INTRODUCCIÓN

La seguridad y privacidad de la información como habilitador transversal de la Política de Gobierno Digital se desarrolla a través del Modelo de Seguridad y Privacidad de la Información -MSPI, orientando la gestión e implementación del Sistema de Gestión de Seguridad de la Información SGSI, con el fin de incorporar la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información del Cuerpo Oficial de Bomberos de Dosquebradas, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

En atención a lo anterior, la entidad asumió el reto de implementar el Modelo de Seguridad y Privacidad de la Información, siguiendo los lineamientos de la Política de Gobierno Digital, reglamentada a través del Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, que en el artículo 2.2.9.1.1.3. Principios, define la seguridad de la información como principio de la Política de Gobierno Digital, y de igual manera en el artículo 2.2.9.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, los cuales permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Teniendo en cuenta lo anterior, se formula el presente Plan, en cumplimiento de la normativa aplicable vigente para el año 2026.

1. OBJETIVO

Garantizar la confidencialidad, integridad y disponibilidad de la información, mediante la formulación e implementación de actividades y controles de seguridad alineadas con las Política de Gobierno Digital y la Política de Seguridad Digital, de acuerdo con el alcance definido por el Cuerpo Oficial de Bomberos de Dosquebradas.

2. ALCANCE

El presente Plan comprende la descripción y programación de las actividades a realizar por el Cuerpo Oficial de Bomberos de Dosquebradas, durante la vigencia 2026, como parte de la implementación del Sistema de Gestión de la Seguridad de la Información

(SGSI), de acuerdo con el Modelo de Seguridad y Privacidad de la Información - MSPI emitido por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, y la Norma ISO/IEC 27001:2022. La cual se aplica al Cuerpo Oficial de Bomberos de Dosquebradas.

3. MARCO NORMATIVO

TIPO DE NORMA	NÚMERO	AÑO	DESCRIPCIÓN - EPÍGRAFE
Ley	1712	2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto	1083	2015	Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Decreto	1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto	1008	2018	Por medio del cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto	2106	2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
Decreto	164	2021	Por el cual se modifica la estructura de la Escuela Superior de Administración
Resolución MINTIC	1519	2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
CONPES	3701	2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES	3854	2016	Política Nacional de Seguridad Digital
CONPES	3975	2019	Política Nacional para la Transformación Digital e Inteligencia Artificial.
CONPES	4086	2022	Política de Ciberseguridad y Ciberdefensa para el fortalecimiento de la seguridad nacional.
NTC / ISO	27001	2022	Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.
NTC / ISO	27002	2022	Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.
NTC / ISO	27005	2022	Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información.
Circular	005	2023	Circular externa MinTIC sobre implementación de la Política de Gobierno Digital.

4. RESPONSABLES

El monitoreo y revisión de la gestión de los riesgos está alineado con el esquema de asignación de responsabilidades y roles, el cual se distribuye en cuatro (4) líneas de defensa, las cuales se despliegan en la Política de Administración de Riesgos vigente de la Entidad.

De igual forma, se detallan las responsabilidades del rol del Oficial de Seguridad y Privacidad de la Información, en lo concerniente a la formulación, implementación y seguimiento del Plan de Seguridad y Privacidad de la Información y su Estrategia de Seguridad Digital.

5. DEFINICIONES

- **Activo:** En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- **Contratistas:** Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Guía:** documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Norma:** Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
- **Parte interesada (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Política del SGSI:** Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.
- **Política:** Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.
- **Privacidad de datos:** La privacidad de datos, también llamada protección de datos es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros
- **Procedimiento:** Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Rol:** Papel, función que alguien o algo desempeña.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

6. DESARROLLO DEL PLAN

De acuerdo con lo estipulado en el numeral 2.1.3 del Manual de Gobierno Digital del MINTIC, el Plan de Seguridad y Privacidad de la Información debe establecer los detalles de cómo se realizará la implementación de la seguridad de la información en cada uno de los procesos de la entidad, estipulando directrices, tiempo y responsables para lograr un adecuado proceso de gestión, administración, evaluación y resultados del plan desarrollado.

6.1 OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

Su operativización busca establecer, implementar, monitorear, revisar, mantener y mejorar el sistema en el Cuerpo Oficial de Bomberos de Dosquebradas, reportando su estado de avance, de manera que fomente la consulta y cooperación con organismos especializados para la obtención de asesoría en dicha materia para garantizar la aplicación de medidas de seguridad adecuadas, en los accesos a la información de la Entidad.

6.2 POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

El Cuerpo Oficial de Bomberos de Dosquebradas, en el marco de sus funciones, se compromete a proteger y asegurar la información tanto física como digital, a través de acciones, estrategias y recursos necesarios, con el fin de cumplir con los requisitos

legales y de la entidad, en pro del fortalecimiento y mejora del sistema de gestión de seguridad de la información y sus objetivos, de acuerdo con lo establecido en el Manual Sistema Integrado de Gestión.

Esta política puede ser consultada a detalle en el M-TI-01-Manual Políticas Seguridad Información, y se complementa con las Políticas de Seguridad y Privacidad de la Información, documentadas en el Manual de Políticas TI DC-A-GT-32.

6.3 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- Implementar y fortalecer los controles para la protección de los activos de información.
- Prevenir la materialización de los riesgos de seguridad de la información identificados.
- Controlar y minimizar los incidentes de Seguridad de Información.
- Cumplir los requisitos normativos, legales y de seguridad de la información, a través de políticas, lineamientos, guías y directrices del Sistema de Gestión de Seguridad de la Información SGSI.
- Generar una cultura en seguridad de la información.
- Evaluar y mejorar el Sistema de Gestión de Seguridad de la Información, con el fin de lograr la eficiencia y su mejora continua.
- Fortalecer las competencias del personal en materia de seguridad y privacidad de la información.
- Garantizar la protección de datos personales conforme a la normatividad vigente.

6.4 DIAGNÓSTICO DEL SISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SGSI

Con el fin de dar cumplimiento al cierre de la vigencia 2025, en el mes de diciembre de 2025 se realizó la medición del instrumento de identificación de la línea base de seguridad del MINTIC, el cual es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, donde se evidencia avances en el tema.

Teniendo en cuenta los anteriores resultados, para la vigencia 2026 se debe definir el Plan de Seguridad y privacidad de la información por parte del Oficial de Seguridad de la información y llevar a cabo su implementación, considerando las siguientes fases del ciclo de mejora continua: Identificar, Proteger, Detectar, Responder y Recuperar.

6.5 IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

(Estrategia de planificación y control operacional)

Dentro del proceso de implementación del Modelo de Seguridad y privacidad de la información de MINTIC, se ha utilizado el instrumento de Identificación de la Línea Base de Seguridad, en la cual se definen y priorizan las acciones a seguir y se realiza el seguimiento al avance en dicha implementación.

Actualmente se han implementado y operado diferentes procedimientos, guías, manuales y formatos, Gestión Documental, vigencias anteriores como en el 2020 y con continuidad. Con el fin de dar cumplimiento a los controles establecidos en la Norma ISO 27001:2022 Anexo A con sus 114 Controles de Seguridad de la Información, y los establecidos por la política de Gobiernos Digital y el FURAG dentro de los cuales se encuentran:

El levantamiento de los instrumentos de gestión de la información pública, para dar cumplimiento a la Ley 1712 de 2014- Ley de transparencia de acceso a la información pública. Estos instrumentos fueron aprobados por el Comité Institucional de Gestión y desempeño.

Una vez los propietarios de los activos de Información realicen el reporte de cumplimiento de sus planes de tratamiento y controles, el Oficial de Seguridad y Privacidad de la Información, realizarán la revisión y validación de esta información, con el fin de reportar la medición de la gestión del riesgo, a través de la implementación de los controles definidos en el Mapa de Riesgos Institucional para los riesgos de Seguridad y Privacidad de la Información.

6.6 CRONOGRAMA DE ACTIVIDADES

A continuación, se presenta el cronograma de actividades planificadas para la vigencia 2026:

DOMINIO ISO 27001	ACTIVIDAD	RESPONSABLE	FECHA INICIO	FECHA FIN	ESTADO
Políticas de la seguridad de la información	Actualización y socialización del Plan de Seguridad y Privacidad de la Información y del Manual del Sistema Integrado de Gestión, en lo concerniente a la	Oficial de Seguridad de la Información	Enero 2026	Febrero 2026	Programado

	seguridad privacidad de la información.				
Organización de la seguridad de la información	Realizar una capacitación a todo el personal de la entidad, a través del canal institucional de videos y capacitaciones y para cada uno de los procesos, las aplicaciones y la aprobación por parte de los dueños de la información.	Oficial de Seguridad de la Información	Marzo 2026	Abril 2026	Programado
Organización de la seguridad de la información	Realizar, actualizar y/o mantener contratado con autoridades, grupos de (Actividades 2.4, y 5) seguridad nacional e internacional con expertos en Seguridad y contacto con los especialistas de la Información y Oficina de Tecnologías de la Información y las Comunicaciones (Actividades 3, y 4)	Oficial de Seguridad de la Información	Enero 2026	Diciembre 2026	Programado
Seguridad de los recursos humanos	Dar continuidad al plan de sensibilización en seguridad de la información dentro del proceso de inducción institucional. Actualizar los temas de políticas, procedimientos, cultura de seguridad para toda la comunidad	Oficial de Seguridad de la Información	Enero 2026	Diciembre 2026	Programado
Control de acceso	Alinear el proceso de gestión de accesos y	Oficial de Seguridad de la Información	Marzo 2026	Mayo 2026	Programado

	permisos para eliminar los errores que pueden surgir por el aprovisionamiento para eliminar los errores				
Control de acceso	Validar el control y la recepción de responsabilidades sobre las políticas de control y cada sistema de información para realizar la segregación de los derechos de acceso a los controles de vídeo y perfiles de cada sistema de información para tener el control y la segregación de los derechos de acceso a los derechos	Oficial de Seguridad de la Información	Marzo 2026	Junio 2026	Programado
Seguridad física y del entorno	Monitorear los controles físicos en aquellas áreas con información sensible o crítica, e instalaciones de manejo de información	Oficial de Seguridad de la Información (Actividad v. 2)	Enero 2026	Diciembre 2026	Programado
Seguridad física y del entorno	Información del cumplimiento de normas de seguridad física, adecuación y mantenimiento del Centro de Datos y Cableado.	Oficina de Tecnologías de la Información y las Comunicaciones (Actividades 3, y 4)	Marzo 2026	Junio 2026	Programado
Seguridad física y del entorno	Fortalecer el mantenimiento de planta eléctrica y UPS.	Oficina de Tecnologías de la Información y las Comunicaciones (Actividades 3, y 4)	Enero 2026	Diciembre 2026	Programado
Seguridad de las operaciones	Monitorear la implementación en la herramienta Service Manager, procedimientos de gestión de cambios, la	Oficina de Tecnologías de la Información y las Comunicaciones (Actividades 3, y 4)	Enero 2026	Diciembre 2026	Programado

	capacidad, disponibilidad de la infraestructura e incidentes.				
Seguridad de las operaciones	Aplicación de los procedimientos de monitoreo de disponibilidad	Oficina de Tecnologías de la Información y las Comunicaciones (Actividades 3, y 4)	Enero 2026	Diciembre 2026	Programado
Seguridad de las comunicaciones	Realizar el monitoreo y remediación de las vulnerabilidades, sistema para la gestión de Backups, respaldo y recuperación de Antivirus, NGSL, Barracuda, Firewall y demás elementos que aseguridad de información Administración	Oficial de Seguridad de la Información	Enero 2026	Diciembre 2026	Programado
Seguridad de las comunicaciones	Monitorear las herramientas de código malicioso.	Oficial de Seguridad de la Información	Enero 2026	Diciembre 2026	Programado
Seguridad de las comunicaciones	Documentar las guías de retiro y recuperación del sistema para revisión del Plan de recuperación de Desastres	Oficial de Seguridad de la Información	Marzo 2026	Junio 2026	Programado
Seguridad de las comunicaciones	Ejecutar el procedimiento de monitoreo para conservar y revisar, mantener el sistema de activación del Plan de recuperación de Desastres y fallas, fallos y eventos de seguridad de la información.	Oficial de Seguridad de la Información	Enero 2026	Diciembre 2026	Programado
Adquisición, desarrollo y mantenimiento de sistemas	Implementar y monitorear la separación de los redes para los(Oficina de Tecnologías de diferentes	Oficial de Seguridad de la Información	Marzo 2026	Junio 2026	Programado

	ambientes, usuarios y sistemas de información vistas de la Información y las Comunicaciones y sistemas de información vistas de las Información y los Comunicaciones				
Adquisición, desarrollo y mantenimiento de sistemas	Monitorear el cumplimiento de las normas para la transferencia de información.	Oficina de Tecnologías de la Información y las Comunicaciones	Enero 2026	Diciembre 2026	Programado
Adquisición, desarrollo y mantenimiento de sistemas	Monitorear la continuidad de protección de los códigos fuente de los	Oficina de Tecnologías de la Información y las Comunicaciones	Enero 2026	Diciembre 2026	Programado
Adquisición, desarrollo y mantenimiento de sistemas	procedimientos externos el según desarrollo de seguridad Oficial y de políticas de	Oficina de Tecnologías de la Información y las Comunicaciones	Enero 2026	Diciembre 2026	Programado
Adquisición, desarrollo y mantenimiento de sistemas	cumplimiento de las políticas y principios de desarrollo seguro Oficial de la Información	Oficial de Seguridad de la Información	Enero 2026	Diciembre 2026	Programado
Adquisición, desarrollo y mantenimiento de sistemas	Monitorear la implementación de la protección de datos de prueba, de ordenamiento o data scrambling.	Oficial de Seguridad de la Información	Enero 2026	Diciembre 2026	Programado
Relaciones con los proveedores	Socializar e implementar los aspectos de seguridad de la información para proveedores y terceras partes.	Oficial de Seguridad de la Información	Febrero 2026	Abril 2026	Programado
Relaciones con los proveedores	Mantener el cumplimiento de los niveles de servicios de seguridad de la Información para proveedores existentes.	Oficial de Seguridad de la Información	Enero 2026	Diciembre 2026	Programado

Aspectos de seguridad de la información de la gestión de la continuidad del negocio	Revisar la seguridad digital para la estrategia de contingencia	Oficial de Seguridad de la Información	Enero 2026	Marzo 2026	Programado
Aspectos de seguridad de la información de la gestión de la continuidad del negocio	Ejecutar pruebas del escenario de simulación y respuesta a ataques (Oficina de Tecnologías de la Información y las Comunicaciones cibernéticos.	Oficina de Tecnologías de la Información y las Comunicaciones	Abril 2026	Junio 2026	Programado
Aspectos de seguridad de la información de la gestión de la continuidad del negocio	Implementar la Guía para la identificación de infraestructura crítica cibernética	Oficial de Seguridad de la Información	Enero 2026	Marzo 2026	Programado
Cumplimiento	Realizar el monitoreo al cumplimiento de los procedimientos de la administración de los softwares.	Oficial de Seguridad de la Información	Enero 2026	Diciembre 2026	Programado
Cumplimiento	Monitorear la actualización de los lineamientos para la protección de datos personales.	Oficial de Seguridad de la Información	Enero 2026	Diciembre 2026	Programado
Cumplimiento	Monitorear el cumplimiento de las guías definidas para criptografía, máximo 2 y mínimo una vez	Oficina de Tecnologías de la Información y las Comunicaciones	Enero 2026	Diciembre 2026	Programado
Cumplimiento	Ejecutar los análisis de vulnerabilidades máximo 2 y mínimo una vez al año.	Oficina de Tecnologías de la Información y las Comunicaciones	Marzo 2026	Noviembre 2026	Programado
A.19 Privacidad y Protección de Datos Personales	Realizar la recopilación de bases de datos personales de acuerdo al decreto con los estándares emitidos por la SIC-LA	Oficial de Seguridad de la Información	Enero 2026	Marzo 2026	Programado

	Superintendencia de la Información				
A.19 Privacidad y Protección de Datos Personales	Registrar y actualizar de manera permanente las bases de datos.	Oficial de Seguridad de la Información	Enero 2026	Diciembre 2026	Programado

7. RECURSOS

La estimación y asignación de los recursos para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se llevará a cabo con recursos del proyecto de inversión, Mantener el Sistema de Gestión de la Seguridad de la Información, que tiene por objetivo fortalecer la Seguridad y Privacidad de la Información, en sus tres pilares fundamentales que son, confidencialidad, integridad y disponibilidad, de acuerdo con las políticas y lineamientos.

Toda vez que la vigencia de este plan es para el año 2026, este proyecto de inversión será actualizado en la siguiente anualidad.

8. SEGUIMIENTO Y MEDICIÓN DEL PLAN

Se prevé realizar monitoreo y seguimiento al cumplimiento de las actividades del plan definidas en el cronograma.

Toda vez que el presente Plan está integrado al Plan de Acción Institucional de la vigencia, el seguimiento se realizará cuatrimestralmente y se reportará el resultado de cada período, en el instrumento de seguimiento al Plan de Acción, en el compromiso asociado al Plan de Seguridad y Privacidad de la Información.

En atención a lo dispuesto en el Procedimiento para la Gestión de Planes Institucionales PT-S-PE-06, al final de la vigencia se reportará el Informe Anual de Implementación de Planes Institucionales establecido para tal fin.

8.1 INDICADORES

La medición se realiza con el indicador "Cumplimiento en la implementación del SGSI", que está orientado principalmente a aumentar el nivel de madurez de la implementación y operación del SGSI.

Para este fin, se utilizará el Instrumento de identificación de la línea base de seguridad, proporcionado por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Porcentaje de cumplimiento del SGSI / Meta de cumplimiento programadas del SGSI

Adicionalmente, el Oficial de Seguridad de la Información y la Dirección de Entornos y Servicios Virtuales, los cuales son los responsables del PSPI, realizarán análisis y medirán el cumplimiento del presente Plan, a través del resultado del siguiente indicador, para el cual la meta es 100%.

Número de actividades ejecutadas/N° de Actividades Programada

CONTROL DE CAMBIOS Y ACTUALIZACIÓN DOCUMENTAL

FECHA	VERSIÓN	DESCRIPCIÓN	RESPONSABLE
30/01/2026	3	Se modifica de forma general el documento para la vigencia 2026	JOHSON BETANCUR

ELABORADO POR:	REVISADO POR:	APROBADO POR:
JOHSON BETANCUR	ERICA CARDENAS - SANDRA GIRALDO	JOSE JOAQUIN OCAMPO P.
TICS	Calidad - MIPG	Director general