CONTENIDO

1. OBJETIVOS 3
1.1. Objetivo General 3
1.2. Objetivos Específicos 3
2. ALCANCE 3
3. RESPONSABLES 4
4. DESARROLLO 4
4.1. Fase Diagnóstico 4
4.1.1 Resultado de la Herramienta de Diagnóstico de Seguridad y Privacidad de la Información 5
4.2. Fase de Planificación 8
4.2.1 Metas, Resultados e Instrumentos de la Fase de Planificación 8
4.3. Fase de Operación 10
4.3.1 Metas, Resultados e Instrumentos de la Fase de Operación 10
4.4. Fase de Evaluación y Desempeño 11
4.4.1 Metas, Resultados e Instrumentos de la Fase de evaluación y desempeño 11
4.5. Fase de Mejora Continua 11
4.5.1 Metas, Resultados e Instrumentos de la Fase de mejora continua 11
5. SEGUIMIENTO 12
6. CONTROL DE CAMBIOS 15

LISTA DE GRÁFICOS

Ilustración 1: Ciclo de operación del Modelo de Seguridad y Privacidad de la Información.... 4
Ilustración 2: Evaluación de efectividad de los controles de la entidad 5
Ilustración 3: ANEXO A ISO 27001:2013 6
Ilustración 4: Avance PHVA 6
Ilustración 5: NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 7
Ilustración 6: - Calificación frente a mejores prácticas..... 8

1. OBJETIVOS

1.1. Objetivo General

Establecer un conjunto de medidas, políticas y procedimientos, teniendo como guía los distintos lineamientos proporcionados por el MINTIC y alineados a la norma ISO/IEC 27001, para garantizar la protección, confidencialidad, integridad y disponibilidad de la información manejada por la entidad, así como para prevenir y gestionar los riesgos asociados a su manejo. De esta manera, se busca asegurar la continuidad de los servicios y procesos de la Alcaldía de Fusagasugá.

1.2. Objetivos Específicos

- Realizar el diagnóstico de la seguridad de la información de la entidad mediante el instrumento de evaluación del Modelo de Seguridad y Privacidad de la Información (MSPI), para garantizar la mejora continua del plan.
- Acatar los lineamientos para la implementación de mejores prácticas de seguridad que permitan identificar y proteger la infraestructuras críticas en la entidad.
- Sensibilizar a los servidores públicos y contratistas de la Entidad acerca del MSPI, fortaleciendo el nivel de conciencia de estos, en cuanto a la necesidad de salvaguardar los activos de información de la Entidad.
- Implementar acciones correctivas y de mejora para la Seguridad de la Información en la entidad.

2. ALCANCE

El Plan de Seguridad y Privacidad de la Información identifica e incluye la gestión del Ciclo Planificar -Hacer-Verificar-Actuar (PHVA) de operación del Modelo de Seguridad y Privacidad de la Información (MSPI), el cual abarca todas las áreas y procesos de la entidad que manejan información, incluyendo datos personales, financieros, estratégicos y de carácter sensible, el plan se aplica a todos los sistemas, equipos y dispositivos utilizados en la gestión de la información, así como a todos los usuarios y terceros que acceden a ella.

El presente documento aplica para la vigencia 2024, el cual fortalecerá las acciones de mejora frente a las debilidades encontradas mediante en el instrumento de evaluación del MSPI del año anterior. Este instrumento indica que el nivel de madurez de Alcaldía de Fusagasugá se encuentra optimizado, lo que significa que existe un mejoramiento continuo del MSPI.

Además, el plan establece los lineamientos para la gestión de incidentes de seguridad y privacidad de la información, incluyendo la identificación, notificación, gestión y respuesta a incidentes y vulnerabilidades. También se incluye la definición de los requisitos para la capacitación y concientización de los usuarios en temas de seguridad y privacidad de la información, y la evaluación y seguimiento continuo del plan para garantizar su efectividad y cumplimiento de los objetivos establecidos.

3. RESPONSABLES

Las responsabilidades del Plan de Seguridad y Privacidad de la Información recaen en todos los servidores públicos de la Alcaldía de Fusagasugá (funcionarios y contratistas), debido a que todos los funcionarios públicos son los encargados de crear, recolectar, procesar, analizar datos para entidad.

Sin embargo, realizando el ajuste a lo establecido con la guía N° 4 Roles y responsabilidades de los documentos del Modelo de Seguridad y Privacidad de la Información y mediante la aprobación de los miembros del Comité Institucional de Gestión y Desempeño, se conforma el equipo líder, que supervisara el Plan de Seguridad y Privacidad de la Información. Este equipo líder estará conformado por los miembros del Comité Institucional de Gestión y Desempeño, en conjunto con oficial de seguridad, representante de la oficina de las TIC y Transformación Digital, un representante de la Oficina de Control Interno y un representante de la Secretaría Jurídica.

4. DESARROLLO

La metodología de implementación del Plan de Seguridad y Privacidad de la información está basada en el ciclo PHVA y lo establecido en el Modelo de Seguridad y Privacidad de MinTIC, el cual cuenta con 5 fases, cada una de ellas contienen objetivos, metas y herramientas (guías) que permiten que el modelo sea sostenible en una entidad.

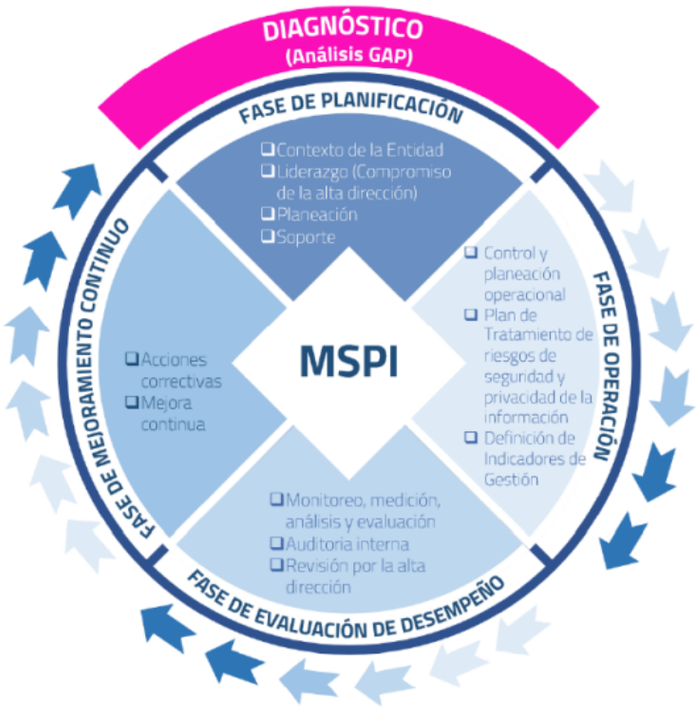

Ilustración 1: *Ciclo de operación del Modelo de Seguridad y Privacidad de la Información*

4.1. Fase Diagnóstico

En la fase previa conocida como diagnóstico del MSPI permite que a través del uso de herramientas de diagnóstico, actividades de reconocimiento y valoración de controles de

seguridad de la información, se pueda identificar el estado actual de la Entidad en temas de seguridad y privacidad; el resultado de este diagnóstico permitirá establecer el nivel de madurez en cuanto a seguridad y privacidad de la información, y así definir la hoja de ruta para las actividades en las siguientes fases del modelo.

4.1.1 Resultado de la Herramienta de Diagnóstico de Seguridad y Privacidad de la Información

Esta herramienta tiene como función evaluar la seguridad y privacidad de la información manejada por la entidad, con el fin de identificar posibles vulnerabilidades y riesgos de seguridad que pueden afectar la confidencialidad y disponibilidad de los datos. A través de esta herramienta, se busca implementar medidas de seguridad efectivas y garantizar la protección de la información ante posibles amenazas y ataques cibernéticos.

A continuación, se relacionan los resultados obtenidos por la herramienta de Evaluación MSPI de la Política Nacional de Gobierno Digital proporcionado por MinTIC.

- **El porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2013:**

En este componente se muestra el resultado del análisis de brecha frente a los controles del Anexo A, del estándar ISO 27001:2013, y la guía de controles (Guía #8) del Modelo de Seguridad de Privacidad de la Información.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	96	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	91	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	93	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	100	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	80	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	91	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	90	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	83	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	80	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	91	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	100	100	OPTIMIZADO
A.18	CUMPLIMIENTO	93,5	100	OPTIMIZADO
	PROMEDIO EVALUACIÓN DE CONTROLES	92	100	OPTIMIZADO

***Ilustración 2*:** Evaluación de efectividad de los controles de la entidad

La entidad en la vigencia 2023 obtuvo un puntaje promedio de evaluación de controles en 92/100, lo que indica que se encuentra en un nivel de efectividad **OPTIMIZADO**, este nivel evidencia que existe un mejoramiento continuo del MSPI en la entidad con relación a las actividades señaladas el dominio que son realizadas en la entidad con la orientación de la Oficina TIC y Transformación Digital, de esta manera, se logran avances frente a los lineamientos del MSPI.

Ilustración 3: *ANEXO A ISO 27001:2013*

Como se evidencia en el gráfico anterior (ilustración 2. Brecha de ANEXO A ISO 27001:2013) la Alcaldía de Fusagasugá debe generar un plan de acción para dar cumplimiento al 100% de cada uno de los controles. Es importante señalar, que la Alcaldía de Fusagasugá debe continuar realizando acciones que permitan dar cumplimiento al MSPI, lo que sugiere el compromiso de la administración a nivel presupuestal y en recursos humanos para adquirir equipos, infraestructura, software, y proponer y efectuar estrategias, proyectos y soluciones específicas para dar continuidad a la ejecución del MSPI.

- **AVANCE DEL CICLO PHVA**

A través del diligenciamiento y la formulación de esta hoja de la herramienta se determina el nivel de cumplimiento de acuerdo con el ciclo PHVA del Modelo de Seguridad MSPI, el ciclo evaluado incluye cuatro (4) componentes: Planificación, Implementación, Gestión y Mejora Continua.

AVANCE PHVA		
COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
Planificación	33%	40%
Implementación	13%	20%
Evaluación de desempeño	15%	20%
Mejora continua	16%	20%
TOTAL	**76%**	**100%**

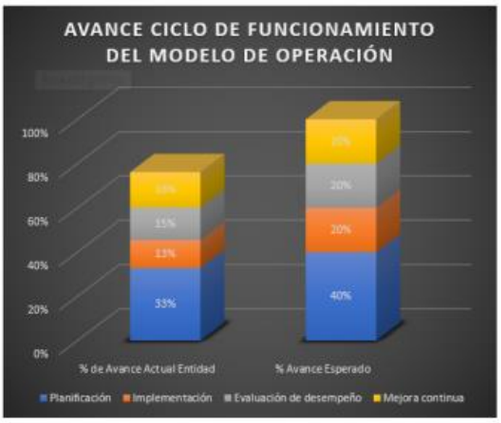

Ilustración 4*: Avance PHVA*

Este componente permite evidenciar el avance en el Ciclo del Modelo de Seguridad definido en el documento MSPI para la entidad, en el que se evidencia un resultado de 76/100, puntaje que corresponde a las actividades realizadas en cada uno de los componentes y sugiere la responsabilidad de continuar con la actualización, mejoramiento, actualización y retroalimentación. Algunas de las actividades sujetas a actualización son las siguientes:

- Mapa de riesgos de seguridad y privacidad de la información
- Declaración de aplicabilidad del Modelo de Seguridad y Privacidad de la Información
- Manual de Seguridad de la Información
- Plan de transición de protocolo IPv4 a IPv6
- Procedimiento de identificación y clasificación de activos de información
- Gestión de medios removibles
- Procedimiento mapa de riesgos seguridad y privacidad de la información.

- **NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

En la hoja de madurez del MSPI del Instrumento de Evaluación se identificaron los requisitos necesarios para cumplir los niveles de madurez definidos. La mayoría de estos requisitos ya fueron evaluados previamente en las hojas Administrativas, Técnicas y PHVA. Sin embargo, hay tres requisitos de madurez que no fueron identificados en las hojas mencionadas, por lo que el evaluador deberá realizar la valoración y calificación manualmente en estos casos. Para el resto de la tabla, los controles se calificarán automáticamente al diligenciar las otras hojas mencionadas.

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	SUFICIENTE
Definido	SUFICIENTE
Administrado	SUFICIENTE
Optimizado	INTERMEDIO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

Ilustración 5: *NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN*

La anterior ilustración muestra el resultado obtenido por la Alcaldía de Fusagasugá y se evidencia que se encuentra en un nivel de madurez **OPTIMIZADO** lo que indica que existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

- **CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)**

En esta evaluación se busca determinar en qué medida la entidad cumple con las mejores prácticas en ciberseguridad definidas por el Instituto Nacional de Estándares y Tecnología (NIST), con el objetivo de realizar un diagnóstico sobre el grado de cumplimiento de los lineamientos de la Política de Ciberseguridad y Ciberdefensa establecidos en los documentos CONPES 3701 y CONPES 3854.

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	Promedio de CALIFICACIÓN	NIVEL IDEAL CSF
DETECTAR	86	100
IDENTIFICAR	81	100
PROTEGER	89	100
RECUPERAR	60	100
RESPONDER	87	100

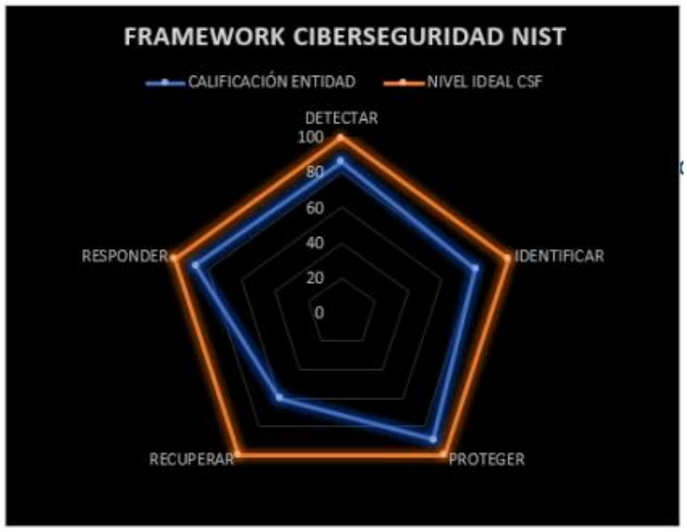

Ilustración 6: - *Calificación frente a mejores prácticas*

En este componente se muestra una tabla con los resultados de comparar la calificación de acuerdo con la escala de evaluación de los controles existentes en la entidad frente a la mejor práctica en Ciberseguridad definida por NIST. La gráfica muestra la brecha entre la calificación alcanzada y la calificación objetivo, como se puede observar, la calificación frente a cada etiqueta de fila en la mayoría de los casos es superior a 80, es decir, se ha logrado mejorar y responder a los lineamientos en materia de seguridad.

4.2. Fase de Planificación

La Fase de Planificación del MSPI proporciona la base para la implementación de medidas de seguridad eficaces y permite a la entidad identificar y reducir los riesgos de seguridad de la información.

4.2.1 Metas, Resultados e Instrumentos de la Fase de Planificación

Metas	Resultados requeridos en el instrumento	MSPI	Actividades realizadas por la Alcaldía de Fusagasugá
Política de Seguridad y Privacidad de la Información.	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Guía No 2 – Política General MSPI	La entidad cuenta con 10 políticas de seguridad: • Control de acceso • Escritorio y pantalla limpia • Uso aceptable de los activos • Desarrollo seguro de software • Construcción de sistemas

			seguros • Generación y restauración de copias de respaldo • Uso de dispositivos móviles • Trasferencia de la información • Seguridad de proveedores • Legislación aplicable y requisitos contractuales Las cuales se encuentran en el **MA-GT-002** Manual de Seguridad y Privacidad de la Información MSPI
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información	Se realiza la actualización de **PR-GT-005** procedimiento protocolo copia de seguridad. Se crea el procedimiento **PR-GT-007** procedimiento proceso de construcción de software
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información	Se cuenta con el Decreto 058 del 13 de junio de 2023, por medio del cual se compila y se actualiza la implementación del Modelo Integrado de Planeación y Gestión (MIPG), en el documento se establece que el líder de la Política de Seguridad Digital es la Oficina TIC y Transformación Digital con el apoyo de todos los procesos. En reuniones de Comité Institucional de Gestión y Desempeño se creó un equipo líder para el seguimiento y toma de decisiones en seguridad, el cual estará conformado por los miembros del Comité Institucional de Gestión y Desempeño, en conjunto con oficial de seguridad, representante de la oficina de las TIC y Transformación Digital, un representante de la Oficina de Control Interno y un representante de la Secretaría Jurídica.
Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6	Guía No 5 - Gestión De Activos Guía No 20 - Transición Ipv4 a Ipv6	Seguimiento del inventario de activos de información mediante en el formato **FO-GT-013** INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN. Se realizó el levantamiento de 478 activos de información para la Alcaldía de Fusagasugá. El formato **FO-GT-013** INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN, debe ser revisado y actualizado por cada una de las dependencias de la entidad cuando el líder del proceso lo considere necesario y de esta manera reportar a la Oficina TIC y Transformación Digital los cambios o ajustes

			realizados.
Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Guía No 6 - Gestión Documental	La actividad se encuentra inmersa en el plan de acción del MSPI
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección	Guía No 7 - Gestión de Riesgos Guía No 8 - Controles de Seguridad	Se cuenta con el **PL-GT-007** Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Guía No 14 - Plan de comunicación, sensibilización y capacitación	La actividad se encuentra inmersa en el plan de acción del MSPI
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Guía No 20 - Transición IPv4 a IPv6	Se crea el **PL-GT-003** Plan de diagnóstico para la adopción IPv6

4.3. Fase de Operación

La Fase de Operación del MSPI permite la implementación y el mantenimiento efectivo de los controles de seguridad definidos en la Fase de Planificación. La realización adecuada de estas actividades contribuye a proteger la información crítica de la entidad y a reducir los riesgos de seguridad.

4.3.1 Metas, Resultados e Instrumentos de la Fase de Operación

Metas	Resultados requeridos en el instrumento	MSPI	Actividades realizadas por la Alcaldía de Fusagasugá
Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad.	Se cuenta con el **PL-GT-007** Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos.	Se cuenta con el **PL-GT-007** Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, del cual se cuenta con informes de ejecución de las actividades.
Indicadores De Gestión	Documento con la descripción de los indicadores de gestión de seguridad y	Guía No 9 - Indicadores de Gestión SI.	La entidad cuenta con el **FO-DE-023** ficha técnica de indicadores de gestión del proceso Gestión TIC. Se deben actualizar los indicadores de

	privacidad de la información.		gestión de seguridad y privacidad de la información,
Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. Guía No 20 - Transición de IPv4 a IPv6 para Colombia. Guía No 19 – Aseguramiento del Protocolo IPv6.	Se cuenta con el **PL-GT-003** Plan de diagnóstico para la adopción IPv6

4.4. Fase de Evaluación y Desempeño

La Fase de Evaluación y Desempeño del MSPI permite la evaluación continua de los controles de seguridad implementados y la identificación de áreas de mejora. La realización adecuada de estas actividades ayuda a garantizar la protección de la información crítica de la organización ya reducir los riesgos de seguridad.

4.4.1 Metas, Resultados e Instrumentos de la Fase de evaluación y desempeño

Metas	Resultados requeridos en el instrumento	MSPI	Actividades realizadas por la Alcaldía de Fusagasugá
Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Guía No 16 – Evaluación del desempeño.	Se actualiza el **PL-GT-008** Plan de Seguridad y Privacidad de la Información según el seguimiento realizado.
Plan de Ejecución de Auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	Guía No 15 – Guía de Auditoría	Se crea el **PL-CSG-001** Plan Estratégico de Auditoria.

4.5. Fase de Mejora Continua

La Fase de Mejora Continua es la etapa en la que se implementan planos para mejorar y mantener los controles de seguridad de manera constante.

4.5.1 Metas, Resultados e Instrumentos de la Fase de mejora continua

Metas	Resultados requeridos en el instrumento	MSPI	Actividades realizadas por la Alcaldía de Fusagasugá
Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan	Resultados de la ejecución del Plan de	Se cuenta con un plan de mejora del Modelo de Seguridad y Privacidad de la Información, el cual se encuentra

	de comunicación de resultados.	Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Guía No 17 – Mejora Continua	monitoreado por la Oficina de Control Interno

5. SEGUIMIENTO

Para realizar el seguimiento del Plan de Seguridad y Privacidad de la Información, se pueden seguir los siguientes pasos:

1. Establecer el comité de seguimiento: Es importante contar con un equipo encargado de realizar el seguimiento del plan y de tomar decisiones en caso de que se presentan desviaciones o problemas. El equipo líder está conformado por los miembros del Comité Institucional de Gestión y Desempeño, en conjunto con oficial de seguridad, representante de la oficina de las TIC y Transformación Digital, un representante de la Oficina de Control Interno y un representante de la Secretaría Jurídica.

2. Establecer un cronograma de seguimiento: Se debe establecer un cronograma de seguimiento que permita realizar un monitoreo periódico del avance del plan y de los indicadores definidos.

Ítem	Metas	Actividad	MSPI	Responsable	Periodo de entrega
1	Política de Seguridad y Privacidad de la Información.	1) Crear la Política de Seguridad y Privacidad de la Información. 2) Presentar para su aprobación y disponer la información en el punto de uso oficial (intranet)	Guía No 2 – Política General MSPI	Oficina de las TIC y Transformación Digital Secretaría Jurídica Comité Institucional de Gestión y Desempeño	Anual

2	Procedimientos de seguridad de la información.	1) Listado maestro de los procedimientos, formatos, guías, planes y demás documentos relacionados al MSPI 2) Actualizar los procedimientos, formatos, guías, planes y demás documentos que se requieran para la mejora del MSPI. 3) Presentar para su aprobación y disponer la información en el punto de uso oficial (intranet)	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información	Oficina de las TIC y Transformación Digital	Semestral
3	Roles y responsabilidades de seguridad y privacidad de la información	Socialización del Decreto 058 del 13 de junio de 2023, por medio del cual se compila y se actualiza la implementación del Modelo Integrado de Planeación y Gestión (MIPG), en el documento se establece que el líder de la Política de Seguridad Digital es la Oficina TIC y Transformación Digital con el apoyo de todos los procesos.	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información	Dirección de Desarrollo Organizacional Oficina de las TIC y Transformación Digital	Semestral
4	Inventario de activos de información.	1) Realizar mesas de trabajo con los lideres de proceso, servidores públicos asignados y áreas de trabajo involucradas para capacitar en el Formato FO-GT-013 y Procedimiento PR-GT-003 frente a la identificación, clasificación y registro de los activos de información. 2) Realizar los ajustes y/o actualizaciones del Formato FO-GT-013 cuando el líder de proceso lo requiera.	Guía No 5 - Gestión De Activos	Oficina de las TIC y Transformación Digital Oficina Asesora de Comunicaciones secretaria Administrativa Secretaría Jurídica.	Anual
5	Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Guía No 6 - Gestión Documental	Oficina de las TIC y Transformación Digital Secretaría Administrativa	Anual
6	Identificación, Valoración y tratamiento de riesgo	1) Realizar las actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Guía No 7 - Gestión de Riesgos Guía No 8 - Controles de Seguridad	Oficina de las TIC y Transformación Digital Dependencias que tengan responsabilidad en las	Definidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

				actividades del plan.	
7	Plan de Comunicaciones.	1) Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Guía No 14 - Plan de comunicación, sensibilización y capacitación	Oficina de las TIC y Transformación Digital Oficina Asesora de Comunicaciones Dirección de Desarrollo Organizacional	Anual
8	Plan de diagnóstico de IPv4 a IPv6.	1) Actualización del inventario de activos tecnológicos de la entidad 2) Actualización del plan diagnostico para la adopción IPv6 3) Presentar para su aprobación y disponer la información en el punto de uso oficial (intranet)	Guía No 20 - Transición IPv4 a IPv6	Oficina de las TIC y Transformación Digital	Anual
9	Implementación del plan de tratamiento de riesgos	1) Informe de la ejecución del plan de tratamiento de riesgos 2) Presentar para su aprobación y disponer la información en el punto de uso oficial (intranet)	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos.	Oficina de las TIC y Transformación Digital	Semestral
10	Indicadores De Gestión	1) Realizar la actualización del documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información. 2) Presentar para su aprobación y disponer la información en el punto de uso oficial (intranet)	Guía No 9 - Indicadores de Gestión	Oficina de las TIC y Transformación Digital	Anual
11	Plan de Transición de IPv4 a IPv6	1) Actualización del plan de transición del protocolo IPv4 a IPv6 2) Presentar para su aprobación y disponer la información en el punto de uso oficial (intranet)	Documento actualizado y aprobado del Plan de transición del protocolo IPv4 a IPv6	Oficina de las TIC y Transformación Digital	Anual

3. Realizar informes de seguimiento: Se deben elaborar informes de seguimiento que puedan comunicar el avance del plan y los resultados obtenidos a los miembros del comité de seguimiento y a la alta dirección de la organización.

4. Realizar revisiones periódicas del plan: Es importante realizar revisiones periódicas del plan para evaluar su eficacia y realizar ajustes en caso de ser necesario.

5. Realizar auditorías de seguridad: Se deben realizar auditorías de seguridad de manera periódica para evaluar el cumplimiento de las políticas y procedimientos de seguridad de la información y para identificar posibles desviaciones o problemas.

6. CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DEL CAMBIO REALIZADO
01	01/2019	CREACIÓN DEL DOCUMENTO
02	01/2020	Actualización del Plan por cambio a vigencia 2020
03	01/2021	Actualización del Plan por cambio a vigencia 2021
04	01/2022	Actualización del Plan por cambio a vigencia 2022
05	30/01/2023	Actualización del Plan por cambio a vigencia 2023
06	19/09/2023	Se actualiza el plan dando cumplimiento a la normatividad vigente, y basado en los resultados del instrumento de evaluación del MSPI
07	30/01/2024	**Se actualiza el documento con los resultados del instrumento de evaluación del MSPI del MINTIC y se actualizan actividades para la vigencia 2024.**