



**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN  
2025**



**GOBERNACIÓN DE ANTIOQUIA**  
República de Colombia



**Maria Cristina Giraldo Ospina**  
Directora de Tecnología e Información

# **Dirección de Tecnología e Información**

2025



**GOBERNACIÓN DE ANTIOQUIA**  
República de Colombia



## TABLA DE CONTENIDO

INTRODUCCIÓN.....	¡ERROR! MARCADOR NO DEFINIDO.
1. GENERALIDADES.....	¡ERROR! MARCADOR NO DEFINIDO.
2. OBJETIVO.....	¡ERROR! MARCADOR NO DEFINIDO.
2.1. OBJETIVOS ESPECÍFICOS.....	¡ERROR! MARCADOR NO DEFINIDO.
3. ALCANCE.....	¡ERROR! MARCADOR NO DEFINIDO.
4. MARCO NORMATIVO.....	¡ERROR! MARCADOR NO DEFINIDO.
5. DEFINICIONES.....	¡ERROR! MARCADOR NO DEFINIDO.
6. ESTADO ACTUAL DE LA ENTIDAD.....	¡ERROR! MARCADOR NO DEFINIDO.
6.1. RESPONSABLES EN SEGURIDAD DE LA INFORMACIÓN.....	¡ERROR! MARCADOR NO DEFINIDO.
6.2. RESULTADO FURAG.....	¡ERROR! MARCADOR NO DEFINIDO.
6.3. EJECUCIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI).....	¡ERROR! MARCADOR NO DEFINIDO.
7. ESTRATEGIA DE SEGURIDAD DIGITAL.....	¡ERROR! MARCADOR NO DEFINIDO.
7.1. DESCRIPCIÓN DE LA ESTRATEGIAS.....	¡ERROR! MARCADOR NO DEFINIDO.
7.2. PORTAFOLIO DE PROYECTOS Y PRODUCTOS ESPERADOS.....	¡ERROR! MARCADOR NO DEFINIDO.
7.3. CRONOGRAMA DE PROYECTOS.....	¡ERROR! MARCADOR NO DEFINIDO.
8. DOCUMENTOS DE REFERENCIA.....	¡ERROR! MARCADOR NO DEFINIDO.
TABLAS.....	¡ERROR! MARCADOR NO DEFINIDO.
IMÁGENES.....	¡ERROR! MARCADOR NO DEFINIDO.





## 1. INTRODUCCIÓN

La Gobernación de Antioquia, establece el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información, con el cual busca mitigar los riesgos que afecta la Confidencialidad, Integridad y Disponibilidad de los activos de información.

En este sentido, se proyectan acciones que reduzcan la afectación a la Entidad en caso de una eventual materialización; al igual a que desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con el fin de evitar escenarios que impidan el logro de los objetivos de la Entidad.

El presente Plan se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes y posibles eventos que puedan llegar a materializarse; lo anterior, dando cumplimiento a la normatividad legal vigente y los requisitos establecidos por las partes interesadas en la gestión de la Información.

## 2. DEFINICIONES

- Activos de Información:** Los activos de información son datos o información propietaria en medios electrónicos, impreso o entre otros medios, considerados sensitivos o críticos para los objetivos del proceso.
- 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).
- Confidencialidad:** La información no se pone a disposición ni se revela a individuos, Entidades o procesos no autorizados.
- Control o Medida:** Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una Entidad.
- Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, Entidades o procesos autorizados cuando lo requieran.
- Evento de Seguridad de la Información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.





**GOBERNACIÓN DE ANTIOQUIA**  
República de Colombia

<b>Incidente de seguridad de la Información:</b>	de la	Un evento o serie de eventos de seguridad de la Información no deseados o inesperados, que tiene una la probabilidad significativa de comprometer las operaciones del negocio o amenazar la seguridad de la información de los activos críticos que almacenen, procesen y/o gestionen información.
<b>Integridad:</b>		Propiedad de Salvaguardar la exactitud y estado completo de los activos.
<b>Impacto:</b>		Son las consecuencias que genera un riesgo una vez se materialice.
<b>Vulnerabilidad:</b>		Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

### 3. OBJETIVO

Establecer y desarrollar un Plan de Tratamiento con el fin de gestionar los riesgos de Seguridad de la Información tomando como marco de referencia la metodología de riesgos de la Gobernación de Antioquia, con la finalidad de preservar la Confidencialidad, Integridad y Disponibilidad de los activos de información de la Entidad.

### 4. ALCANCE

Este plan se enfocará en la identificación, análisis, evaluación, tratamiento y seguimiento de riesgos asociados a los activos de información de la Gobernación de Antioquia.

### 5. MARCO DE REFERENCIA

La Gobernación de Antioquia debe evaluar sus prácticas procesos existentes de la administración y/o gestión de riesgos y evaluar cualquier brecha de seguridad.





**GOBERNACIÓN DE ANTIOQUIA**  
República de Colombia

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información de la Gobernación de Antioquia, contempla y define actividades a desarrollar en aras de mitigar los riesgos sobre los activos para lo cual se estructura las siguientes actividades:

ACTIVIDAD	TAREA	RESPONSABLE DE LA TAREA	RECURSOS	FECHAS PROGRAMADAS	
				FECHA INICIO	FECHA FIN
Identificación y valoración de riesgos de seguridad de la información con cada proceso de la Entidad.	Realizar mesas de trabajo para la identificación, análisis y evaluación de riesgos de Seguridad Digital.	Dirección de Desarrollo Organizacional.  Todos los Procesos de la Gobernación de Antioquia.	Recurso Humano  Recurso Técnico  Recursos Logísticos	2025	2025
	Aceptación y aprobación de la Matriz de Riesgos de Seguridad Digital y su Plan de Tratamiento.	Dirección de Desarrollo Organizacional.  Todos los Procesos de la Gobernación de Antioquia.	Recurso Humano  Recursos Logísticos  Recurso Financiero	2025	2025
	Publicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Dirección de Desarrollo Organizacional.	Recurso Humano  Recurso Tecnológico	2025	2025
Seguimiento al plan de tratamiento de riesgos de seguridad de la información	Seguimiento al estado del plan de tratamiento de Riesgos de Seguridad identificados y verificación de evidencias.	Dirección de Desarrollo Organizacional.	Recurso Humano  Recurso Técnico  Recursos Logísticos  Recurso Financiero  Recurso Tecnológico	2025	2025
	Evaluación de los Riesgos Residuales.	Dirección de Desarrollo Organizacional.	Recurso Humano  Recurso Financiero	2025	2025

**Tabla No. 1 – Actividades del Plan de Tratamiento.**







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

Como primera medida, se debe tener en cuenta que la “Política de Seguridad Digital” vincula al Modelo de Seguridad y Privacidad de la Información (MSPI)<sup>1</sup>, el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta los habilitadores de la “Política de Gobierno Digital”.

El proceso de gestión de riesgos implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de:

- Comunicación y consulta.
- Establecimiento del contexto.
- Evaluación.
- Tratamiento.
- Seguimiento.

Como se ilustra en la siguiente imagen No.1.



Imagen No.1 – Proceso de Administración y/o Gestión de Riesgo.

<sup>1</sup> Fuente de información: <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>





**GOBERNACIÓN DE ANTIOQUIA**  
República de Colombia

Este proceso de gestión de riesgos es una parte integral en la toma de decisiones la cual se debe integrar en la estructura de la operación y de los procesos de la Gobernación de Antioquia.

Razón por la cual la Entidad desarrolla una metodología de riesgos propia la cual sigue las directrices establecidas por el Departamento Administrativo de la Función Pública (DAFP)<sup>2</sup> y el Ministerio de Tecnología y las Comunicaciones (MinTIC) en materia de gestión de riesgos con el fin de promover la mejora continua de los procesos y los servicios prestados a la ciudadanía.

Este ciclo detalla la ejecución de las actividades propuestas para asegurar una gestión efectiva y actualizada de los riesgos asociados a la seguridad de la información.



Imagen No.2 – Gestión de riesgo.

### 5.1.1. EVALUACIÓN DE RIESGOS

Cabe resaltar que el riesgo se define como la posibilidad que se presente un evento o suceso que obstaculice o impida el cumplimiento del objetivo del proceso, es necesario gestionar los Riesgos de Seguridad de la información, teniendo en cuenta que, para ello, se debe contar previamente con la Identificación de los activos de información del proceso siguiendo los pasos que se observan en la **imagen No.3**.

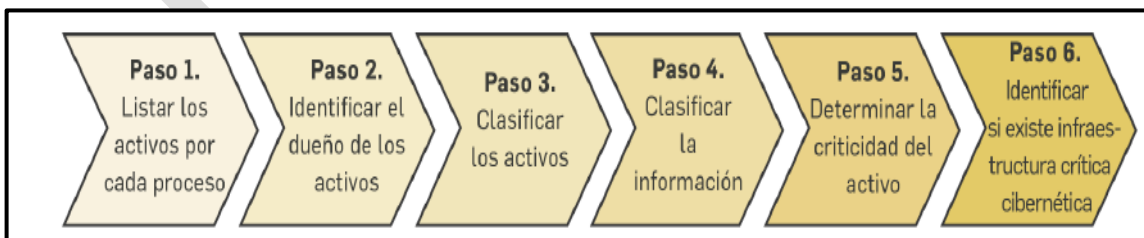


Imagen No.3 – Identificación de Activos de Información.

<sup>2</sup> Fuente de consulta: [https://www1.funcionpublica.gov.co/documents/28587410/34299967/Guia\\_administracion\\_riesgos\\_capitulo\\_riesgo\\_fiscal.pdf](https://www1.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf)







### 5.1.1.1. IDENTIFICACIÓN DE RIESGOS

El propósito de la identificación es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir el cumplimiento los objetivos de la Entidad. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada.

En la identificación de riesgos se debe tener en cuenta las incertidumbres y fuentes que están dentro o fuera de su control y que pueda afectar uno o varios objetivos. A continuación, se listan algunos:

- Las fuentes de riesgos tangibles e intangibles.
- Las causas y los eventos.
- Las amenazas y las oportunidades.
- Las vulnerabilidades y las capacidades.
- Los cambios en los contextos interno y externo.
- Las consecuencias y sus impactos en los objetivos.
- Las limitaciones de conocimiento y la confiabilidad de la información.
- Los sesgos, los supuestos y las creencias de las personas involucradas.

Teniendo en cuenta las fuentes de información y las incertidumbres se debe evaluar las amenazas y vulnerabilidades que puedan afectar los activos de información, analizando sus posibles consecuencias y estimando la probabilidad e impacto en la seguridad de la información.



Imagen No.4 – Identificación de riesgos.





En este proceso se examina cómo cada amenaza detectada podría interrumpir o comprometer uno o varios aspectos de la **TRIADA de la información** (Confidencialidad, Integridad y Disponibilidad).

Se considerarán factores como la naturaleza de la amenaza (interna o externa), la sensibilidad de los activos de información afectados, y el contexto operativo de la Entidad.

### 5.1.1.2. ANÁLISIS DE RIESGOS

El propósito del análisis de riesgos es comprender la naturaleza de los riesgos y sus características, en el que se debe considerar las incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su efectividad. Un evento puede tener múltiples causas y consecuencias y puede afectar a múltiples objetivos. A continuación, se listan algunos:

- La probabilidad de los eventos y de las consecuencias.
- La naturaleza y la magnitud de las consecuencias.
- La complejidad y la interconexión.
- Los factores relacionados con el tiempo y la volatilidad.
- La efectividad de los controles existentes.
- Los niveles de sensibilidad y de confianza.

### 5.1.1.3. EVALUACIÓN DE RIESGOS

El propósito de la evaluación de los riesgos es apoyar a la toma de decisiones, dicha evaluación implica comparar los resultados del análisis del riesgo con los criterios para riesgos establecidos con el fin de determinar cuándo se requiere una acción adicional. Esto puede conducir a una decisión de:

- No hacer nada más.
- Considerar opciones para el tratamiento de riesgos.
- Realizar un análisis adicional para comprender mejor el riesgo.
- Mantener los controles existentes.
- Reconsiderar los objetivos.





**GOBERNACIÓN DE ANTIOQUIA**  
República de Colombia

Para poder realizar una evaluación del riesgo es necesario apoyarse con las siguientes tablas de “Probabilidad” e “Impacto” de acuerdo con la metodología de riesgos definida por la Gobernación de Antioquia.

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Imagen No.5 - Tabla de Probabilidad.

La determinación del impacto se debe llevar a cabo de acuerdo con lo establecido en la metodología de la Gobernación de Antioquia, entendiéndose que el impacto puede generar lo siguiente:

- Reprocesos.
- Daño de la imagen y reputación.
- Costos financieros.
- Sanciones por no cumplimiento normativo y legal.

Dando como resultado una: “Consecuencia económica y reputacional” que se genera por la materialización del riesgo.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Imagen No.6 - Tabla de Impacto.





**GOBERNACIÓN DE ANTIOQUIA**  
República de Colombia

Para el análisis preliminar del “riesgo inherente”, en esta etapa, el nivel de severidad para el riesgo de seguridad de la información identificado y para ello se aplica la matriz de calor establecida en la metodología de riesgos. Al igual que se debe tomar el nivel de severidad para el análisis de “riesgo residual”.

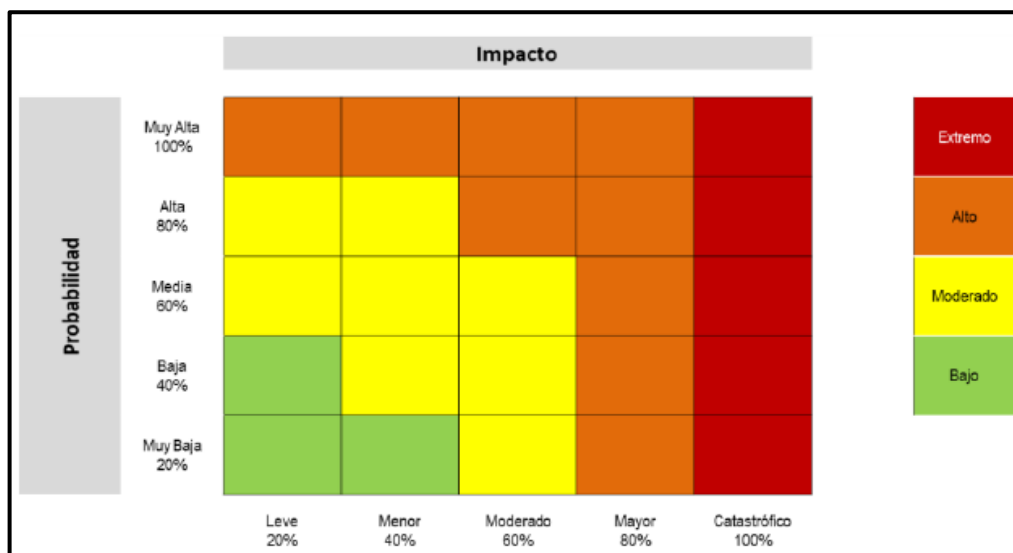


Imagen No.7 – Nivel del Riesgo.

### 5.1.2. TRATAMIENTO DE RIESGOS

El propósito del tratamiento de los riesgos es seleccionar e implementar opciones para abordar los riesgos como:

- Aceptar el riesgo.
- Evitar el riesgo.
- Reducir, mitigar o tratar el riesgo.
- Compartir o transferir el riesgo.

Para el tratamiento de riesgos de seguridad de la información en la opción **(c y d)** se debe empleando como mínimo los controles del Anexo A de la NTC-ISO/IEC 27001 siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

### 5.1.3. SEGUIMIENTO Y REVISIÓN

La Gobernación de Antioquia, debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos, es por ellos que el modelo integrado de planeación y gestión (MIPG), en la





dimensión 7 “Control interno”, desarrolla a través de las líneas de defensa la responsabilidad de la gestión del riesgo y control.

Las líneas de defensa son un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una Entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos.

## 5.2. RECURSOS

En el marco de la gestión de riesgos de seguridad y privacidad de la información se debe establecer los siguientes recursos para abordar la gestión:

Definición	Recursos
Humanos	La Dirección de Desarrollo Organizacional serán los responsables de: <ul style="list-style-type: none"><li>• Coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos para la identificación de los riesgos de la Entidad.</li></ul>
Técnicos	Se basa en los instrumentos definidos como: <ul style="list-style-type: none"><li>• Guía para la administración de riesgos.</li><li>• Instrumento para la gestión de riesgos (Matriz de riesgos SGSI).</li><li>• Guía para la administración del riesgo y el diseño de controles en Entidades públicas.</li><li>• Manual Operativo del Modelo Integrado de Planeación y Gestión – Política de Seguridad Digital y Política de Gobierno Digital.</li></ul>
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Para las actividades de logística, recursos humanos, técnicos, tecnológicos, entre otros.
Tecnológicos	Se basa en contar con las herramientas tanto de hardware como software para la aplicación de controles tecnológicos que se requieran para mitigar los riesgos.

Tabla No.2 – Recursos.





## TABLAS

Tabla No. 1 – Actividades del Plan de Tratamiento.....	6
Tabla No.2 – Recursos.....	13

## IMÁGENES

Imagen No.1 – Proceso de Administración y/o Gestión de Riesgo.....	7
Imagen No.2 – Gestión de riesgo.....	8
Imagen No.3 – Identificación de Activos de Información.....	8
Imagen No.4 – Identificación de riesgos.....	9
Imagen No.5 - Tabla de Probabilidad.....	11
Imagen No.6 - Tabla de Impacto.....	11
Imagen No.7 – Nivel del Riesgo.....	12

