ALCALDIA MUNICIPAL DE TESALIA – HUILA

TESALIA Productiva y Empresarial #MomentoDeLaGente

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

Vigencia 2023

Proyecto:	Reviso:	Aprobó:
Firma:	Firma:	Firma:

1. INTRODUCCIÓN

Si en un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, las consecuencias derivadas de sucesos posteriores y relevantes como el terrorismo, la inestabilidad política, las pandemias y los códigos maliciosos, entre otros, han señalado la necesidad de incorporar nuevas amenazas presentes no solamente en el mundo físico sino también en el entorno digital, cuando se trate de comprender los riesgos más significativos a los activos de información.

El análisis de riesgos de los activos de información nos permite entender de una manera efectiva y eficiente los riesgos de pérdida de confidencialidad, integridad y disponibilidad sobre cada uno de los activos definidos como parte del alcance del análisis.

Gestionar eficazmente la seguridad de la información, los riesgos de seguridad digital de los activos de información de la entidad, así como los sistemas e infraestructura que participan en sus procesos y que se encuentran expuestos, permite mantener la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de las opciones apropiadas de tratamiento de riesgos de seguridad de la información y seguridad digital, teniendo en cuenta la evaluación de los resultados de la valoración de los riesgos del Sistema de Gestión de Seguridad de la Información SGSI y en concordancia a la normativa aplicable.

Teniendo en cuenta lo anterior, se formula el presente Plan, en cumplimiento de la normativa aplicable vigente, y en particular, como parte de los planes institucionales establecidos en el Decreto 612 de 2018

En este documento se presentan los objetivos generales y específicos que se persiguen con el plan, su alcance, el marco normativo tenido en cuenta para su elaboración, los responsables por roles, un conjunto de definiciones que permiten tener un mejor entendimiento de los conceptos para los lectores no expertos en tecnología, cronograma, estrategia de comunicación y mecanismo de seguimiento del plan.

2. OBJETIVO

Definir las actividades tendientes a gestionar los riesgos de seguridad de la información identificados por los procesos de la Alcaldía Municipal de Tesalia, con el fin de mitigarlos hasta llevarlos a un nivel de riesgos aceptable.

3 ALCANCE

El presente Plan comprende las actividades a realizar para la identificación, valoración y gestión de los riesgos de seguridad de la información y la definición de las actividades a realizar por los procesos de la administración municipal durante la vigencia 2023, para la mitigación de los riesgos no aceptables identificados. Aplica a todas las dependencias de la Alcaldía de Tesalia.

4. MARCO NORMATIVO

A continuación, se presenta la normatividad que se tuvo en cuenta para realizar el presente Plan.

NORMA	DESCRIPCIÓN
Decreto 1078 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 1008 2018	Por medio del cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
CONPES 3854 2016	Política Nacional de Seguridad Digital

DOCUMENTO TÉCNICO EXTERNO 2016	Modelo de Seguridad y Privacidad de la Información – MSPI Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Versión 3.0.2, julio de 2016
DOCUMENTO TÉCNICO EXTERNO 2019	Manual para la Implementación de la Política de Gobierno Digital Implementación de la Política de Gobierno Digital (Decreto 1008 de 2018). Versión 7, abril de 2019
DOCUMENTO TÉCNICO EXTERNO 2019	Guía para la administración del riesgo y el diseño de controles en entidades públicas. Metodología para la administración del riesgo, articulada con la Política de Seguridad Digital liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones. Versión 5, diciembre de 2020.

5. RESPONSABLES

- Secretaria de Gobierno
- Coordinador TIC
- Control Interno
- Comité Institucional de Gestión y Desempeño

6. DEFINICIONES

- **Activo:** cualquier elemento que tenga valor para la organización.

- **Análisis del riesgo**: Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.

- **Causa:** Elemento específico que origina el evento.

- **Contexto externo**: Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).

- **Contexto interno:** Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).

- **Controles**: Procesos, políticas y/o actividades que pueden modificar el riesgo.

- **Criterios de riesgos**: Términos de referencia frente a los cuales se evaluará la importancia del riesgo.

- **Evaluación del Riesgo**: Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.

- **Evento**: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.

- **Fuente**: Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.

- **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

- **Identificación del riesgo**: Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.

- **Riesgo:** Posibilidad o probabilidad de que un evento pueda afectar las funciones de la entidad e impactar el logro de sus objetivos.

- **Riesgo aceptable**: Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.

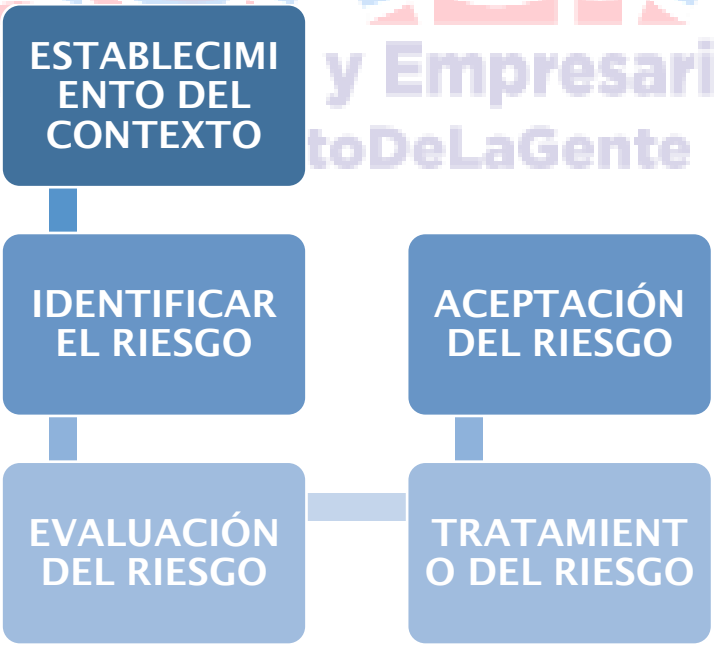
- **Riesgo residual**: Nivel de riesgo que permanece luego de tomar medidas de tratamiento

7. DESARROLLO DEL PLAN

La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto la administración municipal.

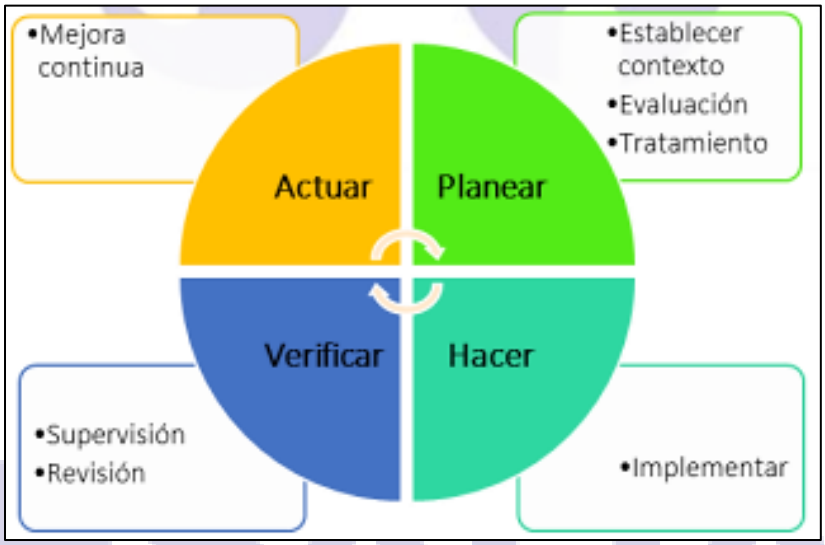
Es recomendable contar con técnicas tradicionales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla.

El cronograma de actividades propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo, guardando coherencia con la metodología emitida por el Departamento Administrativo de la Función Pública, en su versión vigente. A continuación, se presentan las actividades generales para la implementación del Plan:



Tesalia Productiva y Empresarial - #MomentoDeLaGente
Carrera 9 # 6-11 - Telefax 8377022 - Correo Electrónico - tesalia@yahoo.com
Código Postal - 415001

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA)



7.1. TRATAMIENTO DE RIESGOS

7.1.1 Factores de riesgo

Para la vigencia 2023 se priorizan los siguientes factores de riesgo digital en nuestro plan de tratamiento de riesgos:

- Nivel de conocimiento del personal en amenazas digitales, políticas y controles de seguridad
- Disponibilidad permanente de servicios esenciales como telecomunicaciones, energía e infraestructura.
- Identificación y protección de los datos de carácter personal
- Adecuada clasificación de la información bajo custodia de la Entidad de acuerdo con el marco legal vigente.
- Entorno global digital inseguro.
- Aislamiento forzoso del personal en sus residencias.

- Segregación apropiada de roles y privilegios en todos los sistemas de información.

7.1.2. Valoración del riesgo

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y valorándolos con el fin de obtener información para establecer su nivel y las posibles acciones a implementar.

Dicho análisis incluye las fuentes, así como los factores que generan las consecuencias y aumentan la probabilidad de que ocurran. En la etapa de análisis se identifican los controles existentes ya sean administrativos, técnicos y/o procedimientos implementados en la entidad. Por lo tanto, se analiza el riesgo combinando estimaciones de impacto y probabilidades en el contexto de las medidas de control existente.

La aplicación de análisis cualitativo facilita la calificación y evaluación de los riesgos al aplicar formas descriptivas para presentar la magnitud de las consecuencias potenciales (consecuencia) y la posibilidad de ocurrencia (probabilidad). La siguiente tabla describe la valoración de los riesgos definidos por la Alcaldía Municipal de Tesalia.

7.1.3 Estrategia de tratamiento de riesgo

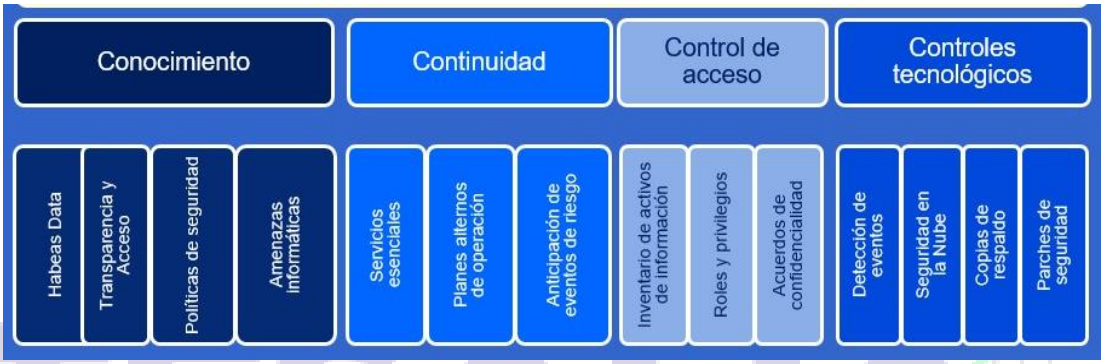
Las estrategias en el tratamiento de riesgos consisten en minimizar la probabilidad de materialización del riesgo. Para ello, se puede evidenciar cuatro opciones:

- Transferir: Son procedimientos que permiten eliminar el riesgo por medio de la transferencia.
- Mitigar: Permite reducir la probabilidad de ocurrencia del riesgo o reducir sus consecuencias. La probabilidad de ocurrencia de un riesgo puede reducirse a través de controles de gestión, políticas y procedimientos encaminados a reducir la materialización del riesgo.

- Evitar: Puede evitarse el riesgo no procediendo con la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad que logren el mismo resultado y no incorporen el riesgo detectado.

- Aceptar: consiste en hacer frente a un riesgo (positivo o negativo) o porque no se ha identificado ninguna otra estrategia de respuesta adecuada.

La estrategia de control de riesgos para la vigencia 2023, contempla cuatro ejes que son: conocimiento, continuidad, control de acceso y controles tecnológicos, así:



7.1.4 Estrategias Orientadas al Conocimiento

Mediante actividades de inducción, sensibilización y capacitación periódica se busca que todos los servidores, contratistas y pasantes apropien conocimientos en materia de:

- Ley de protección de datos personales.
- Ley de transparencia y acceso a la información.
- Políticas institucionales de seguridad digital.
- Modalidades y control de ataques informáticos.
- Uso seguro de los recursos informáticos.

7.1.5 Estrategias Orientadas al Conocimiento

Con el fin de prevenir y controlar el acceso no autorizado a activos de información clasificados y reservados la Entidad emprenderá en la vigencia 2023 acciones específicas para:

- Actualizar los instrumentos de acceso a la información pública
- Reforzar los controles de acceso a activos de información con roles y privilegios más precisos
- Reforzar el cumplimiento de los acuerdos de confidencialidad y los acuerdos de intercambio seguro de información

7.1.6. Estrategias de fortalecimiento de controles técnicos

Ante el aumento del tipo y complejidad de amenazas informáticas la entidad implementará estrategias específicas en:

- Identificación de eventos potencialmente nocivos
- Reforzamiento de controles de acceso a servicios en la nube
- Verificación y control de copias de respaldo
- Control de cambios en plataformas tecnológicas
- Aplicación de parches de seguridad y actualización de equipos de procesamiento de datos.

8. RECURSOS

La estimación y asignación de los recursos para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, para los riesgos identificados en el Entidad, corresponderá al líder del proceso, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en este Plan.

Si el establecimiento de los controles implica la adquisición de herramientas o servicios tecnológicos bajo la responsabilidad de la coordinación de TIC, los recursos se tomarán de proyectos de inversión

9. SEGUIMIENTO Y MEDICIÓN DEL PLAN

La Secretaria de Gobierno es la responsable del seguimiento a la implementación del presente Plan, toda vez que el presente Plan está integrado al Plan de Acción Institucional de la

vigencia, el seguimiento se realizará cuatrimestralmente y se reportará el resultado de cada período, en el instrumento de seguimiento al Plan de Acción, en el compromiso asociado al Plan de Seguridad y Privacidad de la Información.

Al final de la vigencia se reportará el Informe Anual de Implementación de Planes Institucionales

El seguimiento a los controles se realiza de acuerdo con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.

9.1. INDICADORES

La Secretaria de Gobierno medirá el cumplimiento del presente Plan, a través del resultado del siguiente indicador, para el cual la meta es 100%:

$$\frac{N° \text{ de Actividades Ejecutadas}}{N° \text{ de Actividades Programada}}$$

10. CRONOGRAMA

A continuación, se presenta el cronograma de implementación de las iniciativas.

OBJETIVO	ACCCIONES	RESPONSABLE	EVIDENCIA	PLAZO
Definir lineamientos internos que orienten a la entidad a correcta identificación, análisis valoración y seguimiento de los riesgos que puedan afectar el	Actualizar el Plan de Tratamiento de riesgos de seguridad y privacidad de la información	Coordinador TIC	Documento actualizado	A 31 de enero de 2023
	Realizar identificación en primera instancia de los riesgos de seguridad y privacidad de la información de acuerdo de los activos de información de la	Funcionarios de la administración municipal Coordinador TIC	Matriz de riesgos identificados	A 31 de marzo

logro de los objetivos institucionales	Administración Municipal			
	Realizar priorización De tres (3) riesgos de seguridad y privacidad de la información Con mayor impacto	Funcionarios de la administración municipal Coordinador TIC	Matriz de riesgos priorizados	A 31 de marzo
	Diseñar acciones para mitigar el impacto de los riesgos priorizados	Coordinador TIC	Plan de acción	A 15 de abril de 2023
	Ejecutar las acciones diseñadas para mitigar los riesgos priorizados	Funcionarios de la administración municipal	Matriz de seguimiento de las acciones diseñadas	A 31 de noviembre de 2023
	Presentación de Informe final de la gestión realizada al Secretario General y de Gobierno	Coordinador TIC	Documento presentado	A Diciembre de 2023

ISNELDA VARGAS CAMACHO
Secretaria de Gobierno

Proyecto:	Reviso:	Aprobó:
Firma:	Firma:	Firma: