SECRETARÍA DISTRITAL DE PLANEACIÓN

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Responsable:

Comité Institucional de Gestión y Desempeño Secretaría Distrital de Planeación
Actualización presentada y aprobada en sesión del Comité Institucional de Gestión y Desempeño de la SDP realizada el 22 de enero de 2025

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La información es uno de los activos más valiosos de cualquier organización. Para la Secretaría Distrital de Planeación (SDP), garantizar su seguridad y privacidad es primordial. Esto implica implementar estrategias robustas para proteger los activos de información contra las crecientes amenazas, previniendo incidentes de seguridad que puedan impactar la imagen institucional, las relaciones con usuarios internos y externos, generar pérdidas económicas o acarrear consecuencias legales.

La SDP tiene como objetivo principal orientar y liderar la formulación y seguimiento de las políticas y la planeación territorial, económica, social y ambiental del Distrito Capital, en coordinación con otros sectores. En el marco de la política de Gobierno Digital, la SDP busca optimizar su funcionamiento y la interacción con otras entidades públicas mediante el uso estratégico de las TIC y el fortalecimiento de las capacidades de gestión de las tecnologías de información. Esto permite procesos internos seguros y eficientes, que a su vez se traducen en la entrega de servicios de valor a la ciudadanía.

En consonancia con estos objetivos y buscando la eficiencia administrativa, la SDP expidió la Resolución No. 2153 del 29 de septiembre de 2023, la cual actualiza el Sistema de Gestión (SG) bajo el Modelo Integrado de Planeación y Gestión (MIPG). Esta resolución responde a los requisitos normativos, la dinámica organizacional y la necesidad de articular modelos y sistemas como el MIPG, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los modelos internos de trabajo. El artículo 7 de la Resolución 2153 de 2023 asigna al Comité Institucional de Gestión y Desempeño, entre otras funciones, las de:

- Orientar la implementación de las Políticas de Gobierno Digital y Seguridad Digital, asegurando los recursos necesarios para la transformación digital de la SDP, siguiendo los lineamientos definidos para los componentes TIC para el Estado y TIC para la Sociedad.

- Apoyar estratégicamente las actividades de desarrollo, implementación y apropiación de la seguridad de la información, preservando la confidencialidad, integridad, disponibilidad y privacidad de los datos que maneja la SDP.

En cumplimiento de la política de Gobierno Digital y su habilitador, el MSPI, y la política de Seguridad Digital, la SDP incluyó en su Sistema de Gestión el desarrollo de las siete (7) dimensiones y diecinueve (19) políticas de gestión del MIPG, añadiendo un componente ambiental. Se definieron las dependencias responsables de liderar la implementación, correspondiendo a la Dirección de Tecnologías de la Información y las Comunicaciones el liderazgo en las políticas de Gobierno Digital y Seguridad Digital.

Reconociendo la seguridad de la información como un tema estratégico, la alta dirección de la SDP apoya la implementación del MSPI y el desarrollo de planes para la gestión del riesgo. Revisa y aprueba las Políticas de Seguridad de la Información - **GTI-PO-015** y los instrumentos asociados al sistema de gestión de seguridad de la información, demostrando un firme compromiso con la

seguridad de la información.

La implementación del MSPI se soporta en diversos instrumentos, entre ellos el Plan de Seguridad y Privacidad de la Información de la SDP - **GTI-PL-005**. Este plan facilita el desarrollo evolutivo del Sistema de Gestión de Seguridad de la Información y la implementación de la estrategia de seguridad digital, fortaleciendo la seguridad en términos de integridad, confiabilidad y disponibilidad y en cumplimiento del Decreto 612 de 2018 y el artículo 5 de la resolución 500 de 2021, siguiendo las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones es actualizado anualmente.

1. OBJETIVO

Optimizar el nivel de seguridad y privacidad de la información de la SDP, mediante la actualización e implementación del Plan de Seguridad y Privacidad de la Información, en concordancia con el Decreto 612 de 2018 y la Resolución 500 de 2021. Este plan se enfocará en fortalecer los controles existentes y establecer nuevos controles para garantizar la integridad, confidencialidad y disponibilidad de los activos de información, reduciendo los riesgos a niveles aceptables, aplicando las estrategias de seguridad digital y las recomendaciones de la evaluación del Modelo de Seguridad y Privacidad de Información MSPI.

1.1. Objetivos específicos

- **Asegurar el cumplimiento del marco legal y normativo**: Propender por el cumplimiento de los requisitos legales, reglamentarios, regulatorios y normas vigentes en Colombia en materia de Seguridad y Privacidad de la Información, identificando y documentando las obligaciones aplicables a la SDP, y estableciendo mecanismos de verificación de su cumplimiento.

- **Fortalecer el Sistema de Gestión de Seguridad de la Información (SGSPI)**: Implementar, mantener y/o mejorar los controles de seguridad del SGSPI de la SDP, alineados con el Modelo de Seguridad y Privacidad de la Información (MSPI), la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública y la Norma ISO27001, priorizando aquellos controles que mitiguen los riesgos identificados en la evaluación del MSPI.

- **Identificar las necesidades de actualización e implementación del SGSI**: Realizar un diagnóstico de las necesidades de actualización e implementación de nuevos componentes en el SGSI, documentando las brechas existentes y proponiendo soluciones específicas, incluyendo la definición de criterios de priorización para su implementación. (Autodiagnóstico MSPI)

- **Priorizar y planificar la implementación de mejoras al SGSI**: Establecer un plan de trabajo con cronograma y recursos asignados para la implementación de las mejoras priorizadas al SGSI, incluyendo la definición de indicadores de seguimiento y evaluación.

(Plan de Implementación de controles.)

- **Evaluar y realizar seguimiento a la efectividad del SGSI**: Implementar un programa de evaluación y seguimiento periódico de los controles y lineamientos implementados en el marco del SGSI, utilizando indicadores de desempeño y realizando auditorías internas para verificar su efectividad y proponer mejoras. (Plan de Implementación de controles revisado de manera periódica.)

- **Promover la cultura de seguridad y privacidad de la información**: Desarrollar e implementar un plan de capacitación y sensibilización en gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación dirigido a todos los funcionarios y contratistas de la SDP, con el fin de fortalecer la cultura institucional en estos temas.

2. ALCANCE

El presente Plan de Seguridad y Privacidad de la Información (PSPI) de la SDP define el marco para la gestión de la seguridad de la información en la entidad, abarcando:

- **Activos de Información:** Todos los activos de información de la SDP, independientemente de su formato (físico o electrónico), ubicación o medio de almacenamiento, incluyendo, pero no limitándose a: datos personales, información financiera, información de proyectos, información estratégica, entre otros.

- **Procesos:** Todos los procesos de la SDP que involucran la creación, recepción, procesamiento, almacenamiento, transmisión y disposición de información.

- **Infraestructura:** La infraestructura tecnológica que soporta los procesos de la SDP, incluyendo redes, servidores, equipos de cómputo, dispositivos móviles y sistemas de información.

- **Software:** Abarca todos los aspectos relacionados con el software utilizado por la SDP para la gestión de la información, incluyendo sistemas misionales, sistemas de apoyo, software de infraestructura, aplicaciones móviles, software en la nube, software de desarrollo propio y software de terceros (comercial o de código abierto), así como las bibliotecas y componentes de software utilizados. El alcance cubre todas las fases del ciclo de vida del software, desde la adquisición/desarrollo hasta el retiro, e incluye consideraciones de seguridad en el desarrollo, gestión de vulnerabilidades, control de cambios, gestión de licencias y mantenimiento de un inventario de software actualizado.

- **Partes Interesadas:** Todas las partes interesadas relevantes para la seguridad de la información de la SDP, incluyendo funcionarios, contratistas, proveedores, ciudadanos y otras entidades públicas.

- **Marco Normativo:** El cumplimiento del marco legal y normativo vigente en Colombia en materia de seguridad y privacidad de la información, incluyendo, pero no limitándose a: el Decreto 612 de 2018, la Resolución 500 de 2021, la Ley 1581 de 2012 (Protección de Datos Personales), la norma ISO/IEC 27001 y la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública.

- **Controles de Seguridad:** La implementación, mantenimiento y mejora de los controles de seguridad del SGSI, incluyendo los controles del Anexo A de la ISO/IEC 27001 que apliquen a la SDP, priorizando aquellos que mitiguen los riesgos identificados en la evaluación del MSPI. La Declaración de Aplicabilidad del SGSI en la SDP - **GTI-MA-005** detalla la aplicabilidad de estos controles y sus justificaciones.

- **Cultura de Seguridad:** El fortalecimiento de la cultura de seguridad y privacidad de la información en la SDP a través de programas de capacitación y sensibilización dirigidos a todos los funcionarios y contratistas. (GTI-PO-009 Política de Capacitación y Sensibilización en Seguridad de la Información en la SDP)

3. MARCO DE REFERENCIA

El Plan de Seguridad y Privacidad de la Información (PSPI) de la SDP se fundamenta en el siguiente marco normativo, que proporciona la base legal, técnica y conceptual para su estructura y funcionamiento:

3.1. Normativa Nacional:

- **Constitución Política de Colombia**: Fundamento principal que establece los derechos fundamentales, como el derecho a la intimidad, el habeas data y el acceso a la información pública, que son la base para la seguridad y privacidad de la información.
- **Ley 1581 de 2012 (Protección de Datos Personales)**: "Por la cual se dictan disposiciones generales para la protección de datos personales." Esta ley regula el tratamiento de datos personales en Colombia y establece los derechos de los titulares de los datos.
- **Decreto 1078 de 2015** (Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones): Recopila y actualiza la normatividad del sector TIC, incluyendo aspectos relacionados con la seguridad de la información.
- **Decreto 612 de 2018** (Integración de Planes Institucionales): "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." Este decreto establece la obligatoriedad de incluir el Plan de

Seguridad y Privacidad de la Información dentro de la planificación estratégica de las entidades públicas.

- **Resolución 500 de 2021** (Estrategia de Seguridad Digital y MSPI): "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". Esta resolución es crucial, ya que adopta el MSPI y define lineamientos para la seguridad digital.

3.2. Lineamientos y Estándares del MINTIC:

- **Política de Gobierno Digital**: Marco general que orienta el uso estratégico de las TIC en el sector público, incluyendo la seguridad de la información como un habilitador fundamental.
- **Modelo de Seguridad y Privacidad de la Información (MSPI)**: Metodología del MINTIC que proporciona un marco de referencia para la gestión de la seguridad y privacidad de la información en las entidades públicas.
- **Manual de Gobierno Digital**: Documento que desarrolla la Política de Gobierno Digital y proporciona orientaciones para su implementación, incluyendo aspectos de seguridad de la información.
- **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (DAFP)**: Aunque emitida por el Departamento Administrativo de la Función Pública (DAFP), esta guía es relevante para la gestión de riesgos de seguridad de la información.

3.3. Normas Técnicas Internacionales:

- **ISO/IEC 27001:2013** (Sistemas de Gestión de Seguridad de la Información): Norma internacional que especifica los requisitos para un sistema de gestión de seguridad de la información (SGSI). (Referencia el modelo implementado en la SDP y sustento del autodiagnóstico MSPI)
- **ISO/IEC 27001:2022** (Sistemas de Gestión de Seguridad de la Información): Norma internacional que especifica los requisitos para un sistema de gestión de seguridad de la información (SGSI). (Referencia a la migración del MSPI y el SGSI implementados por la SDP a la última versión de la norma)
- **ISO/IEC 27002:2022** (Código de Buenas Prácticas para los Controles de Seguridad de la Información): Norma internacional que proporciona directrices para la implementación de controles de seguridad de la información. (Referencia a la migración del MSPI y el SGSI implementados por la SDP a la última versión de la norma)
- **ISO/IEC 27701:2019** (Extensión de la ISO/IEC 27001 para la Gestión de la Privacidad de la Información): Norma internacional que proporciona directrices para la gestión de la privacidad de la información.

4. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE

SEGURIDAD DE LA INFORMACIÓN

El presente apartado tiene como objetivo ofrecer una visión integral del estado actual del Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, correspondiente a la evaluación con corte a 31 de diciembre del año 2024. Para ello, se analizarán tres componentes fundamentales que permiten comprender la madurez y eficacia del SGSI; Evaluación de efectividad de controles 2024, avance PHVA y modelo Framework ciberseguridad NIST 2024.

4.1. Evaluación de Efectividad de Controles

En este numeral se presenta los resultados sobre la efectividad de los controles de seguridad implementados en la entidad. Esta evaluación permite observar si los controles están funcionando según lo previsto y si son adecuados para mitigar los riesgos de seguridad de la información identificados. Se analizaron los resultados de la evaluación realizada, identificando fortalezas, debilidades y oportunidades de mejora. Esta evaluación esta alineada con las mejores prácticas y estándares internacionales, buscando la mejora continua del SGSI. Así mismo, este análisis permite identificar las principales diferencias y tendencias en el desempeño de cada dominio evaluado. A continuación, se presenta los resultados obtenidos en la evaluación de efectividad de controles de seguridad de la información en la vigencia 2024.

Tabla 1. *Evaluación Efectividad de Controles 2024*

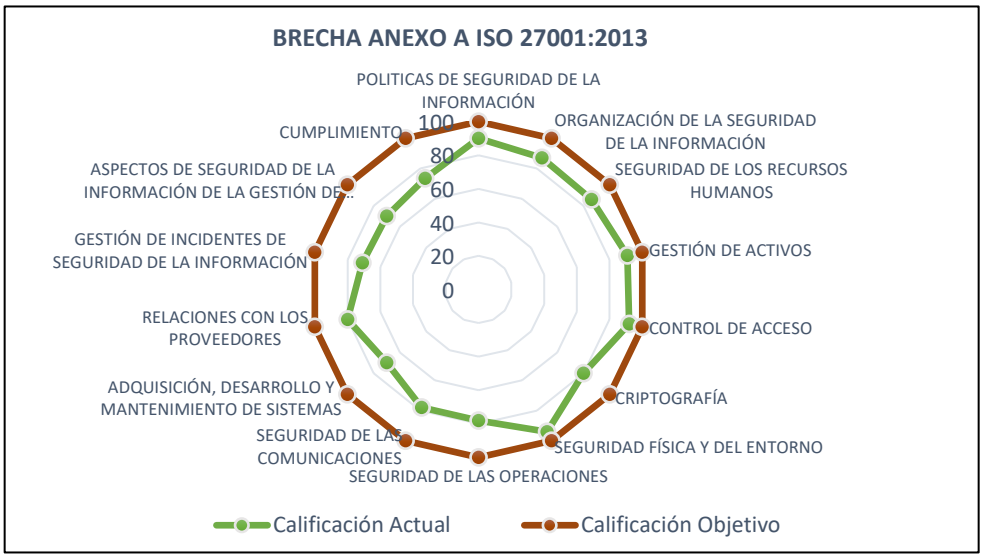
o.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	87	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	86	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	91	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	92	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	80	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	94	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	78	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	78	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	70	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	80	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	71	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	100	GESTIONADO
A.18	CUMPLIMIENTO	73,5	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES 2024		**81**	**100**	OPTIMIZADO

Fuente: *Diseño Propio*

En general, se observa una tendencia al alza en las calificaciones obtenidas en 2024 en comparación con 2023. Esto indica que la entidad ha realizado esfuerzos significativos para fortalecer su postura de seguridad.

De forma gráfica, podemos ver los resultados obtenidos en la evaluación sobre el nivel de implementación de controles técnicos y administrativos con corte al 31 de diciembre de 2024:

Figura 1. *Anexo A ISO 27001:2013 vigencia 2024*



Fuente: *Diseño Propio*

Los dominios como Políticas de Seguridad de la Información, Organización de la Seguridad de la Información, Seguridad de los Recursos Humanos, Gestión de Activos y Control de Acceso mantuvieron calificaciones altas y consistentes en ambos años, lo que sugiere una sólida base en estos aspectos.

El dominio de Criptografía experimentó una mejora significativa en 2024, pasando de "Efectivo" a "Gestionado". Esto indica un avance importante en la implementación de medidas criptográficas robustas.

Los dominios de Seguridad de las Operaciones, Seguridad de las Comunicaciones, Adquisición, Desarrollo y Mantenimiento de Sistemas, Gestión de Incidentes de Seguridad de la Información y Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio mostraron calificaciones relativamente bajas en ambos años, lo que deja ver que estas áreas requieren mayor atención y mejora.

El dominio de Cumplimiento mantuvo una calificación similar en ambos años, lo que indica un compromiso continuo con el cumplimiento normativo.

4.1.1. Áreas de Mejora Relevantes

Seguridad de las Operaciones: Es fundamental mejorar los procesos y controles relacionados con las operaciones diarias para reducir el riesgo de incidentes de seguridad.

Seguridad de las Comunicaciones: Se deben implementar medidas más robustas para proteger las comunicaciones internas y externas de la organización.

Ciclo de Vida de los Sistemas: Se deben establecer procesos más rigurosos para la adquisición, desarrollo y mantenimiento de sistemas, asegurando que se incorporen controles de seguridad desde el inicio.

Gestión de Incidentes de Seguridad: Es necesario fortalecer los procesos de detección, respuesta y recuperación ante incidentes de seguridad para minimizar su impacto.

Integrar la Seguridad en la Gestión de la Continuidad del Negocio: Se debe garantizar que los planes de continuidad del negocio incluyan medidas de seguridad robustas para asegurar la continuidad de las operaciones en caso de un incidente.

Dentro de las acciones a seguir, se realizará inversión en herramientas de control y monitoreo, así como la contratación de personal especializado para apoyar el desarrollo de las actividades definidas en este plan.

4.2. AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

El ciclo PHVA proporciona un marco para la mejora continua del sistema, asegurando que se planifiquen las acciones, se implementen, se verifiquen sus resultados y se actúe sobre las desviaciones para optimizar el SGSI. Se detallará el progreso en cada una de las fases del ciclo: Planificar (actividades de planificación realizadas, como la definición de objetivos, la identificación de riesgos y la selección de controles), Hacer (acciones implementadas, incluyendo la ejecución de los controles de seguridad y la capacitación del personal), Verificar (resultados de las actividades de verificación, como las auditorías internas, las pruebas de penetración y el monitoreo de la seguridad), Actuar (acciones correctivas y preventivas tomadas en base a los resultados de la

verificación, buscando la mejora continua del SGSI).

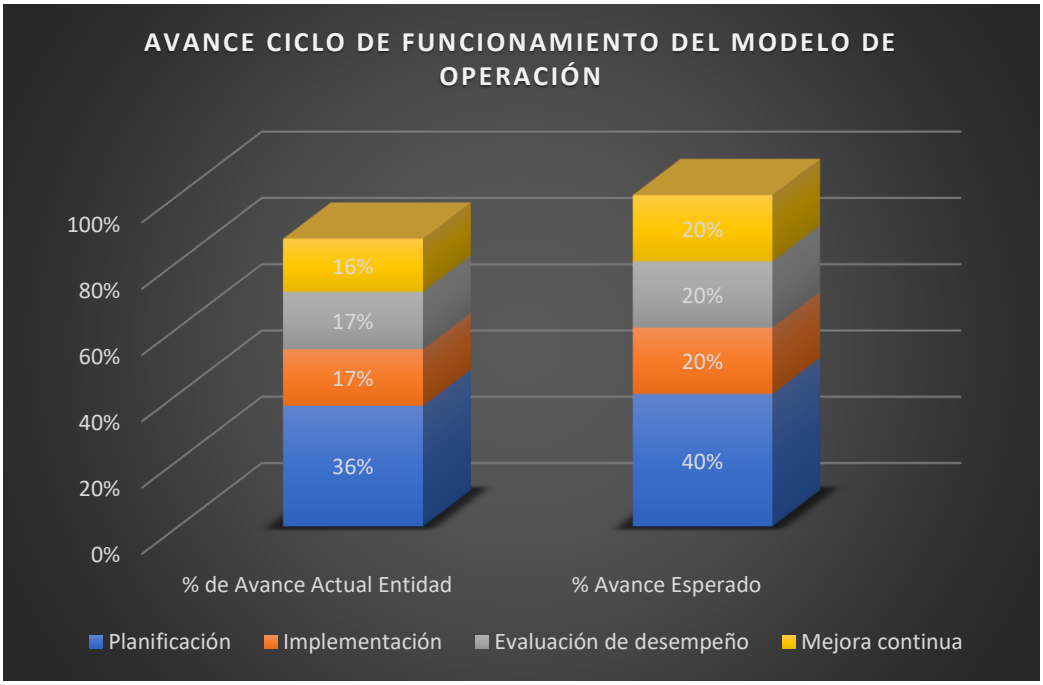
De acuerdo con lo anterior, se realizó la medición del ciclo PHVA dando como resultado que para la vigencia 2024, las calificaciones para cada etapa del ciclo se mantuvieron en un nivel alto de implementación.

__Tabla 2__. Avance PHVA 2024

AVANCE PHVA		
COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
Planificación	36%	40%
Implementación	17%	20%
Evaluación de desempeño	17%	20%
Mejora continua	16%	20%
TOTAL	**87%**	**100%**

Fuente: *Diseño Propio*

__Figura 2.__ Avance Ciclo de Funcionamiento MSPI vigencia 2023



Fuente: *Diseño Propio*

Si bien ambos años presentan un avance considerable en el ciclo PHVA, se evidencia una ligera disminución en el porcentaje total de avance en 2024 comparado con 2023. Sin embargo, es importante notar que esta disminución es marginal y que, en general, el proceso se mantiene en un nivel alto de implementación.

Análisis por Componente:

- **Planificación:** Se observa una ligera disminución en el porcentaje de avance en 2024. Esto debido a la identificación de brechas en este componente. La calificación se disminuye para ajustar los planes a las nuevas realidades.
- **Implementación, Evaluación de Desempeño y Mejora Continua:** Los porcentajes de avance en estas etapas se mantienen prácticamente iguales entre ambos años. Esto sugiere que la entidad ha logrado mantener un ritmo constante en la ejecución de las actividades planificadas y en la evaluación de los resultados.

Razones para la Disminución en el Avance Total:

- **Brechas Identificadas:** En la revisión anual se identificó brechas en algunos componentes que no se resolvieron en la vigencia lo cual influye en los resultados obtenidos con respecto al ciclo PHVA

En general, los resultados obtenidos indican que la entidad ha logrado avanzar significativamente en la implementación del ciclo PHVA. Sin embargo, es necesario continuar trabajando para mejorar el proceso y alcanzar los objetivos establecidos. Un análisis más profundo de los datos y la implementación de las recomendaciones mencionadas anteriormente permitirán optimizar el ciclo PHVA y obtener mejores resultados en el futuro.

4.3. MODELO FRAMEWORK CIBERSEGURIDAD NIST 2024

Se analizará la alineación del SGSI con el Modelo Framework de Ciberseguridad del NIST (National Institute of Standards and Technology). Este modelo ofrece un conjunto de estándares, directrices y mejores prácticas para gestionar los riesgos de ciberseguridad. La evaluación del avance en la adopción de este marco permite observar el nivel de madurez de la entidad en materia de ciberseguridad y las acciones necesarias para fortalecerla. Se evaluaron las funciones del NIST

Framework (Identificar, Proteger, Detectar, Responder, Recuperar), buscando una cobertura integral de los riesgos de ciberseguridad.

En el resultado del autodiagnóstico en el cual se evaluó el modelo, se puede observar que la entidad tiene un promedio alto de calificación en las etapas definidas en el modelo. La calificación por cada componente se muestra en el siguiente cuadro:

Tabla 3. *Calificación Modelo Ciberseguridad NIST Vigencia 2024*

MODELO FRAMEWORK CIBERSEGURIDAD NIST 2024		
Etiquetas de fila	**CALIFICACIÓN ENTIDAD**	**NIVEL IDEAL CSF**
IDENTIFICAR	80	100
DETECTAR	69	100
RESPONDER	77	100
RECUPERAR	80	100
PROTEGER	84	100

Fuente: *Diseño Propio*

Para una mejor visualización, a continuación, se presenta gráficamente el resultado frente a la calificación deseada:

Figura 3. *Framework Ciberseguridad NIST Vigencia 2024*

Fuente: *Diseño Propio*

Al analizar los datos de ambos años, se evidencia un desempeño sólido y consistente de la entidad en cuanto a la implementación del modelo de ciberseguridad NIST. Las calificaciones obtenidas se mantienen en un nivel elevado, lo que indica un compromiso sólido con la seguridad de la información.

Análisis por Función del Marco NIST:

- **Identificar:** Se observa un ligero incremento en la calificación para 2024, lo que sugiere una mejora en la identificación de activos, datos y sistemas críticos. Esto indica una mayor conciencia y un inventario más detallado de los recursos de la organización.
- **Detectar:** La calificación se mantiene estable entre ambos años. Esto indica que los sistemas de detección de amenazas están funcionando de manera adecuada y que se están realizando las acciones necesarias para identificar incidentes de seguridad a tiempo.
- **Responder:** Se observa una ligera disminución en la calificación para 2024. Esto se debe a ajustes en la calificación dado que se identificó brechas en los procedimientos de respuesta a incidentes y en la implementación de nuevas medidas de seguridad que aún no han sido completamente evaluadas.
- **Recuperar:** La calificación se mantiene estable, lo que indica que los planes de recuperación ante desastres están bien encaminados y se ejecutan de manera efectiva.
- **Proteger:** Se observa un ligero incremento en la calificación para 2024, lo que sugiere una mejora en las medidas de protección implementadas, como controles de acceso, cifrado y hardening de sistemas.

Conclusiones y Recomendaciones:

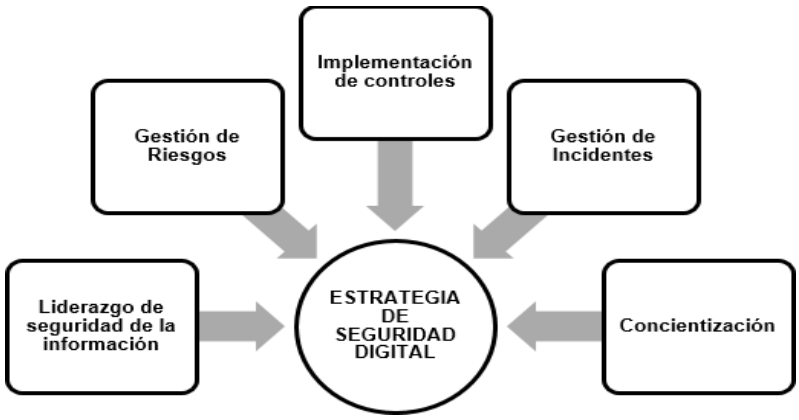
- **Sólido desempeño:** La entidad ha demostrado un sólido desempeño en la implementación del modelo de ciberseguridad NIST, manteniendo un alto nivel de madurez en todas las funciones del marco.
- **Áreas de mejora:** Si bien el desempeño general es positivo, existen áreas específicas donde se pueden realizar mejoras, como en la función de responder.
- **Continuidad:** Es importante mantener el enfoque en la mejora continua, realizando evaluaciones periódicas y ajustando las medidas de seguridad según sea necesario.
- **Adaptación a nuevas amenazas:** Se debe estar atento a las nuevas amenazas cibernéticas y adaptar las medidas de seguridad en consecuencia.
- **Capacitación del personal:** La capacitación continua del personal es fundamental para garantizar que se sigan las mejores prácticas de seguridad y se respondan de manera efectiva a los incidentes.
- **Automatización:** La automatización de tareas repetitivas puede mejorar la eficiencia y reducir el riesgo de errores humanos.

La entidad ha logrado un nivel de madurez en ciberseguridad Alto. Sin embargo, es importante continuar trabajando en la mejora continua y adaptarse a las cambiantes amenazas del ciberespacio.

5. ESTRATEGIA DE SEGURIDAD DIGITAL

La Secretaría Distrital de Planeación - SDP ha adoptado una estrategia de seguridad digital que integra principios, políticas, procedimientos, guías y lineamientos para la gestión de la seguridad de la información. Dicha estrategia se basa en el Modelo de Seguridad y Privacidad de la Información (MSPI), en la guía de gestión de riesgos, el procedimiento de gestión de incidentes, y cumple con la Resolución 500 de 2011[1] y los lineamientos del MinTIC. En este sentido, la Secretaría Distrital de Planeación definió cinco habilitadores, los cuales permitirán establecer en su conjunto una estrategia general de seguridad digital.

Figura 4. *Estrategia de Seguridad Digital – MINTIC*



[1] https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf
Anexo 1 – Resolución 500 de 2021 – MSPI
https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf

Fuente: *Diseño Propio*

5.1. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (COMPONENTES)

A continuación, se describe el objetivo de cada una de los habilitadores a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021 emitidos por MINTIC.

Tabla 4. *Estrategias para implementar el MSPI – MINTIC*

COMPONENTE	DESCRIPCIÓN
Liderazgo de seguridad de la información	Actualizar el Modelo de Seguridad y Privacidad de la Información (MSPI) de conformidad con la Política de Gobierno Digital, Política de Seguridad Digital, Decreto 432 de 2022, Norma ISO27001. Actualizar las dependencias del SDP en el instrumento de autodiagnóstico. Realizar la revisión y actualización de lineamientos buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información. Revisar, planificar e implementar acciones para cerrar las brechas identificadas en el autodiagnóstico con corte a 31/12/2024
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo a la implementación de controles de seguridad para el tratamiento de los riesgos.
Sensibilización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que se convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, implementando controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis y comunicación de los eventos minimizando el impacto en la Entidad.

Fuente: *Diseño Propio*

5.2. PORTAFOLIO DE PROYECTOS:

Para cada estrategia específica, la Secretaría Distrital de Planeación definió los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

Tabla 5. *Portafolio de Proyectos Asociados a MSPI 2025*

Liderazgo de seguridad de la información	**Revisión y actualización del MSPI** • Actualización de la documentación del MSPI alineado a la ISO27001:2022 • Revisión de aplicabilidad, Roles y Responsabilidades de Seguridad de la Información. • Actualizar e implementar una política de seguridad para controles criptográficos • Migración de servicios a la nube pública • Revisar y presentar avances cada dos meses sobre la implementación del MSPI. De acuerdo con el plan de mejora establecido como producto del del seguimiento al MSPI realizado por la Oficina de Control Interno en la vigencia 2024.	Modelo de seguridad y privacidad de la Información actualizado
Gestión de riesgos[2]	**Identificación y tratamiento de riesgos de seguridad** • Actualizar la matriz de activos de información • Identificar, valorar y clasificar los riesgos asociados a los activos de información. • Definir y ejecutar planes de tratamiento de riesgos de seguridad	Matriz de riesgos de seguridad digital
Sensibilización	**Definir y ejecutar el plan de sensibilización** • Realizar jornadas de sensibilización a todo el personal. • Realizar trasferencia de conocimiento a colaboradores de la Entidad en temas de Seguridad Digital • Medir el grado de sensibilización a toda la Entidad	Plan de Sensibilización
Implementación de controles	**Implementación de controles de acuerdo con el resultado del autodiagnóstico** • Respaldo de información. • Gestión de Cambios. • Clasificación de la información. • Desarrollo Seguro • Soluciones de seguridad informática • Hacking Ethical • Gestión de vulnerabilidades **Nota**: Rediseñar el formato del plan de implementación de controles atendiendo las recomendaciones del seguimiento al MSPI realizado por la Oficina de Control Interno en la vigencia 2024.	Informe implementación de controles

2. Para establecer los proyectos relacionados con la gestión de los riesgos, consultar el **artículo 6 de la resolución 500 de 2021**, donde están los lineamientos que se deben cumplir. https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

Gestión de incidentes[3]	Actualizar y formalizar los procedimientos, guías, manuales de Gestión de Incidentes de seguridad de la información.	Procedimientos, guías, manuales de Gestión de Incidentes de seguridad de la información actualizados y formalizados.

Fuente: *Diseño Propio*

5.3. ANÁLISIS PRESUPUESTAL

5.3.1. PROYECTO DE INVERSION

En este apartado se desglosan los procesos incluidos en el proyecto de inversión a cargo de la Dirección de Tecnologías de la Información y la Comunicaciones que aportan a la estrategia de seguridad y privacidad de la información de la SDP, referenciando los montos presupuestales estimados que hacen parte del anteproyecto de presupuesto de la vigencia 2025.

Tabla 6. *Procesos por el proyecto de Inversión vigencia 2025*

PROCESOS	INVERSIÓN
1. Actualización de licencias MAGIC INFO para los servicios de divulgación de información en las pantallas digitales de la SDP (PAQUETES DE SOFTWARE) Controles Relacionados: – A.8.1 Gestión de activos: Inventario de software, control de licencias. – A.9.4 Gestión de la información: Control de la información mostrada en pantallas públicas, gestión de la configuración. – A.12.5 Gestión de la seguridad de la información para el uso de servicios en la nube: Si aplica, control del proveedor de software. – A.18 Cumplimiento: Cumplimiento de licencias de software.	4.200.000

[3] Para establecer los proyectos relacionados con la gestión de los incidentes, consultar el **artículo 9 de la resolución 500 de 2021**, donde están los lineamientos que se deben cumplir. https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

Se debe tener presente en el establecimiento de los procedimientos y lineamientos, el reporte al **CSIRT DE GOBIERNO**.

2. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y Comunicaciones en la identificación de requerimientos de los usuarios del sistema SEGPLAN 2,0, elaboración y actualización de documentos técnicos y soporte al usuario final (SERVICIOS DE DISEÑO Y DESARROLLO DE APLICACIONES EN TECNOLOGÍAS DE LA INFORMACIÓN (TI)) Controles Relacionados: – A.12.1 Requisitos de seguridad de los sistemas de información: Definición de requerimientos de seguridad para el sistema. – A.12.2 Seguridad en los procesos de desarrollo y de soporte: Gestión del ciclo de vida del desarrollo de software, pruebas de seguridad, gestión de cambios. – A.12.4 Pruebas de seguridad de sistemas: Pruebas de funcionalidad y seguridad del sistema SDP 2.0.	75.000.000
3. Prestar los servicios profesionales a la Dirección de Tecnologías de Información y Comunicaciones en el seguimiento a la ejecución de los proyectos de la Dirección (SERVICIOS DE GESTIÓN DE DESARROLLO EMPRESARIAL) Controles Relacionados: – A.6.1 Responsabilidades de la dirección: Supervisión y gestión de proyectos de TI. – A.17.1 Planificación de la continuidad del negocio: Gestión de proyectos para asegurar la continuidad de los servicios.	58.710.000
4. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones en la administración de los motores de bases de datos que soportan los sistemas de información de la SDP (SERVICIOS DE SOPORTE EN TECNOLOGÍAS DE LA INFORMACIÓN (TI)) Controles Relacionados: – A.9.2 Gestión del acceso a los sistemas y las aplicaciones: Control de acceso a las bases de datos. – A.12.6 Gestión de vulnerabilidades técnicas: Mantenimiento y actualización de los motores de bases de datos. – A.17.2 Implementación de la continuidad del negocio: Respaldo y recuperación de bases de datos.	104.475.000
5. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones en la ejecución de procesos de configuración, actualización y mantenimiento a los sistemas operativos Linux de la SDP (SERVICIOS DE SOPORTE EN TECNOLOGÍAS DE LA INFORMACIÓN (TI)) Controles Relacionados: – A.12.6 Gestión de vulnerabilidades técnicas: Gestión de parches y actualizaciones de seguridad para sistemas operativos. – A.12.1 Requisitos de seguridad de los sistemas de información: Configuración segura de los sistemas operativos.	66.150.000

6. Prestar servicios profesionales a la Dirección de Tecnologías de Información y las Comunicaciones en la ejecución de actividades de instalación, actualización, configuración, monitoreo y soporte a los sistemas operativos Windows que soportan la infraestructura tecnológica de la SDP (SERVICIOS DE SOPORTE EN TECNOLOGÍAS DE LA INFORMACIÓN (TI)) Controles Relacionados: - A.12.6 Gestión de vulnerabilidades técnicas: Gestión de parches y actualizaciones de seguridad para sistemas operativos. - A.12.1 Requisitos de seguridad de los sistemas de información: Configuración segura de los sistemas operativos.	83.448.000
7. Realizar en el sistema SINU POT la implementación de nuevas funcionalidades y ajustar las existentes en concordancia con la normatividad vigente (SERVICIOS DE DISEÑO Y DESARROLLO DE APLICACIONES EN TECNOLOGÍAS DE LA INFORMACIÓN (TI)) Controles Relacionados: - A.12.1 Requisitos de seguridad de los sistemas de información: Definición de requerimientos de seguridad para las nuevas funcionalidades. - A.12.2 Seguridad en los procesos de desarrollo y de soporte: Desarrollo seguro, pruebas de seguridad. - A.12.4 Pruebas de seguridad de sistemas: Pruebas de funcionalidad y seguridad.	500.000.000
8. Renovar el servicio de centro de datos por collocation para la infraestructura On-Premise de la SDP (OTROS SERVICIOS DE ALOJAMIENTO Y SUMINISTRO DE INFRAESTRUCTURA EN TECNOLOGÍA DE LA INFORMACIÓN (TI)) Controles Relacionados: - A.11 Seguridad física y del entorno: Seguridad física del centro de datos, control de acceso físico. - A.12.5 Gestión de la seguridad de la información para el uso de servicios en la nube: Si aplica, control del proveedor de collocation.	360.217.000
9. Adquirir licenciamiento base y soporte para la infraestructura tecnológica de la SDP (PAQUETES DE SOFTWARE) Controles Relacionados: - A.8.1 Gestión de activos: Inventario de software, control de licencias. - A.18 Cumplimiento: Cumplimiento de licencias de software.	350.000.000
10. Proveer servicios de licenciamiento y actualización de las herramientas ArcGIS para asegurar la sostenibilidad y soporte del componente geográfico de la Secretaría Distrital de Planeación (PAQUETES DE SOFTWARE) Controles Relacionados: - A.8.1 Gestión de activos: Inventario de software, control de licencias. - A.18 Cumplimiento: Cumplimiento de licencias de software.	2.600.000.000

11. Actualizar las licencias de software estadístico y matemático que soportan los procesos misionales de la Secretaría Distrital De Planeación (PAQUETES DE SOFTWARE) Controles Relacionados: - A.8.1 Gestión de activos: Inventario de software, control de licencias. - A.18 Cumplimiento: Cumplimiento de licencias de software.	100.000.000
12. Adquirir los certificados de servidor seguro y los certificados de firma digital para los funcionarios de la Secretaría Distrital De Planeación (PAQUETES DE SOFTWARE): Controles Relacionados: - A.10.1 Política sobre el uso de controles criptográficos: Uso de certificados digitales y firma digital. - A.10.2 Gestión de claves: Gestión del ciclo de vida de los certificados. - A.14.3 Información de registro de eventos: Registro de uso de certificados.	90.000.000
13. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones (DTIC) para apoyar en la implementación técnica y el seguimiento del Plan Estratégico de Tecnologías de La Información y las Comunicaciones (PETIC) Controles Relacionados: - A.5 Políticas de seguridad de la información: El seguimiento del PETIC asegura que las políticas de seguridad se implementen y se cumplan. - A.6 Organización de la seguridad de la información: Este servicio apoya la estructura organizativa de la seguridad, la asignación de responsabilidades y la gestión de la seguridad de la información en general. - A.17 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio: El PETIC debe contemplar la continuidad del negocio y la recuperación ante desastres, por lo que este servicio contribuye a asegurar que se consideren los aspectos de seguridad en estos planes.	90.000.000

14. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones en la conceptualización de los aspectos jurídico, que soportan los proyectos y procesos contractuales a cargo de la Dirección Controles Relacionados: - A.12 Seguridad en los procesos de desarrollo, soporte y mantenimiento: Asegura que los contratos de desarrollo y mantenimiento incluyan cláusulas de seguridad. - A.15 Relaciones con los proveedores: Define los requisitos de seguridad que deben cumplir los proveedores. - A.18 Cumplimiento: Garantiza el cumplimiento de las leyes y regulaciones aplicables en materia de seguridad de la información en los contratos. -	113.300.000
15. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones para monitorear la infraestructura de red, los servicios de seguridad de aplicación, servicios de seguridad perimetral y servicios de análisis de vulnerabilidades de la SDP. Controles Relacionados: - A.9 Control de acceso: El monitoreo de la infraestructura de red ayuda a detectar accesos no autorizados. - A.12.6 Gestión de vulnerabilidades técnicas: Los análisis de vulnerabilidades identifican debilidades en los sistemas. - A.13 Seguridad de las comunicaciones: El monitoreo de la red y la seguridad perimetral asegura la confidencialidad e integridad de la información transmitida. - A.16 Gestión de incidentes de seguridad de la información: El monitoreo continuo facilita la detección temprana de incidentes.	108.900.000
16. Prestar servicios profesionales a la Dirección De Tecnologías de la Información y las Comunicaciones en la ejecución de actividades de seguimiento, control y gestión de pagos de los contratos de responsabilidad de la Dirección Controles Relacionados: - A.7 Seguridad de los recursos humanos: Controla el acceso a la información financiera y sensible relacionada con los pagos. - A.15 Relaciones con los proveedores: Gestiona los aspectos financieros de la relación con los proveedores.	82.000.000

17. Prestar servicios profesionales a la Dirección De Tecnologías de la Información y las Comunicaciones en las fases de implementación de las Políticas de Seguridad Digital y Políticas De Gobierno Digital de acuerdo con los lineamientos vigentes en la materia. Controles Relacionados: - A.5 Políticas de seguridad de la información: Implementa las políticas de seguridad digital. - A.6 Organización de la seguridad de la información: Define roles y responsabilidades para la seguridad. - A.18 Cumplimiento: Asegura el cumplimiento de las regulaciones de Gobierno Digital y Seguridad Digital.	80.000.000
18. Prestar servicios profesionales a la Dirección De Tecnologías de la Información y las Comunicaciones en la estructuración desde el ámbito jurídico de los documentos que soportan los procesos de contratación y en la gestión de liquidación y cierre de expediente de los contratos a cargo de la Dirección Controles Relacionados: - A.12 Seguridad en los procesos de desarrollo, soporte y mantenimiento: Asegura la inclusión de cláusulas de seguridad en los contratos. - A.15 Relaciones con los proveedores: Define las obligaciones de seguridad de los proveedores. - A.18 Cumplimiento: Asegura el cumplimiento legal en la contratación.	78.100.000
19. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones en la etapa precontractual, contractual y poscontractual de las necesidades a cargo de la Dirección TIC. Controles Relacionados: - A.15 Relaciones con los proveedores: Cubre todas las fases de la gestión de proveedores, incluyendo la seguridad.	72.000.000
20. Prestar Servicios Profesionales a la Dirección De Tecnologías de la Información y las Comunicaciones en la ejecución de las actividades inherentes al seguimiento a las metas del proyecto de inversión a cargo de la Dirección y seguimiento al Plan Operativo Anual y Elaborar los informes y reportes correspondientes Controles Relacionados: - A.6 Organización de la seguridad de la información: El seguimiento de metas y planes operativos asegura que la seguridad sea considerada en la gestión de la DTIC. - A.8 Gestión de activos: El seguimiento de proyectos de inversión implica el seguimiento de activos de información.	38.950.000

21. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones en las actividades inherentes a la conformación de los expedientes digitales de la Dirección. Controles Relacionados: - A.8 Gestión de activos: La conformación de expedientes digitales implica la gestión de información como un activo. - A.9.4 Gestión de la información: Controla el acceso y la gestión de los expedientes digitales. - A.14.3 Información de registro de eventos: Se deben registrar los accesos y modificaciones a los expedientes.	38.950.000
22. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones en las actividades de administración de la base de datos geográfica y en la construcción y/o mantenimiento de las aplicaciones y sistemas de información con componente geográfico de la SDP. Controles Relacionados: - A.9.2 Gestión del acceso a los sistemas y las aplicaciones: Control de acceso a la base de datos geográfica y a las aplicaciones. - A.12.2 Seguridad en los procesos de desarrollo y de soporte: Asegura la seguridad en el desarrollo y mantenimiento de aplicaciones con componente geográfico. - A.12.6 Gestión de vulnerabilidades técnicas: Mantenimiento y actualización de la base de datos geográfica y las aplicaciones	119.700.000

23. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones en la planeación, gestión y control de los servicios prestado a través de la mesa de ayuda y cumplimiento de los acuerdos de nivel de servicio (ANS) (servicios de soporte en tecnologías de la información). Este contrato se centra en la gestión de la Mesa de Ayuda y el cumplimiento de ANS, lo cual impacta en varios controles de seguridad Controles Relacionados: - A.6 Organización de la seguridad de la información: Define roles y responsabilidades dentro de la Mesa de Ayuda en relación con la seguridad. - A.12.3 Gestión de la capacidad: Asegura que la Mesa de Ayuda tenga la capacidad para atender incidentes de seguridad. - A.15 Relaciones con los proveedores: La Mesa de Ayuda es gestionada por un proveedor externo, este control es crucial para definir las responsabilidades de seguridad del proveedor. - A.16 Gestión de incidentes de seguridad de la información: La Mesa de Ayuda es el primer punto de contacto para reportar incidentes, por lo que este contrato influye directamente en la gestión de incidentes. Los ANS deben incluir tiempos de respuesta para incidentes de seguridad. - A.17.2 Implementación de la continuidad del negocio: La Mesa de Ayuda debe tener un plan de contingencia para asegurar su disponibilidad en caso de interrupciones.	99.000.000
24. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones, en la ejecución de actividades de uso y apropiación de las tecnologías de la información y las comunicaciones (TIC) para los usuarios finales de la Secretaría Distrital de Planeación (SERVICIOS DE DISEÑO Y DESARROLLO DE APLICACIONES) Controles Relacionados: Este contrato se enfoca en la capacitación y el soporte a usuarios finales en el uso de las TIC, lo que impacta principalmente en: - A.7.2 Concienciación, educación y formación en seguridad de la información: Este es el control más directamente relacionado. El contrato debe especificar la inclusión de temas de seguridad en las capacitaciones, como el manejo de contraseñas, la prevención de phishing, el uso seguro de internet, etc. - A.9 Control de acceso: La capacitación a usuarios debe reforzar las políticas de control de acceso y el uso adecuado de las credenciales.	48.400.000

25. Adquisición de servicios de nube pública para soportar procesos misionales de la SDP (OTROS SERVICIOS DE ALOJAMIENTO Y SUMINISTRO DE INFRAESTRUCTURA EN TECNOLOGÍA DE LA INFORMACIÓN) Controles Relacionados: La adquisición de servicios de nube pública implica una serie de consideraciones de seguridad: - A.5 Políticas de seguridad de la información: Se deben adaptar las políticas existentes para el entorno de nube. - A.8 Gestión de activos: Se debe gestionar el inventario de los recursos en la nube. - A.9 Control de acceso: Se deben implementar controles de acceso a los recursos en la nube. - A.12.5 Gestión de la seguridad de la información para el uso de servicios en la nube: Este es un control clave. Se deben definir los requisitos de seguridad que debe cumplir el proveedor de la nube, incluyendo: ▪ Seguridad física de los centros de datos. ▪ Seguridad lógica de la infraestructura en la nube. ▪ Cumplimiento de normativas y certificaciones de seguridad (ISO 27001, SOC 2, etc.). ▪ Gestión de la identidad y el acceso (IAM). ▪ Cifrado de datos en tránsito y en reposo. ▪ Respuesta a incidentes. ▪ Continuidad del negocio y recuperación ante desastres. - A.13 Seguridad de las comunicaciones: Se deben asegurar las comunicaciones entre la SDP y la nube. - A.15 Relaciones con los proveedores: Se debe definir un acuerdo de nivel de servicio (SLA) que incluya aspectos de seguridad.	718.257.000
26. Renovar las garantías y soporte de la solución de copias de seguridad Veeam Backup Exagrid de propiedad de la SDP (PAQUETES DE SOFTWARE) Controles Relacionados: Este contrato se centra en la continuidad del negocio y la recuperación ante desastres: - A.17.2 Implementación de la continuidad del negocio: Este es el control principal. La renovación de garantías y soporte asegura la disponibilidad de la solución de respaldo y recuperación. - A.12.6 Gestión de vulnerabilidades técnicas: Mantener el software de respaldo actualizado ayuda a prevenir vulnerabilidades que podrían comprometer las copias de seguridad. - A.9.2 Gestión del acceso a los sistemas y las aplicaciones: Se deben controlar estrictamente los accesos a la solución de respaldo para evitar modificaciones no autorizadas o la eliminación de copias de seguridad.	450.000.000

27. Adquirir y renovar las suscripciones de las licencias Adobe Creative Cloud Para La SDP (PAQUETES DE SOFTWARE) Controles Relacionados: Este contrato se relaciona principalmente con la gestión de activos y el cumplimiento de licencias: - A.8.1 Gestión de activos: Se debe mantener un inventario de las licencias de Adobe Creative Cloud. - A.18 Cumplimiento: Se debe asegurar el cumplimiento de los términos de la licencia de Adobe.	72.460.000
28. Prestar servicios profesionales a la Dirección De Tecnologías de la Información y las Comunicaciones para definir la arquitectura de software de los sistemas de información y apoyar el desarrollo de software en la Secretaría Distrital De Planeación (SERVICIOS DE CONSULTORÍA EN TECNOLOGÍAS DE LA INFORMACIÓN (TI)) Controles Relacionados: - A.12.1 Requisitos de seguridad de los sistemas de información: La definición de la arquitectura debe considerar los requisitos de seguridad desde el inicio (seguridad por diseño). - A.12.2 Seguridad en los procesos de desarrollo y de soporte: Este servicio impacta directamente en la seguridad del ciclo de vida del desarrollo, incluyendo: ▪ Definición de estándares de codificación segura. ▪ Gestión de configuración y control de versiones. ▪ Pruebas de seguridad integradas en el ciclo de desarrollo (SAST, DAST). - A.14 Adquisición, desarrollo y mantenimiento de sistemas: Abarca la gestión de proyectos de desarrollo, incluyendo la gestión de riesgos de seguridad.	100.000.000
29. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones en la implementación de nuevas funcionalidades y optimización de las existentes del sistema de seguimiento de la política pública para la superación de la pobreza (SERVICIOS DE SOPORTE EN TECNOLOGÍAS DE LA INFORMACIÓN (TI)) Controles Relacionados: - A.12.1 Requisitos de seguridad de los sistemas de información: Los cambios deben alinearse con los requisitos de seguridad del sistema. - A.12.2 Seguridad en los procesos de desarrollo y de soporte: Se aplican controles de gestión de cambios para asegurar la seguridad de las implementaciones y optimizaciones. - A.12.4 Pruebas de seguridad de sistemas: Las nuevas funcionalidades y optimizaciones deben ser probadas para verificar su seguridad.	85.000.000

30. Prestar servicios profesionales de apoyo a la Dirección de Tecnologías de la Información y las Comunicaciones en las actividades inherentes a la ejecución de las etapas de identificación de necesidades de usuario, verificación de calidad, pruebas funcionales y operación de las soluciones de software de la SDP (SERVICIOS DE DISEÑO Y DESARROLLO DE APLICACIONES EN TECNOLOGÍAS DE LA INFORMACIÓN (TI)) Controles Relacionados: - A.12.1 Requisitos de seguridad de los sistemas de información: La identificación de necesidades debe incluir la definición de requisitos de seguridad. - A.12.2 Seguridad en los procesos de desarrollo y de soporte: Este servicio abarca varias etapas del ciclo de vida del desarrollo, incluyendo la verificación de calidad y las pruebas, que deben considerar la seguridad. - A.12.4 Pruebas de seguridad de sistemas: Las pruebas funcionales deben complementarse con pruebas de seguridad.	78.177.000
31. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones, para apoyar en el diseño e implementación de la arquitectura de analítica de datos sobre la plataforma tecnología dispuesta por la SDP para tal fin (SERVICIOS DE DISEÑO Y DESARROLLO DE APLICACIONES EN TECNOLOGÍAS DE LA INFORMACIÓN (TI)) Controles Relacionados: - A.9.4 Gestión de la información: La arquitectura de analítica de datos debe considerar la clasificación, el almacenamiento y el acceso seguro a los datos. - A.12.1 Requisitos de seguridad de los sistemas de información: Se deben definir requisitos de seguridad específicos para la plataforma de analítica de datos. - A.14.3 Información de registro de eventos: Se debe auditar el acceso y el uso de los datos para fines de analítica.	103.950.000
32. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones para la implementación de ajustes y mejoras a los módulos que integran el sistema seguimiento de políticas públicas (servicios de diseño y desarrollo de aplicaciones en tecnologías de la información (TI)) Controles Relacionados: - A.12.1 Requisitos de seguridad de los sistemas de información: Los ajustes y mejoras deben cumplir con los requisitos de seguridad. - A.12.2 Seguridad en los procesos de desarrollo y de soporte: Gestión de cambios y control de versiones. - A.12.4 Pruebas de seguridad de sistemas: Pruebas de regresión para asegurar que los cambios no introducen vulnerabilidades. -	100.000.000

33. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones en la implementación de las soluciones de software que requiere la dirección de planeación del desarrollo económico (servicios de diseño y desarrollo de aplicaciones en tecnologías de la información (TI)) Controles Relacionados: - A.12.1 Requisitos de seguridad de los sistemas de información: Definición de requisitos de seguridad para las soluciones de software. - A.12.2 Seguridad en los procesos de desarrollo y de soporte: Desarrollo seguro y pruebas de seguridad. - A.14 Adquisición, desarrollo y mantenimiento de sistemas: Gestión del proyecto de desarrollo	105.000.000
34. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones en la implementación de soluciones de software con componente geográfico que requiere la dirección de planeación del desarrollo económico (servicios de diseño y desarrollo de aplicaciones en tecnologías de la información (ti)) Controles Relacionados: - A.9.4 Gestión de la información: Seguridad de la información geográfica. - A.12.1 Requisitos de seguridad de los sistemas de información: Requisitos de seguridad para software con componente geográfico. - A.12.2 Seguridad en los procesos de desarrollo y de soporte: Desarrollo seguro y pruebas de seguridad. - A.14.3 Información de registro de eventos: Auditoría del acceso y uso de la información geográfica.	94.500.000
35. Prestar servicios profesionales a la Dirección de Tecnologías de la Información y las Comunicaciones en el levantamiento de requerimientos y construcción de las mejoras al sistema SEGPLAN 2.0 que requieran los usuarios funcionales (servicios de diseño y desarrollo de aplicaciones en tecnologías de la información (TI)) Controles Relacionados: - A.12.1 Requisitos de seguridad de los sistemas de información: Asegurar que los requerimientos incluyan aspectos de seguridad. - A.12.2 Seguridad en los procesos de desarrollo y de soporte: Gestión de cambios y control de versiones.	90.000.000
36. Prestar servicios profesionales a la Dirección de Tecnologías de la Informacion y las Comunicaciones en el levantamiento de requerimientos y construcción de las mejoras al sistema SEGPLAN 2.0 que requieran los usuarios funcionales (servicios de diseño y desarrollo de aplicaciones en tecnologías de la información (TI)) Controles Relacionados: - A.12.1 Requisitos de seguridad de los sistemas de información: Asegurar que los requerimientos incluyan aspectos de seguridad - A.12.2 Seguridad en los procesos de desarrollo y de soporte: Gestión de cambios y control de versiones.	90.000.000

37. Adquirir y renovar las suscripciones de las licencias adobe Acrobat pro para la SDP (paquetes de software) Controles Relacionados: - A.8.1 Gestión de activos: Control del inventario de software y gestión de licencias. - A.18 Cumplimiento: Asegurar el cumplimiento de los términos de la licencia de software.	140.000.000
TOTAL PRESUPUESTO INVERSIÓN VIGENCIA 2025	**$ 7.588.844.000**

Fuente: *Diseño Propio*

5.3.2. PROYECTO DE FUNCIONAMIENTO

Este apartado presenta un análisis de los proyectos que se ejecutan con recursos de funcionamiento de la entidad que se destinan al sostenimiento y la operación continua.

Tabla 7*. Procesos por el proyecto de funcionamiento*

PROCESOS	INVERSIÓN
1. Proveer servicios de licenciamiento y actualización de las herramientas ArcGIS para	450.000.000

asegurar la sostenibilidad y soporte del componente geográfico de la Secretaría Distrital de Planeación. Controles Asociados: - A.8.1 Gestión de activos: Control de inventario de software y licencias. - A.12.6 Gestión de vulnerabilidades técnicas: Las actualizaciones son cruciales para corregir vulnerabilidades. - A.18 Cumplimiento: Cumplimiento de los términos de licencia del software.	
2. Actualización y soporte técnico de los productos Oracle: Controles Relacionados: - A.12.6 Gestión de vulnerabilidades técnicas: Aplicación de parches y actualizaciones de seguridad. - A.12.1 Requisitos de seguridad de los sistemas de información: Configuración segura de las bases de datos Oracle. - A.17.2 Implementación de la continuidad del negocio: Soporte para la recuperación ante desastres de las bases de datos.	1.300.000.000
3. Actualizar la licencia de software del Paquete Estadístico SAS: Controles Relacionados: - A.8.1 Gestión de activos: Control de licencias de software. - A.18 Cumplimiento: Cumplimiento de los términos de la licencia.	35.000.000
4. Actualizar las licencias de software Visum y Vissim, para el manejo de información de transporte y transito: Controles Relacionados: - A.8.1 Gestión de activos: Control de licencias de software. - A.18 Cumplimiento: Cumplimiento de los términos de la licencia.	70.000.000
6. Prestar el servicio de guarda, custodia y transporte de medios magnéticos y digitales de la Secretaría Distrital de Planeación: Controles Relacionados:	6.200.000

- A.11 Seguridad física y del entorno: Control de acceso físico a los medios, seguridad en el transporte. - A.8.2 Clasificación de la información: Los medios deben estar etiquetados y clasificados según su nivel de sensibilidad. - A.9.4 Gestión de la información: Control del ciclo de vida de los medios	
7. Garantías y soporte técnico para equipos de seguridad perimetral Firewall: Controles Relacionados: - A.13 Seguridad de las comunicaciones: Mantenimiento y actualización del firewall para proteger el perímetro de la red. - A.12.6 Gestión de vulnerabilidades técnicas: Aplicación de parches de seguridad al firewall. - A.16 Gestión de incidentes de seguridad de la información: Soporte para la configuración y respuesta ante incidentes detectados por el firewall.	210.000.000
8. Soporte Técnico para los Servidores, librería y Equipos de Conectividad: Controles Relacionados: - A.12.6 Gestión de vulnerabilidades técnicas: Mantenimiento y actualización de servidores y equipos de red. - A.12.1 Requisitos de seguridad de los sistemas de información: Configuración segura de servidores y equipos de red. - A.13 Seguridad de las comunicaciones: Asegurar la disponibilidad y seguridad de la red.	300.000.000
9. Renovación de garantías y soporte técnico del sistema de almacenamiento de la SDP Controles Relacionados: - A.9.2 Gestión del acceso a los sistemas y las aplicaciones: Control de acceso al sistema de almacenamiento. - A.17.2 Implementación de la continuidad del negocio: Soporte para la recuperación de datos en caso de fallos. - A.12.6 Gestión de vulnerabilidades técnicas: Mantenimiento y actualizaciones del sistema de almacenamiento.	190.000.000
10. Garantías y soporte técnico del Appliance para ancho de banda Controles Relacionados:	135.000.000

- A.13 Seguridad de las comunicaciones: Gestión del ancho de banda para asegurar la disponibilidad de los servicios. - A.12.6 Gestión de vulnerabilidades técnicas: Mantenimiento y actualizaciones del appliance.	
11. Renovación de garantías y soporte técnico de la solución de análisis de vulnerabilidades de la infraestructura de la SDP Controles Relacionados: - A.12.6 Gestión de vulnerabilidades técnicas: Asegura la continuidad de la identificación y gestión de vulnerabilidades.	105.000.000
12. Renovación de garantías y soporte técnico de los switches de borde de la infraestructura de conectividad de la SDP Controles Relacionados: - A.13 Seguridad de las comunicaciones: Mantenimiento y actualización de los switches para asegurar la seguridad y disponibilidad de la red. - A.12.6 Gestión de vulnerabilidades técnicas: Aplicación de parches de seguridad.	197.000.000
13. Renovación de garantías y soporte técnico de la solución de hiperconvergencia implementada en la SDP Controles Relacionados: - A.12.6 Gestión de vulnerabilidades técnicas: Mantenimiento y actualización de la solución de hiperconvergencia. - A.17.2 Implementación de la continuidad del negocio: Soporte para la recuperación ante desastres.	196.137.000
14. Prestar los servicios de soporte y actualización del software Antivirus para la Secretaría Distrital De Planeación Controles Relacionados: - A.12.2 Protección contra código malicioso: Mantenimiento y actualización del software antivirus.	400.000.000
15. Renovación de garantías y soporte técnico de la solución integrada de Firewall de	265.000.000

aplicaciones Web – WAF Controles Relacionados: - A.13 Seguridad de las comunicaciones: Protección de aplicaciones web contra ataques. - A.12.6 Gestión de vulnerabilidades técnicas: Actualizaciones y parches para el WAF.	
16. Renovación de garantías y soporte técnico para los equipos de balanceo de cargas de la Secretaría Distrital De Planeación Controles Relacionados: - A.13 Seguridad de las comunicaciones: Asegura la disponibilidad y el rendimiento de las aplicaciones. - A.17.2 Implementación de la continuidad del negocio: Soporte para la alta disponibilidad de los servicios.	83.000.000
17. Adición y prorroga al contrato No. 941-2024 cuyo objeto es "Soporte y Actualización del Sistema De Procesos Automáticos - SIPA" Controles Relacionados: - A.12.2 Seguridad en los procesos de desarrollo y de soporte: Mantenimiento y actualización del sistema. - A.12.6 Gestión de vulnerabilidades técnicas: Corrección de vulnerabilidades en el sistema.	90.176.472
18. Actualización y soporte técnico de la aplicación Documanager Controles Relacionados: - A.9.4 Gestión de la información: Control de acceso y gestión de documentos. - A.12.6 Gestión de vulnerabilidades técnicas: Actualizaciones de seguridad para la aplicación.	17.500.000
19. Soporte y actualización del sistema de procesos automáticos – SIPA Controles Relacionados: - A.12.2 Seguridad en los procesos de desarrollo y de soporte: Mantenimiento y actualización del sistema.	389.823.528

- A.12.6 Gestión de vulnerabilidades técnicas: Corrección de vulnerabilidades en el sistema.	
20. Prestar el servicio de conectividad y telecomunicaciones para el funcionamiento de la SDP Controles Relacionados: - A.13 Seguridad de las comunicaciones: Asegura la disponibilidad y seguridad de las comunicaciones. - A.12.6 Gestión de vulnerabilidades técnicas: Mantenimiento y actualización de equipos de telecomunicaciones.	216.000.000
21. Adquisición del licenciamiento de la suite colaborativa para la SDP Controles Relacionados: - A.8 Gestión de activos: La adquisición de licencias implica la gestión de un activo de información: el software. ▪ A.8.1.1 Inventario de activos: Se debe mantener un inventario actualizado de las licencias adquiridas, incluyendo el tipo de licencia, la cantidad, la fecha de expiración y el usuario asignado. ▪ A.8.1.2 Propiedad de los activos: Se debe definir claramente la propiedad de las licencias y los derechos de uso. - A.9 Control de acceso: La suite colaborativa proporcionará acceso a información y recursos compartidos, por lo que los controles de acceso son cruciales: ▪ A.9.2 Gestión del acceso a los sistemas y las aplicaciones: Se deben definir políticas de acceso basadas en roles y responsabilidades. ▪ A.9.3 Gestión de derechos de acceso de usuarios: Se debe gestionar el ciclo de vida de las cuentas de usuario, incluyendo la creación, modificación y eliminación de cuentas. ▪ A.9.4 Gestión de la información: Se debe clasificar la información almacenada en la suite y aplicar controles de acceso según su nivel de sensibilidad. - A.12 Seguridad en los procesos de desarrollo, soporte y mantenimiento: Si la suite requiere alguna configuración o personalización, se deben aplicar controles de desarrollo seguro. ▪ A.12.1 Requisitos de seguridad de los sistemas de información: Se deben definir requisitos de seguridad para la configuración de la suite.	1.300.000.000

- A.13 Seguridad de las comunicaciones: Se debe asegurar la confidencialidad e integridad de las comunicaciones dentro de la suite. ▪ A.13.2 Servicios de seguridad de red: Se deben utilizar protocolos seguros (como HTTPS) para el acceso a la suite. - A.15 Relaciones con los proveedores: Se debe establecer un acuerdo de nivel de servicio (SLA) con el proveedor de la suite, que incluya aspectos de seguridad: ▪ A.15.1 Seguridad de la información en las relaciones con los proveedores: El SLA debe definir las responsabilidades del proveedor en materia de seguridad, como la gestión de incidentes, la disponibilidad del servicio y la protección de datos. - A.17 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio: Se debe considerar la disponibilidad de la suite en el plan de continuidad del negocio. - A.18 Cumplimiento: Se debe asegurar el cumplimiento de los términos de la licencia del software y de cualquier otra regulación aplicable.	
22. Prestar el servicio de conectividad y telecomunicaciones para el funcionamiento de la SDP Controles Relacionados: - A.13 Seguridad de las comunicaciones: Asegura la disponibilidad y seguridad de las comunicaciones. - A.12.6 Gestión de vulnerabilidades técnicas: Mantenimiento y actualización de equipos de telecomunicaciones.	308.000.000
23. Prestar el servicio de mesa de ayuda para los servicios TIC, incluyendo soporte técnico, mantenimiento preventivo y correctivo de los equipos de cómputo e infraestructura de puestos de trabajo, propiedad de la SDP, con reposición de elementos Controles Relacionados: - A.12.3 Gestión de la capacidad: Asegura la disponibilidad del soporte técnico. - A.16 Gestión de incidentes de seguridad de la información: Punto de contacto para reportar incidentes. - A.11 Seguridad física y del entorno: Mantenimiento de equipos y puestos de trabajo, lo que puede incluir aspectos de seguridad física.	730.000.000
24. Soporte y mantenimiento de la red contra incendio, aires acondicionados y ups de	98.000.000

los centros de cómputo de la SDP Controles Relacionados: - A.11 Seguridad física y del entorno: Este control es el principal. El mantenimiento de la red contra incendios, aires acondicionados y UPS es crucial para la protección física de los centros de cómputo y la continuidad de las operaciones. Específicamente: ▪ A.11.1 Áreas seguras: Se asegura la protección física de las instalaciones que albergan los sistemas de información. ▪ A.11.2 Controles de entrada física: Se controla el acceso a los centros de cómputo. ▪ A.11.3 Seguridad de oficinas, recintos e instalaciones: Se mantienen las condiciones ambientales adecuadas para el funcionamiento de los equipos. ▪ A.11.4 Protección contra amenazas externas y ambientales: Se mitigan riesgos como incendios, inundaciones, fallos de energía, etc. ▪ A.11.5 Trabajo en áreas seguras: Se establecen procedimientos para el trabajo seguro en los centros de cómputo. ▪ A.11.7 Servicios de suministro: Se asegura la disponibilidad de energía eléctrica y refrigeración.	
25. Prestar el servicio de mantenimiento preventivo y correctivo del sistema de control de acceso con repuestos Controles Relacionados: - A.9.1 Requisitos del negocio para el control de acceso: Se asegura el funcionamiento del sistema que controla el acceso a las instalaciones. - A.11.2 Controles de entrada física: El mantenimiento del sistema de control de acceso físico es fundamental para este control.	30.000.000
26. Soporte y mantenimiento de las UPS marca PEI de los centros de cómputo y cableado Controles Relacionados: - A.11.7 Servicios de suministro: El mantenimiento de las UPS asegura el suministro ininterrumpido de energía a los equipos. - A.11.6 Cableado de seguridad: El mantenimiento del cableado asegura la integridad y disponibilidad de las conexiones de red. - A.17.2 Implementación de la continuidad del negocio: Las UPS son un componente clave para la continuidad del servicio en caso de fallos de energía.	25.000.000

TOTAL PRESUPUESTO FUNCIONAMIENTO 2025	**$7.146.837.000**

Fuente: *Diseño Propio*

6. CRONOGRAMA DE ACTIVIDADES PARA LA ACTUALIZACIÓN DEL SISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Tabla 8. Cronograma Detallado de Actividades para el mantenimiento del MSPI 2025

N°	Categoría / Actividad / Tarea	Fecha Inicio	Fecha Fin
1.	**Revisión y Actualización del MSPI**	**02/01/2025**	**15/12/2025**
1.1.	Formulación y ejecución del plan de implementación del MSPI 2025.	01/02/2025	01/08/2025
1.2.	Actualización de los documentos priorizados del MSPI.	02/01/2025	15/12/2025
1.3.	Revisión de aplicabilidad, Roles y Responsabilidades de acuerdo con el Decreto 432 de 2022.	02/01/2025	29/03/2025
1.4.	Revisar y actualizar los indicadores del SGSI.	01/08/2025	30/08/2025
2.	**Identificación y tratamiento de riesgos de seguridad**	**02/01/2025**	**15/12/2025**
2.1.	Formulación y ejecución Plan de tratamiento de riesgos de seguridad y privacidad de la información.	02/01/2025	15/12/2025
3.	**Definir y ejecutar el plan de sensibilización**	**15/01/2025**	**15/12/2025**
3.1.	Realizar jornadas de sensibilización a todo el personal.	15/01/2025	30/11/2025
3.2.	Realizar trasferencia de conocimiento a colaboradores de la Entidad en temas de Seguridad Digital.	15/01/2025	15/11/2025
3.3.	Medir el grado de sensibilización a toda la Entidad.	15/11/2025	15/12/2025
4.	**Gestión de incidentes de Seguridad y Privacidad de la Información**	**01/03/2025**	**31/12/2025**
4.1.	Actualizar y formalizar los procedimientos, guías, manuales de Gestión de Incidentes de seguridad de la información de acuerdo con la Norma ISO 27035.	01/03/2025	01/04/2025
4.2.	Socializar cuando sea requerido, el procedimiento a los especialistas de la Dirección de Tecnologías de la Información y las Comunicaciones, soportes en sitio, y personal de Mesa de Servicios indicando los cambios en el procedimiento. Socializar el procedimiento a los colabores de la Entidad.	01/04/2025	01/05/2025
4.3.	Seguimiento a los incidentes de seguridad de la información reportados a la mesa de servicio de acuerdo con lo establecido en el procedimiento definido.	01/01/2025	31/12/2025
4.4.	Socializar los boletines informativos de seguridad, emitidos por CSIRT de Gobierno.	01/01/2025	31/12/2025
5.	**Realizar Autodiagnóstico del MSPI**	**01/01/0225**	**15/07/2025**
5.1	Efectuar Autodiagnóstico con corte 31/12/2023.	01/01/2025	30/01/2025
5.2	Efectuar Autodiagnóstico segundo semestre.	15/06/2025	15/07/2025
6.	**Implementación de controles de acuerdo con el resultado del autodiagnóstico**	**01/02/2025**	**15/12/2025**
6.1.	Formulación y ejecución del Plan de Controles del Sistema de Gestión de Seguridad y Privacidad de la Información.	01/02/2025	15/12/2025
7.	**Gestión de Vulnerabilidades técnicas**	01/02/2025	15/12/2025

7.1.	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades y Pentest.	04/03/2025	01/05/2025
7.2.	Ejecución de las pruebas de vulnerabilidades y Pentest.	01/05/2025	30/09/2025
7.3.	Simulacros controlados sobre ataques de ingeniería social.	01/07/2025	30/10/2025
8.	**Plan de Continuidad del Negocio**	**03/06/2025**	**28/06/2025**
8.1.	Revisión y actualización de la documentación del Análisis de Impacto de la Operación.	03/06/2025	28/06/2025
8.2.	identificar los diferentes Servicios Esenciales y/o Infraestructura Críticas Cibernéticas.	03/06/2025	28/06/2025
8.	**Registro de bases de datos personales** (Sujeto a la generación de nuevas BD o Actualización de las Existentes)	**02/02/2025**	**15/12/2025**
8.1.	Recolección de bases de datos de las áreas.	02/02/2025	15/12/2025
8.2.	Actualización de bases de datos personales en el RNBD.	02/02/2025	02/02/2025
9.	**Cumplimiento**	**01/02/2025**	**15/12/2024**
9.1.	Participar en las auditorías internas y externas de la norma ISO 27001 programadas en la vigencia.	01/02/2025	15/12/2025
9.2.	Formular y ejecutar plan de mejoramiento.	01/06/2025	15/12/2025
9.3.	Revisión y Seguimiento planes MSPI I trimestre	01/04/2025	10/04/2025
9.3.	Revisión y Seguimiento planes MSPI II trimestre	01/07/2025	10/07/2025
9.3.	Revisión y Seguimiento planes MSPI III trimestre	01/10/2025	10/10/2025
9.3.	Revisión y Seguimiento planes MSPI IV trimestre	01/12/2025	10/12/2025

Fuente: *Diseño Propio*

7. RESPONSABLES

1. Comité Institucional de Gestión y Desempeño
2. Director de Tecnologías de la Información y las Comunicaciones
3. Dirección de Planeación Institucional
4. Líderes de Procesos
5. Oficial Seguridad Digital