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

REGIÓN ADMINISTRATIVA Y DE PLANEACIÓN ESPECIAL
RAP-E REGION CENTRAL

DIRECCIÓN ADMINISTRATIVA Y FINANCIERA
PROCESO DE GESTIÓN TIC
2026

BOGOTÁ BOYACÁ CUNDINAMARCA META TOLIMA HUILA

REGIÓN CENTRAL
RAP-E | Estamos Construyendo Región

Tabla de contenido

I. Introducción 3
II. Definiciones 3
III. Objetivos 4
IV. Articulación institucional y normativa 4
V. Alcance 4
VI. Desarrollo del plan 4
VII. Normatividad 7
VIII. Cronograma 8
IX. Control de cambios 9

I. Introducción

La Región Administrativa y de Planificación Especial (RAP-E) es consciente de la necesidad de velar por la seguridad y la privacidad de la información, para contribuir a la confianza de las partes interesadas y a garantizar las oportunidades de alcanzar su estrategia institucional, pues en la sociedad del conocimiento, cada vez más interconectada y amenazada, es necesario garantizar un marco sistematizado y definido para identificar, valorar y, cuando sea necesario, minimizar los riesgos que puedan amenazar la confidencialidad, integridad y disponibilidad de la información.

Este documento, el Plan de Tratamiento de Riesgos de Seguridad de la Información y Privacidad de la Información, recoge la forma en que la RAP-E quiere afrontar la Gestión de la Seguridad de la Información, convirtiendo en acciones los riesgos que se hayan identificado e incorporando, desde su inicio, las acciones diseñadas para la reducción de riesgos. Este documento se ha elaborado en línea con normas nacionales y estándares internacionales pertinentes, con la intención de establecer un proceso formal y sistemático que dé soporte a la misión de la RAP-E para la gestión de la seguridad de la información basado en la mejora continua.

II. Definiciones

1. **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
2. **Riesgo de Seguridad de la Información**: 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. (ISO/IEC 27000).
3. **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
4. **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
5. **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.
6. **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.
7. **Control o Medida:** Medida que permite reducir o mitigar un riesgo.
8. **Propietario del riesgo:** Persona o Entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
9. **Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
10. **Valoración del riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
11. **Tratamiento del Riesgo:** Proceso para modificar el riesgo.
12. **Triada de la información:** Conjunto de las propiedades derivadas de la Confidencialidad, Integridad y Disponibilidad de la Información.

III. Objetivos

1. Garantizar la protección de los activos de información y minimizar los riesgos asociados a estos.
2. Determinar y asignar controles específicos para cada riesgo identificado, diseñando un plan de implementación que contribuya a su mitigación.
3. Monitorear y dar seguimiento a los planes de manejo establecidos para el tratamiento de los riesgos detectados.

IV. Articulación institucional y normativa

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la RAP-E Región Central se articula con el Modelo Integrado de Planeación y Gestión – MIPG, en especial con la dimensión de Control Interno y el habilitador de Seguridad y Privacidad de la Información de la Política de Gobierno Digital.

Así mismo, este Plan da cumplimiento a lo dispuesto en el Decreto 612 de 2018, integrándose como instrumento de planeación institucional, alineado con el Plan Estratégico Institucional, el Plan de Acción Anual y el Plan Estratégico de Tecnologías de la Información – PETI, contribuyendo a la gestión integral del riesgo y a la mejora continua de la seguridad de la información en la Entidad.

V. Alcance

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la RAP-E es aplicable a los activos de Información que se han identificado y que pertenecen a la Entidad. Este plan comprende la identificación, el análisis, la valoración y el tratamiento de los riesgos de la información y, por tanto, incluso aquellos que ponen en peligro la confidencialidad, la integridad, la disponibilidad de la información y la privacidad.

El Plan incluye las acciones que sean necesarias para implementar y dar seguimiento a los controles que se hayan determinado, atendiendo los requerimientos legales, reglamentarios y estándares aplicables y asegurando la protección de la información en relación con las amenazas externas e internas.

VI. Desarrollo del plan

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la RAP-E, se basa en dos documentos fundamentales que establecen los lineamientos necesarios para la gestión de riesgos de las entidades públicas colombianas: la Guía para la Administración del Riesgo y el Diseño de Controles en las

Entidades Públicas que emite el Departamento Administrativo de la Función Pública (DAFP) y la Guía de Gestión de Riesgos que emite el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

- **Análisis de la información**

En la identificación del riesgo empieza en identificando, clasificando y actualizando los activos de la información de cada área de la entidad. Esta actividad, que ha de ser la base de la gestión de la seguridad de la información, se tiene que llevar a cabo un estudio exhaustivo que permita clasificar estos activos según su relación con la importancia o sensibilidad, y que permita representar plenamente su valor estratégico.

El responsable del área será el que llevará a cabo todo el proceso de identificar, clasificar y priorizar los activos que hayan recibido una calificación de riesgo alto, priorizarlos de acuerdo con determinados criterios y objetivos claros que habrán de estar sustentados en un documento elaborado a tal fin. El responsable también habría de incluir en el proceso de la identificación aquellos activos que, aun no recibiendo una calificación de riesgo alto, son de interés para la gestión del riesgo por sus usos, su naturaleza, o su importancia estratégica.

Este enfoque propone una manifestación de un proceso integral, sistemático y global respecto la seguridad de la información alineando los riesgos y necesidades de cada proceso institucional con la estrategia general de gestión de riesgos de la entidad y, de esta manera, garantizando una mejor protección de los activos relevantes.

- **Identificación de riesgos**

Por consiguiente, identificar riesgos implica analizar y valorar las amenazas y vulnerabilidades que pueden llegar a comprometer los activos de información, puntos del análisis que analizaran las consecuencias de un suceso, las probabilidades de que se produzca el suceso y los impactos que puede producir sobre la seguridad de la información. Este análisis se centra en cómo cada amenaza detectada puede comprometer la integridad, la confidencialidad y la disponibilidad de la información.

Este proceso tiene en cuenta la naturaleza de la amenaza (interna o externa), la naturaleza de los activos comprometidos y el contexto de operaciones de la entidad. Una vez que un riesgo ha sido identificado, se calculará el nivel de riesgo aplicando un conjunto de procedimientos que relacionan la probabilidad con la magnitud del impacto objetivo, de forma que se priorizan tanto aquellos riesgos de producto frecuente, como los riesgos de alto impacto y baja probabilidad.

Se trata de un enfoque con un carácter dinámico y en transformación; capaz de adaptarse a las transformaciones del ámbito operativo, al mismo tiempo que las amenazas y vulnerabilidades son detectadas. La correcta identificación de los riesgos es la base para poder avanzar en las estrategias de mitigación alcanzando una gestión de riesgos de seguridad de la información integral y proactiva.

- **Evaluación y análisis del riesgo**

En la gestión de riesgos de seguridad de la información, se caracterizan en el análisis del riesgo y en la evaluación del riesgo, criterios de valores específicos, los cuales son fundacionales para un recorrido estructurado y que no presenta incoherencias.

Análisis del Riesgo:

En esta fase analítica, las fuentes de riesgo, los tipos de amenazas y vulnerabilidades y la forma como interaccionan y afectan los activos de información, son todos los elementos que se deben tener en cuenta. Esta fase analítica incorpora incluso la interrelación de distintos riesgos al analizar cómo pueden influir e intensificarse mutuamente. De esta forma, es además la fase que permite disponer de una visión más completa de todas las circunstancias que podrían dañar los activos de información y comprometer la seguridad de la información.

Evaluación del Riesgo:

Una vez realizada la fase de análisis le sigue la fase de evaluación de los riesgos detectados. Esta fase implica una determinación de la probabilidad de que cada riesgo ocurra y del impacto potencial de este. Los criterios en esta fase para llevar a cabo la evaluación han de ser especificados y lo más comunes posible, ya que el objetivo de la evaluación de riesgos es valorar el nivel de riesgo inherente a los activos seleccionados. Los criterios incluyen la existencia de escalas cuantitativas o cualitativas, así como la determinación de la probabilidad de ocurrencia de un riesgo a partir de proveedores de información como parámetros de evaluación, como la severidad de la posible pérdida, los activos vulnerables y el flanco de la entidad para controlar los riesgos de forma efectiva.

Esta forma de proceder es lo que garantiza que la gestión de riesgos sea exhaustiva, sistemática y tiene que ir orientada a la decisión que se deben priorizar para proteger los activos de información de la entidad.

La evaluación del riesgo se realiza a partir de la combinación de la probabilidad de ocurrencia y el impacto asociado, utilizando criterios cualitativos definidos por la Entidad.

El tratamiento del riesgo podrá contemplar una o varias de las siguientes opciones: mitigar, aceptar, transferir o evitar el riesgo, de acuerdo con su nivel y con los criterios de aceptación definidos por la RAP-E. El riesgo residual resultante será objeto de seguimiento periódico para verificar la efectividad de los controles implementados.

- **Control del riesgo**

Se implementan medidas específicas para mitigar o reducir la probabilidad y el impacto de los riesgos identificados. Esto implica la selección y aplicación de controles adecuados, tanto técnicos como organizativos, que puedan abordar las amenazas y vulnerabilidades de manera efectiva. Los controles incluyen, pero no se limitan a, la encriptación de datos, la autenticación multifactor, la capacitación del personal y la definición de políticas de acceso. Además, se debe realizar un monitoreo continuo para asegurar que estos controles permanezcan eficaces, realizando ajustes cuando sea necesario para adaptarse a cambios en el panorama de riesgos o a nuevas amenazas que puedan surgir. Esta actividad busca garantizar la protección de la información y minimizar los riesgos asociados a incidentes de seguridad.

- **Monitoreo y revisión de riesgos**

El monitoreo y revisión de los riesgos se realizará de manera semestral por el Proceso de Gestión TIC, mediante la verificación del cumplimiento de los controles definidos, el análisis de incidentes de seguridad y la identificación de cambios en el contexto institucional o tecnológico, con el fin de actualizar el mapa de riesgos y fortalecer la mejora continua.

- **Desarrollo del plan**

Para la correcta implementación y seguimiento del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se definen los siguientes roles y responsabilidades:

- **Alta Dirección:** Aprobar el Plan, respaldar la asignación de recursos y tomar decisiones frente a riesgos críticos.
- **Proceso de Gestión TIC:** Liderar la identificación, análisis, tratamiento y seguimiento de los riesgos de seguridad y privacidad de la información.
- **Propietarios de los activos de información:** Identificar y valorar los riesgos asociados a los activos bajo su responsabilidad y apoyar la implementación de controles.
- **Usuarios de la información:** Cumplir las políticas, lineamientos y controles definidos para la protección de la información.

VII. Normatividad

1. Ley 1581 de 2012 - Ley de Protección de Datos Personales: Esta ley establece las disposiciones generales para la protección de los datos personales en Colombia

2. Decreto 1377 de 2013: Este decreto reglamenta la Ley 1581 de 2012, estableciendo las condiciones en las que los datos personales pueden ser tratados, y las excepciones a la obligación de obtener el consentimiento del titular de los datos en ciertas circunstancias.

3. Ley 1266 de 2008 - Derecho de Habeas Data: Esta ley establece el derecho de los ciudadanos a conocer, actualizar y rectificar la información personal que se encuentra en bases de datos. Además, regula la protección de la información financiera.

4. Ley 1273 de 2009 - Delitos Informáticos: La Ley 1273 establece las sanciones y medidas para prevenir y sancionar delitos informáticos, como el acceso no autorizado a sistemas, la alteración de información y la interceptación de comunicaciones.

5. Norma Técnica NTC-ISO/IEC 27001:2013 - Sistema de Gestión de Seguridad de la Información (SGSI): Aunque no es exclusiva de Colombia, esta norma es ampliamente adoptada por las organizaciones colombianas para gestionar la seguridad de la información. Establece un sistema de gestión de seguridad de

la información (SGSI) y proporciona un marco para identificar, evaluar y tratar los riesgos asociados a la seguridad de la información.

6. Superintendencia de Industria y Comercio (SIC): La SIC es la entidad encargada de la supervisión y vigilancia del cumplimiento de la Ley 1581 de 2012 y otras normativas relacionadas con la protección de datos personales.

7. Circular Externa 029 de 2021 de la Superintendencia de Industria y Comercio: Esta circular proporciona directrices adicionales sobre la gestión de riesgos en el tratamiento de datos personales, especialmente en cuanto a la implementación de medidas de seguridad para proteger los datos personales y evitar brechas de seguridad.

VIII.Cronograma

Para alcanzar los objetivos del plan, se presenta el siguiente cronograma de actividades que detalla los temas a tratar y los canales de comunicación a utilizar para su divulgación.

Actividad	Descripción	Duración	Responsable	Entregable
Actualizar la documentación del PTRSP.	Actualizar y publicar guías y formatos del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	I Trimestre	Gestión TIC	Documentos actualizados y publicados.
Identificación y evaluación de riesgos	Identificar activos críticos, evaluar amenazas, vulnerabilidades, y analizar el impacto y la probabilidad de los riesgos.	II Trimestre	Gestión TIC	Formato Mapa de Riesgos RAP-E
Selección de controles y políticas	Seleccionar y diseñar controles de seguridad y políticas de tratamiento de datos.	III Trimestre	Gestión TIC	Formato Mapa de Riesgos RAP-E, controles y planes de mejora asociados.
Capacitación y concienciación	Capacitar al personal en medidas de seguridad, políticas de privacidad y manejo de datos personales.	Anual	Gestión TIC	Listado de asistencia.

Monitoreo, revisión y mejora continua	Monitorear el desempeño de los controles, realizar auditorías periódicas y ajustar el plan según los incidentes y cambios en el entorno.	Semestral	Gestión TIC	Informe de seguimiento.

IX.Control de cambios

VERSIÓN	FECHA	PROCESO	DESCRIPCIÓN
1	Enero 2025	Gestión TIC	Versión inicial
2	Enero 2026	Gestión TIC	Se incluyo el apartado de Articulación institucional, normatividad y Desarrollo de plan.