

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

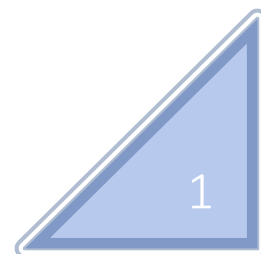
GOBERNACIÓN DEL MAGDALENA

SANTA MARTA MAYO DE 2023

| | | |
|---|-------------------------|--|
| PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | Proceso asociado | Tecnología de Información y Comunicaciones |
| | Código | |
| | Versión | 1.0 |

CONTENIDO

| | | |
|------|--|---|
| 1. | OBJETIVO | 2 |
| 2. | ALCANCE | 2 |
| 3. | TÉRMINOS Y DEFINICIONES..... | 2 |
| 4. | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | 3 |
| 4.1. | Planes Desarrollados de Riesgos de Seguridad y Privacidad de la Información | 3 |
| 4.2. | Riesgos de Seguridad y Privacidad de la Información..... | 4 |
| 4.3. | Actividades Para Desarrollar sobre los Riesgos de Seguridad y Privacidad de la Información. | 5 |
| 4.4. | Programación de Monitoreo de Controles de Riesgos de Seguridad y Privacidad de la Información..... | 6 |
| 5. | MARCO LEGAL..... | 8 |
| 6. | REQUISITOS TÉCNICOS..... | 8 |
| 7. | DOCUMENTOS ASOCIADOS..... | 8 |
| 8. | RESPONSABLE DEL DOCUMENTO..... | 8 |



| | | |
|--|------------------|--|
| PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | Proceso asociado | Tecnología de Información y Comunicaciones |
| | Código | |
| | Versión | 1.0 |

1. OBJETIVO

Detallar el plan de tratamiento de riesgos que hace parte del Sistema de Gestión de Seguridad de la Información – SGSI de la GOBERNACIÓN DEL MAGDALENA; de tal forma que se definen y aplican los controles con los cuales se buscan mitigar la materialización de los riesgos de seguridad de la información en la Gobernación del Magdalena. De esta forma, se busca que, mediante el tratamiento de los riesgos y la mejora continua de la Seguridad y Privacidad de la Información, las partes interesadas tengan mayor confianza en el tratamiento de la información que se almacena y maneja en la Entidad.

2. ALCANCE

El plan de tratamiento de riesgos tiene alcance para los procesos de la Gobernación del Magdalena, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información. el cual hace parte del Sistema Integrado de Gestión de la Gobernación del Magdalena.

3. TÉRMINOS Y DEFINICIONES

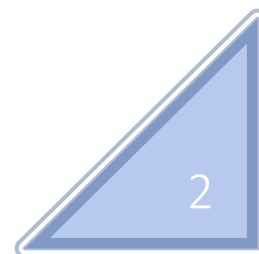
Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; *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 en el beneficio que se genera

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: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses 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.



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

Proceso
asociado

Tecnología de Información
y Comunicaciones

Código

Versión

01

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.¹

Sistema Integrado de Gestión: Es el sistema integrado de Gestión de la Gobernación, que permite armonizar los procesos en búsqueda de una gestión eficiente, eficaz y transparente, con el fin de aumentar la satisfacción de los clientes.

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

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información –SGSI de la Gobernación del Magdalena, se busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información, por lo cual es importante controlar y establecer los riesgos de seguridad de la información.

De esta forma, se garantiza el tratamiento de los riesgos de seguridad de la información y la gestión de riesgo positivo u oportunidad, acorde con lo establecido en el **Lineamiento de Administración de Riesgos** y la **Guía para La Formulación, Seguimiento y Evaluación de Planes de Mejoramiento**.

4.1. Planes Desarrollados de Riesgos de Seguridad y Privacidad de la Información

Durante la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI, se declararon como eficaz la Creación de nuevos riesgos de seguridad de la información – SGSI y Creación y documentación de Matriz de riesgos de seguridad de la información versus controles – SGSI; de tal forma se definen nuevos riesgos de seguridad de la información y se asocian a los existentes, aplicando controles según el Anexo A de la Norma ISO 27001:2013.

La oportunidad de mejora Plan de seguridad y privacidad de la información – SGSI, fue declarada eficaz. Con la realización de esta oportunidad de mejora se actualizaron los riesgos que hacen parte del Sistema de Gestión de Seguridad de la Información – SGSI de la Gobernación.

¹ Decreto 1008 de 14 de junio de 2018, por el cual se establecen los lineamientos generales de la Política de Gobierno Digital.

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

Proceso
asociado

Tecnología de Información
y Comunicaciones

Código

Versión

01

Los siguientes planes de mejoramiento se encuentran finalizadas: SGSI buenas prácticas para el buen uso y manejo de las contraseñas seguras, Incumplimiento de la Política de escritorio y pantalla limpia, de igual forma los siguientes con relación a los riesgos:

| Nombre Riesgo - SGSI | | Plan de Mejoramiento |
|----------------------|--|---|
| 1 | Posibilidad que los sistemas de información sean afectados por ataques cibernéticos generando pérdida de información - SGSI. | SGSI buenas prácticas para prevenir Ataques Cibernéticos DDos. |
| 2 | Activos documentales de los archivos de la Gobernación con eventos de hurto, pérdida, daño de los documentos o fuga de su información - SGSI. | Materialización del riesgo Activos documentales de los archivos con eventos de hurto, pérdida, daño de los documentos o fuga de su información - SGSI |
| 3 | Posibilidad que los servicios TICS presenten pérdida de disponibilidad - SGSI | SGSI prevenir ataques de tipo defacement o cambio de apariencia visual de sitio Web |

4.2. Riesgos de Seguridad y Privacidad de la Información

A continuación, se visualizan los riesgos de Seguridad de la Información, los cuales se encuentran asociados al Sistema de Gestión de Seguridad de la Información – SGSI de la Gobernación del Magdalena.

Después de llevar a cabo en la Entidad la actualización de los riesgos y teniendo en cuenta el **Lineamiento para la Administración del Riesgo**, se especifican de la siguiente forma:

| N | Nombre | Estado del riesgo | Responsable | Proceso Realiza Monitoreo | Materializados en el último monitoreo |
|---|---|-------------------|-------------|---|---------------------------------------|
| 1 | Posibilidad que la documentación pública reservada o pública clasificada, que se encuentra en la plataforma de TI, esté con pérdida de información – SGSI. | Gestionado | | Tecnologías de Información y Comunicaciones | No |
| 2 | Posibilidad que la información clasificada o reservada se emplee para uso indebido – SGSI. | Gestionado | | Tecnologías de Información y Comunicaciones | No |
| 3 | Posibilidad que los servicios TICS presenten pérdida de disponibilidad - SGSI. | Gestionado | | Tecnologías de Información y Comunicaciones | No |

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

| | |
|------------------|--|
| Proceso asociado | Tecnología de Información y Comunicaciones |
| Código | |
| Versión | 01 |

| | | | | | |
|---|---|------------|--|---|----|
| 4 | Posibilidad que los sistemas de información sean afectados por ataques cibernéticos generando pérdida de información - SGSI. | Gestionado | | Tecnologías de Información y Comunicaciones | Si |
| 5 | Posibilidad que los activos de información se afecten o presenten situaciones adversas por pérdida de disponibilidad – SGSI. | Gestionado | | Tecnologías de Información y Comunicaciones | No |
| 6 | Información de carácter reservado con riesgo de fuga y pérdida - SGSI. | Gestionado | | Tecnologías de Información y Comunicaciones | No |
| 7 | Activos documentales de los archivos con eventos de hurto, pérdida, daño de los documentos o fuga de su información - SGSI. | Gestionado | | Gestión Documental | Si |

4.3. Actividades Para Desarrollar sobre los Riesgos de Seguridad y Privacidad de la Información

| Actividad | Descripción | Responsable | Fecha Inicial Planificada | Fecha Final Planificada |
|---|---|-------------|---------------------------|-------------------------|
| Ejecutar el plan de aplicación y mejora continua del Sistema de Gestión de Seguridad y privacidad de la Información - SGSI | Se ejecutará el cronograma de aplicación y mejoramiento del Sistema de Gestión de Seguridad de la Información - SGSI el cual consiste en el desarrollo de las tareas correspondientes a la vigencia 2022, como la verificación por parte de la alta dirección del SGSI, cumplimiento de los objetivos e indicadores definidos | | 03/01/2022 | 30/12/2022 |

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

Proceso
asociado

Tecnología de Información
y Comunicaciones

Código

Versión

01

| | | | | |
|---|--|----------------------------|-------------------|-------------------|
| <p>Actualizar en el módulo de seguridad de la información los activos de seguridad de la información, teniendo en cuenta la criticidad desde disponibilidad, integridad y confidencialidad</p> | <p>Actualizar en el módulo de seguridad de la información los activos de seguridad de la información, teniendo en cuenta la criticidad desde disponibilidad, integridad y confidencialidad</p> | | <p>03/01/2022</p> | <p>30/12/2022</p> |
| <p>Seguridad Digital y Modelo de Seguridad y Privacidad MSPI (Gobierno Digital)</p> | <p>De acuerdo con la Resolución 500 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”, y del Anexo 1 – Modelo de Seguridad y Privacidad de la Información, emitidos por el Ministerio de Tecnologías de la Información y las comunicaciones, se definen las actividades a desarrollar sobre el Sistema de Gestión de Seguridad de la Información – SGSI de la Gobernación del Magdalena.</p> | <p>José Ramón Iglesias</p> | <p>01/01/2022</p> | <p>31/03/2023</p> |

4.4. Programación de Monitoreo de Controles de Riesgos de Seguridad y Privacidad de la Información

Se programa el monitoreo de los controles definidos en cada uno de los riesgos de seguridad y privacidad de la Información, identificados con la sigla SGSI (Sistema de Gestión de Seguridad de la Información); siguiendo el **Lineamiento para la Administración del Riesgo**, definido en la Gobernación del Magdalena, es realizado trimestralmente y la documentación del monitoreo tiene un plazo de 10 días hábiles, como se puede ver en la siguiente programación:

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

Proceso
asociado

Tecnología de Información
y Comunicaciones

Código

Versión

01

| Documentación de Monitoreo de riesgos de SGSI | Responsable | Fecha Inicial Planificada | Fecha Final Planificada |
|---|---------------------|---------------------------|-------------------------|
| Cuarto Trimestre 2021 | José Ramón Iglesias | 01/01/2022 | 17/01/2022 |
| Primer Trimestre 2022 | José Ramón Iglesias | 01/04/2021 | 18/04/2022 |
| Segundo Trimestre 2022 | José Ramón Iglesias | 01/07/2022 | 15/07/2022 |
| Tercer Trimestre 2022 | José Ramón Iglesias | 01/10/2022 | 14/10/2022 |
| Cuarto Trimestre 2022 | José Ramón Iglesias | 01/01/2023 | 16/01/2023 |

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

Proceso
asociado

Tecnología de Información
y Comunicaciones

Código

Versión

01

5. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Resolución 500 de marzo 10 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

6. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- Anexo 1 – Modelo de Seguridad y Privacidad de la Información, emitidos por el Ministerio de Tecnologías de la Información y las comunicaciones.

7. DOCUMENTOS ASOCIADOS

- Lineamientos para la Administración del Riesgo.
- Guía Para La Formulación, Seguimiento y Evaluación De Planes De Mejoramiento.
- Manual de Políticas de Seguridad de la Información.

8. RESPONSABLE DEL DOCUMENTO

José Ramón Iglesias. Gobierno Digital de la Gobernación del Magdalena.