



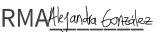
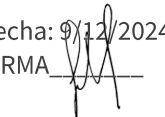

# PLANES OFICIALES

## PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

VERSIÓN 01

FECHA: 09/12/2024



ELABORÓ/ACTUALIZÓ	Jaiber Ortiz Valdés Profesional de TI	Fecha: 9/12/2024 FIRMA 
ELABORÓ/ACTUALIZÓ	María Alejandra González Jiménez Profesional de TI	Fecha: 9/12/2024 FIRMA 
REVISÓ	Sebastián Marín Loaiza Líder de infraestructura & TI	Fecha: 9/12/2024 FIRMA 
APROBÓ	Virmar Yessid David Valle Subdirector administrativo y financiero	Fecha: 11/12/2024 FIRMA 

## INDICE

INDICE .....	3
1. OBJETIVO.....	4
2. ALCANCE .....	4
3. REQUISITOS Y/O MARCO NORMATIVO .....	4
4. DEFINICIONES.....	5
5. RESPONSABILIDADES.....	8
6. DESARROLLO DEL PLAN .....	8

## 1. OBJETIVO

Diseñar, desarrollar e implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en cumplimiento del Modelo de Privacidad y Seguridad de la Información (MSPI), la Guía No. 7.3.3 – Plan de Tratamiento de Riesgos de Seguridad de la Información, y la Guía No. 8 – Controles de Seguridad y Privacidad de la Información. Este plan tiene como propósito establecer medidas y acciones concretas para identificar, modificar, reducir o eliminar riesgos asociados con la infraestructura de Tecnologías de la Información de la Corporación Ruta N. Además, se buscará garantizar un monitoreo continuo de la efectividad de las medidas adoptadas, promoviendo una cultura de mejora continua y alineación con las mejores prácticas internacionales en seguridad y privacidad de la información.

## 2. ALCANCE

El Plan se alinea con las directrices establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), que promueve la adopción del Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD) como referencia para la gestión de riesgos en organizaciones públicas, privadas o mixtas.

1. **Cumplimiento Normativo:** Aplicar el MSPI y las guías mencionadas, incorporando el MGRSD según lo dispuesto por MinTIC, con especial atención a las guías sectoriales requeridas y a las metodologías descritas en los documentos base.
2. **Adaptación a Contextos Existentes:** Construir sobre las metodologías o modelos de gestión de riesgos ya adoptados por la Corporación Ruta N, adaptando las recomendaciones del modelo y las guías, en consonancia con la premisa de “Construir sobre lo construido”.
3. **Cobertura Organizacional:** Garantizar que las medidas abarquen todos los niveles organizacionales, fomentando la integración de prácticas de seguridad y privacidad como componentes fundamentales de la transformación digital de la entidad.
4. **Reporte de Información de Riesgos:** Cumplir con las disposiciones de reporte establecidas por el Gobierno. Para entidades públicas, el reporte será obligatorio, mientras que para entidades privadas será opcional, alineándose con los lineamientos de transparencia y colaboración establecidos por MinTIC.
5. **Aplicación de Medidas:** Adoptar medidas dirigidas a modificar, reducir o eliminar riesgos relacionados con la infraestructura de Tecnologías de la Información de la Corporación Ruta N, con énfasis en proteger la seguridad digital y la privacidad de la información.
6. **Monitoreo y Mejora Continua:** Asegurar un monitoreo constante de las acciones implementadas para evaluar su efectividad, permitiendo la actualización del plan y el fortalecimiento de las estrategias de seguridad y privacidad en un entorno de mejora continua.

Este alcance asegura que la implementación del plan sea eficaz, adaptable y en consonancia con las mejores prácticas establecidas por MinTIC y los marcos regulatorios aplicables.

## 3. REQUISITOS Y/O MARCO NORMATIVO

El desarrollo y la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se fundamentan en las siguientes normativas y lineamientos:

### 1. Normas Técnicas Colombianas:

- **NTC ISO/IEC 27001 (versión vigente):** Proporciona políticas, definiciones y requisitos fundamentales para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI).

- **ISO/IEC 27005 (versión vigente):** Especifica las directrices para la gestión de riesgos relacionados con la seguridad de la información, detallando procesos para su identificación, evaluación y tratamiento.

*Nota:* Se tendrán en cuenta los anexos y contenidos asociados a estas normativas, que cuentan con derechos reservados por parte de ISO/CONTEC.

2. **Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información – MinTIC:**  
Este documento establece las directrices específicas para la identificación, análisis y tratamiento de riesgos de seguridad y privacidad de la información en el contexto colombiano.

La integración de estas normativas y guías asegura que el plan esté alineado con estándares internacionales, así como con los requerimientos y mejores prácticas definidas a nivel nacional.

## 4. DEFINICIONES

**Acceso a la información pública:** Derecho fundamental que consiste en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014)

**Actitud hacia el riesgo:** Enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del riesgo (NTC ISO 31000:2011).

**Activo:** Elementos de hardware o software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo (CONPES 3854:2016, pág.56).

**Amenaza cibernética:** Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (CONPES3854).

**Análisis del riesgo:** Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo (NTC ISO31000:2011).

**Apetito de riesgo:** Es el máximo nivel de riesgo que los accionistas están dispuestos a aceptar (Componente COSO ERM II).

**Ataque cibernético:** Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio (Ministerio de Defensa de Colombia).

**Ciberseguridad:** Conjunto de recursos, políticas, directrices, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio (CONPES 3854, pág. 87).

**Ciberterrorismo:** Uso del ciberespacio, con el propósito de generar terror o miedogeneralizado en la población, nación o Estado trayendo como consecuencia una violación a la voluntad de las personas (CONPES 3854, pág. 88).

**Ciberdelito/Delito cibernético:** Actividad delictiva relacionada con ordenadores y redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito (Ministerio de Defensa de Colombia).

**Ciberespacio:** Es el ambiente compuesto por computadores, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios (Resolución CRC 2258 de 2009).

**Cibernética:** Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas (Diccionario de la lengua española).

**Convergencia:** Evolución coordinada de redes que antes eran independientes hacia una uniformidad que permita el soporte común de servicios y aplicaciones (Rec. UIT-T Q.1761, 3.1).

**Consulta:** Proceso de comunicación informada entre una organización y sus partes involucradas, acerca de algún tema, antes de tomar una decisión o determinar una dirección para dicho tema (NTC ISO 31000 definición 2.12.).

**Compartir el riesgo:** Compartir con otra de las partes el peso de la pérdida o el beneficio de la ganancia proveniente de un riesgo particular (NTC ISO 31000:2011).

**Contexto externo:** Ambiente externo en el cual la organización busca alcanzar sus objetivos (NTC ISO 31000:2011).

**Contexto interno:** Ambiente interno en el cual la organización busca alcanzar sus objetivos (NTC ISO 31000:2011).

**Control:** Medida que modifica al riesgo (NTC ISO 31000:2011), medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización.

**Criterios del riesgo:** Términos de referencia frente a los cuales se evalúa la importancia de un riesgo (NTC ISO 31000:2011).

**Entorno digital:** Ambiente, sobre el cual se soporta la economía digital. Siendo esta la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías (CONPES3854, pág. 87).

**Entorno digital abierto:** Es aquel en el que no se restringe el flujo de tecnologías, comunicaciones o información, y en el que se asegura la provisión de los servicios esenciales (CONPES 3854, pág. 87).

**Evaluación del control:** Revisión sistemática de los procesos para garantizar que los controles son adecuados y eficaces (NTCISO 31000:2011).

**Evaluación del riesgo:** Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables (NTC ISO 31000:2011).

**Evento de seguridad de la información:** Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles (ISO/IEC 27035:2016).

**Evitar el riesgo:** Decisión de no involucrarse o de retirarse de una situación de riesgo (NTC ISO 31000:2011).

**Evento:** Presencia o cambio de un conjunto particular de circunstancias (NTC ISO 31000:2011).

**Fuente de riesgo:** Elemento que tiene el potencial intrínseco de originar un riesgo (NTC ISO31000:2011).

**Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo (NTC ISO 31000:2011).

**Gestión de riesgos de seguridad digital:** Conjunto de actividades coordinadas para abordar el riesgo de seguridad digital, es parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales (CONPES 3854, pág. 24).

**Identificación del riesgo:** Proceso para encontrar, reconocer y describir el riesgo (NTC ISO 31000:2011).

**Incidente digital:** Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos (CONPES 3854, pág. 87).

**Incidente de seguridad de la información:** Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información o comprometer sus operaciones. (ISO/IEC 27035:2016).

**Infraestructura crítica cibernética nacional:** Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales (CONPES 3854, pág. 29).

**Inventario de activos:** Aquellos recursos (físicos, de información, software, documentos, servicios, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos (ISO 27000:ES).

**Marco de referencia para la gestión del riesgo:** Conjunto de componentes que brindan las bases de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo (NTC ISO 31000:2011).

**Monitoreo:** Verificación, supervisión, observación crítica o determinación continua del Estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado (NTC ISO 31000:2011).

**Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad (NTC ISO 31000:2011).

**Parte involucrada:** Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada, por una decisión o una actividad (NTC ISO 31000:2011).

**Peligro:** Una fuente de daño potencial (NTC ISO 31000:2011).

**Pérdida:** Cualquier consecuencia negativa o efecto adverso, financiero u otro (NTC ISO 31000:2011).

**Perfil del riesgo:** Descripción de cualquier conjunto de riesgos (NTC ISO 31000:2011).

**Política:** Intenciones y dirección de una organización como las expresa formalmente su alta dirección (ISO/IEC 27000:2016).

**Posibilidad:** Se utiliza como descripción general de la probabilidad o la frecuencia (NTC ISO 31000:2011).

**Plan para la gestión del riesgo:** Esquema dentro del marco de referencia para la gestión del riesgo que especifica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la gestión del riesgo (NTC ISO 31000:2011).

**Probabilidad:** Oportunidad de que algo suceda (NTC ISO 31000:2011).

**Proceso para la gestión del riesgo:** Aplicación de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, establecimiento del contexto, análisis, evaluación, tratamiento y monitoreo (NTC ISO 31000:2011).

**Revisión:** Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos (NTC ISO 31000:2011).

**Reducción del riesgo:** Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo (NTC ISO 31000:2011).

**Resiliencia:** Es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha sido sometido a una perturbación a la que había estado sometido (CONPES 3854, pág. 87).

**Retención del riesgo:** Aceptación del peso de la pérdida o del beneficio de la ganancia proveniente de un riesgo particular (NTC ISO 31000:2011).

**Riesgo:** Efecto de la incertidumbre sobre los objetivos (NTC ISO 31000:2011).

**Riesgo inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto (NTC ISO 31000:2011).

**Riesgo residual:** Remanente después del tratamiento del riesgo (NTC ISO 31000:2011).

**Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, propiedades como autenticidad, responsabilidad, no repudio y confiabilidad (ISO/IEC 27001:2016).

**Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital, derivada de la realización de los fines esenciales del Estado mediante la gestión del riesgo de seguridad digital, la implementación efectiva de medidas de ciberseguridad y el uso efectivo de las capacidades de ciberdefensa (CONPES 3854, pág. 29).

**Servicios esenciales:** Los necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos (Tomado del documento ICC del CCOC).

**Sistema para la gestión del riesgo:** Conjunto de elementos del sistema de gestión de una organización involucrados en la gestión del riesgo (NTC ISO 31000:2011).

**Telecomunicaciones:** Transmisión y recepción de señales, escritos, imágenes y sonidos, datos o información de cualquier naturaleza por hilo, radiofrecuencia, medios ópticos u otros sistemas electromagnéticos (Resolución MinTIC 202 de 2010).

**TIC (Tecnologías de la información y las comunicaciones):** Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes (Ley 1341/2009 TIC).

**Tratamiento del riesgo:** Proceso para modificar el riesgo (ISO/IEC Guía 73:2009).

**Valoración del riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo. (ISO GUÍA 73:2009).

**Vulnerabilidad:** Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).

## 5. RESPONSABILIDADES

La implementación y el seguimiento del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información están distribuidos de la siguiente manera:

### Subdirección Administrativa y Financiera – Infraestructura TI:

- Liderar la ejecución del plan, asegurando la implementación de las acciones definidas en los cronogramas establecidos.
- Coordinar el monitoreo y seguimiento del cumplimiento de las medidas adoptadas, evaluando su efectividad y proponiendo ajustes cuando sea necesario.
- Actuar como el principal enlace técnico y administrativo para garantizar que las actividades del plan estén alineadas con los objetivos estratégicos de la organización.

### Direcciones y Subdirecciones de Apoyo:

- Brindar soporte y colaboración activa para facilitar la implementación de las acciones del plan en sus respectivas áreas.
- Asegurar la disponibilidad de recursos humanos, técnicos y financieros requeridos para la ejecución del plan.
- Garantizar la integración de las medidas de seguridad y privacidad de la información en los procesos, proyectos y operaciones bajo su gestión.

La colaboración entre Infraestructura TI y las demás áreas garantiza que el plan se implemente de manera integral, promoviendo la gestión efectiva de los riesgos y la consolidación de una cultura organizacional orientada a la seguridad y privacidad de la información.

## 6. DESARROLLO DEL PLAN

Para garantizar una gestión efectiva de los riesgos de seguridad y privacidad de la información, se ha definido el proceso que se ilustra en la Figura 1, basado en las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).



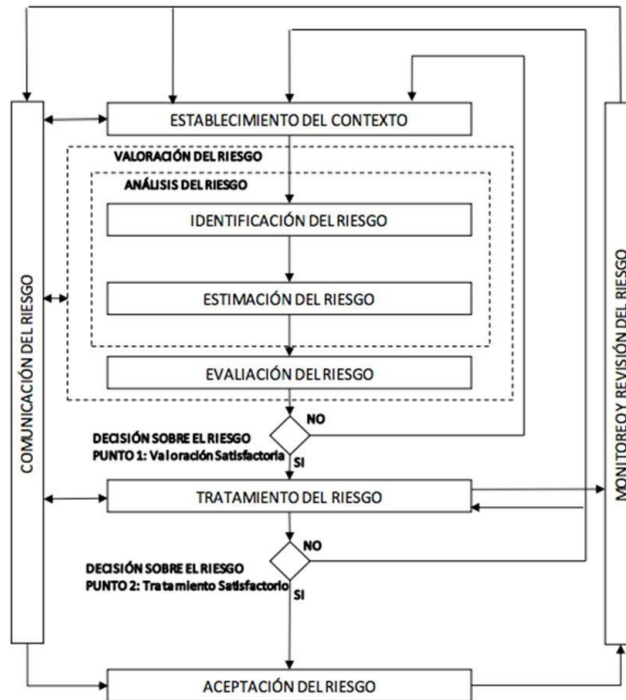


Figura 1. Proceso para la administración de Riesgos de Seguridad y Privacidad de la Información

Fuente: [https://www.mintic.gov.co/gestionti/615/articles-5482\\_G7\\_Gestion\\_Riesgos.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf)

La Matriz de Activos de Información será la base para la evaluación, identificando los activos que requieran medidas de seguridad específicas según su clasificación en criterios de confidencialidad, integridad y disponibilidad.

<b>ALTA</b>	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
<b>MEDIA</b>	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
<b>BAJA</b>	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Figura 2. Criterios de calificación.

Fuente: [https://www.mintic.gov.co/gestionti/615/articles-5482\\_G7\\_Gestion\\_Riesgos.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf)

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PÚBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Figura 3. Niveles de clasificación

Fuente: [https://www.mintic.gov.co/gestionti/615/articles-5482\\_G7\\_Gestion\\_Riesgos.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf)

**Actividades macro:**

El plan consta de dos actividades macro:

**1. Sensibilización Institucional sobre Política de Seguridad de la Información.**

- **Objetivo:** Divulgar las directrices de uso de los sistemas de información y fomentar el cumplimiento de las políticas y procedimientos de seguridad establecidos por la Corporación.
- **Acciones:**
  - Realizar sesiones de capacitación en colaboración con el área de Marca y comunicaciones.
  - Socializar las políticas de seguridad de la información, dirigidas a todo el personal, tanto vinculados, como contratistas.
- **Consideraciones:**
  - Las capacitaciones son obligatorias y se relacionan directamente con la posibilidad de imponer sanciones en caso de incumplimientos.
  - Las capacitaciones incluirán buenas prácticas de seguridad en función de los roles y responsabilidades del personal.

**2. Campañas capsula para divulgación de medidas de seguridad por medio de campañas publicitarias internas.**

- **Objetivo:** Aumentar la conciencia sobre la importancia de implementar buenas prácticas de seguridad y privacidad a través de comunicaciones internas.
- **Acciones:**
  - Enviar campañas de sensibilización por correo interno, abordando los siguientes temas:
    - Incumplimiento al principio de legalidad en el tratamiento de datos.
    - Carencia de finalidad en el manejo de datos.
    - Divulgación no autorizada de datos.
    - Falta de calidad y veracidad en el tratamiento de datos.
    - Incumplimiento de los principios de transparencia, acceso, circulación restringida y seguridad en el tratamiento de datos.
    - Ausencia del principio de confiabilidad en el tratamiento de datos.

**Indicadores de desempeño:**

**Porcentaje de Implementación de Controles:**

$$\text{Porcentaje de implementación: } \frac{\text{Número de controles implementados}}{\text{Total de controles planificados}} \times 100$$

**Número de controles implementados:** Cantidad de controles o medidas de seguridad que se han implementado de acuerdo con el plan.

**Total de controles planificados:** Controles totales que se han definido en el plan de tratamiento de riesgos, basados en los riesgos identificados y priorizados.

**Frecuencia de medición:** Mensual, trimestral o según el cronograma del plan.