SECRETARIA DE PLANEACION MUNICIPAL

GOBIERNO DIGITAL

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDADDE LA INFORMACIÓN

VIGENCIA 2024 - 2027

San José del Guaviare enero 2024

CONTROL DE VERSIONES

Versión	Fecha	Modificación
1.0	31/01/2023	Versión inicial del documento
2.0	31/01/2024	Actualización

TABLA DE CONTENIDO

1. 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.

2. 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 implementaciónde una metodología que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos en función de la tecnología, equipos, infraestructura y otros; asociados con unaactividad, 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 esencialespara 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.

3. ALCANCE

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

- Base de datos
- servidores
- Internet
- Correo electrónico

- Diseño y publicación de páginas web
- Sistemas de información
- Sistema de Gestión de Correspondencia
- Activos informáticos

La gestión de riesgos de seguridad de la información y su tratamiento, podrá será aplicada sobre cualquier proceso, a cualquier sistema de información o aspecto particular de control de la Entidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información , análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

El plan debe garantizar que se realiza un análisis y valoración de riesgos asociados a cada uno de los activos identificados, lo cual permite establecer cuáles son los controles que deben desplegarse para reducir los niveles de riesgo calculados. La implementación de los controles debe ser realizada a través de un procedimiento adecuado de cambios y liberaciones, garantizando que las pruebas requeridas son ejecutadas al igual que los procedimientos necesarios para operación son elaborados y formalmente establecidos. Es importante mencionar que existe una relación estrecha tanto con los lineamientos de incidentes y de monitoreo, dada la necesidad de gestionar de forma adecuada de los incidentes de seguridad que puedan presentarse.

4. OBJETIVOS

4.1 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.

4.2 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.

5. MARCO LEGAL.

5.1 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.

5.2 Normatividad Aplicable

La normatividad aplicable al Plan de Tratamiento de Riesgos de Seguridad y

Privacidad de la Información es la siguiente:

CONPES 3854 de 2017: Política Nacional de Seguridad Digital –

CONPES 3854 de 2016: Por medio del cual se establece la política nacional de seguridad digital.

CONPES 3701 de 2011: Lineamientos de Política para Ciberseguridad y Ciberdefensa

Decreto 1078 de 2015: Decreto único reglamentario del sector de Tecnología e Información y las comunicaciones (define el componente de seguridad y privacidad de la información)

Decreto 1377 de 2013: Por medio del cual se reglamenta parcialmente la ley 1581 de 2012

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 Tecnología e Información y las Comunicaciones.

Ley 1581 de 2012: Disposiciones generales para la protección de datos personales.

Ley 1712 de 2014: Ley de transparencia y del derecho de acceso a la información pública.

Ley 1581 de 2012: Disposiciones generales para la protección de datos personales.

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.

Resolución 303 de 2018: Creación del Comité Institucional de Gestión y Desempeño

Resolución No. 00500: 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. LINEAMIENTOS CONCEPTUALES.

6.1 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.

6.2 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 desujetos 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 dañosa 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 auditoría y obviamente para determinar el grado en el que se cumplenlos criterios de auditoría. (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 conotros, 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 unadefinición 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 titularo 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.
- **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 riesgoen 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 ausenciade controles o acciones para modificar su probabilidad o impacto.
- **Riesgo Residual:** nivel de riesgo que permanece luego de determinar y aplicarcontroles para su administración.
- **Seguridad de la Información:** preservación de la confidencialidad, la integridad yla disponibilidad de la información.
- **Tratamiento de Datos Personales:** cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulacióno 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 serexplotada por una o más amenazas.

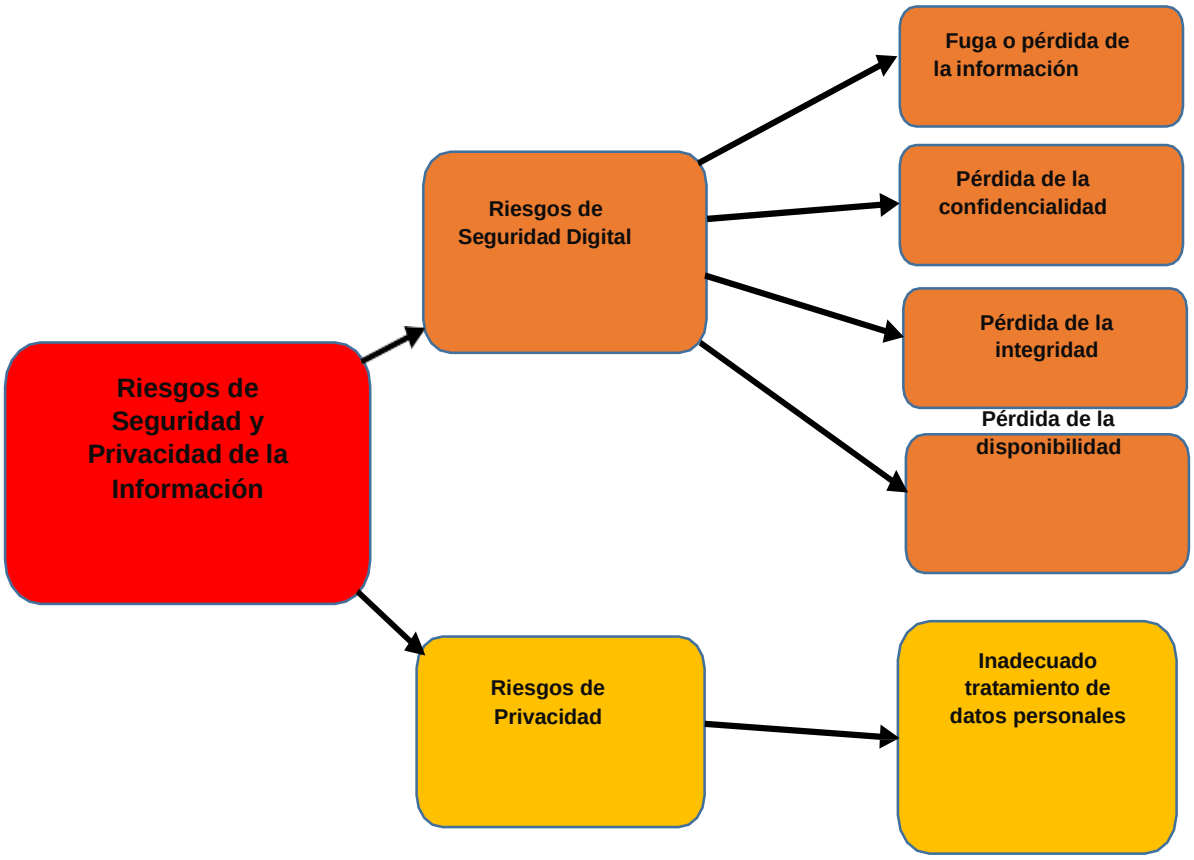
7. METODOLOGÍA.

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 laguía 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

7.1 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 ausar una pérdida o daño en un activo de información; suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias".

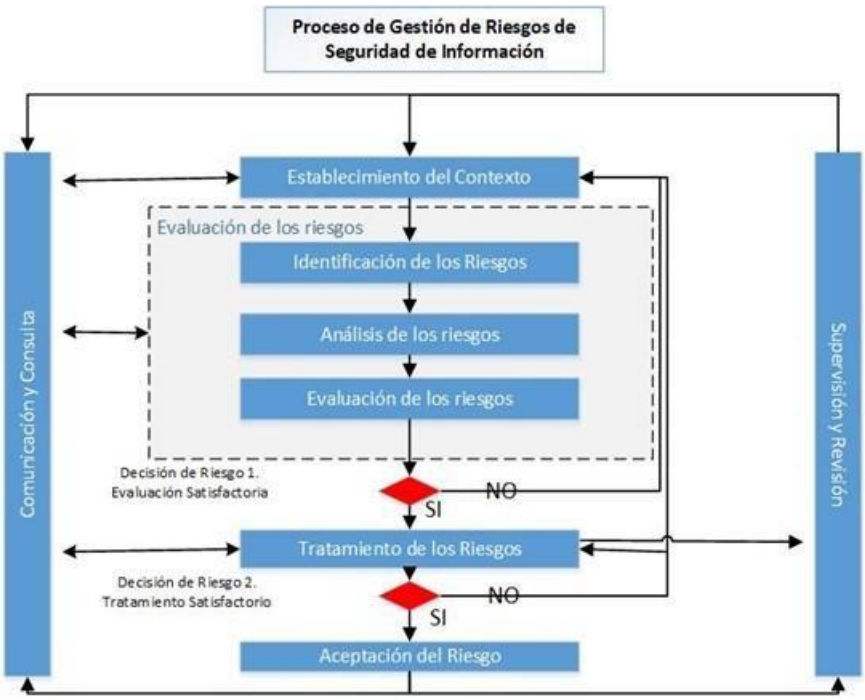


7.2 Riesgos de Seguridad Digital

Son los riesgos que resultan de la combinación deamenazas y vulnerabilidades en el ambiente digital y dado su naturaleza dinámica incluye también aspectos relacionados con el entorno físico.

7.3 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

7.4 Identificación de Activos

Tabla 1 Tipos de activos

ACTIVOS		
TIPO		**DESCRIPCION**
INFRAESTRUCTURA FISICA		Centro de datos, oficinas.
DISPOSITIVOS DE TECNOLOGIA		Servidores, UPS, dispositivos de comunicaciones, computadoras de escritorio, lap-tops, impresoras, red LAN, router,
SISTEMAS DE INFORMACION Y APLICACIONES DE SOFTWARE		Aplicaciones, Pagina Web, Sistemas de Información, Plataformas nacionales etc.
INFORMACION	Electrónica	Información importante para la entidad (bases de datos) e información de soporte (procesos, políticas, procedimientos, guías y estándares) en medios electrónicos.
	Física	Información importante para el negocio (reportes) e información de soporte (procesos, políticas, procedimientos, guías, contratos, información de clientes y estándares) en papel.
RECURSO HUMANO	Dueños de información	Nivel directivo dueño de la información que asigna permisos para leer utilizar y modificar la información.
	Usuarios	Personal que utiliza la información para el desempeño de su trabajo diario y que da soporte a los sistemas de información.
SERVICIOS		Correo electrónico, Acceso a red LAN.

SOPORTE PARA ALMACENAMIENTO DE INFORMACION	Servidor de backup, nube, CD, USD, Disco Externo, etc.

7.5 Riesgos de seguridad digital

Una vez identificados los activos se realizará la valoración de cada uno de ellos en términos de valor para la entidad según la perdida de:

- Disponibilidad.
- Confidencialidad
- Integridad

7.6 Identificación de amenazas

Una vez valorados los activos es necesario identificar las amenazas a las cuales está expuesto cada activo; es importante que esta consideración se realice sin tener en cuenta los controles establecidos.

Las amenazas son resultados de actos deliberados o mal intencionados que pueden afectar nuestros activos, sin embargo, existen eventos naturales o accidentales que deben ser considerados por su capacidad de generar incidentes no deseados.

Las amenazas a la cuales están expuestos los diferentes activos pueden ser según su origen las siguientes:

Tabla 2 Identificación de Amenazas

ORIGEN	AMENAZA
Daño Físico	Incendios, inundaciones, sismos, tormentas.

Condiciones externas	Aspectos regulatorios, caída de energía, campos electromagnéticos, contaminación, crisis financieras, daño de agua, excesivo calor, excesivo frio, explosiones, perdida de proveedores, problemas de transporte, sobrecargas.
Condiciones internas	Campos electromagnéticos, contaminación, daños en los equipos, escapes, fallas en la red, fallas en líneas telefónicas, fallas mecánicas, falta de insumos, fugas, humedad, mala publicidad, pérdida de acceso, perdida de proveedores, polvo, problemas de transporte, registros errados, sobrecargas, suciedad, vibraciones.
Entorno social	Motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo.
Actos deliberados	Abuso privilegios de acceso, análisis de tráfico, ataque físico a los equipos, bombas lógicas, código malicioso, destrucción de información, divulgación de información, errores en código, espías (spyware),extorsión, Espionaje industrial, fallas de hardware, fallas de software, fallas en la red, fallas en líneas telefónicas, gusanos, incendios, interceptación de información, manipulación de programas, perdida de datos, robo de información, suplantación de identidad, troyanos, usos no autorizados, Virus
Actos accidentales	Destrucción de información, Incendios, pérdida de claves, perdida de dispositivos. Humano Epidemias, huelgas, indisponibilidad de personal, perdida de personal clave.

Humano	Epidemias, huelgas, indisponibilidad de personal, perdida de personal clave.

7.7 Identificación de Vulnerabilidad

Debe identificarse la forma como cada una de las amenazas podría materializarse, es decir, que vulnerabilidades permiten que las amenazas se conviertan en situaciones de riesgo reales.

Algunas vulnerabilidades pueden ser:

- Ausencia o desconocimiento de políticas.
- Ausencia de validación de autenticación de la información
- Mal manejo de los manuales de la información
- Ausencia de copias de respaldo o backups de la información
- Configuraciones no seguras.
- Ausencia o deficiencia en los sistemas de autenticación de los aplicativos
- Deficiencia en la autorización de permisos de la información.
- Susceptibilidad a la humedad, el polvo y la suciedad
- Errores de configuración.
- Falta de mantenimiento
- Susceptibilidad a las variaciones de voltaje
- Errores del administrador.
- Almacenamiento sin protección
- Fechas incorrectas
- Conexión deficiente de los cables
- Arquitectura insegura de la red
- Conexiones de red pública sin protección
- Ausencia de terminación de la sesión cuando se abandona la estación de trabajo

- Gestión deficiente de las contraseñas
- Descarga y usos no controlados de software
- Ausencia de copias de respaldo
- Ausencia de protección física de la edificación, puertas y ventanas
- Entrenamiento insuficiente en seguridad
- Uso incorrecto de software y hardware
- Falla de conciencia acerca de la seguridad
- Ausencia de mecanismos de monitoreo
- Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
- Ausencia de protección física de la edificación, puertas y ventanas
- Fallas de usuarios.
- Manuales de uso no documentados.
- Medidas de protección de acceso inadecuadas.
- Medidas de protección física inadecuadas.
- Procesos o procedimientos no documentados.
- Usuario desinformado.
- Tecnología inadecuada.
- Debilidad o inexistencia de controles.
- Condiciones de locales inadecuadas o no seguras
- Identificación de agentes generadores

7.8 Descripción del riesgo

(Vulnerabilidades) + "pueden permitir/generar/facilitar la" + Amenaza + "," + "lo cual causaría la" + Riesgo + "de/en el/la" + Activo de información.

7.9 Responsable del riesgo

- Son los sujetos que deben de tomar acciones frente al riesgo del que son responsables.
- Implementar y controlar las acciones definidas para el riesgo del que son responsables.

7.10 Probabilidad de ocurrencia

Establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos, a fin de determinar la capacidad de la organización para su aceptación o manejo.

Tabla 3 Probabilidad de ocurrencia

NIVEL	PROBABILIDAD	DESCRIPCION	FRECUENCIA
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en cualquier momento.	Al menos una vez en los últimos 5 años
3	Posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	Probable	El evento probablemente	Al menos una vez en el último año

		ocurrirá en la mayoría de las circunstancias	
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

7.11 Impacto

Hace referencia a las consecuencias que puede ocasionar a la Agencia la materialización del riesgo; se refiere a la magnitud de sus efectos.

Tabla 4 Impacto

NIVEL	PROBABILIDAD	DESCRIPCION
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimo sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efectos sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.

5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

La calificación del riesgo se logra a través del producto de la estimación de la frecuencia y de la gravedad de los efectos causados por la materialización del riesgo. La primera representa el número de veces que se ha presentado o puede presentarse el riesgo, y la segunda se refiere a la magnitud de sus efectos.

7.12 Mapa de riesgo

Es una herramienta de gestión que permite determinar objetivamente cuáles son los **riesgos** relevantes.

El análisis del riesgo determinado por su probabilidad e impacto permite tener una primera evaluación del riesgo inherente (escenario sin controles) y ver el grado de exposición al riesgo que tiene la entidad. La exposición al riesgo es la ponderación de la probabilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

Tabla 5 Zona de Riesgo – MAPA DE RIESGO

PROBABILIDAD		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		1	2	3	4	5
Rara Vez	1	B	B	M	A	A
Improbable	2	B	B	M	A	E
Posible	3	B	M	A	E	E
Probable	4	M	A	A	E	E
Casi Seguro	5	A	A	E	E	E

Zona de Riesgo

B: Baja: Asumir el riesgo

M: Moderada: Asumir el riesgo, Reducir el riesgo.

A: Alta: Reducir el riesgo, Evitar el riesgo, Evitar el riesgo, Transferir el riesgo.

E: Extrema: Reducir el riesgo, Evitar el riesgo, Evitar el riesgo, Transferir el riesgo .

7.13 Opciones de manejo del riesgo

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos. De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

Tabla 6 Opciones de manejo del riesgo

OPCIONES	DESCRIPCION
Reducir el riesgo	Aplicar controles de seguridad e incluye la implementación de medida de seguridad
Asumir el riesgo	Cuando las acciones necesarias para eliminar el riesgo tienen un costo demasiado alto, superior a las consecuencias previstas en la ocurrencia del incidente.
Evitar el riesgo	Eliminando la causa del incidente o modificándola de tal forma que se elimine el riesgo
Compartir el riesgo	Compra de pólizas, Contratar una compañía de seguridad etc.

7.14 Controles a implementar, instalar o configurar

Con los controles se busca eliminar, modificar o disminuir las condiciones de riesgo existentes y evitar que estos se presenten, los controles que se definan en el tratamiento de los riesgos deben ser conocidos por los responsables con el fin de que en el momento de aplicarlos se haga de manera correcta y que la mitigación sea de, de manera oportuna, es por esto que la capacitación es muy importante.

7.15 Actividades para instalar, implementar o configurar los controles

Una vez llevada a cabo la evaluación de riesgos y en función de los resultados obtenidos, se procederá a planificar la acción preventiva para implantar las medidas pertinentes, incluyendo para cada actividad el plazo para llevarla a cabo, la designación de responsables y los recursos humanos y materiales necesarios para su ejecución.

7.16 Objetivos de los controles a implementar

Los controles sirven para:

- Prevenir
- Detectar
- Corregir
- Compensar
- Disuadir

7.17 Riesgo residual

El riesgo residual hace referencia a aquel que permanece después de haber aplicado controles. Para definir su zona de riesgo se utiliza la tabla de probabilidad de ocurrencia y la tabla de impacto.

7.18 Indicador de cumplimiento

- (Actividades implementadas) / (Actividades Planteadas)

8. RESPONSABLE

- La secretaria de Planeación y OO. PP
- Profesional de apoyo de Gobierno Digital
- Soporte Técnico

9. 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.

10. SEGUIMIENTO Y EVALUACIÓN

La Secretaría de Planeación a través del profesional de Gobierno Digital, será la dependencia encargada de realizar el seguimiento y la Oficina de Control Interno de Gestión la encargada de la evaluación.

11 APROBACION DEL PLAN

El Comité Institucional de Gestión y Desempeño será el encargadode aprobar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

12. MECANISMOS DE SOCIALIZACIÓN DEL PLAN

Socializar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para 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, el medio que se utilizara será la página web una vez sea aprobado el Plan por el CIGD.

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

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad con las actividades necesarias para tratar de manera preventiva e integral los riesgos de Seguridad y Privacidad de la Información a los que la entidad puede estar expuesta.

La Alcaldía de San José del - Guaviare, ha adoptado la Política de Seguridad de la Información, como parte del sistema integral de gestión del Municipio, y para lograr su implementación y fortalecimiento se programarán actividades **(CRONOGRAMA DE ACTIVIDADES DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION**) para cada vigencia basados en el autodiagnóstico y avances de las vigencias anteriores-

ALCALDIA DE SAN JOSE DEL GUAVIARE
SECRETARIA DE PLANEACION MUNICIPAL
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
CRONOGRAMA DE ACTIVIDADES 2024

Elaboró: Secretaria de Planeación
Revisó: Ariel Mosquera Morales - Secretario de Planeación Municipal
Aprobó: Comité Institucional de Gestión y Desempeño en el Acta No. Del 2024

ITEM	ACTIVIDAD	OFICINA Y/O DEPENDENCIA RESPONSABLE	INDICADOR	META	CTDA	SOPORTE	FECHA DE CUMPLIMIENTO
1	Construcción o actualización de la matriz de riesgos de los activos de información, estableciendo controles y responsables	Secretaría de Planeación - Profesional de apoyo Gobierno Digital	Matriz de Riesgos Elaborada, aprobada por el CIGD y publicada	Identificar, evaluar y gestionar los riesgos asociados con la seguridad de la información	1	Link de publicación	20/12/2024
2	Notificar por escrito a los responsables de implementar los controles para mitigar o evitar el riesgo identificado	Secretaría de Planeación - Profesional de apoyo Gobierno Digital	Documento de notificación	Que los responsables de implementar o aplicar los controles tome la responsabilidad.	1	Link de publicación	20/12/2024
3	Realizar un monitoreo del cumplimiento de la aplicación de los controles que se establecieron en el mapa de riesgos de seguridad	Secretaría de Planeación - Profesional de apoyo Gobierno Digital	Informe del monitoreo Anual	Establecer el estado de los controles de seguridad de la información	1	Link de publicación	20/12/2024
4	Formular un Sistemas de Gestión de Incidentes	Secretaría de Planeación - Profesional de apoyo Gobierno Digital	Documento elaborado, aprobado por el CIGD y publicado	Mejorar significativamente su capacidad para enfrentar y mitigar los riesgos asociados con la seguridad de la información y responder de manera efectiva a posibles amenazas y eventos adversos.	1	30/11/2023	20/12/2024
5	Elaborar el documento de los lineamientos para el manejo de terminales en el área financiera.	Secretaría de Planeación - Profesional de apoyo Gobierno Digital	Documento elaborado, aprobado por el CIGD y publicado	Garantizar la seguridad, integridad y confidencialidad de la información financiera y transacciones realizadas a través de terminales electrónicos	1	Link de publicación y acto administrativo	20/12/2024