



REPUBLICA DE COLOMBIA
MUNICIPIO DE SAN JOSE DEL GUAVIARE

PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION
Y LAS COMUNICACIONES

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACION

SECRETARIA DE PLANEACION MUNICIPAL


GOBIERNO DIGITAL

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Vigencia 2024 - 2027



San José del Guaviare enero 2024

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

CONTROL DE VERSIONES

Versión	Fecha	Modificación
1.0	31/01/2022	Versión inicial del documento
2.0	22/01/2024	Actualización vigencia 2024



	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	4
2. JUSTIFICACIÓN.....	5
3. OBJETIVOS.	6
3.2 Objetivos Específicos	6
4. ALCANCE.....	6
5. MARCO LEGAL.....	7
6. LINEAMIENTOS CONCEPTUALES.	9
6.2 Marco Conceptual.	9
6.3 Glosario.....	9
7. METODOLOGÍA.	11
8. RESPONSABLES.....	14
9. EJECUCIÓN DEL PRESUPUESTO.....	14
10. SEGUIMIENTO Y EVALUACIÓN	15
11. APROBACIÓN DEL PLAN.....	15
12. MECANISMOS DE SOCIALIZACIÓN DEL PLAN:	15
13. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	15

	REPUBLICA DE COLOMBIA
	MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION


1. INTRODUCCIÓN.

Hoy en día, la información está definida como uno de los activos más valiosos y primordiales para cualquier tipo de organización, la cual, sólo tiene sentido cuando está disponible y es utilizada de forma adecuada, integra, oportuna, responsable y segura, lo que implica, que es necesario que las organizaciones tengan una adecuada gestión de sus recursos y activos de información con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información.

El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial. Cualquier tipo de organización independiente de su tamaño y naturaleza, debe ser consciente que la diversidad de amenazas existentes que actualmente atentan contra la seguridad y privacidad de la información, representan un riesgo que al materializarse no solo les puede acarrear costos económicos, sanciones legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia del negocio.

Lo anterior, sumando a un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar, genera que cada vez más la seguridad de la información forme parte de los objetivos y planes estratégicos de las organizaciones. Por lo tanto, es indispensable que los responsables dentro de las organizaciones encargados de velar por la protección y seguridad de sus recursos, infraestructura e información, constantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del negocio, independientemente si está es de carácter organizacional o personal, o de tipo pública o privada.

En la medida que las organizaciones tengan una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, podrán establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad tanto de la información del negocio como los datos de carácter personal de sus empleados, usuarios y partes interesadas. Es indispensable que las organizaciones realicen una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riesgos que pueden afectar su seguridad, con el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2. JUSTIFICACIÓN.


El manual de la Política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones, para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

El manual en mención, precisa que el habilitador de seguridad de la información busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El Ministerio de las Tecnologías de la Información y de las Comunicaciones MINTIC, ha establecido que para proteger los activos de información y garantizar su disponibilidad, integridad y confidencialidad debe adoptarse y aplicarse el Modelo de Seguridad y Privacidad de la Información.

El documento denominado Modelo de Seguridad y Privacidad de la Información – MSPI, expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción del mismo, por las entidades del Estado, conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas.

Siguiendo las directrices del Marco de Referencia de Arquitectura Empresarial para la Gestión T.I. del Estado Colombiano, el Plan de Seguridad y Privacidad de la Información, se convertirá en una herramienta fundamental para la toma de decisiones en la administración municipal, siendo el resultado de un adecuado ejercicio de planeación estratégica de TI.

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

3. OBJETIVOS.

3.1 Objetivo Estratégico


Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la alcaldía municipal de San José del Guaviare, para reducir los riesgos a los que está expuesta la entidad hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2024-2027.

3.2 Objetivos Específicos

- Proteger los Activos de Información.
- Implementar el Sistema de Gestión de Seguridad de la Información – SGSI.
- Establecer actividades de concienciación sobre Seguridad de la Información.
- Velar por el cumplimiento de las políticas de seguridad de la información.
- Mantener la Información íntegra, disponible y con niveles de confidencialidad adecuados.
- Implementar políticas y procedimientos enfocados en la de seguridad de la información.
- Mitigar los riesgos asociados a la seguridad de la Información que afecten la integridad, confidencialidad, disponibilidad y privacidad de la Información.
- Fomentar una cultura de seguridad de la información en los servidores públicos (funcionarios, contratistas, pasantes y demás).
- Revisar y valorar la Política de Seguridad de la Información a intervalos planificados, o cuando se produzcan cambios que afecten los activos de información, de tal forma que permanezca actualizada, operativa y auditada asegurando su nivel de eficiencia y eficacia.

4. ALCANCE.

El Plan de Seguridad y Privacidad de la Información, para la vigencia 2024 - 2027, se enfocará en fortalecer la implementación de acciones de acuerdo a los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, orientados a la seguridad informática de la plataforma tecnológica de la Alcaldía de San José del Guaviare, teniendo en cuenta las capacidades y recursos disponibles para fortalecer la confianza de los ciudadanos, usuarios, terceros y demás partes interesadas.

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La seguridad de la información es un proceso que se realiza con todos los actores de la Entidad, los cuales se comprometen a seguirlas y cumplirlas adecuadamente

5. MARCO LEGAL.

Principios Rectores: de conformidad con artículo 1 del 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”, que adiciona el Decreto 1083 de 2015 Único Reglamentario del Sector de la Función Pública, las entidades del Estado de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011.

Normatividad Aplicable:


Artículo 15 De La Constitución Política De Colombia: se establece que "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en los archivos de entidades públicas y privadas".

CONPES NO. 3854 de 2016: Por medio del cual se establece la política nacional de seguridad digital.

Ley 527 de 1999: por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 1266 de 2008: por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1581 De 2012: por la cual se dictan disposiciones generales para la protección de datos personales tiene como objeto "(. .) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y todos los demás derechos, libertades y garantías constitucionales" y que dicta, además de las disposiciones generales para la protección de datos personales.

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

constitucionales" y que dicta, además de las disposiciones generales para la protección de datos personales.

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Decreto NO. 103 de 2015: por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto NO. 1494 de 2015: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

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 del 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 las Comunicaciones.

Decreto NO. 1078 de 2015: a través del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

Decreto No. 1413 de 2017: mediante su artículo 2.2.17.5.10, derechos de los usuarios de los servicios ciudadanos digitales: registrarse de manera gratuita eligiendo al operador de servicios ciudadanos digitales de su preferencia entre aquellos que estén vinculados por el articulador.

- Aceptar, actualizar y revocarlas autorizaciones para recibir información, comunicaciones y notificaciones electrónicas desde las entidades públicas a su elección a través de los servicios ciudadanos digitales.
- Hacer uso responsable de los servicios ciudadanos digitales a los cuáles se registre.
- Interponer peticiones, quejas, reclamos y solicitudes de información en relación con la prestación a los servicios ciudadanos digitales. Elegir y cambiar libremente el operador de servicios ciudadanos digitales.
- Solicitar en cualquier momento, y a través de cualquiera de los medios de atención al usuario, su retiro de la plataforma de servicios en cuyo caso podrá descargar su información a un medio de almacenamiento propio.

Decreto No. 1413 DE 2017: mediante su artículo 2.2.17.2.1.1, descripción de los servicios ciudadanos digitales, 1.5 servicio de interoperabilidad: cualquier desarrollo en el marco de los servicios ciudadanos digitales especiales deberá

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

hacer uso de o estar soportado en los servicios ciudadanos digitales básicas cuando lo requieran.

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.


6.2 Marco Conceptual.

El Plan de Seguridad y Privacidad de la Información representa la posición de la administración municipal de la Alcaldía de San José del Guaviare con respecto a la protección de los activos de información (funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Modelo de Seguridad y Privacidad de la Información; por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades para la gestión de la seguridad de la información.


Así mismo, para poder entender de manera precisa cada aspecto plasmado mediante este Plan de Seguridad y Privacidad de la Información, se hace necesario definir los conceptos más importantes que se identifican en el desarrollo y cumplimiento de los objetivos establecidos.

6.3 Glosario

- **Acceso a la Información Pública:** 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, documentos, edificios, personas) que tenga valor para la organización. (ISO/IEC 27000).
- **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 controle en su calidad de tal

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- Amenazas: causa potencial de un incidente no deseado, que puede provocar daños a un sistema u organización. (ISO/IEC 27000).
- Análisis de Riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel del mismo. (ISO/IEC 27000).
- Bases de Datos Personales: conjunto organizado de datos personales que sean objeto de Tratamiento (Ley 1581 de 2012, art 3).
- Datos Abiertos: son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).
- Datos Personales: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- Datos Personales Públicos: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- 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 Mixtos: para efectos de este plan es la información que contiene datos personales públicos junto con datos privados o sensibles.
- Ley de Habeas Data: se refiere a la Ley Estatutaria 1266 de 2008.
- Ley de Transparencia y Acceso a la Información Pública Nacional: Se refiere a la Ley 1712 de 2014.
- Mecanismos de Protección de Datos Personales: lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION


los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- 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.
- Seguridad de la Información: preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- Sistema de Gestión de Seguridad de la Información – SGSI: conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

7. METODOLOGÍA.

Estado actual de la entidad: La administración municipal realizó el diligenciamiento del formato **Autodiagnóstico Política de Gobierno Digital**, con el fin de medir el estado de la política de gobierno digital y así contar con una línea base que permita establecer los aspectos a fortalecer en la entidad.

La siguiente información revela el nivel de cumplimiento de la entidad en relación con el fortalecimiento de la seguridad y privacidad de la información:

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE	
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	

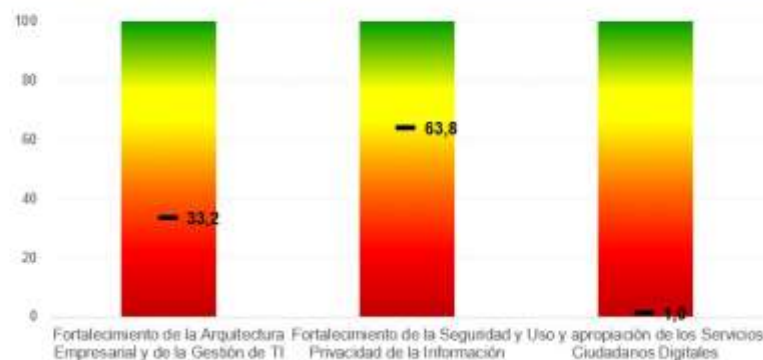
Fortalecimiento de la Seguridad y Privacidad de la Información	63,8	Porcentaje de proyectos de TI del 2020 que están ejecución o que han finalizado	1
		Porcentaje de presupuesto ejecutado en proyectos y operación de TI en la vigencia 2020	1
		La entidad cuenta con un diagnóstico de seguridad y privacidad de la información para la agencia, construido a través de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPi)	20
		La política de seguridad y privacidad de la información de la entidad: Está aprobada, implementada y se actualiza mediante un proceso de mejora continua	90
		La entidad cuenta con procedimientos de seguridad y privacidad de la información aprobados, implementados y se actualizan mediante un proceso de mejora continua	50
		Con respecto al inventario de activos de seguridad y privacidad de la información de la entidad: El inventario está aprobado, clasificado y se actualiza mediante un proceso de mejora continua	60
		Con respecto a los riesgos de seguridad y privacidad de la información de la entidad: Identifica, valora y actualiza los riesgos mediante un proceso de mejora continua	90
		La entidad implementó el plan de tratamiento de riesgos de seguridad de la información y cuenta con las evidencias	100
		Con respecto al plan operacional de seguridad y privacidad de la información, la entidad: Cuenta con un plan aprobado, implementado y se actualiza mediante un proceso de mejora continua	50
		Con respecto a los indicadores del sistema de gestión de seguridad y privacidad de la información (MSPi) de la entidad: Los indicadores están aprobados, miden la eficiencia y eficacia del sistema y se actualizan mediante un proceso de mejora continua	30

RESULTADOS AUTODIAGNÓSTICO POLÍTICA DE GOBIERNO DIGITAL


1. Calificación total:



2. Calificación de los habilitadores de la Política de Gobierno Digital:



La calificación que se obtiene es de 63.8 y de acuerdo al formato de autodiagnóstico se califica con nivel 4; lo que demuestra que a pesar de los avances que presenta la entidad en seguridad y privacidad de la información, existen problemas que se deben tener en cuenta y resolverlos tomando las medidas correspondientes.

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION


Ciclo de Operación: El Modelo de Seguridad y Privacidad de la Información de la Política de Gobierno Digital, contempla el siguiente ciclo de operación que contiene cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.



Ciclo del Modelo de Seguridad y Privacidad de la Información

Fuente: https://www.mintic.gov.co/gestionti/615/articles-482_Modelo_de_Seguridad_Privacidad.pdf

- **Fase Diagnóstico:** Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información
- **Fase Planificación (Planear):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- **Fase Implementación (Hacer):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- **Fase Evaluación de Desempeño (Verificar):** Una vez establecida la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- **Fase Mejora Continua (Actuar):** Se analizan los resultados de las acciones implementadas y si estas no cumplen los objetivos definidos, se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION



Relación entre la ciberseguridad y otros ámbitos de la seguridad


Fuente: [ISO/IEC 27032](https://www.iso.org/standard/54549.html)

8. RESPONSABLES

- Alcalde municipal
- Secretarios de despacho
- Profesional de apoyo en gobierno digital
- Técnico de sistemas

9. EJECUCIÓN DEL PRESUPUESTO

El presupuesto para la ejecución del Plan 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 software y hardware durante la vigencia 2024 – 2025. Así mismo, el presupuesto estará consolidado en el Plan Anual de Adquisiciones para las respectivas vigencias.

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

10. SEGUIMIENTO Y EVALUACIÓN

La secretaría de planeación será la dependencia encargada de realizar el seguimiento y evaluación al Plan de Seguridad y Privacidad de la Información.


11. APROBACIÓN DEL PLAN

El Comité Institucional de Gestión y Desempeño será el encargado de revisar y aprobar el Plan de Seguridad y Privacidad de la Información.


12. MECANISMOS DE SOCIALIZACIÓN DEL PLAN:

ACTIVIDAD	OBJETIVO	MEDIO DE SOCIALIZACIÓN	FECHA
Socializar el Plan de Seguridad y Privacidad de la Información	Lograr que todos los funcionarios de la entidad tanto de planta como contratistas, conozcan sus responsabilidades frente a la seguridad y privacidad de la información	*Página web *Correos electrónicos	Febrero de 2024
Aplicar 2 encuestas sobre seguridad y privacidad de la información al personal administrativo que labora en la entidad	Conocer la disposición que tiene el personal de la alcaldía y el nivel de conocimiento frente a la seguridad y privacidad de la información y crear una cultura de prevención frente a pérdida de información	*Formulario en línea	*Primer semestre de 2024 *Segundo semestre de 2024

13. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

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 SEGURIDAD Y PRIVACIDAD DE LA INFORMACION)** para cada vigencia basados en el autodiagnóstico y avances de las vigencias.

	REPUBLICA DE COLOMBIA MUNICIPIO DE SAN JOSE DEL GUAVIARE
	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION



ALCALDIA DE SAN JOSE DEL GUAVIARE

SECRETARIA DE PLANEACION MUNICIPAL

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION CRONOGRAMA DE ACTIVIDADES 2024

Elaboró: Secretaría 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	Realizar el autodiagnóstico específico en materia de seguridad y privacidad de la información, mediante la aplicación del instrumento de evaluación dispuesto en el sitio web del modelo.	Secretaría de Planeación - Profesional de apoyo Seguridad Digital	Documento publicado	Diligenciar la Herramienta de diagnóstico	1	Link de publicación	30/04/2024
2	Elaborar el Informe Técnico basado en el Diagnóstico de Seguridad y Privacidad de la Información - Vigencia 2024	Secretaría de Planeación - Profesional de apoyo Seguridad Digital	Documento presentado al CIGD, aprobado y publicado	Documento formulado, aprobado por el CIGD y publicado en la sede electrónica	1	Link de publicación - Acto administrativo de aprobación	30/05/2024
3	Elaborar el Modelo de Seguridad y Privacidad de la Información - MSPI, basados en el resultado del Autodiagnóstico y aplicar la Norma ISO 27001	Secretaría de Planeación - profesional de apoyo Seguridad Digital	Documento presentado al CIGD, aprobado y publicado	Actualizar el MSPI para la vigencia 2024, Aprobado por el CIGD y publicado en la sede electrónica	1	Link de publicación - Acto administrativo de aprobación	20/05/2024
4	Generar una estrategia de sensibilización con el fin de apropiar los temas de seguridad de la información con los funcionarios y contratista	Secretaría de Planeación - profesional de apoyo de Seguridad Digital	(Talleres, videos, correos y listas de asistencias) realizadas / (Talleres, videos, correos y listas de asistencias) programadas	Que el 80% de los funcionarios y contratistas conozcan: ► La Política de Seguridad y privacidad de la Información ► Todos los manuales, lineamientos, instructivos y procedimientos de la Seguridad de la Información de la entidad.	2	Videos, Listas de asistencia, correos enviados, alertas de seguridad enviadas	20/12/2024
5	Revisar los acuerdos contractuales estableciendo responsabilidades en la seguridad de la información.	oficina Jurídica - Profesional de apoyo de Gobierno Digital	Acción tomada con jurídica, previa aprobación del CIGD	Presentar al CIGD y su aprobación aplicarla a los contratos de Servicios	1	Acto administrativo de aprobación	20/12/2024
6	Elaborar el documento de Roles y Responsabilidades de Seguridad de Información.	Secretaría de Planeación - profesional de apoyo de Gobierno Digital	Documento presentado al CIGD, aprobado y publicado	Documento formulado, aprobado por el CIGD y publicado en la sede electrónica	1	Link de publicación	20/12/2024
7	Elaborar procedimientos de la Seguridad y Privacidad de la Información	Secretaría de Planeación - profesional de apoyo de Gobierno Digital	Documento presentado al CIGD, aprobado y publicado	Documento formulado, aprobado por el CIGD y publicado en la sede electrónica	3	Link de publicación	20/12/2024
8	Revisar el documento de las Políticas de Seguridad y Privacidad de la Información y actualizarlo	Secretaría de Planeación - profesional de apoyo de Gobierno Digital	Documento presentado al CIGD, aprobado y publicado	Documento formulado, aprobado por el CIGD y publicado en la sede electrónica	1	Link de publicación	20/12/2024
9	Revisar, Elaborar o actualizar el Inventario de Activos de Información	Secretaría de Planeación - profesional de apoyo de Gobierno Digital	Documento presentado al CIGD, aprobado y publicado	Documento formulado, aprobado por el CIGD y publicado en la sede electrónica	1	Link de publicación	20/12/2024
10	Crear el Instructivo de renovación y compra de equipos tecnológicos.	Secretaría de Planeación - profesional de apoyo de Gobierno Digital y Soporte Técnico	Documento presentado al CIGD, aprobado y publicado	Documento formulado, aprobado por el CIGD y publicado en la sede electrónica	1	Link de publicación	20/12/2024
11	Sensibilizar a los funcionarios y contratistas el procedimientos de copias de seguridad	Secretaría de Planeación - profesional de apoyo de Gobierno Digital	Documento presentado al CIGD, aprobado y publicado	Documento formulado, aprobado por el CIGD y publicado en la sede electrónica	1	Link de publicación	20/12/2024