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

ALCALDÍA DEL MUNICIPIO DE SAN JOSÉ DEL GUAVIARE
OPORTUNIDAD Y PROGRESO PARA TODOS
2023

CONTROL DE VERSIONES

Versión	Fecha	Modificación
1.0	31/01/2023	Versión inicial del documento

INTRODUCCIÓN.

La alcaldía municipal de San José del Guaviare, reconoce la información como un recurso que, como el resto de los activos, tiene valor para la entidad y por consiguiente debe ser debidamente protegida; las políticas de seguridad y privacidad de la información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos y asegurar el eficiente cumplimiento de los objetivos de las entidades del Estado.

En el presente documento se presentan las actividades que se compromete a realizar la alcaldía municipal de San José del Guaviare para garantizar la seguridad y privacidad de la información. Así mismo, este plan contempla la importancia de realizar medidas de control y evaluación que contribuyan a gestionar y reducir las vulnerabilidades a las cuales se encuentra expuesta la información de la entidad.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información es una actividad prevista en el Plan de Seguridad y Privacidad de la Información en su fase de planeación, cuyo propósito principal es adoptar el Modelo de Seguridad y Privacidad de la Información - MSPI, como habilitador de la nueva Política de Gobierno Digital.

JUSTIFICACIÓN.

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se define en cumplimiento a los propósitos y obligaciones tanto internos como sectoriales en cuanto a la contribución de un estado más eficiente, transparente y participativo. La alcaldía municipal de San José del Guaviare mediante dicho plan busca la implementación de una metodología que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos en función de la tecnología, equipos, infraestructura y otros; asociados con una actividad, función o proceso de tal forma que permita a la entidad minimizar pérdidas y maximizar oportunidades.

Una vez identificados los riesgos que puedan afectar los activos de información de la alcaldía municipal de San José del Guaviare, es necesario adoptar las medidas esenciales para mantener la seguridad y privacidad de los mismos, con el fin de que en los procesos misionales y de apoyo no se presenten mayores afectaciones.

ALCANCE.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene alcance para todos los procesos de la alcaldía municipal de San José del Guaviare que involucren la manipulación de información, en concordancia con la normatividad nacional vigente.

OBJETIVOS.

Objetivo Estratégico:

Minimizar los riesgos de seguridad y privacidad de la información asociados a los procesos, con el fin de salvaguardar los activos de información de la entidad.

Objetivos de Gestión:

- Aplicar los lineamientos y metodologías establecidos por el Ministerio TIC para identificar y valorar los riesgos a la seguridad y privacidad de la información.
- Identificar las principales amenazas que afectan los activos de información.
- Definir los principales activos a proteger en la entidad.
- Brindar protección a los activos de información mediante la implementación de acciones eficaces y seguras en la alcaldía municipal de San José del Guaviare.

MARCO LEGAL.

Principios Rectores: para la elaboración del presente plan se utilizaron las siguientes guías metodológicas:

- Guía - Modelo de Seguridad y Privacidad de la Información.
- Guía 5 - Gestión de Activos.
- Guía 7 - Gestión de Riesgos.
- Guía 8 - Controles de Seguridad.

Normatividad Aplicable: La normatividad aplicable al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información es la siguiente:

NORMATIVIDAD	DESCRIPCIÓN
Ley 1581 de 2012	Por la cual se dictan disposiciones para la protección de datos personales.
Decreto 1377 de 2013	Por medio del cual se reglamenta parcialmente la ley 1581 de 2012.
Ley 1712 de 2014	Ley de transparencia y del derecho de acceso a la información pública.
CONPES 3854 de 2016	Por medio del cual se establece la política nacional de seguridad digital.
Decreto 415 de 2016	Por el cual se adiciona el Decreto Reglamentario del Sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Decreto 1413 de 2017	Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de tecnología de la información y las comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la ley 1437 de 2015 y el artículo 45 de la ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Decreto 612 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 2018	Por el 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 comunicaciones.

LINEAMIENTOS CONCEPTUALES.

Marco Conceptual: a continuación, se definen los términos basados en la Norma ISO 27001 (ISO/IEC 27000), la Guía 7 - Gestión de Riesgos y la Guía 8 - Controles de Seguridad.

Glosario:

- **Ley de Transparencia y Acceso a la información Pública Nacional:** derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

- **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) que tenga valor para la organización.

- **Activo de Información:** en relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

- **Administración de Riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

- **Amenaza:** causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO/IEC 27000).

- **Archivo:** conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada.

- **Auditoría:** proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Calificación del Riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

- **Consecuencia:** son los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- **Control:** también utilizado como sinónimo de salvaguardar o contramedida; en una definición más simple, es una medida que modifica el riesgo.

- **Datos Personales Mixtos:** es la información que contiene datos personales públicos y datos privados o sensibles.

- **Datos Personales Privados:** es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular, (Ley 1581 de 2012, art 3, literal h).

- **Datos Personales Públicos:** son los datos que no sean privados, privados o sensibles. Son considerados datos personales públicos los relativos al estado civil, profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos en otros, como registros públicos, gacetas, boletines, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva (Decreto 1377 de 2013).

- **Datos Personales Sensibles:** son aquellos datos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como: origen racial o étnico, orientación política, convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, datos relativos a la salud y la vida sexual y los datos biométricos (Decreto 1377 de 2013, art 3).

- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.

- **Factores de Riesgo:** son las fuentes generadoras de riesgos.

- **Gestión de incidentes de seguridad de la información**: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Integridad:** propiedad de exactitud y completitud.

- **Ley de Habeas Data:** Ley Estatutaria 1266 de 2008 que establece el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en Bancos de Datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución política, particularmente en relación con la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

- **Plan de Tratamiento de Riesgos:** documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma (ISO/IEC 27000).

- **Privacidad:** en el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

- **Riesgo:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000). Seguridad de la información Preservación de la confidencialidad, integridad, y disponibilidad de la información.

- **Riesgo Inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles o acciones para modificar su probabilidad o impacto.

- **Riesgo Residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

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

- **Tratamiento de Datos Personales:** cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (Ley 1581 de 2012, art 3).

- **Valoración del Riesgo:** proceso de análisis y evaluación del riesgo. Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

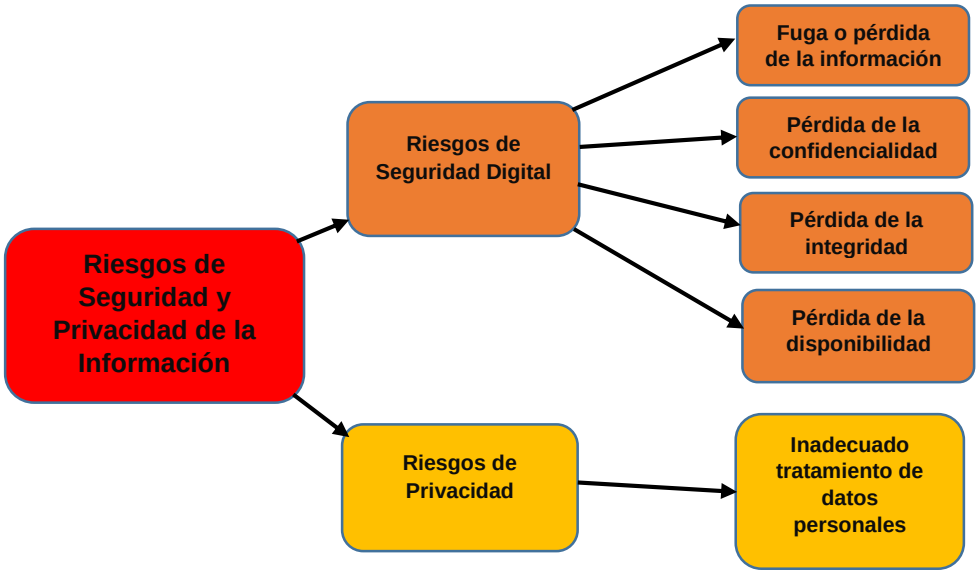
- **Vulnerabilidad:** representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

METODOLOGÍA.

Para llevar a cabo la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, la alcaldía municipal de San José del Guaviare cuenta con la guía para la metodología PHVA (Planear – Hacer – Verificar - Actuar) así como los lineamientos expuestos por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, a través a través de la normatividad proferida por el mismo.

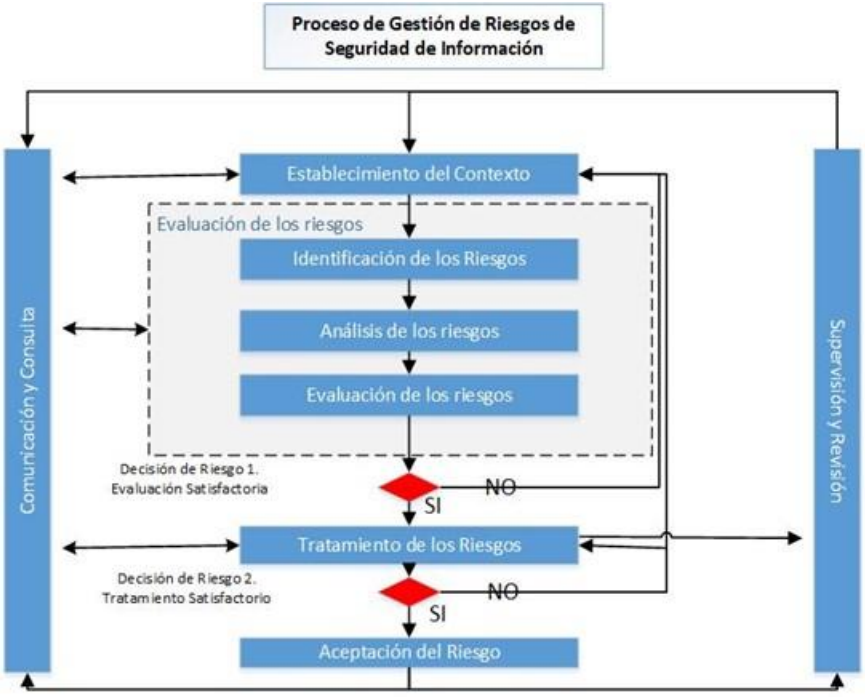
Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Definición de Riesgo: de acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la "posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información; suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias".



Riesgos de Seguridad Digital: son los riesgos que resultan de la combinación de amenazas y vulnerabilidades en el ambiente digital y dado su naturaleza dinámica incluye también aspectos relacionados con el entorno físico.

Riesgos de Privacidad: son los riesgos que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.



Proceso de gestión del riesgo en la seguridad de la información
Fuente: NTC-ISO/IEC 27005

CRONOGRAMA DE ACTIVIDADES.

ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
*Identificar los activos de información que están más expuestos a posibles riesgos y diligenciar la matriz de identificación de riesgos de seguridad y privacidad de la información.	*Servidores públicos de la alcaldía. * Profesional de apoyo en gobierno digital	01-02-2023 hasta 30-04-2023
*Publicar en la página web la matriz de identificación de riesgos de seguridad y privacidad de la información.	*Profesional de apoyo en gobierno digital	01-05-2023 hasta 31-05-2023
*Mantener informados a los servidores públicos de la alcaldía sobre la importancia de evitar los riesgos que afectan la seguridad de la información	*Profesional de apoyo en gobierno digital	01-05-2023 hasta 31-12-2023
*Realizar el seguimiento a la matriz de identificación de riesgos de seguridad y privacidad de la información.	*Profesional de apoyo en gobierno digital	01-06-2023 hasta 31-12-2023
*Aplicar 1 encuesta semestral sobre el tratamiento de riesgos de seguridad y privacidad de la información al personal administrativo de la alcaldía.	*Personal administrativo de la alcaldía municipal de San José del Guaviare	01-06-2023 hasta 31-12-2023

RESPONSABLES DE ELABORACIÓN.

- Secretaría de planeación
- Profesional de apoyo en gobierno digital
- Técnico de sistemas

EJECUCIÓN DEL PRESUPUESTO.

El presupuesto para la ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, es el que se destinará para la contratación tanto de la prestación de servicios de personas naturales (entre profesionales y técnicos) como la adquisición de posible software y hardware durante la vigencia 2023. Así mismo, el presupuesto estará consolidado en el Plan Anual de Adquisiciones para la respectiva vigencia.

SEGUIMIENTO Y EVALUACIÓN

La Secretaría de Planeación a través del profesional de Gobierno Digital, será la dependencia encargada de realizar el seguimiento al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Participación:

- Secretaría de planeación
- Profesional de apoyo en gobierno digital
- Técnico de sistemas

Aprobación del Plan: El Comité Institucional de Gestión y Desempeño será el encargado de aprobar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Mecanismos de Socialización del Plan:

ACTIVIDAD	OBJETIVO	MEDIO DE SOCIALIZACIÓN	FECHA
Socializar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Lograr que todos los funcionarios de la entidad tanto de planta como contratistas, conozcan sus responsabilidades frente al tratamiento de riesgos de seguridad y privacidad de la información	*Página web	Febrero de 2023

Elaboró: Carlos Julián Flórez Villamil	**Aprobó:** Ramón Guevara Gómez
Cargo: Profesional de apoyo en gobierno digital	**Cargo:** Presidente Comité Institucional de Gestión y Desempeño
Firma:	**Firma:**

Se expide el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2023, a los 31 (treinta y uno) días del mes de enero de 2023 (dos mil veintitrés).