TABLA DE CONTENIDO

1. INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer la disponibilidad, integridad y confiabilidad de la información.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2022, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - emitida por el DAFP.

2. OBJETIVO

Realizar la identificación, análisis, valoración y tratamiento de los riesgos y controles de seguridad de la información a los procesos del - RAP EJE CAFETERO - Región Administrativa y de Planificación.

3. ALCANCE

El plan está proyectado para aplicar a los activos de información que hacen parte de los procesos de las operaciones procesos del - RAP EJE CAFETERO - Región Administrativa y de Planificación.

La gestión de riesgos de seguridad de la información se realiza con base a la metodología del Departamento Administrativo de Función Pública (DAFP), el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD) y para la identificación de controles se tiene como referencia la norma ISO 27001 e ISO 27002.

4. DEFINICIONES

Con el propósito de facilitar la comprensión de este documento se describen las siguientes definiciones:

- **Activo de Información:** Todo lo que tiene valor para la Entidad y que contiene, genera, procesa, almacena y le da un tratamiento a la información o se relaciona con la misma. Existen diferentes tipos de activos como: Información (bases de datos, bases de conocimiento), tecnológicos o digitales (hardware y software), infraestructura física (instalaciones, oficinas), organizacionales (procesos, metodologías, servicios) y el recurso humano (Empleados de Planta, Contratistas, proveedores, Terceros).

- **Ciberseguridad**: Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan.

- **Confidencialidad:** Atributo de la información que determina quién está autorizado a acceder a la información y previene su divulgación no autorizada dentro de la Entidad.

- **Contraseña Fuerte:** Contraseña que consta mínimo de nueve caracteres, mayúsculas, minúsculas, números y caracteres especiales.

- **Control:** las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

- **Copias de Seguridad:** Es el proceso mediante el cual se realiza la copia de la información existente, con el fin de poder recuperarla en caso de que ocurra un fallo que afecte a esta y pueda estar disponible.

- **Custodio de activo de información**: Parte designada de la organización, un cargo, proceso, o grupo de trabajo encargado de administrar, modificar, leer, procesar y hacer efectivos los controles de seguridad definidos, tales como copias de seguridad.

- **Disponibilidad:** Atributo de la información que determina para quién está disponible y los permisos de su uso dentro de las gestiones que se adelanten en la Entidad.

- **Gestión de claves:** son controles que se realizan mediante la gestión de claves criptográficas.

- **Gestión de incidentes de seguridad de la información:** Son las acciones de control para garantizar la seguridad de los activos de información y su apropiada gestión, implementando las acciones para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información en la RAP.

- **Gestión de riesgos:** Son las acciones que realiza la RAP para la identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

- **Impacto**: El costo para la organización de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc. Consecuencia que sobre un activo tiene la materialización de una amenaza.

- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que compromete a la Entidad.

- **Información:** Es un activo de valor que hace parte de la Agencia Nacional Digital, por la cual asume funciones como responsable o encargada de la misma en cumplimiento de los requisitos legales, normativos e institucionales. La información corresponde a todo dato de la Entidad (tecnológico, administrativo, financiero, contable, entre otros), propio o de Terceros con las cuales dispone de un acuerdo o convenio; y datos personales de las cuales asume un rol como responsable o encargado.

- **Integridad:** Atributo de la información que protege los activos de información sobre posibles alteraciones, modificaciones no autorizadas formalmente por la Entidad.

- **Inventario de activos:** lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la RAP y necesiten por tanto ser protegidos de potenciales riesgos.

- **Plan de continuidad del negocio:** plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

- **Principios de Seguridad de la Información**: son características propias de la protección de la información: la Confidencialidad, Integridad y Disponibilidad.

- **Proceso:** conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

- **Responsable de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

- **Riesgo:** Es la probabilidad de que una amenaza o vulnerabilidad pueda ocasionar la pérdida y/o alteración de la información de la RAP.

- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Sistema de Gestión de Seguridad de la Información (SGSI):** Es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la Accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información

- **Vulnerabilidad:** Es la debilidad o fallo del sistema que pone en riesgo la confidencialidad, integridad y disponibilidad de la información de la Entidad.

- **Norma:** Principio que se dispone de carácter general, donde se establecen las obligaciones, restricciones y orientaciones para el acceso y uso de los activos de información.

- **Política:** Declaración de alto nivel que describe la posición de la RAP sobre un tema específico.

- **Procedimiento:** Documento que define los pasos a seguir y que deben ser implementados en una situación dada.

5. DOCUMENTOS DE REFERENCIA

- **Guías de implementación del MSPI – Mintic.** 1. articles-5482 Modelo de Seguridad Privacidad.
- **ISO 27001.** Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.
- **ISO 27002.** Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.
- **ISO 27005.** Gestión de Riesgos de Seguridad de la Información.
- **ISO 27017.** Código de buenas prácticas de seguridad servicios en la nube.
- **ISO 27018.** Código de práctica protección de información personal en nubes públicas.
- **ISO 27035.** Buenas prácticas de gestión de incidentes de seguridad de información.
- **ISO 22301.** Requisitos Sistema de Gestión de la Continuidad del Negocio.
- **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas**. Guía de gestión de riesgos del DAFP.
- **NIST framework Ciberseguridad**, es el marco que permite a las organizaciones comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos, proporciona un lenguaje común y un resumen de las mejores prácticas en ciberseguridad.
- **Ley 1581 de 2012.** Protección datos personales. Circular 005 de 2017 SIC (Países Autorizados).
- **Ley 1712 de 2014.** Transparencia y del Derecho de Acceso a la Información Pública.
- **Ley 1273 de 2009.** Delitos informáticos
- **Ley 597 de 1999.** Acceso y uso mensajes de datos, comercio electrónico y firmas digitales.
- **Ley 23 de 1982**. Derechos de autor.

- **Ley 594 de 2000**. Ley general de archivo.
- **Decreto 2578 de 2012.** Reglamenta el Sistema Nacional de Archivos
- **CONPES 3854 de 2016** – Política de Seguridad Digital del Estado Colombiano.
- **Decreto 1008 de 2018**. Política de gobierno digital.
- **Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD)**
- **Decreto 620 de 2020**. Lineamientos generales en el uso y operación de los Servicios Ciudadanos Digitales.
- **Resolución 1519 de 2020.** Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

6. DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1. Política de Administración de riesgos

La Región Administrativa y de Planificación - RAP EJE CAFETERO - a través de su Modelo Integrado de Gestión, se compromete a mantener una cultura de la gestión del riesgo de seguridad y privacidad de la Información y Seguridad Digital de manera Integral.

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos y establecen las guías de acción necesarias a todos los colaboradores de la Entidad.

Se deben tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

- Evitar: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área.

- Prevenir: corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos

- Reducir o mitigar: corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia, planes de continencia, equipos de protección personal, ambiental, de acceso, mantener copias de respaldo.

- Dispersar: es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos.

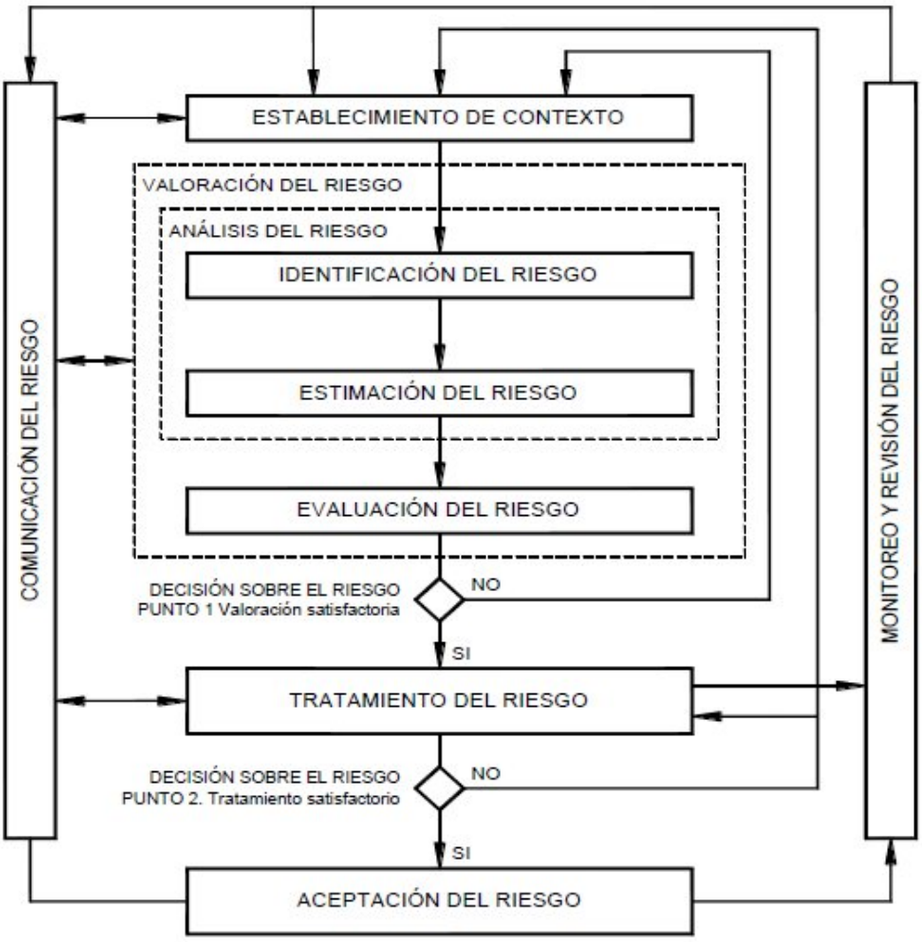
- Compartir: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explicita por medio de cláusulas contractuales, derivados financieros.

Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento. Así mismo, teniendo en cuenta lo expuesto en la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)1, las "*(…) no se debe olvidar que dentro del análisis de los controles se debe tener en cuenta al dueño del riesgo (dueño del proceso), ya que la definición de los controles es el resultado de los análisis realizados a través del seguimiento y aplicación de los pasos descritos anteriormente en el tratamiento del riesgo y los cuales deben tener el concurso de todos los interesados*"(…).

6.2. Metodología

La metodología de gestión de identificación, evaluación y gestión de riesgos de seguridad y privacidad de la información de la RAP, se basa en la NTC-ISO 27005, la Guía de Gestión del Riesgo del Departamento Administrativo de la Función Pública - DAFP y la Guía de la Secretaria de Transparencia de la Presidencia de la República, denominada Guía para la Gestión de Riesgo de Corrupción y Modelo de Gestión de Riesgos de Seguridad Digital - MGRSD. Su propósito es la identificación, estimación y evaluación de los riesgos de la Entidad para definir un plan de tratamiento que se ajuste a los objetivos de cada uno de los procesos.

6.3. Ciclo de Gestión de Riesgos



Contexto - Información sobre la evaluación de riesgos

Se establece un contexto del proceso con los siguientes aspectos:

- Contexto del Proceso: Se determinan las características o aspectos esenciales del proceso y sus interrelaciones.
- Diseño del proceso: Claridad en la descripción del alcance y objetivo del proceso.
- Interrelación con otros procesos: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
- Transversalidad: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
- Procedimientos asociados: Pertinencia en los procedimientos que desarrollan los procesos.
- Responsables del proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
- Comunicación entre los procesos: Efectividad en los flujos de información determinados en la interacción de los procesos.

Y luego se establece el tipo de proceso: Misional, Estratégicos, de Apoyo y Evaluación y Control.

Análisis de riesgos

Se realiza la identificación de causas, vulnerabilidades, amenazas (identificación, descripción, tipo), consecuencias y se determina la clase de riesgo (probabilidad e impacto), todo esto asociado a aquellos eventos o situaciones que afecten los activos de información que pueden entorpecer el normal desarrollo de los procesos.

Tratamiento de Riesgos

El tratamiento del riesgo consiste en seleccionar y aplicar las medidas adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos, para lo cual se definen Medidas de Respuesta ante los Riesgos (asumir, reducir, compartir, trasferir o evitar), luego se definen acciones de mitigación de riesgos (actividades o tareas, responsables, plazo de ejecución y seguimiento).

Comunicación de Riesgos

Participan todos los procesos e involucran a todos los colaboradores para el levantamiento de los mapas de riesgo, contando con el aporte de los colaboradores con mayor experticia tanto para la identificación como para el tratamiento de riesgos.

Cuando se identifica un riesgo la RAP suministra, comparte u obtiene información a través de un diálogo con las partes involucradas con respecto a la gestión del riesgo. La información está relacionada con la existencia, la naturaleza, la forma, la probabilidad, el significado, la evaluación, la aceptabilidad y el tratamiento de la Gestión de riesgo.

Monitoreo - Información de Riesgos y revisión

Los riesgos identificados traen consigo controles que incluyen el monitoreo de los eventos correspondientes, invirtiendo los recursos de acuerdo a la criticidad del riesgo asociado, las responsabilidades del monitoreo comprenden todos los aspectos del proceso para la gestión del riesgo con el fin de:

- Garantizar que los controles son eficaces y eficientes tanto en el diseño como en la operación.
- Obtener información adicional para mejorar la valoración del riesgo.
- Analizar y aprender lecciones a partir de los eventos.
- Detectar cambios en el contexto externo e interno, incluyendo los cambios en los criterios de riesgo y en el riesgo mismo que puedan exigir revisión de los tratamientos del riesgo y las prioridades.

6.4. Mapa de Ruta

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información.

ACCIONES	RESPONSABLE	FECHA INICIO	FECHA FIN	RESULTADO
Actualizar política y metodología de gestión de riesgos.	-Contratistas Sistemas -Comité MIPG	01-Feb-2026	28-Feb-2026	Política y metodología
Socialización de la guía y herramienta de gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	-Contratistas Sistemas -Comunicaciones	01-Mar-2026	15-Mar-2026	
Identificación, análisis y evaluación de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	-Contratistas Sistemas -Líderes de Procesos	16-Mar-2026	15-Jun-2026	Matriz de Riesgos
Retroalimentación, revisión y verificación de los riesgos identificados (ajustes)	-Contratistas Sistemas -Líderes de Procesos	16-Jun-2026	30-Jun-2026	Matriz de Riesgos
Aceptación, aprobación riesgos identificados y planes de tratamiento	-Contratistas Sistemas -Comité MIPG	01-Jul-2026	15-Jul-2026	Actas de Reunión Matriz de Riesgos
Publicación y socialización matriz de riesgos	- Contratistas Sistemas -Comunicaciones	16-Jul-2026	30-Jul-2026	Link de Transparencia
Tratamiento de riesgos identificados	-Contratistas Sistemas	01-ago-2026	1-dic-2026	Matriz de Riesgos
Evaluación riesgos residuales	-Contratistas Sistemas	01-ago-2026	31-dic-2026	Matriz de Riesgos
Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	-Contratistas Sistemas -Líderes procesos De	01-ago-2026	31-dic-2026	

Actualización gestión de riesgos seguridad de la información, de acuerdo a los cambios solicitados	-Contratistas Sistemas	01-ago-2026	31-dic-2026	
Generación, presentación y reporte de indicadores seguimiento de riesgos de seguridad y privacidad de la información	-Contratistas Sistemas	01-ago-2026	31-dic-2026	Informe de riesgos