemas de información que pueden poner en riesgo la seguridad y privacidad de

la información, ahora, es importante mencionar que no todas las vulnerabilidades son producto de amenazas o ataques recibidos, o de errores cometidos por parte de los usuarios finales, existen otras tales como:

- ✓ Puntos de red insuficientes en las áreas de trabajo de la entidad, no hay una correcta planificación, se definen a medida que se vayan presentando las necesidades.
- ✓ Fallas en el tendido u organización del cableado y puntos de energía, distribuidos de manera incorrecta o insuficientes para la cantidad de equipos en las oficinas, la vulnerabilidad se representa en que puedan ser desconectados accidentalmente y la información procesada en el momento por el talento humano no logre ser asegurada.
- ✓ El desconocimiento de las políticas y normas de seguridad de la información existentes en la entidad, por la no socialización de estas.
- ✓ Inconsistencias en los planes de contingencia que permitan volver a ser operativos ante cualquier desastre ocurrido.
- ✓ Insuficiencia en la capacidad de la planta de energía de la sede Barranquilla, cuenta con poca autonomía ante la interrupción del flujo de energía eléctrica, lo que a veces representa apagón súbito de los equipos.
- ✓ Equipos de cómputo insuficientes de acuerdo con el personal contratado, esto incentiva a que los usuarios deban verse obligados a compartir los equipos y con esto se incrementa el riesgo de pérdida de información.
- ✓ Almacenar información de la entidad en memorias o discos duros portables personales.
- ✓ El uso de dispositivos de almacenamiento extraíbles en los equipos de la entidad, pueden representar infecciones de los equipos de cómputo con virus o softwares maliciosos.
- ✓ El incumplimiento a las reglas básicas de cuidado de los equipos informáticos, la información física y/o digital. En este punto se pueden mencionar algunas:
    - Consumir bebidas y/o alimentos cerca de los equipos de cómputo.
    - Filtrar información sensible en hojas reutilizables.
    - Apertura de correos maliciosos sin la previa verificación de la fuente.
    - Compartir deliberadamente las credenciales de acceso a los diversos servicios de la entidad.
    - Instalar y/o utilizar aplicaciones de software no licencias o no autorizadas por la entidad.
    - Visitar sitios web inseguros.
    - Entre otros.

## 8. Propuesta de seguridad

- ✓ Replantear las políticas de seguridad y privacidad de la información como también las políticas de seguridad informática.
- ✓ Revisar las políticas existentes para identificar debilidades y fortalezas, si es necesario, hacer ajustes.
- ✓ Socializar constantemente las políticas de seguridad y privacidad de la información con el talento humano del Instituto.
- ✓ Revisar, organizar y ubicar las conexiones de electricidad y de puntos de red según las verdaderas necesidades de cada oficina del Instituto.

### 8.1. Plan de copias de seguridad

- ✓ Definir los recursos físicos o en la nube necesarios para almacenar las copias de seguridad de la información esencial de la entidad.
- ✓ Contar con un plan alternativo que asegure la continuidad de la actividad del Instituto en caso de que ocurran incidentes graves.

### 8.2. Plan de continuidad del negocio

- ✓ Diseñar un formato de chequeo de acuerdo con las necesidades de la organización que permita realizar las auditorías periódicas con la finalidad de verificar que los objetivos de control, procesos y procedimientos se cumplan.
- ✓ Socializar con los directivos, secretaría general y oficina de las TIC la importancia del Plan de continuidad de negocio, para hacer frente a incidentes graves de seguridad en la entidad.
- ✓ Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.
- ✓ Diseñar un plan de contingencia teniendo en cuenta que la continuidad en el negocio dependerá de los riesgos y amenazas potenciales que serán tratados de acuerdo con lo siguiente:
    - Política de copia de seguridad de datos.
    - Procedimientos de almacenamiento fuera del Instituto.
    - Procedimientos de gestión de emergencias, por desastre natural, por incendio o por inundaciones.

### 8.3. Implementación de políticas de seguridad para la información

El análisis permitió identificar que se desconocen o poco se cumplen las políticas de seguridad; por lo que se recomienda tener en cuenta:

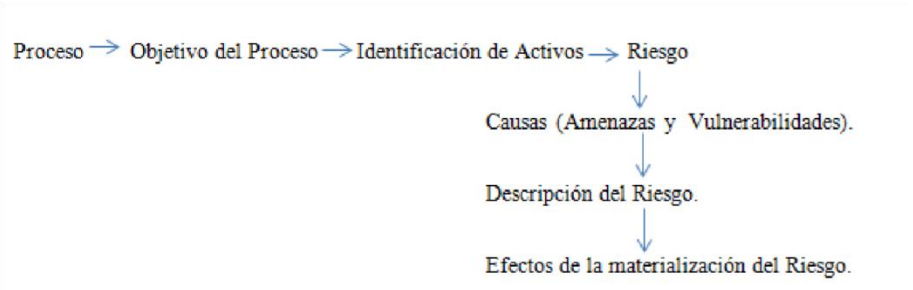
- ✓ Socialización y capacitación constante al talento humano en temas de seguridad y privacidad de la información.
- ✓ Asegurar un ambiente con la seguridad física adecuada.
- ✓ Adquirir sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas.

### 8.4. Valoración de los riesgos

El objetivo de este paso es generar una lista completa de los riesgos sobre la base de los acontecimientos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar la consecución de los objetivos del Instituto.

Las debilidades de los procesos en cuanto a seguridad de la información, los riesgos a los cuales se encuentran expuestos y las causas que podrían comprometer la confidencialidad, integridad y disponibilidad de los procesos del Instituto de Tránsito del Atlántico deben ser identificadas y evaluadas teniendo en cuenta los criterios de evaluación definidos. En este proceso se debe realizar las siguientes actividades:

- ✓ Identificar el flujo de información de cada uno de los procesos.
- ✓ Identificar las vulnerabilidades que existen en el proceso.
- ✓ Identificar las amenazas que podrían materializarse, dadas las vulnerabilidades existentes.
- ✓ Definir las escalas a utilizar.




De acuerdo con los Lineamientos para la gestión de riesgos digital en entidades públicas emitida por el DAFP, se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- ✓ Pérdida de la confidencialidad.
- ✓ Pérdida de la integridad.
- ✓ Pérdida de la disponibilidad.

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso y conjuntamente analizar las posibles amenazas y, vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de

amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

### 8.5. Identificación de las amenazas

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

Deliberadas (D), fortuito (F) o ambientales (A).

***Tabla No. 1 – Listado de amenazas.***

| Tipo | Amenaza | Origen |
|---|---|---|
| Daño físico | Fuego | F, D, A |
| | Agua | F, D, A |
| Eventos naturales | Fenómenos climáticos | F |
| | Fenómenos sísmicos | F |
| Pérdidas de los servicios esenciales | Fallas en el sistema de suministro de agua | F,D,A |
| Pérdidas de los servicios esenciales | Fallas en el suministro de aire acondicionado | F, D, A |
| Perturbación debida a la radiación | Radiación electromagnética | F, D, A |
| | Radiación térmica | F, D, A |
| Compromiso de la información | Interceptación de servicios de señales de interferencia comprometida | D |
| | Espionaje remoto | D |
| Fallas técnicas | Fallas del equipo | D, F |
| | Mal funcionamiento del equipo | D, F |
| | Saturación del sistema de información | D, F |
| | Mal funcionamiento del software | D, F |
| | Incumplimiento en el mantenimiento del sistema de información | D, F |
| Acciones no autorizadas | Uso no autorizado del equipo | D, F |
| | Copia fraudulenta del software | D, F |
| Compromiso de las funciones | Error en el uso o abuso de derechos | D, F |
| | Falsificación de derechos | D |
| Dirigidas por el hombre | Piratería | D |
| | Ingeniería social | D |
| | Crimen por computador | D |
| | Acto fraudulento | D |
| | Ataques contra el sistema | D |
| | DDoS | D |
| | Penetración en el sistema | D |
| | Ventaja de defensa | D |

| | | |
|---|---|---|
| | Hurto de información | D |
| | Asalto a un empleado | D |
| | Chantaje | D |

## 8.6. Identificación de las vulnerabilidades.

Se pueden identificar vulnerabilidades de acuerdo con los siguientes tipos:

***Tabla No. 2 – Listado de vulnerabilidades.***

| Tipo | Vulnerabilidad |
|---|---|
| Hardware | Mantenimiento insuficiente. |
| | Ausencia de esquemas de reemplazo periódico. |
| | Sensibilidad a la radiación electromagnética. |
| | Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad). |
| | Almacenamiento sin protección. |
| | Falta de cuidado en la disposición final. |
| Software | Copia no controlada. |
| | Ausencia o insuficiencia de pruebas de software. |
| | Ausencia de terminación de sesión. |
| | Ausencia de registros de auditoría. |
| | Asignación errada de los derechos de acceso. |
| | Interfaz de usuario compleja. |
| | Ausencia de documentación. |
| | Fechas incorrectas. |
| | Ausencia de mecanismos de identificación y autenticación de usuarios. |
| | Contraseñas sin protección. |
| | Software nuevo o inmaduro. |
| Red | Ausencia de pruebas de envío o recepción de mensajes. |
| | Líneas de comunicación sin protección. |
| | Conexión deficiente de cableado. |
| | Tráfico sensible sin protección. |
| | Punto único de falla. |
| Personal | Ausencia del personal. |
| | Entrenamiento insuficiente. |
| | Falta de conciencia en seguridad. |
| | Ausencia de políticas de uso aceptable. |
| | Trabajo no supervisado de personal externo o de limpieza. |
| Lugar | Uso inadecuado de los controles de acceso al edificio. |
| | Áreas susceptibles a inundación. |
| | Red eléctrica inestable. |

| | |
|---|---|
| | Ausencia de protección en puertas o ventanas. |
| Organización | Ausencia de procedimiento de registro/retiro de usuarios. |
| | Ausencia de proceso para supervisión de derechos de acceso. |
| | Ausencia de control de los activos que se encuentran fuera de las instalaciones. |
| | Ausencia de acuerdos de nivel de servicio (ANS o SLA). |
| | Ausencia de mecanismos de monitoreo para brechas en la seguridad. |
| | Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros). |

## 8.7. Análisis del riesgo de seguridad de la información

El objetivo del análisis de riesgos es identificar y valorar los riesgos a los cuales están expuestos los procesos y los flujos de información en el Instituto, para identificar y seleccionar los controles apropiados de seguridad.

En esta etapa se definen los criterios que se deben utilizar para evaluar la importancia del riesgo. Los criterios reflejarán los valores del Instituto, los objetivos y los recursos existentes. Estos criterios de riesgo estarán revisándose de forma permanente, dado los cambios que pueden ocurrir en la organización.

Al definir los criterios de riesgo, se tendrán en cuenta:

- ✓ La naturaleza, los tipos de causas y consecuencias que pueden ocurrir y como se van a medir.
- ✓ La manera de definir la probabilidad de ocurrencia de un evento.
- ✓ La forma de determinar el nivel de riesgo.
- ✓ Niveles de riesgo aceptable para la organización.

Las actividades realizadas para ejecutar el análisis de riesgos se realizan de acuerdo con el siguiente esquema:

- ✓ Definición de las áreas del Instituto de Tránsito del Atlántico que se incluirán dentro del alcance del proceso de gestión de riesgos de seguridad digital y ciberseguridad.
- ✓ Levantamiento de información relacionada con el proceso seleccionado.
- ✓ Entrevistas con personas claves dentro del proceso para conocer su percepción del riesgo al cual se encuentra expuesta la información.
- ✓ Ejecución de la evaluación de riesgos a los que se encuentra expuesto el proceso, por medio de valoración de hallazgos y evaluación de probabilidad de ocurrencia de amenazas y vulnerabilidades.

- ✓ Análisis y diagnóstico del nivel de riesgo para el proceso definido. Se llevará a cabo la elaboración de informe de resultados.

Para la identificación de Amenazas, vulnerabilidades y riesgos, se tienen en cuenta los resultados de las entrevistas con los dueños y/o responsables de los procesos del negocio y los análisis de riesgos existentes. Con el fin de establecer los niveles de riesgos a los cuales se encuentran expuestos los procesos, se mide la probabilidad de ocurrencia de las amenazas y el impacto que tendría las consecuencias de su materialización.

Se determina la probabilidad de ocurrencia para cada riesgo de acuerdo con la siguiente escala:

***Tabla No. 3 – Escala de probabilidad de ocurrencia de amenazas.***

| Valoración asignada | Valor Asignado | Frecuencia |
|---|---|---|
| Insignificante | 1 | Ha ocurrido una vez en los últimos tres a cinco años |
| Bajo | 2 | Ha ocurrido una vez en los últimos >= tres y < cinco años |
| Moderado | 3 | Ha ocurrido >= una vez en el período >= un año y < tres años |
| Mayor | 4 | Ha ocurrido entre una y tres veces en el último año |
| Catastrófico | 5 | Ha ocurrido más de tres veces en el último año |

Se determina el impacto de cada riesgo de acuerdo con la siguiente escala:

***Tabla No. 4 – Escala de impacto de cada riesgo.***

| Valoración asignada | Valor asignado | Impacto Cuantitativo | Impacto Cualitativo |
|---|---|---|---|
| Insignificante | 1 | Afectación <= 1% de la población. | Sin afectación de la integridad. |
| | | No hay afectación medioambiental | Sin afectación de la disponibilidad. |
| | | No hay afectación a la divulgación / no hay fuga de información | Sin afectación de la confidencialidad. |
| Bajo | 2 | Afectación <= 2% de la población. | Afectación leve de la integridad. |
| | | Afectación <=1% del presupuesto anual de la entidad. | Afectación leve de la disponibilidad. |
| | | Afectación leve del medio ambiente requiere de 1 semanas de recuperación. | Afectación leve de la confidencialidad. |

| | | | |
|---|---|---|---|
| Moderado | 3 | Afectación <=5% de la población. | Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. |
| | | Afectación <=3% del presupuesto anual de la entidad. | Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. |
| | | Afectación leve del medio ambiente requiere de 3 semanas de recuperación. | Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros. |
| Mayor | 4 | Afectación <=10% de la población. | Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. |
| | | Afectación <=5% del presupuesto anual de la entidad. | Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. |
| | | Afectación importante del medio ambiente que requiere de <=2 meses de recuperación. | Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. |
| Catastrófico | 5 | Afectación <=30% de la población. | Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. |
| | | Afectación <=10% del presupuesto anual de la entidad. | Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. |
| | | Afectación muy grave del medio ambiente que requiere de <=2 años de recuperación. | Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. |

La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

### 8.8. Seguimiento y revisión del proceso de tratamiento de riesgos de seguridad y privacidad de la Información

El seguimiento y la revisión son una parte importante del proceso de Gestión de Riesgos, donde las responsabilidades de seguimiento, monitoreo y evaluación deben estar claramente definidas y deben abarcar todos los aspectos del proceso de gestión.

El responsable del seguimiento del presente plan es el Profesional Universitario de la Oficina Asesora de Planeación del Tránsito del Atlántico en coordinación con el área de Planeación de la entidad como área que lidera y articula los procesos en el Instituto de Tránsito del Atlántico.

Dentro de las actividades que se ejecutan en esta fase, se tienen:

- ✓ Analizar los cambios, las tendencias, los éxitos y los fracasos dentro del proceso de gestión de riesgos de seguridad de la información.
- ✓ Detectar cambios en el contexto interno o externo, incluyendo los cambios que se puedan presentar en los criterios de riesgos de seguridad de la información.
- ✓ Revisar la implementación de los planes de tratamiento de riesgo de seguridad de la información y las prioridades de implementación de estos.
- ✓ Identificación de nuevos riesgos de seguridad de la información.
- ✓ La revisión de la gestión de riesgos se debe hacer por lo menos una vez al año, el seguimiento a los riesgos debe ser permanente por parte de los líderes de los procesos.

## 9. Términos y definiciones

- ✓ **Activo:** en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- ✓ **Aceptación de riesgo:** decisión de asumir un riesgo.
- ✓ **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- ✓ **Análisis de Riesgo:** uso sistemático de la información para identificar fuentes y estimar el riesgo (Guía ISO/IEC 73:2002).
- ✓ **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- ✓ **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

- ✓ **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- ✓ **Control:** medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- ✓ **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- ✓ **Dueño del riesgo sobre el activo:** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- ✓ **Evaluación del riesgo:** Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
- ✓ **Factor de riesgo:** Agente ya sea humano o tecnológico que genera el riesgo.
- ✓ **Gestión del riesgo:** proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- ✓ **Impacto:** se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- ✓ **Integridad:** propiedad de exactitud y completitud.
- ✓ **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo.
- ✓ **Nivel de riesgo:** Da el resultado en donde se ubica el riesgo por cada activo de información.
- ✓ **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- ✓ **Riesgo:** Efecto de la incertidumbre sobre el cumplimiento de los objetivos.
- ✓ **Riesgo de seguridad digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- ✓ **Riesgo Inherente:** Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
- ✓ **Riesgo residual:** Nivel restante de riesgo después del tratamiento del riesgo.
- ✓ **Tratamiento del riesgo:** Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.
- ✓ **Valoración del riesgo:** Proceso de análisis y evaluación del riesgo.
- ✓ **Vulnerabilidad:** La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenaza

## 10. Actividades definidas para el PTRSPI

El PTRSPI abarca una serie de actividades por desarrollar con el propósito de mitigar los riesgos sobre los activos identificados en el Instituto, siguiendo las recomendaciones entregadas por MinTIC en la guía de gestión de riesgos de seguridad y privacidad de la información.

| Gestión | Actividades | Tareas | Responsable (s) | Año | Trimestre | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 3 | 4 |
| Gestión de riesgos | Actualización de lineamientos de riesgos. | Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos. | Oficina asesora de planeación – Departamento de sistemas. | 2025 – 2028 | | | | |
| | Sensibilización. | Iniciar y/o continuar las socializaciones a todos los procesos para la gestión de riesgos de seguridad digital. | Oficina asesora de planeación – Departamento de sistemas. | 2025 – 2028 | | | | |
| | Identificación de riesgos de seguridad y privacidad de la información. | Identificación, análisis y evaluación de riesgos de seguridad digital. | Oficina asesora de planeación – Departamento de sistemas. | 2025 – 2028 | | | | |
| | Tratamiento del riesgo. | Definición de controles y planes de tratamiento de riesgos los identificados. | Oficina asesora de planeación – Departamento de sistemas. | 2025 – 2028 | | | | |
| | Mejoramiento. | Revisión y/o actualización de lineamientos de riesgos de seguridad digital de acuerdo con las observaciones presentadas. | Oficina asesora de planeación – Departamento de sistemas. | 2025 – 2028 | | | | |
| | Monitoreo y revisión. | Realizar mediciones periódicas a los controles definidos por cada proceso. | Oficina asesora de planeación – Departamento de sistemas. | 2025 – 2028 | | | | |

## 11. Seguimiento

Deberá ser continuo, se define una iteración semestral para las tareas de revisión y seguimiento por parte de todos los actores involucrados en la ejecución del Plan.

## 12. Biografía

Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC. (mayo de 2023). MGGTI.G.GO - Gobierno de TI: https://www.mintic.gov.co/arquitecturaempresarial/630/articles-237661_recurso_1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC. (2023). Plan de tratamiento de riesgos de seguridad y privacidad de la información versión 5: https://mintic.gov.co/portal/715/articles-135830_plan_tratamiento_riesgos_seguridad_privacidad_informacion_vigencia_2023_v20230124.pdf

F&C Consultores (Bogotá – mayo de 2023). Presentación del Congreso Nacional de Gestión del Riesgo en el Sector Público: Del Riesgo de Seguridad de la Información.

## 13. Control de cambio

| **Nombre documento: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PTRSPI) DEL INSTITUTO DE TRÁNSITO DEL ATLÁNTICO PARA LA VIGENCIA 2025 – 2028.** | | | |
|---|---|---|---|
| Código | No aplica | **Versión** | 1.0 |
| Vigencia | 2025 – 2028 | | |
| Creado por | Irwing Rafael Fontalvo Nieto<br>Profesional Universitario | **Fecha** | Enero, 2025 |
| Revisado por | Alix Arrieta<br>Jefe de Oficina Asesora de Planeación | **Fecha** | Enero, 2025 |
| Aprobado por | Comité de Gestión ITA | **Fecha** | Enero, 2025 |

| **Control de Cambios** | |
|---|---|
| **Fecha** | **Descripción** |
| 15 de enero de 2025 | Creación y elaboración de la versión 1.0 del Plan. |
| | |
| | |
| | |