NIT. 891. 801. 069-8

MODELO DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

INSTITUTO DE TRÁNSITO DE BOYACÁ

Oficina de Planeación y Sistemas

VIGENCIA 2025 – V1
15/01/2025

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA APROBACIÓN
1	Creación MSPI	15-01-2025

CONTENIDO

1. INTRODUCCIÓN.

En cumplimiento a lo establecido en el Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones", CONPES 3854 "Política Nacional de Seguridad Digital", CONPES 3701 "Lineamientos de Política para Ciberseguridad y Ciberdefensa" y Norma Técnica Colombiana NTC-ISO/IEC 27001 "Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos", la Entidad debe implementar el Modelo de Seguridad y Privacidad de la Información – MSPI, según sus necesidades y objetivos; requisitos de seguridad; procesos institucionales; y tamaño y estructura.

Que mediante Resolución 500 del 10 de marzo de 2021 "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 Seguridad Digital" el Ministerio de Tecnologías de la Información y Las Comunicaciones estableció los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.

El MSPI imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Seguridad Digital.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

2. ANTECEDENTES.

El 30 de junio de 1983, el Gobierno Departamental, expide el decreto No 00155 por el cual transforma al Departamento Administrativo de Tránsito y Transporte de Boyacá "DATTBOY", en el Instituto de Transito de Boyacá "ITBOY", y adopta su estatuto orgánico, cuyo objeto es dirigir, organizar y controlar lo relacionado con el tránsito, dentro del territorio de su jurisdicción y velar por el cumplimiento de sus disposiciones vigentes, aplicar y hacer cumplir las disposiciones que se dicten sobre tránsito; En el cumplimiento de su objeto, ITBOY ha venido evolucionando y modernizándose mediante la incorporación y adopción de estrategias y modelos estatales como la Estrategia de Seguridad Digital y el Modelo Integrado de Planeación y Gestión – MIPG.

2.1. Modelo Integrado de Planeación y Gestión – MIPG.

El Modelo Integrado de Planeación y Gestión – MIPG, es el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades públicas con el fin de generar resultados que atiendan a los planes de desarrollo y que resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en los servicios.

MIPG presenta los siguientes objetivos:

- Fortalecer el liderazgo y talento humano bajo los principios de integridad y legalidad como motores de la generación de resultados de las entidades públicas.
- Agilizar, simplificar y flexibilizar la operación de las entidades para la generación de bienes y servicios que resuelvan efectivamente las necesidades de los ciudadanos.
- Desarrollar una cultura organizacional fundamentada en la información, el control y la evaluación para la toma de decisiones y la mejora continua.
- Facilitar y promover la efectiva participación ciudadana en la planeación, gestión y evaluación de las entidades públicas.
- Promover la coordinación entre entidades públicas para mejorar su gestión y desempeño.

Y los siguientes principios:

- Integridad, transparencia y confianza.
- Orientación a resultados.
- Excelencia y calidad.
- Aprendizaje e innovación.
- Toma de decisiones basada en evidencia.

El ITBOY mediante la Resolución No 276 del 14 de septiembre de 2023, "Por medio de la cual se actualiza y reglamenta el Modelo Integrado de Planeación y Gestión del Instituto de Transito de Boyacá y se dictan otras disposiciones" adopta lineamentos en el marco de la implementación del Modelo Integrado de Planeación y Gestión.

2.2. Modelo de Seguridad y Privacidad de la Información – MSPI.

El Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC, a través de la Dirección de Estándares y Arquitectura de Tecnologías de la Información - TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones, mediante las cuales contribuye a la construcción de un Estado eficiente, transparente y participativo, publicó el Modelo de Seguridad y Privacidad de la Información - MSPI, dando cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de Seguridad Digital.

El Modelo de Seguridad y Privacidad de la Información – MSPI, lleva a la preservación de la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

El modelo de seguridad y privacidad de la información contempla un ciclo de operación de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de su información, a saber:

- Diagnostico.
- Planificación.
- Implementación.

- Evaluación del Desempeño.
- Mejora Continua.

A través del Decreto Único Reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se definió el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

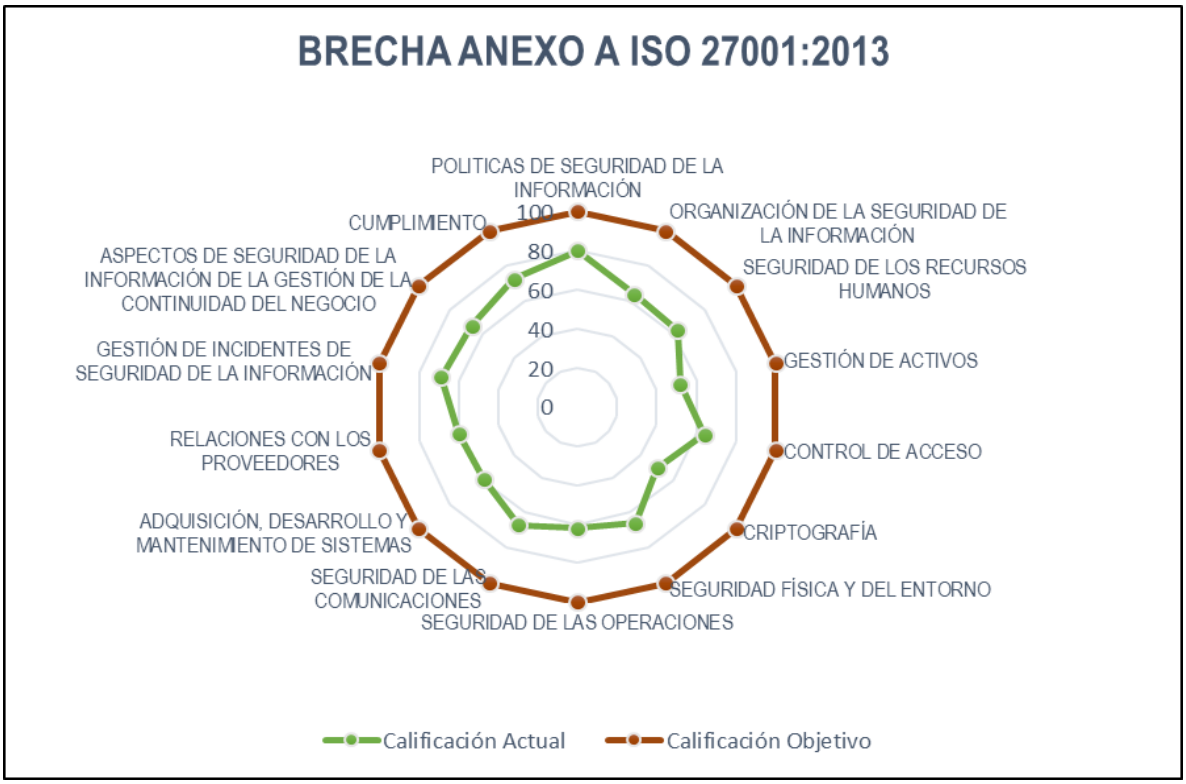
ITBOY con el fin de atender lo establecido en el Decreto Único Reglamentario 1078 de 2015 para la implementación del modelo MSPI, emitirá la resolución mediante la cual adopta las políticas establecidas en el Modelo de Seguridad y Privacidad de la Información, en el marco de la Estrategia de Seguridad Digital.

2.3. Diagnóstico de la Implementación del MSPI en el ITBOY.

2.3.1. Estado Actual del Sistema de Gestión de Seguridad y Privacidad de la Información.

De acuerdo con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la Política de Seguridad Digital, el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2013 es de:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	64	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	63	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	52	100	EFECTIVO
A.9	CONTROL DE ACCESO	64	100	GESTIONADO
A.10	CRIPTOGRAFÍA	50	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	66	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	62	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	67	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	59	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	60	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	69	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	67	100	GESTIONADO
A.18	CUMPLIMIENTO	72,5	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**64**	**100**	GESTIONADO



Fuente: Instrumento de Identificación de la línea Base de Seguridad.

2.3.2. Evaluaciones FURAG.

La evaluación FURAG de la vigencia 2023 para el ITBOY, cuyos resultados fueron presentados en la vigencia 2025, recomendó establecer un plan de mejoramiento para implementar 12 aspectos de Seguridad Digital, así:

Tabla 1. Recomendaciones Seguridad Digital Según Evaluación FURAG 2023.

ITEM	POLITICA	DESCRIPCION
1	POL07: SEGURIDAD DIGITAL	Almacenar las copias de respaldo en un lugar aislado, en un segmento diferente de red a la de servidores y equipos.
2	POL07: SEGURIDAD DIGITAL	Contar con un Plan de Recuperación de Desastres DRP, definido, documentado e implementado para todos los procesos.
3	POL07: SEGURIDAD DIGITAL	Establecer, documentar e implementar un procedimiento para la gestión de incidentes de seguridad digital (Ciberseguridad) que incluya la notificación a las autoridades pertinentes (CSIRT Gobierno / COLCERT).
4	POL07: SEGURIDAD DIGITAL	Garantizar el soporte a la infraestructura tecnológica de la entidad (plataformas, licencias, servicios y sistemas de información).

5	POL07: SEGURIDAD DIGITAL	Identificar y gestionar los posibles riesgos de seguridad digital (Ciberseguridad) de sus infraestructuras on premise.
6	POL07: SEGURIDAD DIGITAL	Identificar y gestionar los posibles riesgos de seguridad digital (Ciberseguridad) en los servicios de Nube Pública/Privada que utiliza.
7	POL07: SEGURIDAD DIGITAL	Implementar el Modelo de Seguridad y Privacidad de la Información (MSPI).
8	POL07: SEGURIDAD DIGITAL	Realizar análisis de vulnerabilidades para Portal Web, Sede electrónica y Servicios expuestos en Internet.
9	POL07: SEGURIDAD DIGITAL	Realizar pruebas de recuperación de cada una de los sistemas de información críticos.
10	POL07: SEGURIDAD DIGITAL	Realizar pruebas de respaldo a las copias de seguridad de la información de los aplicativos misionales, estratégicos, soporte y de mejora, de manera programada para asegurar la disponibilidad de los datos en caso de Ransomware, de manera coordinada con los responsables del proceso.
11	POL07: SEGURIDAD DIGITAL	Separar los equipos que realizan las copias de respaldo de la información, del software e imágenes de los sistemas de la red de servidores y computadores.
12	POL07: SEGURIDAD DIGITAL	Verificar y asegurar que los proveedores y contratistas de la entidad cumplan con las políticas de ciberseguridad internas.

Fuente: Plataforma de Medición Desempeño institucional “recomendaciones de mejora por entidad territorial, vigencia 2023”.

3. OBJETIVO GENERAL.

Implementar el Modelo de Seguridad y Privacidad de la Información – MSPI en el ITBOY para incorporar la seguridad informática en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.

4. OBJETIVOS ESPECÍFICOS.

- Orientar la gestión e implementación del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua) en el ITBOY.
- Preservar la confidencialidad, integridad y disponibilidad de la información, contribuyendo al cumplimiento de la misión y los objetivos estratégicos Institucionales de la Entidad, mediante la implementación del Modelo MSPI
- Articular la Seguridad Informática con el componente de Tecnologías de la Información y las Comunicaciones – TIC para implementar los requisitos de seguridad operativa y seguridad y privacidad de la información, definidos por los procesos institucionales acorde al tamaño y estructura de la Entidad.
- Fortalecimiento de los Sistemas de Información, Servicios de gestión de Información, Servicios Tecnológicos e Infraestructura tecnológica.
- Habilitar la implementación de la Política de Seguridad Digital.

5. ALCANCE.

Desarrollar y apoyar la implementación, construcción y disposición de las actividades programadas en el Plan de Implementación del MSPI del ITBOY para la vigencia 2025.

6. BENEFICIOS.

En términos generales, el MSPI le permite a la Entidad, proteger su información institucional y cumplir con las leyes y regulaciones aplicables, minimizar riesgos, mejorar la eficiencia y la cultura de seguridad informática, y aumentar la confianza de los ciudadanos.

La implementación del MSPI en el ITBOY, redundara en los siguientes beneficios específicos:

- Cumplimiento de los aspectos relacionados con la información institucional, como es la protección, seguridad, privacidad y control de los activos de información, junto con la protección de la infraestructura tecnológica.
- Reducción del riesgo de que se produzcan pérdidas de información en la Entidad.
- Establecer una metodología que permita gestionar la seguridad informática (seguridad operativa y seguridad y privacidad de la información) en la Entidad.
- Implementar medidas de seguridad informática para que los funcionarios, contratistas, proveedores o terceros que tengan alguna relación con el ITBOY, puedan acceder a la información de forma segura y controlada.
- Obligar a que se realicen auditorías de manera periódica para identificar las incidencias de seguridad informática que pudieran presentarse sobre la infraestructura tecnológica, sistemas de información, servicios de gestión de información y todo tipo de activos, de tal manera que estos activos sean gestionados, administrados y adaptados a las necesidades actuales y futuras de la Entidad.
- Contar un Sistema de Gestión de Seguridad de la Información – SGSI, para garantizar la confidencialidad, integridad y la seguridad de la información institucional.
- Ayuda a identificar y gestionar los riesgos asociados con la gestión de la información. Esto puede incluir amenazas como la pérdida de datos, el robo de información, y la ciberdelincuencia, entre otros.
- Garantiza la continuidad de la operación y servicio institucional con normalidad o en el menor tiempo posible en el caso de producirse hechos disruptivos, tales como ataques de Ramsonware, Phising y Exploits, entre otros. De tal manera que la Entidad puede volver a operar sin pérdidas de información o con las mínimas aceptables establecidas.
- Garantiza que la Entidad esté cumpliendo con la legislación vigente en materia de información personal y propiedad intelectual.
- Optimiza el funcionamiento de los procesos institucionales, sistemas de información y servicios de gestión de información; garantizando así, una reducción de los costos de operación. En este caso, el beneficio no se aprecia en forma de ganancia económica evidente, sino que se observa que los gastos disminuyen en cuanto desciende el número de incidentes relacionados con la seguridad informática.
- Permite establecer la asignación de roles, responsabilidades y obligaciones, para gestionar y administrar los riesgos de seguridad informática de los activos institucionales.
- Contribuye al incremento en la motivación del personal, ya que se desarrolla una cultura

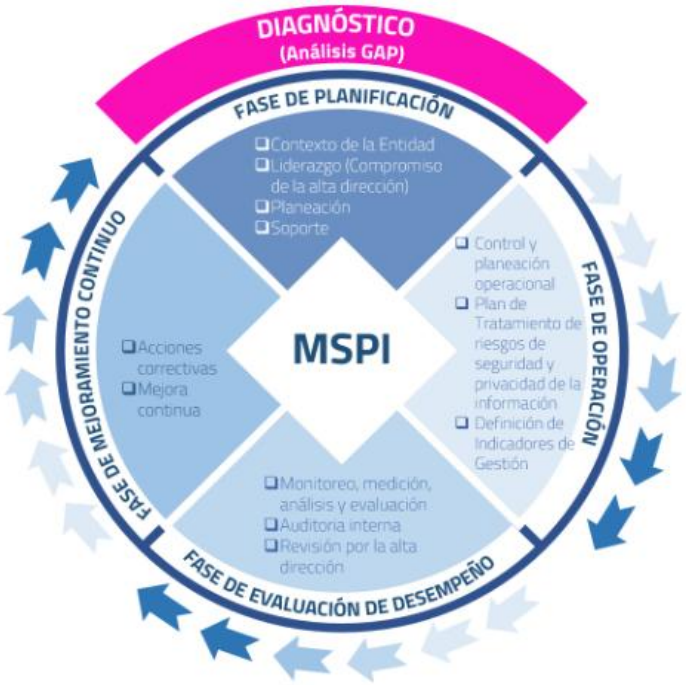
organización comprometida con la seguridad informática.

7. METODOLOGIA.

7.1. Ciclo Operacional

El Modelo MSPI del ITBOY toma como referencia el ciclo definido en el Modelo de Seguridad y Privacidad de la Información emitido por el Ministerio de Tecnologías de la Información y Comunicaciones en su Versión 44, el cual está basado en el ciclo PHVA conforme al estándar internacional ISO/IEC 27001:2022 (Planificación, Implementación, Evaluación de Desempeño y Mejora Continua):

Figura 1. Ciclo del Modelo de Seguridad y Privacidad de la Información



Fuente: Documento del Modelo de Seguridad y Privacidad de la Información de MinTIC

7.2. Marco Metodológico.

El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Seguridad Digital y para que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El MSPI se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión - MIPG y la Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Seguridad Digital; y se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación.

Mediante el aprovechamiento de las TIC, la implementación del modelo de seguridad y privacidad de la información, y el fortalecimiento de la seguridad de la información en las entidades públicas, se garantiza la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación colombiana.

La implementación del MSPI en el ITBOY, requiere el desarrollo de actividades y productos en cuatro (4) fases: Planificación, Implantación, Evaluación de desempeño y Mejora continua. Para cada una de las fases se deben desarrollar los siguientes objetivos y resultados esperados:

7.2.1. Fase de Planeación.

En esta fase se definen las actividades y productos en el plan de seguridad y privacidad de la información establecido para la Entidad, el cual debe estar alineado con el objetivo misional institucional y contener las acciones a nivel de seguridad y privacidad de la información, utilizando una metodología de gestión del riesgo.

La Entidad para esta fase debe establecer el alcance del MSPI, definiendo los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad, con un enfoque basado por procesos.

Para la implementación de la fase, la Entidad debe desarrollar actividades y productos teniendo en cuenta los procesos que impactan la consecución de los objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del MSPI con otros procesos.

Para esta fase, los requerimientos que deben ser atendidos son los siguientes:

Figura 2. Requerimientos Fase de Planificación

Fuente: Documento del Modelo de Seguridad y Privacidad de la Información de MinTIC.

Los objetivos y resultados esperados de la fase de Planeación son:

Tabla 3. Objetivos y Resultados Fase de Planeación.

OBJETIVOS	RESULTADOS ESPERADOS
Política de Seguridad y Privacidad de la Información.	Documento con la política de seguridad de la información, debidamente aprobado por el Comité Institucional de Seguridad y Privacidad del ITBOY y socializada al interior de la Entidad.
Políticas de seguridad y privacidad de la información.	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea el Comité de Seguridad y Privacidad de la Información del ITBOY, en donde se incluyan los temas de seguridad de la información; además, se deberá asignar el encargado de seguridad y privacidad de la información (conocido también como el Oficial de Seguridad) dentro de la Entidad.
Inventario de activos de información.	Documento con la política de Gestión y Administración de los Activos de Información, aprobado por el Comité Institucional de Seguridad y Privacidad de la Información del ITBOY. Ficha Técnica de los activos de información con la caracterización de los activos de información, que contengan datos personales de los inventarios de los activos.
Integración del MSPI con el Sistema de Gestión Documental.	Integración del MSPI, con el sistema de gestión documental de la Entidad.
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 el Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.

Fuente: Documento del Modelo de Seguridad y Privacidad de la Información de MinTIC.

7.2.2. Fase de Implementación.

En esta fase, la entidad debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que le permitan implementar las acciones determinadas en el plan de tratamiento de riesgos. La entidad debe disponer de evidencia documental sobre los procesos que se han llevado a cabo según lo planificado, adicionalmente, debía tener un control de cambios que le permitirían tomar acciones para mitigar efectos adversos cuando sea necesario.

La Entidad para esta fase debe implementar el plan de tratamiento de riesgos de seguridad de la información, en el cual se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable para ella. Es preciso tener en cuenta que la aplicación de los controles sobre los riesgos detectados debe estar aprobados por el líder de cada proceso y por el Comité de Seguridad Digital del ITBOY.

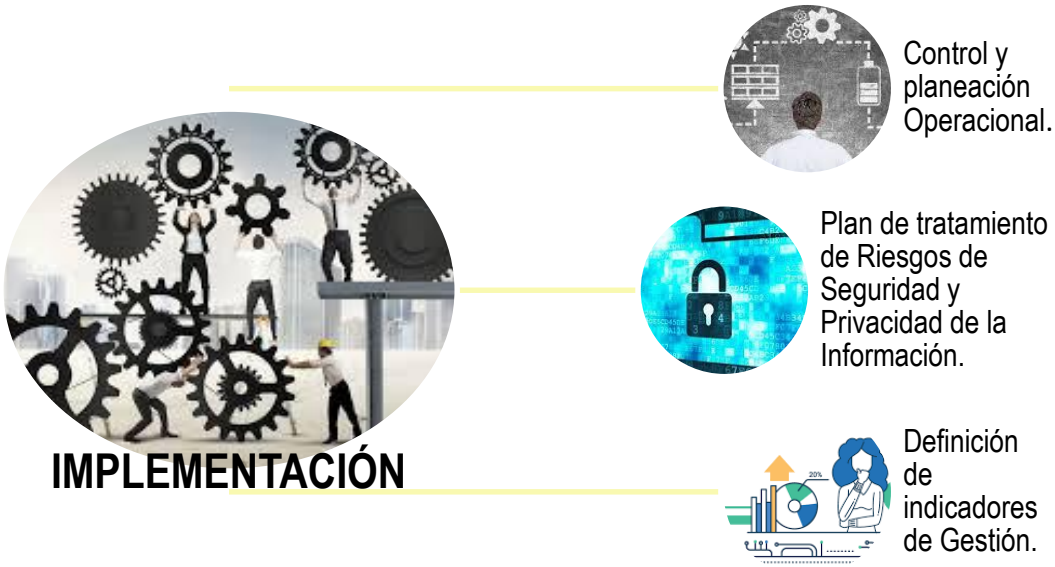
La entidad debe definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.

Los indicadores deben medir:

7.2.2.1. Efectividad en los controles.
7.2.2.2. Eficiencia del MSPI al interior de la entidad.
7.2.2.3. Proveer estados de seguridad que sirvan de guía en las revisiones y la mejora continua.
7.2.2.4. Comunicar valores de seguridad al interior de la entidad.
7.2.2.5. Servir como insumo al plan de control operacional

Para esta fase los requerimientos son:

Figura 3. Requerimientos Fase de Implementación



Fuente: Documento del Modelo de Seguridad y Privacidad de la Información de MinTIC.

Los objetivos y resultados esperados de la fase de Implementación son:

Tabla 4. Objetivos y Resultados Fase de Implementación.

OBJETIVOS	RESULTADOS ESPERADOS
Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por el Comité Institucional de Seguridad y Privacidad del ITBOY.
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso y el Comité Institucional de Seguridad y Privacidad del ITBOY.
Indicadores de Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información aprobado por el Comité Institucional de Seguridad y Privacidad del ITBOY.

Fuente: Documento del Modelo de Seguridad y Privacidad de la Información de MinTIC.

7.2.3. Fase Evaluación de Desempeño.

En esta fase se debe definir los procesos de seguimiento y monitoreo a la implementación del MSPI, según los resultados arrojados por los indicadores de la seguridad de la información para verificar la efectividad, la eficiencia y la eficacia de las acciones implementadas por la Entidad respecto al MSPI.

Para esta fase los requerimientos son:

Figura 4. Requerimientos Fase Evaluación de Desempeño

Fuente: Documento del Modelo de Seguridad y Privacidad de la Información de MinTIC.

En esta fase, la Entidad debe crear un plan que contemple las siguientes actividades:

- **7.2.3.1.** Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- **7.2.3.2.** Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- **7.2.3.3.** Seguimiento a la programación y ejecución de las actividades de auditorías internas y externas del MSPI.
- **7.2.3.4.** Seguimiento al alcance y a la implementación del MSPI.
- **7.2.3.5.** Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- **7.2.3.6.** Medición de los indicadores de gestión del MSPI.
- **7.2.3.7.** Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI)

Al revisar y analizar el plan, la Entidad debe identificar que estén consolidados los indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

La entidad debe generar un documento donde se defina el plan de auditorías para el MSPI, en el cual se especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

La Entidad debe llevar a cabo auditorías y revisiones independientes a intervalos planificados que permitan identificar si el MSPI es conforme con los requisitos de la entidad, está implementado adecuadamente y se mantiene de forma eficaz; así mismo, la difusión a las partes interesadas de los resultados de la ejecución de

las auditorías, junto con la conservación de la información documentada como evidencia de los resultados de las auditorías.

Los objetivos y resultados esperados de la fase Evaluación de Desempeño son:

Tabla 5. Objetivos y Resultados Fase Evaluación de Desempeño

OBJETIVOS	RESULTADOS ESPERADOS
Plan de revisión y seguimiento a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por el Comité Institucional de Seguridad y Privacidad del ITBOY.
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.

Fuente: Documento del Modelo de Seguridad y Privacidad de la Información de MinTIC.

7.2.4. Fase de Mejora Continua.

En esta fase, la Entidad debe consolidar los resultados obtenidos de la fase evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.
Para esta fase los requerimientos son:

Figura 5. Requerimientos Fase de Mejora Continua.

Fuente: Norma ISO IEC/27001 Capítulo 10, que permite orientar como se desarrolla la fase de Mejoramiento Continuo del MSPI.

En esta fase la entidad debe definir y haber ejecutado el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan debe incluir:

7.2.4.1. Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.
7.2.4.2. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

7.2.4.3. Utilizando los insumos anteriores, la Entidad debe efectuar los ajustes a los entregables, controles y procedimientos del MSPI. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por el Comité Institucional de Seguridad y Privacidad del ITBOY. La revisión del Comité de Seguridad debe hacer referencia a las decisiones, cambios y prioridades, entre otras, tomadas por el comité y que impactan el MSPI.

Los objetivos y resultados esperados de la fase de Mejora Continua son:

Tabla 6. Objetivos y Resultados Fase de Mejora Continua.

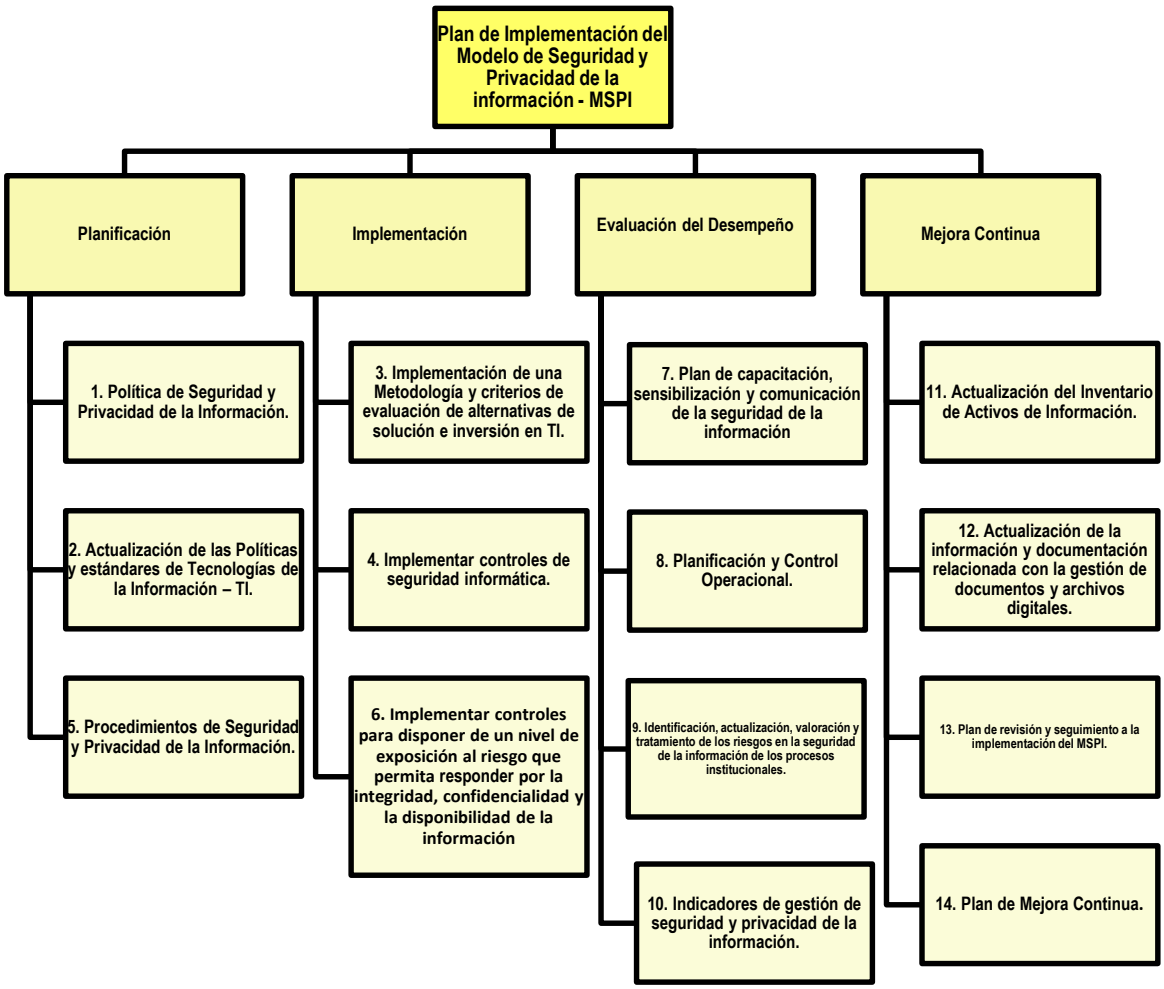
OBJETIVOS	RESULTADOS ESPERADOS
Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.

Fuente: Documento del Modelo de Seguridad y Privacidad de la Información de MinTIC.

7.3. Actividades por Ejecutar y Productos Esperados – Vigencia 2025.

El Plan de implementación aprobado por el Comité Institucional de Seguridad y Privacidad de la información del ITBOY dispone de las siguientes macroactividades:

Figura 6. Macroactividades del Plan de Implementación del Modelo de Seguridad y Privacidad de la Información - MSPI.



Fuente: Estructuración del Plan de Implementación del Modelo de Seguridad y Privacidad de la Información - MSPI.

La Oficina de Tecnologías, estructuró el Plan de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) para incorporar en el ITBOY, la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

7.3.1. Actividades realizadas en la vigencia 2025 para la implementación del MSPI.

A continuación, se detallan las acciones y logros alcanzados en el marco del proyecto de Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) durante la vigencia 2025 en el (ITBOY):

Estructuración del Plan de Implementación del MSPI: Elaboración y presentación del plan ante el Comité Institucional de Gestión y Desempeño para su aprobación.

Promoción del Proyecto MSPI: Difusión activa del proyecto entre la comunidad del ITBOY a través del

Grupo de Comunicaciones.

Contextualización del Plan de Implementación del MSPI: Colaboración con la diversas áreas y dependencias del ITBOY.

Reuniones Sectoriales de Seguridad de la Información: Participación en reuniones para revisar el avance en la implementación del MSPI en la entidad y explicar los resultados en FURAG 2023.

Alertas de Seguridad Digital: Contextualización a las áreas sobre alertas emitidas por el Ministerio TIC, como el Ransomware BlackByte y el Modus Operandi del Grupo Lapsus$.

Asesoramiento y Lineamientos para Proyectos Específicos: Orientación en seguridad de la información para proyectos.

Creación del Comité Institucional de Seguridad y Privacidad de la Información: Expedición de la Resolución para la creación del comité.

Modificaciones a la Política General de Seguridad y Privacidad de la Información: Revisión, análisis y caracterización de las modificaciones realizadas.

Promoción Continua del Proyecto MSPI: Permanente divulgación entre la comunidad del ITBOY.

Gestión de Recomendaciones Preventivas del Ministerio TIC: Atención y aplicación de las recomendaciones emitidas para abordar alertas de seguridad digital.

Contención, Erradicación y Solución de Incidente de Seguridad: Asesoramiento y apoyo en la respuesta a incidentes de acceso no autorizado a activos de información.

Procedimiento de Atención a Incidentes de Seguridad de la Información: Caracterización, estructuración y contextualización del procedimiento.

Reuniones Sectoriales y Evaluación del FURAG: Participación en reuniones para revisar el avance en la implementación del MSPI y gestión de actividades del FURAG en seguridad de la información.

Lineamientos para Gestión de Incidentes de Seguridad Digital: Estructuración de lineamientos según la Resolución 500 de 2021 del Ministerio TIC.

Identificación de Activos de Información: Proceso de identificación de activos de información en el ITBOY.

Equipo de Implementación del MSPI: Apoyo en la creación del equipo por instrucción del Comité Institucional de Seguridad y Privacidad de la Información.

Ajuste de Política Institucional de Administración del Riesgo: Inclusión de la administración del riesgo de seguridad y privacidad de la información y del riesgo digital.

Caracterización y Estructuración de Políticas: Desarrollo y revisión de políticas, como Control de Acceso,

Seguridad y Gestión de Activos de Información, Ciberseguridad y Seguridad y Privacidad de la Información para el Teletrabajo.

Capacitación: Estructuración y caracterización de la Capacitación en Seguridad Digital y seguridad de la Información.

Elaboración de Nuevas Políticas y Protocolos: Desarrollo de nuevas políticas, como la de Implementación y Uso de Antivirus y Antimalware, Separación de Ambientes de Desarrollo, Pruebas y Producción, Protocolo de Intercambio de Información, y Protocolo de Seguridad y Privacidad para Redes Sociales.

Apoyo en Distintas Iniciativas: Colaboración en la elaboración de procedimientos, jornadas de formación en Transformación Digital, y en la implementación de la estrategia de estructuración del Plan Estratégico de Tecnologías de la Información (PETI).

Lo anterior destacara los esfuerzos y avances significativos en la implementación del MSPI, reflejando el compromiso del ITBOY con la seguridad y privacidad de la información en todas sus dimensiones.

7.3.2. Principios para el Desarrollo de Actividades en la vigencia 2025.

En las actividades a desarrollar durante la vigencia 2025 de acuerdo con el Decreto 338 de 2022 se deben aplicar los siguientes principios:

7.3.2.1. **Confianza**. La seguridad digital debe fomentar la confianza mediante la buena comunicación, el intercambio de información y la concreción de acuerdos claros sobre la división de tareas y acciones a realizar.

7.3.2.2. **Coordinación**. Las actuaciones que se realicen en materia de seguridad digital deberán integrar de manera coordinada a las múltiples partes interesadas, para garantizar la armonía en el ejercicio de sus funciones y el logro del objeto del presente título.

7.3.2.3. **Colaboración entre las múltiples partes interesadas.** En la aplicación e interpretación de los lineamientos se deben involucrar activamente a las múltiples partes interesadas, y permitir establecer condiciones para el desarrollo eficiente de alianzas, con el fin de promover la seguridad digital.

7.3.2.4. **Enfoque basado en la gestión de riesgos.** La Entidad debe gestionar el riesgo de forma que el uso de tecnologías de la información y las comunicaciones – TIC, fomente la confianza en el entorno digital, innovación, productividad, competitividad, y ello no suponga la materialización de infracciones a los derechos de los ciudadanos.

7.3.2.5. **Gradualidad.** La Entidad desarrollará herramientas estratégicas y operativas, de alcance definido en tiempo, espacio y recursos presupuestales que permitan la implementación gradual y sostenida de estrategias, programas, planes y proyectos, que se requieran para garantizar la seguridad y protección de la información institucional.

7.3.2.6. **Inclusión.** La seguridad informática debe incluir a todas las partes interesadas, fomentar su participación y establecer condiciones necesarias para el desarrollo eficiente de alianzas.

7.3.2.7. **Proporcionalidad.** Las acciones y operaciones en seguridad informática serán proporcionales con la gestión dinámica de los riesgos derivados de los avances o usos de la ciencia y la tecnología, ponderando circunstancias de necesidad, derechos e intereses en juego, oportunidad, capacidades, amenazas y riesgos.

7.3.2.8. **Uso eficiente de la infraestructura y de los recursos para protección de los activos y los servicios esenciales institucional.** La Entidad velara por las infraestructuras y los recursos tendientes a la protección de los activos y los servicios esenciales para que sean aprovechados de forma eficiente y en beneficio de los ciudadanos.

En la ejecución de las actividades de la vigencia 2025 se presentan las siguientes condiciones:

7.3.2.9. Indistintamente de quien elabora los documentos, estos deben ser revisados y contextualizados en la Entidad por parte de los miembros (enlaces) del equipo de implementación del MSPI.

7.3.2.10. Todos los productos que deben ser entregados (Políticas, Procedimientos, Metodologías y Protocolos entre otros) deben ser aprobados por el Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.

7.3.2.11. La responsabilidad de la implementación de todos los productos a ser entregados (Políticas, Procedimientos, Metodologías y Protocolos entre otros) es del Comité Institucional de Seguridad y Privacidad de la Información del ITBOY y la implementación operativa de los productos a ser entregados es de la Alta Gerencia (Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno), Lideres de proceso, Subgerencias, oficinas y áreas de la institución.

7.3.3. Actividades planificadas para la vigencia 2025.

Las actividades por ejecutar y productos esperados para la vigencia 2025 son:

Tabla 7. Actividades por Ejecutar.

MACROPROCESO / ACTIVIDAD	TIEMPO ESTIMADO (DÍAS)
1. Política de Seguridad y Privacidad de la Información.	**1.471**
Política General de Seguridad y Privacidad de la Información.	**80**
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	80
Política de Gestión de Activos.	**90**
Revisión y contextualización de la Política de Gestión de Activos por parte de los grupos de interés	20
Aprobación de la Política de Gestión de Activos por parte del Comité Institucional de	15

Seguridad y Privacidad de la Información del ITBOY.	
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	55
Políticas de ciberseguridad.	**120**
Revisión y contextualización de las Políticas de Ciberseguridad por parte de los grupos de interés	20
Aprobación de las Políticas de Ciberseguridad por parte del Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	80
Política de Control de Acceso.	**145**
Revisión y contextualización de las Política de Control de Acceso por parte de los grupos de interés.	25
Aprobación de las Política de Control de Acceso por parte del Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	100
Política de No Repudio.	**80**
Revisión y contextualización de la Política de No Repudio por parte de los grupos de interés.	10
Aprobación de la Política de No Repudio por parte del Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	50
Política de gestión del riesgo en la seguridad de la información.	**110**
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	110
Política de Privacidad y Confidencialidad.	**95**
Elaboración borrador de la política de Privacidad y Confidencialidad.	10
Mesas de trabajo con los grupos de interés.	15
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	5
Caracterización, estructuración y redacción de la Política de Privacidad y Confidencialidad.	5
Revisión y contextualización de la Política de Privacidad y Confidencialidad por parte de los grupos de interés.	10
Aprobación de la Política de Privacidad y Confidencialidad por parte del Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	30
Política de Integridad.	**89**
Elaboración borrador de la Política de Integridad.	15
Mesas de trabajo con los grupos de interés.	15
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	5
Caracterización, estructuración y redacción de la Política de Integridad.	6
Revisión y contextualización de la Política de Integridad por parte de los grupos de interés	24

Aprobación de la Política de Integridad por parte del Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	4
Política de Disponibilidad del Servicio e Información.	**148**
Elaboración borrador de la Política de Disponibilidad del Servicio e Información.	20
Mesas de trabajo con los grupos de interés.	30
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	5
Caracterización, estructuración y redacción de la Política de Disponibilidad del Servicio e Información.	8
Revisión y contextualización de la Política de Disponibilidad del Servicio e Información por parte de los grupos de interés.	15
Aprobación de la Política de Disponibilidad del Servicio e Información por parte del Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	50
Política de Registro y Auditoría.	**97**
Elaboración borrador de la Política de Registro y Auditoría.	10
Mesas de trabajo con los grupos de interés.	17
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	3
Caracterización, estructuración y redacción de la Política de Registro y Auditoría.	7
Revisión y contextualización de la Política de Registro y Auditoría por parte de los grupos de interés.	10
Aprobación de la Política de Registro y Auditoría por parte del Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	30
Política de Gestión de Incidentes de Seguridad de la Información.	**107**
Elaboración borrador de la Política de Gestión de Incidentes de Seguridad de la Información.	10
Mesas de trabajo con los grupos de interés.	15
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	7
Caracterización, estructuración y redacción de la Política de Gestión de Incidentes de Seguridad de la Información.	10
Revisión y contextualización de la Política de Gestión de Incidentes de Seguridad de la Información por parte de los grupos de interés.	15
Aprobación de la Política de Gestión de Incidentes de Seguridad de la Información por parte del Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	30
Política de Capacitación y Sensibilización en Seguridad de la Información.	**100**
Elaboración borrador de la Política de Capacitación y Sensibilización en Seguridad de la Información.	8
Mesas de trabajo con los grupos de interés.	10

Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	7
Caracterización, estructuración y redacción de la Política de Capacitación y Sensibilización en Seguridad de la Información.	10
Revisión y contextualización de la Política de Capacitación y Sensibilización en Seguridad de la Información por parte de los grupos de interés.	15
Aprobación de la Política de Capacitación y Sensibilización en Seguridad de la Información por parte del Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	30
2. Actualización de las Políticas y estándares de Tecnologías de la Información – TI.	**191**
Mesas de trabajo con los grupos de interés.	24
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	5
Definición y caracterización de políticas y estándares de Tecnologías de la Información – TI, Tema: Seguridad	18
Definición y caracterización de políticas y estándares de Tecnologías de la Información – TI, Tema: Gestión de información	20
Definición y caracterización de políticas y estándares de Tecnologías de la Información – TI, Tema: Adquisición Tecnológica	17
Definición y caracterización de políticas y estándares de Tecnologías de la Información – TI Tema: Infraestructura Tecnológica	15
Definición y caracterización de políticas y estándares de Tecnologías de la Información – TI Tema: Servicios Tecnológicos	16
Definición y caracterización de políticas y estándares de Tecnologías de la Información – TI Tema: Soporte y Apoyo al Usuario	19
Definición y caracterización de políticas y estándares de Tecnologías de la Información – TI Tema: Acceso a la Tecnología y Uso de las Facilidades por parte de los Usuarios	21
Elaboración del documento con la definición y caracterización de las políticas y estándares de Tecnologías de la Información – TI	5
Revisión y aprobación por parte de los grupos de interés del documento con la definición y caracterización de las políticas y estándares de Tecnologías de la Información – TI	4
Registro, revisión y aprobación del documento con la definición y caracterización de las políticas y estándares de Tecnologías de la Información – TI	27
3. Implementación de una Metodología y criterios de evaluación de alternativas de solución e inversión en TI.	**336**
Revisión, ajustes y aprobación del catálogo de Servicios de TI.	11
Establecer, documentar y aprobar el Plan de capacidad de TI para cada uno de los servicios de TI según el catálogo de Servicios de TI.	19
Definir, adoptar, documentar y aprobar la metodología de evaluación de alternativas de solución e inversión en TI.	34
Definir, caracterizar, documentar y aprobar los criterios de tipo técnico, funcional y financiero.	15
Definir, adoptar, documentar y aprobar la metodología de cuantificación del valor	39

público y el retorno de la inversión del resultado de la implementación de los proyectos de TI.	
Definir, adoptar, documentar y aprobar la metodología de planeación, ejecución y seguimiento a los proyectos de TI.	34
Definir, documentar y aprobar el procedimiento para la planeación, ejecución y seguimiento a los proyectos de TI.	15
Definir, adoptar, documentar y aprobar la metodología de ejecución y seguimiento a los proyectos de la entidad que incluyen componentes de TI y son liderados por otras áreas.	24
Definir, documentar y aprobar el procedimiento para la ejecución y seguimiento a los proyectos de la entidad que incluyen componentes de TI y son liderados por otras áreas.	24
Definir, adoptar, documentar y aprobar la metodología de gestión de proyectos para gestionar las iniciativas y proyectos de TI.	20
Definir, documentar y aprobar el procedimiento para gestionar las iniciativas y proyectos de TI.	16
Definir, adoptar, documentar y aprobar el esquema de gestión de cambios para iniciativas y proyectos de Tecnología.	15
Definir, documentar y aprobar el procedimiento de gestión de cambios para iniciativas y proyectos de Tecnología.	15
Implementación de la seguridad de la información en el ciclo de vida de los Proyectos.	**55**
Definir, adoptar, documentar y aprobar para la entidad, el ciclo de vida de los proyectos de TI y los proyectos liderados por otras áreas que incluyen componentes de TI.	29
Establecer, documentar y aprobar el procedimiento de ejecución del ciclo de vida de los proyectos de TI y de los proyectos liderados por otras áreas que incluyen componentes de TI.	26
4. Implementar controles de seguridad informática.	**90**
Definir, adoptar, documentar y aprobar la metodología para identificar y caracterizar los controles físicos; junto con la definición de su plan de tratamiento.	20
Definir, adoptar, documentar y aprobar el sistema de métricas para medir la eficacia de los controles físicos.	12
Definir, adoptar, documentar y aprobar la metodología para identificar y caracterizar los controles técnicos; junto con la definición de su plan de tratamiento.	20
Definir, adoptar, documentar y aprobar el sistema de métricas para medir la eficacia de los controles técnicos.	12
Definir, adoptar, documentar y aprobar la metodología para identificar y caracterizar los controles administrativos; junto con la definición de su plan de tratamiento.	15
Definir, adoptar, documentar y aprobar el sistema de métricas para medir la eficacia de los controles administrativos.	11
5. Procedimientos de Seguridad y Privacidad de la Información.	**806**
Procedimientos de Seguridad del Recurso Humano.	**706**

Procedimiento de Capacitación y Sensibilización del Personal (Funcionarios y Contratistas).	**115**
Elaboración borrador del procedimiento Capacitación y Sensibilización del Personal (Funcionarios y Contratistas).	10
Mesas de trabajo con los grupos de interés.	15
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	5
Caracterización, estructuración y redacción del procedimiento.	10
Revisión y VoBo del procedimiento por parte de los grupos de interés.	15
Aprobación del procedimiento de Capacitación y Sensibilización del Personal (Funcionarios, Contratistas) por parte del Comité Institucional de Seguridad y Privacidad de la Información.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	40
Procedimiento de Ingreso y Desvinculación de Funcionarios.	**120**
Elaboración borrador del procedimiento de Ingreso y Desvinculación de Contratistas.	10
Mesas de trabajo con los grupos de interés.	15
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	10
Caracterización, estructuración y redacción del procedimiento.	10
Revisión y VoBo del procedimiento por parte de los grupos de interés.	20
Aprobación del procedimiento de Ingreso y Desvinculación de Contratistas por parte del Comité Institucional de Seguridad y Privacidad de la Información.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	30
Procedimiento de gestión del riesgo en la seguridad de la información.	**111**
Elaboración borrador del procedimiento de Procedimiento de gestión del riesgo en la seguridad de la información.	54
Criterios de Evaluación del Riesgo en la seguridad de la información.	5
Criterios de Impacto en la seguridad de la información.	5
Criterios de Aceptación del Riesgo en la seguridad de la información.	7
Alcance y Límites para la Gestión de Riesgos en Seguridad de la Información.	5
Identificación de Riesgos en la seguridad de la información.	10
Análisis de Riesgos en la seguridad de la información.	15
Valoración de Controles para el Tratamiento de Riesgos en la Seguridad de la Información.	10
Procedimiento de Identificación y Clasificación de Activos de Información.	**90**
Metodología para identificación, clasificación y valoración de activos de información.	**90**
Elaboración borrador de la Metodología para identificación, clasificación y valoración de activos de información.	10
Mesas de trabajo con los grupos de interés.	20
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	15
Caracterización, estructuración y redacción de la metodología para identificación, clasificación y valoración de activos de información.	10
Revisión y VoBo de la metodología por parte de los grupos de interés.	15
Aprobación de la metodología por parte del Comité Institucional de Seguridad	20

y Privacidad de la Información.	
Procedimientos para la administración de documentos electrónicos, documentos digitales, bases de datos y demás registros de información digital.	**155**
Elaboración borradores de los Procedimientos para la administración de documentos electrónicos, documentos digitales, bases de datos y demás registros de información digital.	25
Mesas de trabajo con los grupos de interés.	30
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	20
Caracterización, estructuración y redacción de los procedimientos.	15
Revisión y VoBo de los procedimientos por parte de los grupos de interés.	15
Aprobación de los procedimientos por parte del Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	30
Procedimientos de Control de Acceso.	**100**
Procedimiento de Gestión de Usuarios y Contraseñas.	**100**
Elaboración borrador del Procedimiento para Gestión de Usuarios y Contraseñas.	15
Mesas de trabajo con los grupos de interés.	10
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	10
Caracterización, estructuración y redacción del procedimiento.	10
Revisión y VoBo del procedimiento por parte de los grupos de interés.	15
Aprobación del Procedimiento Para Ingreso Seguro a los Sistemas de Información por parte del Comité Institucional de Seguridad y Privacidad de la Información.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	20
6. Implementar controles para disponer de un nivel de exposición al riesgo que permita responder por la integridad, confidencialidad y la disponibilidad de la información.	**112**
Definir, adoptar, documentar y aprobar el modelo o esquema de gobierno de información	**57**
Implementación del modelo o esquema de gobierno de información.	**55**
Etapa de Identificación. Identificación de datos maestros y definición de metadatos funcionales para soporte del dato.	**55**
Identificar el uso de los datos maestros en los directorios de componentes de información y en los sistemas de información asociados con el dato a gobernar.	25
Identificación de metadatos para el dato a gobernar (Directorio de metadatos).	30
7. Plan de capacitación, sensibilización y comunicación de la seguridad de la información.	**215**
Metodología para identificar las necesidades de capacitación en seguridad de la información.	**115**
Elaboración borrador de la Metodología para identificar las necesidades de capacitación en seguridad de la información.	10
Mesas de trabajo con los grupos de interés.	20
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	10

Caracterización, estructuración y redacción de la metodología para identificar las necesidades de capacitación en seguridad de la información.	15
Revisión y VoBo de la metodología por parte de los grupos de interés.	20
Aprobación de la Metodología para identificar las necesidades de capacitación en seguridad de la información por parte del Comité Institucional de Seguridad y Privacidad de la Información.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	20
Diseño del programa de sensibilización y capacitación.	**100**
Identificar las necesidades y prioridades de entrenamiento y sensibilización del personal independientemente del tipo de contratación.	15
Establecer el modelo del programa de sensibilización.	10
Establecer los niveles de complejidad y de financiamiento del plan.	15
Definir, adoptar y documentar los indicadores del programa.	10
Revisión y VoBo del programa de sensibilización y capacitación por parte de los grupos de interés.	15
Aprobación de la Metodología para identificar las necesidades de capacitación en seguridad de la información por parte del Comité Institucional de Seguridad y Privacidad de la Información.	15
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	20
8. Planificación y Control Operacional.	**215**
Estrategia de planificación y control operacional.	**120**
Mesas de trabajo con los grupos de interés.	30
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	20
Caracterización, estructuración y redacción de la estrategia de planificación y control operacional.	15
Revisión y VoBo de la estrategia de planificación y control operacional por parte de los grupos de interés.	15
Aprobación de la Estrategia de planificación y control operacional por parte del Comité Institucional de Seguridad y Privacidad de la Información.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	20
Declaración de aplicabilidad.	**95**
Mesas de trabajo con los grupos de interés.	20
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	10
Caracterización, estructuración y redacción de la declaración de aplicabilidad.	10
Revisión y VoBo de la estrategia de la declaración de aplicabilidad por parte de los grupos de interés.	15
Aprobación de la Declaración de aplicabilidad por parte del Comité Institucional de Seguridad y Privacidad de la Información.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	20
9. Identificación, actualización, valoración y tratamiento de los riesgos en la seguridad de la información de los procesos institucionales.	**240**
Revisión y análisis de la información y documentación relacionada con la gestión de	20

los procesos institucionales.	
Mesas de trabajo con los líderes de procesos y dependencias para la identificación, actualización, valoración y tratamiento de los riesgos en la seguridad de la información.	60
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	15
Revisión y VoBo de la consolidación de la información y documentación relacionada con la identificación, actualización, valoración y/o valoración de los riesgos en la seguridad de la información por parte de los grupos de interés.	20
Registro y/o actualización de la matriz riesgos de seguridad de la información.	15
Actualización de la caracterización de los procesos institucionales para incluir o modificar los riesgos de seguridad de la información.	60
Aprobación de la Identificación, actualización, valoración y tratamiento de los riesgos en la seguridad de la información de los procesos institucionales por parte del Comité Institucional de Seguridad y Privacidad de la Información.	20
Capacitaciones y Talleres de implementación con las Áreas o Dependencias del ITBOY.	30
10. Indicadores de gestión de seguridad y privacidad de la información.	**613**
Indicador Organización de Seguridad de la Información.	**14**
Mesas de trabajo con los grupos de interés.	5
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	3
Caracterización, estructuración y redacción del indicador.	3
Revisión y VoBo del indicador por parte de los grupos de interés.	3
Indicador Gestión de Activos de Información.	**19**
Mesas de trabajo con los grupos de interés.	9
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	4
Caracterización, estructuración y redacción del indicador.	3
Revisión y VoBo del indicador por parte de los grupos de interés.	3
Indicador de Tratamientos de Eventos Relacionados en Marco de Seguridad y Privacidad de la Información.	**36**
Mesas de trabajo con los grupos de interés.	13
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	8
Caracterización, estructuración y redacción del indicador.	10
Revisión y VoBo del indicador por parte de los grupos de interés.	5
Indicador Plan de Sensibilización.	**18**
Mesas de trabajo con los grupos de interés.	5
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	3
Caracterización, estructuración y redacción del indicador.	7
Revisión y VoBo del indicador por parte de los grupos de interés.	3
Indicador Cumplimiento de Políticas de Seguridad de la Información en la Entidad.	**40**
Mesas de trabajo con los grupos de interés.	15
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	11
Caracterización, estructuración y redacción del indicador.	9
Revisión y VoBo del indicador por parte de los grupos de interés.	5
Indicador de Identificación de Lineamientos de Seguridad de la Entidad.	**19**

Mesas de trabajo con los grupos de interés.	8
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	4
Caracterización, estructuración y redacción del indicador.	3
Revisión y VoBo del indicador por parte de los grupos de interés.	4
Indicador de Verificación del Control de Acceso.	**20**
Mesas de trabajo con los grupos de interés.	9
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	5
Caracterización, estructuración y redacción del indicador.	3
Revisión y VoBo del indicador por parte de los grupos de interés.	3
Indicador del Aseguramiento en la Adquisición y Mantenimiento de Software.	**44**
Mesas de trabajo con los grupos de interés.	12
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	13
Caracterización, estructuración y redacción del indicador.	12
Revisión y VoBo del indicador por parte de los grupos de interés.	7
Indicador de la Implementación de los Procesos de Registro y Auditoría.	**32**
Mesas de trabajo con los grupos de interés.	12
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	12
Caracterización, estructuración y redacción del indicador.	4
Revisión y VoBo del indicador por parte de los grupos de interés.	4
Indicador de Políticas de Privacidad y Confidencialidad.	**38**
Mesas de trabajo con los grupos de interés.	13
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	10
Caracterización, estructuración y redacción del indicador.	10
Revisión y VoBo del indicador por parte de los grupos de interés.	5
Indicador de Verificación de las Políticas de Integridad de la Información.	**52**
Mesas de trabajo con los grupos de interés.	20
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	10
Caracterización, estructuración y redacción del indicador.	15
Revisión y VoBo del indicador por parte de los grupos de interés.	7
Indicador de las Políticas de Disponibilidad del Servicio y la Información.	**70**
Mesas de trabajo con los grupos de interés.	25
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	15
Caracterización, estructuración y redacción del indicador.	18
Revisión y VoBo del indicador por parte de los grupos de interés.	12
Indicador Ataques Informáticos a la Entidad.	**59**
Mesas de trabajo con los grupos de interés.	16
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	14
Caracterización, estructuración y redacción del indicador.	21
Revisión y VoBo del indicador por parte de los grupos de interés.	8
Indicador Porcentaje de Disponibilidad de los Servicio que Presta la Entidad.	**76**
Mesas de trabajo con los grupos de interés.	22
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	16
Caracterización, estructuración y redacción del indicador.	22
Revisión y VoBo del indicador por parte de los grupos de interés.	16
Indicador Porcentaje de Implementación de Controles.	**76**

Mesas de trabajo con los grupos de interés.	22
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	16
Caracterización, estructuración y redacción del indicador.	22
Revisión y VoBo del indicador por parte de los grupos de interés.	16
11. Actualización del Inventario de Activos de Información.	**190**
Revisión y análisis de los activos de información definidos y actualizados en la vigencia anterior.	30
Mesas de trabajo con los líderes de procesos y dependencias para definir, actualizar y depurar el inventario de información disponible.	60
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	20
Revisión y VoBo de la consolidación del Inventario de Activos de Información por parte de los grupos de interés.	20
Actualizar los activos de información por parte de los Dueños.	30
Publicación del inventario de activos de información clasificado como "Confidencial".	10
Actualización de la información y documentación relacionada con la gestión de documentos y archivos digitales.	20
12. Actualización de la información y documentación relacionada con la gestión de documentos y archivos digitales.	**146**
Mesas de trabajo con los líderes de procesos y dependencias para definir, actualizar y depurar la información y documentación relacionada con la gestión de documentos digitales.	34
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	29
Revisión y VoBo de la consolidación de la información y documentación relacionada con la gestión de documentos digitales por parte de los grupos de interés.	29
Aprobación de la documentación relacionada con la gestión de documentos digitales por parte del Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.	39
Publicación y promoción actualización de la información y documentación relacionada con la gestión de documentos digitales.	15
13. Plan de revisión y seguimiento a la implementación del MSPI.	**145**
Metodología para revisión y seguimiento a la implementación del MSPI.	**145**
Elaboración del documento borrador con Metodología para revisión y seguimiento a la implementación del MSPI	20
Mesas de trabajo con los grupos de interés.	30
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	15
Caracterización, estructuración y redacción de la metodología para la revisión y seguimiento a la implementación del MSPI.	20
Revisión y VoBo de la metodología por parte de los grupos de interés.	20
Aprobación de la metodología por parte del Comité Institucional de Seguridad y Privacidad de la Información del ITBOY.	20
Publicación y promoción de la metodología.	20
14. Plan de Mejora Continua.	**65**
Metodología para desarrollar el plan de mejora continua.	**65**
Elaboración del documento borrador con la Metodología para desarrollar el plan de	15

mejora continua.	
Mesas de trabajo con los grupos de interés.	20
Revisión, análisis y consolidación del trabajo realizado en las mesas de trabajo.	15
Caracterización, estructuración y redacción de la metodología para desarrollar el plan de mejora continua.	15

Fuente: Plan de Implementación del Modelo de Seguridad y Privacidad de la Información – MSPI

Según lo anterior, para la vigencia 2025 se atenderán catorce (14) Macroprocesos, con un tiempo estimado de 4.835 días, así:

Tabla 8. Tiempo Estimado (Días) Macroprocesos

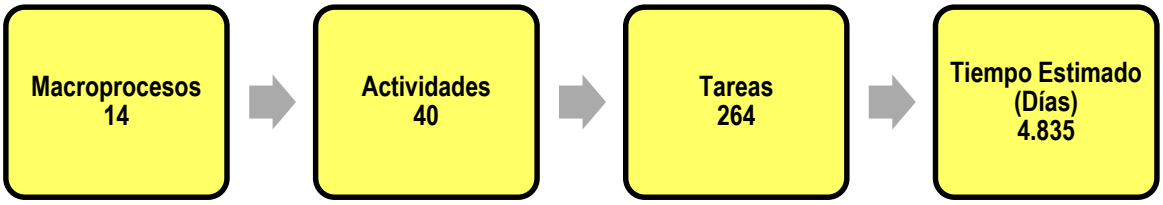
MACROPROCESO / ACTIVIDAD	TIEMPO ESTIMADO (DÍAS)
1. Política de Seguridad y Privacidad de la Información.	**1.471**
2. Actualización de las Políticas y estándares de Tecnologías de la Información – TI.	**191**
3. Implementación de una Metodología y criterios de evaluación de alternativas de solución e inversión en TI.	**336**
4. Implementar controles de seguridad informática.	**90**
5. Procedimientos de Seguridad y Privacidad de la Información.	**806**
6. Implementar controles para disponer de un nivel de exposición al riesgo que permita responder por la integridad, confidencialidad y la disponibilidad de la información.	**112**
7. Plan de capacitación, sensibilización y comunicación de la seguridad de la información.	**215**
8. Planificación y Control Operacional.	**215**
9. Identificación, actualización, valoración y tratamiento de los riesgos en la seguridad de la información de los procesos institucionales.	**240**
10. Indicadores de gestión de seguridad y privacidad de la información.	**613**
11. Actualización del Inventario de Activos de Información.	**190**
12. Actualización de la información y documentación relacionada con la gestión de documentos y archivos digitales.	**146**
13. Plan de revisión y seguimiento a la implementación del MSPI.	**145**

14. Plan de Mejora Continua.	**65**
TOTAL TIEMPO ESTIMADO	**4.835**

Fuente: Plan de Implementación del Modelo de Seguridad y Privacidad de la Información – MSPI

Respecto al detalle de las actividades y tareas tenemos:

Figura 7. Actividades y Tareas.



Elaborado por:
Richard Hernan Ayala Joya
Profesional Especializado
INSTITUTO DE TRANSITO DE BOYACA
2025

Revisado por:
William Rene Higuera Morales
Jefe Oficina Asesora Planeación y Sistemas
INSTITUTO DE TRANSITO DE BOYACA
2025

Fuente: Plan de Implementación del Modelo de Seguridad y Privacidad de la Información – MSPI

En Tunja a los quince (15) días del mes de enero de 2025.

NIDIA CAROLINA PUENTES AGUILAR
Gerente Instituto de Transito de Boyacá