

GOBERNACIÓN DE RISARALDA

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

Proceso: Gestión de Gobierno Electrónico y Servicios Digitales.

Secretaría: Secretaría de Tecnologías de la Información y la Comunicación.

Pereira, agosto de 2022.

DEPENDENCIA	CATEGORIA	COMPONENTE	HABILITADOR TRANSVERSAL
Secretaría de Tecnologías de la Información y la Comunicación	Documento Técnico, Implementación de la Política de Seguridad y Privacidad de la Información	Seguridad y Privacidad	MSPI Gobierno Digital

Formato	Lenguaje	Versión	Estado
PDF - DOC	Español	1.0	Aprobado

DOMINIO	TITULO	AUTOR	REVISÓ
Estrategia TI	Plan de Tratamiento del Riesgo Seguridad y Privacidad de la Información	Ingeniero Juan Camilo Jiménez Contratista de Prestación de Servicios Profesionales	John Jairo Gómez Ramírez Director de Gobierno Electrónico y Servicios Digitales
HERRAMIENTAS		https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf	
RESUMEN		<p>La Gobernación de Risaralda, a través de su Modelo Integrado de Planeación y Gestión, se compromete a mantener una cultura de la gestión de riesgos asociados con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos relacionados con las TIC, regulando así los riesgos de los procesos y proyectos enfocados en la lucha contra la corrupción, mediante mecanismos, sistemas y controles que permitan la prevención y detección de hechos asociados a este; y fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de Seguridad y Privacidad de la Información de manera íntegra.</p>	
PALABRAS CLAVES		<ul style="list-style-type: none"> • Activo de información • Criterio de riesgos • Riesgos de seguridad de la información • Evaluación del riesgo 	



**DEPARTAMENTO DE RISARALDA
SECRETARIA DE TECNOLOGIAS DE LA INFORMACION
Y LA COMUNICACIÓN**

**DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y
SERVICIOS DIGITALES**

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

Versión: 1

Vigencia: 08-2022

HISTÓRICO

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
0	06/04/ 22	Emisión del documento
1	10/08/22	Definición de cronograma de actividades del año 2022 hasta el 2023

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022

Tabla de contenido

1. Introducción	5
2. Objetivos específicos	6
3. Objetivos generales.....	6
4. Alcances	7
5. Conceptos básicos	8
6. Política de tratamiento de riesgos de seguridad y privacidad de la información	9
7. Programación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	12
7.1 Desglose de actividades y tareas para la vigencia 2023	13
7.2 Desglose de actividades y tareas para la vigencia 2022.....	14
7.3 Desglose de actividades y tareas para la vigencia 2021	18
8. Visión General del Proceso de Riesgos de Seguridad de la Información.....	22
9. Oportunidades de mejora.....	23
10. Recursos.....	23
11. Bibliografía	25

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
<p>Versión: 1</p>	<p>Vigencia: 08-2022</p>

1. Introducción

La gestión riesgos de seguridad digital establece procesos, procedimientos y actividades encaminadas a lograr un equilibrio entre la prestación de servicios y los riesgos asociados a los activos de información que dan apoyo y soporte al desarrollo misional de la Gobernación de Risaralda. Por lo anterior, se debe considerar e implementar medidas que implican tiempo, esfuerzos y recursos necesario para el adecuado tratamiento de los riesgos, generando así una estrategia de seguridad y privacidad de la información efectiva que permita controlar y administrar el que dichos eventos o incidentes puedan materializarse, mitigando así los impactos adversos o considerables al interior de la Gobernación de Risaralda.

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
<p>Versión: 1</p>	<p>Vigencia: 08-2022</p>

2. Objetivo General

Establecer un marco de gestión de riesgos de seguridad y privacidad de la información a través del cual se mitiguen las vulnerabilidades y amenazas asociadas a los activos de información con lo que cuenta La Gobernación de Risaralda, con el fin de mantener niveles de aceptación razonables de los riesgos en relación con los atributos de disponibilidad, integridad y confidencialidad de la información de la Gobernación de Risaralda.

3. Objetivos específicos

- Identificar, evaluar y analizar los riesgos y amenazas de Seguridad y Privacidad de la Información relacionados con los activos de información, para así, facilitar el desarrollo de la misionalidad de la Gobernación de Risaralda.
- Identificar las amenazas e impactos de Seguridad y Privacidad de la Información asociadas a los procesos de la Gobernación de Risaralda.
- Identificar e implementar controles que atiendan la gestión de riesgos y que facilite la toma de decisiones.
- Realizar un seguimiento de los riesgos de seguridad y privacidad de la información.

-

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
<p>Versión: 1</p>	<p>Vigencia: 08-2022</p>

4. Alcance

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la Información, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Se dan los lineamientos para identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la Gobernación de Risaralda.

El Plan de Tratamiento de Riesgo tendrá en cuenta todos los riesgos que se encuentren, no obstante, se les dará prioridad a los niveles Alto y Extremo de acuerdo con los lineamientos definidos por la Gobernación de Risaralda, los riesgos que se encuentren en niveles inferiores serán objeto de análisis por la alta dirección sobre si se aceptan o que controles se les aplicarán a estos.

	<p style="text-align: center;">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p style="text-align: center;">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p style="text-align: center;">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022


5. Conceptos Básicos

Para la adecuada gestión de los riesgos de seguridad y privacidad de la información se debe manejar con propiedad los siguientes términos:

- **Activo:** “En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.), que tenga valor para la organización”, según ISO27000.
- **Amenaza:** “Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización”, según ISO 27000. Es también, un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (Materializaría el riesgo).
- **Análisis del riesgo:** “Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel del riesgo”, según NTC ISO 31000:2011.
- **Aceptación del riesgo:** Es el nivel máximo de riesgo que la entidad está dispuesta a aceptar.
- **Consecuencia:** Resultado o impacto de un evento que afecta a los objetivos.
- **Controles:** “Políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel del riesgo asumido. control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo”, según ISO 27000.
- **Criterios del riesgo:** “Términos de referencia frente a los cuales se evalúa la importancia de un riesgo”, según NTC ISO 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”, según NTC ISO 31000:2011.
- **Vulnerabilidad:** Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Riesgo:** Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo a la entidad evitando cumplir con sus objetivos.
- **Probabilidad:** Es la posibilidad de que la amenaza se aproveche de una o varias vulnerabilidades para materializar el riesgo.
- **Impacto:** Son las consecuencias que genera un riesgo al materializarse.

	<p style="text-align: center;">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p style="text-align: center;">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p style="text-align: center;">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022

- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta pueda provechar una vulnerabilidad para causar una pérdida o daño en uno o varios activos de información de la entidad (Estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información), Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta el beneficio que esto conlleva. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.
- **Riesgo de Seguridad Digital:** Es la combinación de análisis des y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, la integridad territorial, el orden constitucional y los intereses departamentales y nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Riesgo positivo:** Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.
- **Seguridad de la Información:** Es el principio que busca crear condiciones de uso confiable del entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades, y de los servicios que prestan al ciudadano.

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022

6. Política de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

La Gobernación de Risaralda, a través de su Modelo Integrado de Planeación y Gestión, se compromete a mantener una cultura de la gestión de riesgos asociados con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos relacionados con las TIC, regulando así los riesgos de los procesos y proyectos enfocados en la lucha contra la corrupción, mediante mecanismos, sistemas y controles que permitan la prevención y detección de hechos asociados a este; y fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de Seguridad y Privacidad de la Información de manera íntegra.

La Política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para la administración de estos; a su vez, transmiten la posición de la institución y establecen las guías que permitan actuar y darlas a conocer a todos los colaboradores de la Gobernación de Risaralda.

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

- **Evitar:** Es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o la fuente del riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar la pérdida de documentación se prohíbe el ingreso a cierta área de personal sin autorización previa.
- **Prevenir:** Corresponde a planear, en esencia es el planear estrategias que conduzcan a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de esto son las inspecciones de mantenimiento preventivo, las Políticas de Seguridad o los seguimientos periódicos a los procesos.
- **Reducir o Mitigar:** Corresponde a la protección en el momento en el que se presenta el riesgo. Esto corresponde a los planes de contingencia para la protección de los activos de información y las copias de respaldo.
- **Compartir:** Es involucrar a un tercero para que corresponda en todo o parte del proceso que genera el riesgo. Dentro de los mecanismos de transferencia se encuentran los siguientes: Contratos de seguro, transferencia explícita por medio de cláusulas contractuales, etc.

Cada uno de los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento, de esta manera, poder realizar un análisis de los controles teniendo en cuenta el dueño del riesgo (responsable del proceso), ya que la definición de controles es el resultado del seguimiento y aplicación de controles y de los cuales deben participar todos los interesados.

Para los riesgos de seguridad y privacidad de la información:

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
<p>Versión: 1</p>	<p>Vigencia: 08-2022</p>

- El mapa de resumen de los riesgos de seguridad y privacidad de la información será presentado por la Secretaría de Tecnologías de la Información y la comunicación, en el Comité Institucional de Gestión y Desempeño, con el fin que los directivos de la entidad tengan conocimiento de los mismos.
- El manejo de los riesgos de Seguridad y Privacidad de la Información cuyo nivel de riesgos residual se encuentre ubicado en zona de riesgo baja o moderada, podrá ser asumido por el Secretario del área respectiva.
- Los riesgos de Seguridad y Privacidad de la Información cuyo nivel de riesgo residual se encuentre ubicado en zona de riesgo alta o extrema, deben contar con la aprobación del Secretario del área respectiva y ser puestos en conocimiento del Gobernador

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022

7. Programación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

7.1 Desglose de actividades y tareas para la vigencia 2023:

Gestión	Actividad	Descripción	Responsable	Fecha de Inicio	Fecha Final
Gestión de riesgos	Actualización de lineamientos de riesgos	Actualizar la política y la programación de tratamiento de riesgos de Seguridad y Privacidad de la Información	Responsable de Seguridad de la Información y Director de Gobierno Electrónico y Servicios Digitales	enero 2023	Diciembre 2023
	Sensibilización	Socializar la Guía y herramienta de identificación de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital	Responsable de Seguridad de la Información	Febrero 2023	Agosto 2023
	Validación de los riesgos actuales e identificación de nuevos riesgos	Realizar la validación de los riesgos existentes, verificando que aún representen un riesgo para la entidad	Responsable de Seguridad de la Información	Junio 2023	octubre 2023
		Realizar el proceso para identificar nuevos riesgos en caso de que existan. (Retroalimentación o ajustes)	Secretaría TIC y Delegados TIC de todas las dependencias	Junio 2023	Diciembre 2023
	Aceptación de Riesgos Identificados	Aceptación, aprobación de riesgos identificados y el plan de tratamiento de cada uno	Responsable de Seguridad de la Información y Alta Dirección	Junio 2023	agosto 2023

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022

Desglose de actividades y tareas para la vigencia 2023:

	Actualización de la Matriz de Riesgos de Seguridad y Privacidad de la Información	Basados en la retroalimentación, actualizar la matriz de riesgos de Seguridad y Privacidad de la Información de acuerdo a la necesidad de la entidad.	Responsable de la Seguridad de la Información	Junio 2023	Diciembre 2023
	Publicación	Publicación de la matriz de riesgos de Seguridad y Privacidad de la Información	Secretaría TIC	Agosto 2023	agosto 2023
	Seguimiento fase de tratamiento	Seguimiento al estado de los planes de tratamiento aprobado para los riesgos identificados y verificación de las evidencias	Enlace MIPG y Control Interno	Julio 2023	Diciembre 2023
	Evaluación de riesgos residuales	Evaluación de los riesgos residuales resultantes del tratamiento de los riesgos identificados	Responsable de la Seguridad de la Información	Julio 2023	Diciembre 2023
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Responsable de la Seguridad de la Información y Secretaría TIC	Julio 2023	Diciembre 2023
		Actualización de la Matriz de Riesgos de Seguridad de la Información de acuerdo a los cambios solicitados	Responsable de la Seguridad De la información	Mayo 2023	Diciembre 2023

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022

	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Responsable de la Seguridad de la Información y Secretaría TIC	Julio 2023	Diciembre 2023
--	----------------------	---	--	------------	----------------

Programación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

7.2 Desglose de actividades y tareas para la vigencia 2022:

Gestión	Actividad	Descripción	Responsable	Fecha de Inicio	Fecha Final
Gestión de riesgos	Actualización de lineamientos de riesgos	Actualizar la política y la programación de tratamiento de riesgos de Seguridad y Privacidad de la Información	Responsable de la Seguridad de la Información y Director de Gobierno Electrónico y Servicios Digitales	Julio 2022	Diciembre 2022
	Sensibilización	Socializar la Guía y herramienta de identificación de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital	Responsable de la Seguridad de la Información	Julio 2022	Septiembre 2022
	Validación de los riesgos actuales e identificación de nuevos riesgos	Realizar la validación de los riesgos existentes, verificando que aún representen un riesgo para la entidad	Responsable de la Seguridad de la Información	Julio 2022	Octubre 2022

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022

Programación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

7.2 Desglose de actividades y tareas para la vigencia 2022:

Gestión de riesgos	Validación de los riesgos actuales e identificación de nuevos riesgos	Realizar el proceso para identificar nuevos riesgos en caso de que existan. (Retroalimentación o ajustes)	Secretaría TIC y Delegados TIC de todas las dependencias	Julio 2022	Diciembre 2022
	Aceptación de Riesgos Identificados	Aceptación, aprobación de riesgos identificados y plan de tratamiento	Responsable de Seguridad de la Información y Alta Dirección	Julio 2022	agosto 2022
	Actualización de la Matriz de Riesgos de Seguridad y Privacidad de la Información	Basados en la retroalimentación, actualizar la matriz de riesgos de Seguridad y Privacidad de la Información de acuerdo a la necesidad de la entidad.	Responsable de Seguridad de la Información	Julio 2022	Diciembre 2022
	Publicación	Publicación de la matriz de riesgos de Seguridad y Privacidad de la Información	Secretaría TIC	Agosto 2022	agosto 2022

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022

Programación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

7.2 Desglose de actividades y tareas para la vigencia 2022:

Gestión de riesgos	Seguimiento fase de tratamiento	Seguimiento al estado de los planes de tratamiento aprobado para los riesgos identificados y verificación de las evidencias	Enlace MIPG y Control Interno	Julio 2022	Diciembre 2022
	Evaluación de riesgos residuales	Evaluación de los riesgos residuales resultantes del tratamiento de los riesgos identificados	Responsable de la Seguridad de la Información	Julio 2022	Diciembre 2022
	Mejoramiento Monitoreo y Revisión	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Responsable de la Seguridad de la Información y Secretaría TIC	Julio 2022	Diciembre 2022
Gestión de riesgos	Mejoramiento Monitoreo y Revisión	Actualización de la Matriz de Riesgos de Seguridad de la Información de acuerdo a los cambios solicitados	Responsable de la Seguridad de la Información y Secretaría TIC	Agosto 2022	Diciembre 2022
Gestión de riesgos	Mejoramiento Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Responsable de la Seguridad de la Información y Secretaría TIC	Agosto 2022	Diciembre 2022

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022

Programación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información


7.3 Desglose de actividades y tareas para la vigencia 2021:

Gestión	Actividad	Descripción	Responsable	Fecha de Inicio	Fecha Final
Gestión de riesgos	Actualización de lineamientos de riesgos	Actualizar la política y la programación de tratamiento de riesgos de Seguridad y Privacidad de la Información	Responsable de la Seguridad de la Información y Director de Gobierno Electrónico y Servicios Digitales	Diciembre 2020	Diciembre 2020
	Sensibilización	Socializar la Guía y herramienta de identificación de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital	Responsable de la Seguridad de la Información	Febrero 2021	Febrero 2021
	Validación de los riesgos actuales e identificación de nuevos riesgos	Realizar la validación de los riesgos existentes, verificando que aún representen un riesgo para la entidad	Responsable de la Seguridad de la Información	Febrero 2021	Febrero 2021
		Realizar el proceso para identificar nuevos riesgos en caso de que existan. (Retroalimentación o ajustes)	Secretaría TIC y Delegados TIC de todas las dependencias	Febrero 2021	Diciembre 2021
	Aceptación de Riesgos Identificados	Aceptación, aprobación de riesgos identificados y el plan de tratamiento	Responsable de la Seguridad de la Información y Alta Dirección	Abril 2021	Mayo 2021

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022

7.3 Desglose de actividades y tareas para la vigencia 2021:

		de cada uno	SecretaríaTIC		
	Actualización de la Matriz de Riesgos de Seguridad y Privacidad de la Información	Basados en la retroalimentación, actualizar la matriz de riesgos de Seguridad y Privacidad de la Información de acuerdo a la necesidad de la entidad.	Responsable de la Seguridad de la Información	Febrero 2021	Diciembre 2021
	Publicación	Publicación de la matriz de riesgos de Seguridad y Privacidad de la Información	SecretaríaTIC	Junio 2021	Junio 2021
	Seguimiento fase de tratamiento	Seguimiento al estado de los planes de tratamiento aprobado para los riesgos identificados y verificación de las evidencias	Enlace MIPG y Control Interno	Julio 2021	Diciembre 2021
	Evaluación de riesgos residuales	Evaluación de los riesgos residuales resultantes del tratamiento de los riesgos identificados	Responsable de la Seguridad de la Información	Julio 2021	Diciembre 2021
	Mejoramiento, monitoreo y revisión	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Responsable de la Seguridad de la Información y Secretaría TIC	Julio 2021	Diciembre 2021
		Actualización de la Matriz de Riesgos de Seguridad de la Información de acuerdo a los cambios solicitados	Responsable de la Seguridad de la Información	Julio 2021	Diciembre 2021
		Generación, presentación y reporte de indicadores	Responsable de la Seguridad de la Información y SecretaríaTIC	Julio 2021	Diciembre 2021

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
<p>Versión: 1</p>	<p>Vigencia: 08-2022</p>

7 . Visión General del Proceso de Riesgos de Seguridad de la Información

A continuación, se expone el modelo de gestión de riesgos de Seguridad de la Información diseñado y basado en la ISO 27005, acorde para la administración de riesgos de Seguridad de la Información:

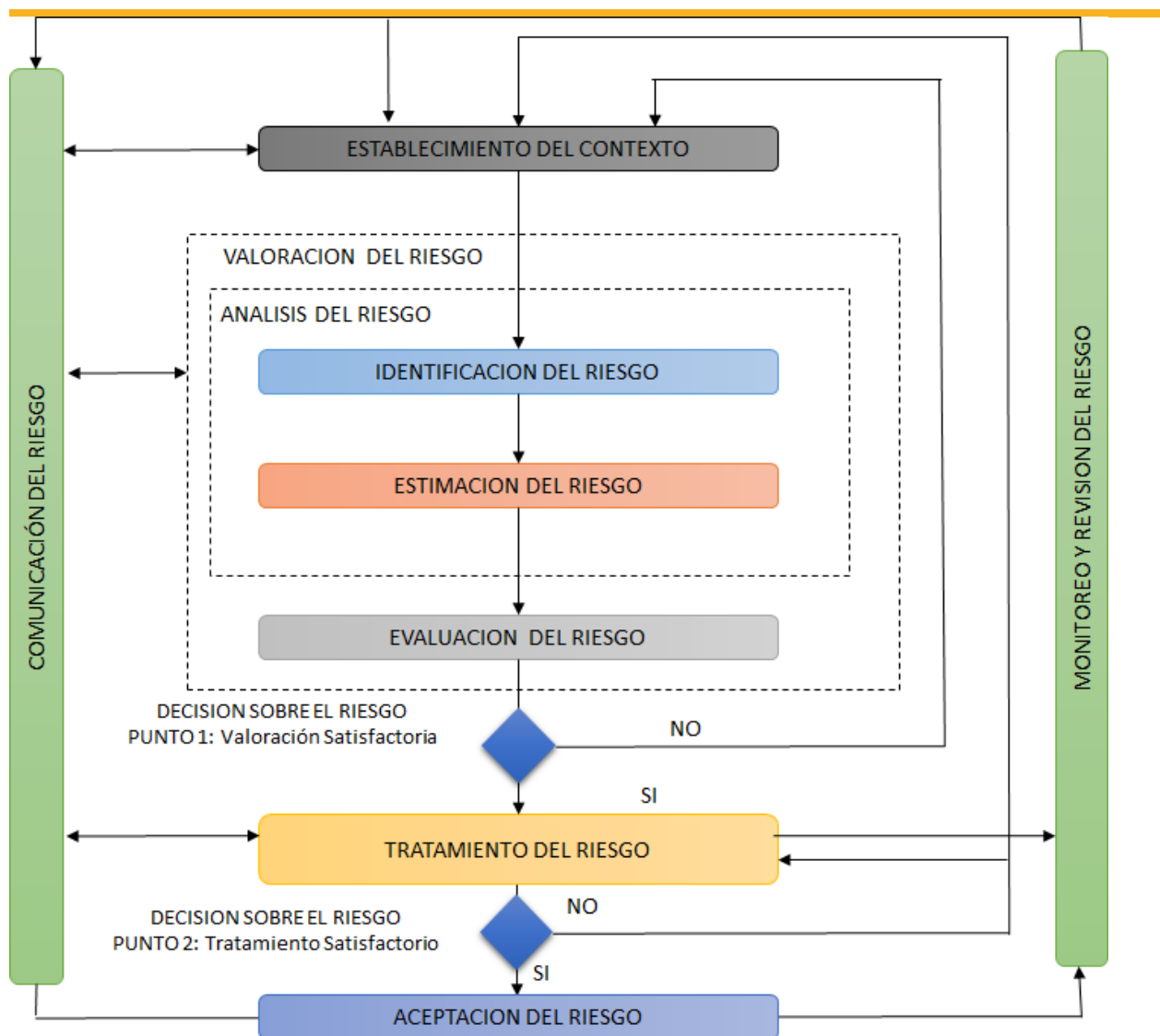


Ilustración 1 Visión del proceso de Riesgos de Seguridad (ISO/IEC 27005)

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022

El MSPI promueve la adopción del enfoque basado en los procesos que realiza la entidad con respecto a Seguridad y Privacidad de la Información, para que la entidad funcione de manera eficaz, se debe identificar y gestionar muchas actividades, por lo que se considera como proceso a cualquier actividad que consume recursos y que adicionalmente, su gestión promueva la transformación de entradas en salidas. El enfoque basado en procesos consiste en que la entidad identifique las actividades del funcionamiento de esta y la interacción entre las actividades, asimismo, para la gestión de Seguridad y Privacidad de la Información se hace hincapié en la importancia de la implementación y adopción del MSPI en la entidad.

7. Desarrollo Metodológico

- Fase 1: Análisis de la Información

En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso de TI, se desarrollarán las siguientes actividades:

- Verificar si dentro de las labores expuestas por cada delegado existe riesgos de Seguridad y Privacidad de la Información.
- Determinar los controles aplicados para este riesgo en la Gobernación de Risaralda.
- Determinar los riesgos que van a ser incluidos en la Matriz de Riesgos de Seguridad y Privacidad.

- Fase 2: Desarrollo de procesos

En esta fase se realizarán las actividades para la estructuración de las correspondientes medidas:

- Generar el nombre de la medida.
- Definir los responsables de cada medida.
- Establecer el alcance y objetivo de cada medida.
- Justificar cada medida.
- Establecer las actividades que se van a realizar para aplicar la medida.

- Fase 3: Análisis de los procesos

En esta fase se realiza el proceso de validación, verificación y establecimiento de controles a los riesgos, además, de la identificación y asignación de los respectivos responsables de cada riesgo a mitigar.

- Definición de los controles relacionados con cada medida.
- Validación de los riesgos mitigados con cada medida.
- Análisis de la aplicabilidad de cada medida.

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
<p>Versión: 1</p>	<p>Vigencia: 08-2022</p>

- Priorización en la aplicación de las medidas de acuerdo a la necesidad de mitigación.
- Identificar y asignar las responsabilidades sobre las medidas a tomar, de acuerdo con el responsable de cada riesgo a mitigar.

- Fase 4: Ciclo de vida el tratamiento de riesgos de Seguridad y Privacidad de la Información

Definir las actividades a realizar por cada elemento del ciclo de vida del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

- Planear: Dentro de esta etapa se desarrollan actividades definidas en la fase 1 de la presente metodología.
- Hacer: En este paso del ciclo de vida del Tratamiento de los Riesgos de Seguridad y Privacidad de la Información se desarrollarán las actividades que se establecieron en la fase 2 de la presente metodología.
- Verificar: En esta etapa se ejecutan las actividades que permitan realizar un seguimiento a la aplicación de cada una de las medidas establecidas.
- Actuar: Dentro de esta etapa se plantearán las mejoras respectivas, teniendo en cuenta el seguimiento realizado y los resultados que de la ejecución de las medidas se hayan obtenido.

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022

8. Oportunidades de Mejora

La Gobernación de Risaralda en el entendimiento de que a través de un riesgo se puede generar un análisis que permita realizar una identificación de las oportunidades que se tienen, entendiéndose por oportunidad una consecuencia positiva tras el tratamiento del Riesgo de Seguridad y Privacidad de la Información, no se centrará solo en el riesgo identificado sino también en las acciones de mejora que pueda aplicar e implementar.

9. Recursos

La Gobernación de Risaralda, para la gestión de los riesgos de Seguridad y Privacidad de la Información dispone de los siguientes tipos de recursos:

Recursos	Descripción
Humanos	La Gobernación de Risaralda a través de la Secretaría de Tecnologías de la Información y la Comunicación y el Responsable de Seguridad de la Información, es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la entidad en lo correspondiente a la Seguridad y Privacidad de la Información.
Técnicos	Guía para la administración del riesgo y diseño de controles en entidades públicas. <ul style="list-style-type: none"> - Riesgos de Gestión, Corrupción y Seguridad Digital – Versión 4 –octubre de 2018 del DAFP - Matriz de riesgos.
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de información y conocimientos, y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos y técnicos.

	<p align="center">DEPARTAMENTO DE RISARALDA SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN</p> <p align="center">DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y SERVICIOS DIGITALES</p> <p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
Versión: 1	Vigencia: 08-2022

Bibliografía

- “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2020 - Min Tic” - https://www.mintic.gov.co/portal/604/articles-100251_plan_tratamiento_seguridad_2020_u20200902.pdf
- “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información” – Universidad Pedagógica y Tecnológica de Colombia - http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf2020.pdf
- “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información” – Departamento Administrativo de Presidencia de la República- <https://dapre.presidencia.gov.co/dapre/DocumentosSIGEPRE/D-TI-24-Plan-Tratamiento-Riesgos-Seguridad-Privacidad-Informacion.pdf>



**DEPARTAMENTO DE RISARALDA
SECRETARIA DE TECNOLOGIAS DE LA INFORMACION
Y LA COMUNICACIÓN**

**DIRECCIÓN DE GOBIERNO ELECTRÓNICO Y
SERVICIOS DIGITALES**

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

Versión: 1

Vigencia: 08-2022