Plan de

Seguridad y Privacidad de la Información

2026

IDEAM

INTRODUCCION

La misión del IDEAM es generar conocimiento y producir información confiable, consistente y oportuna sobre el estado y las dinámicas de los recursos naturales y del medio ambiente. Por ello, la información constituye uno de los activos más importantes del Instituto, ya que sustenta la toma de decisiones, la operación de los procesos y el cumplimiento de los objetivos institucionales.

El Plan de Seguridad y Privacidad de la Inforgmación define el marco estratégico y operativo para proteger la información respecto a confidencialidad, integridad y disponibilidad, que permita mitigar los riesgos, reduciendo la probabilidad de su afectación o impacto sobre la operación, la reputación, los aspectos económicos, legales o normativos.

Alineado al Modelo de Seguridad y Privacidad de la Información establece en la Guía 04. Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional establece siete tipos de activos información, hardware, software, servicios, recursos humanos, instalaciones e infraestructura crítica cibernética.

Este plan es de cumplimiento obligatorio para todos los funcionarios y contratistas del Instituto, y constituye una guía para la adopción de buenas prácticas, procedimientos y mecanismos que fortalezcan la cultura de seguridad en todos los niveles organizacionales.

Este plan va encaminado al desarrollo del cumplimiento de las Políticas de Seguridad de la Información internas, marco regulatorio aplicable externo y las buenas prácticas que permiten incrementar el nivel de madurez del sistema de gestión en el Instituto de Hidrología, Meteorología y Estudios Ambientales.

1. METODOLOGÍA PARA LA ELABORACIÓN DEL PLAN

Como base de la metodología de aplicación para este plan es el Modelo de Seguridad y Privacidad de la Información de MinTIC, el cual contiene los lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales como ISO 27001 y NIST.

Los instrumentos de referencia son 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, toda vez que el modelo pertenece al habilitador transversal de Seguridad y Privacidad. Así mismo, se tiene en cuenta el marco regulatorio vigente aplicable para seguridad y privacidad de la información.

Dentro de las fases técnicas se encuentran como insumo la siguiente información utilizada para la formulación del plan:

- Para el análisis estratégico se realizó un GAP análisis basado en los requerimientos del modelo de seguridad y privacidad de la información MSPI versión vigente.
- Se identificaron las necesidades de las dependencias a través de mesas de trabajo para la gestión de activos de información y gestión de riesgos de seguridad de la información.
- Se realiza una articulación con el MIPG, PETI y demás marcos de referencia de MinTIC

- El plan de seguridad de la información se articula con el plan de acción en la actividad "Realizar el cierre de brechas de la política gobierno digital y seguridad digital".

2. OBJETIVO

Fortalecer la seguridad y privacidad de la información del IDEAM mediante la implementación del SGSI y el Modelo de Seguridad y Privacidad, alineados al contexto organizacional y recursos disponibles, para garantizar la integridad, confidencialidad y disponibilidad de los activos, mitigar riesgos y generar confianza en ciudadanos, usuarios y partes interesadas.

3. ALCANCE

El Plan de Seguridad de la Información del IDEAM, para la vigencia 2026, comprende la adopción del Modelo de Seguridad y Privacidad y la implementación del SGSI, alineados con los lineamientos del Ministerio TIC y la Política General de Seguridad de la Información. Su alcance incluye todos los procesos de la entidad y aplica a funcionarios, contratistas, pasantes y terceros que utilicen recursos del IDEAM. Las políticas y controles definidos deberán revisarse y actualizarse periódicamente para garantizar su adecuación, suficiencia y eficacia, fortaleciendo la protección de la plataforma tecnológica y la información institucional, y generando confianza en ciudadanos, usuarios y partes interesadas.

4. DEFINICIONES

- **Activo de Información:** La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades del instituto y, en consecuencia, necesita una protección adecuada.
- **Administrador de Dominio:** Persona encargada de administrar un conjunto de ordenadores (servidores + estaciones de trabajo) que comparten características comunes en cuanto a accesos.
- **Administrador de TI:** Profesionales encargados de operar y administrar la infraestructura tecnológica, comunicaciones, seguridad, aplicaciones y bases de datos del instituto.
- **Amenaza:** Causa potencial de un incidente no deseado, que pueda ocasionar daño a un sistema u organización.
- **Análisis de Impacto al Negocio:** Donde se determinan los recursos críticos y el tiempo de recuperación con las respectivas ventanas de criticidad mediante las cuales se debe restaurar los activos evaluados.
- **Análisis del Riesgo:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- **Aplicación:** Es un tipo de programa Informático diseñado para facilitar al usuario la realización de un determinado tipo de trabajo.
- **Ataque:** intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo.
- **Cifrar:** quiere decir transformar un mensaje en un documento no legible.
- **Confidencialidad:** Aseguramiento de que la información es accesible sólo para quienes están autorizados.

- **Contratista:** Persona jurídica o natural externa al Instituto encargada de adelantar actividades por encargo del instituto.
- **Cuenta de acceso:** Identificación y contraseña a través de la cual un usuario accede a un servicio o aplicación. Las cuentas de acceso son autorizadas por los Jefes de las diferentes dependencias y suministradas por los Administradores de los servicios o aplicaciones y está sujeta a la disponibilidad de licencias adquiridas por el Instituto.
- **Custodio:** Encargado de guardar el activo con cuidado y vigilancia. Es una parte designada del instituto, un cargo, proceso, o grupo de trabajo encargado de administrar los componentes tecnológicos donde se encuentra la información; además se encarga de hacer efectivos los controles de seguridad administrativos que el propietario de la información haya definido, tales como el manejo de archivos, el uso de copias y la eliminación.
- **Disponibilidad:** Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando lo requieran.
- **Incidente de Seguridad de la Información:** Un evento o serie de eventos de seguridad de la información no deseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad:** Salvaguarda de la exactitud y completitud de la información y sus métodos de procesamiento.

- **Política:** Son instrucciones mandatarias que indican la intención de la alta gerencia respecto a la operación de la organización.
- **Propietario:** El término "Dueño" o "Propietario" identifica a un individuo o a un instituto que tiene responsabilidad aprobada por la Dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término "Propietario" no implica que la persona tenga realmente los derechos de propiedad de los activos.
- **Recurso Informático:** Cualquier componente físico (Hardware) o lógico (Software) empleado para almacenar, manipular, procesar o transmitir información del Ideam.
- **Requerimiento:** es una necesidad documentada sobre el contenido, forma o funcionalidad de un producto o servicio. Se usa en un sentido formal en la ingeniería de sistemas o la ingeniería de software.
- **Riesgo:** Combinación de la probabilidad de un evento y sus consecuencias.
- **Rol:** Grupo de usuarios que cumplen un papel determinado, a los cuales se les asigna o niega permisos dentro de un aplicativo.
- **Servidor:** un computador que ofrece servicios a máquinas de cliente distantes o a aplicaciones, como el suministro de contenidos de páginas u otros recursos.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas [ISO/IEC 27001:2005].

- **Servicio o Aplicación:** Programa o conjunto de programas diseñados para la realización de una(s) tarea(s) concretas. Los servicios están destinados principalmente para apoyar los diferentes procesos del Instituto. Por ejemplo, correo electrónico, Internet, SISAIRE, SNIF, SIRH, etc.

5. SIGLAS

MSPI: Modelo de seguridad y privacidad de la información

PETI: Plan estratégico de tecnología de la Información

MIPG: Modelo Integrado de Planeación y Gestión

PEI: Plan Estratégico Institucional

SGSI: Sistema de gestión de seguridad de la información

IAM: Identity and Access Management (Gestión de Identidad y Acceso)

DRP: Disaster Recovery Plan (Plan de Recuperación ante Desastres)

BIA: Business Impact Analysis (Análisis de Impacto Empresarial o al Negocio)

BCP: Business Continuity Plan (Plan de Continuidad de Negocio)

BYOD: Bring Your Own Device (Trae tu Propio Dispositivo) hace referencia al uso de dispositivos propios de funcionarios y contratistas del IDEAM.

6. MARCO NORMATIVO

La normatividad aplicable para el Presente plan aplica:

- Modelo de seguridad y privacidad de la información MSPI de MinTIC.
- 05. Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas MinTIC

- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas DAFP
- Ley de transparencia 1712 de 2014
- Ley de protección de datos personales 1581 de 2012
- Ley de delitos informáticos 1273 de 2009
- Decreto 612 de 2018 *Directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado*, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI).
- Resolución 500 de 2021 L*ineamientos y estándares para la estrategia de seguridad digital y adopción del modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*.
- Manual de Gobierno Digital – MINTIC.

7. DESCRIPCIÓN DEL PLAN

El Plan de Seguridad y Privacidad de la Información se desarrolla de manera integral, incorporando sus componentes fundamentales; políticas, procedimientos, controles y mecanismos de respuesta dentro de una estructura coherente que abarca la gestión de riesgos, la protección de activos, la continuidad del negocio y la concientización del personal. Establece lineamientos operativos claros para la identificación, prevención, detección y mitigación de incidentes, así como para la asignación de responsabilidades, la administración de accesos, el uso adecuado de recursos tecnológicos y el cumplimiento normativo. Este enfoque permite garantizar la confidencialidad, integridad y disponibilidad

de la información, asegurando un funcionamiento seguro y eficiente de todos los procesos organizacionales.

7.1. ALINEACIÓN ESTRATÉGICA

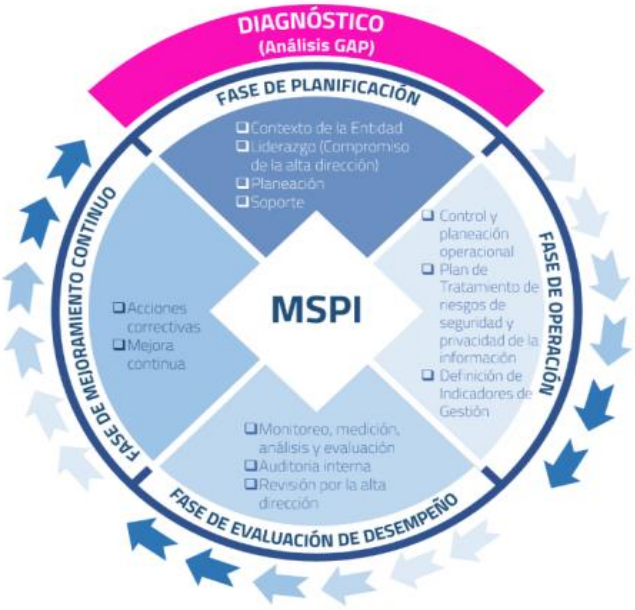
Plan Estratégico Institucional		Modelo Integrado de Planeación y Gestión		Sistema de Gestión Integrado
Línea 1. Gobernanza y Gestión de los datos para proporcionar información ambiental		**1.**Talento Humano		Mapa de Procesos del Ideam | Instituto de Hidrología, Meteorología y Estudios Ambientales Proceso: Gestion del SGI - Sistema de Gestión de Seguridad de la Información
Línea 2. Seguimiento de las condiciones climáticas, hidrometeorológicas y ambientales, promoviendo el monitoreo comunitario y la vigilancia del patrimonio de nuestro país		**2.**Direccionamiento Estratégico y Planeación		
Línea 3. Gestión del conocimiento y análisis de la información ambiental para el desarrollo sostenible del territorio, la gestión del riesgo y el estado del patrimonio		**3.** Gestión con Valores para Resultados	x	
Línea 4. Democratización del acceso y uso de la información ambiental		**4.** Evaluación de Resultados		
Línea 5. Fortalecer y modernizar la capacidad de gestión de la entidad para la generación de valor público y mejora del desempeño institucional	x	**5.** Información y Comunicación		
Línea 6. Comunicación estratégica para proveer y divulgar información científica y ambiental transparente, comprensible y adecuada		**6.** Gestión del Conocimiento		
		7. Control Interno		

El Plan de Seguridad y Privacidad de la Información se encuentra plenamente alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI), garantizando coherencia estratégica y operativa en la gestión y protección de los activos institucionales.

7.2. FASES DEL MSPI

Las siguientes son las diferentes fases que se desarrollan en el proceso de implementación del MSPI.

Ilustración 1 Modelo de seguridad y privacidad de la información



Fuente: Modelo de Seguridad y Privacidad, MINTIC,

Relación entre la ciberseguridad y otros ámbitos de la seguridad (Fuente: ISO/IEC 27032)

Fuente: Documento Modelo de Seguridad y Privacidad de la Información V.4 MINTIC

- **Fase Diagnostico:** Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información
- **Fase Planificación (Planear):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- **Fase Implementación (Hacer):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- **Fase Evaluación de desempeño (Verificar):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

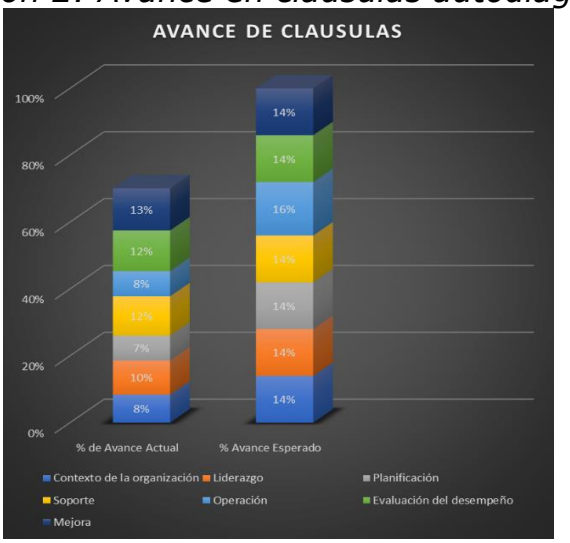
- **Fase Mejora Continua (Actuar):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

8. ESTADO ACTUAL DEL SISTEMA DE GESTION DE SEGURIAD DE LA INFORMACION - MSPI

El Sistema de Gestión de Seguridad de la Información del IDEAM se encuentra en un nivel de madurez Gestionado, con un promedio del 77,25% según la evaluación ISO/IEC 27001:2022, destacando los controles físicos con nivel Optimizado (84%) y avances importantes en los dominios organizacional, personas y tecnológico. El ciclo PHVA presenta un progreso global del 70%, con mayor desarrollo en evaluación y mejora continua, mientras que el marco NIST refleja fortalezas en detección y respuesta (90%) y recuperación (85%), aunque gobernanza y protección requieren fortalecimiento. Entre los logros más relevantes se encuentran la consolidación de controles físicos robustos, la implementación de procedimientos formales para la gestión de incidentes, el cumplimiento normativo mediante auditorías y normograma actualizado, la gestión integral de activos de información y la protección perimetral con herramientas avanzadas. No obstante, persisten brechas en la formalización del alcance del SGSI, actualización del MSPI, gestión de riesgos institucionales, seguridad en la nube, etiquetado, anonimización de datos, protección de información personal, continuidad del negocio, políticas para teletrabajo y activos fuera de las instalaciones.

El diagnóstico de seguridad de la información arrojó los siguientes resultados: El modelo de seguridad y privacidad de la información se encuentra en un 70% de implementación de las cláusulas las cuales están alineadas a la ISO 27001.

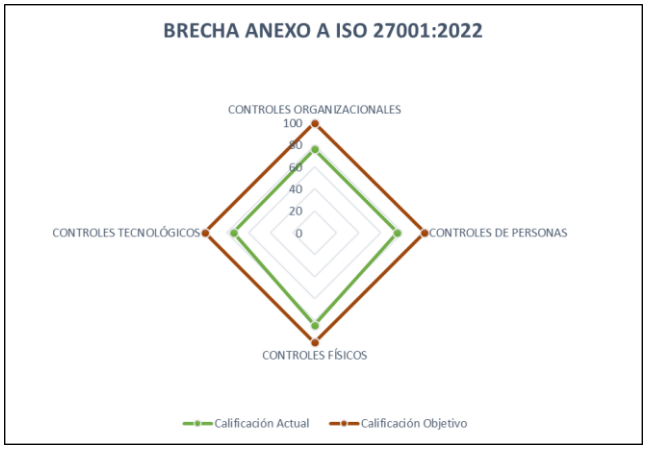
Ilustración 2: Avance en cláusulas autodiagnóstico



Fuente: Elaboración Propia

Un 77% de nivel de madurez de los controles los cuales están alineadas a la ISO 27001, como se puede observar en la siguiente gráfica:

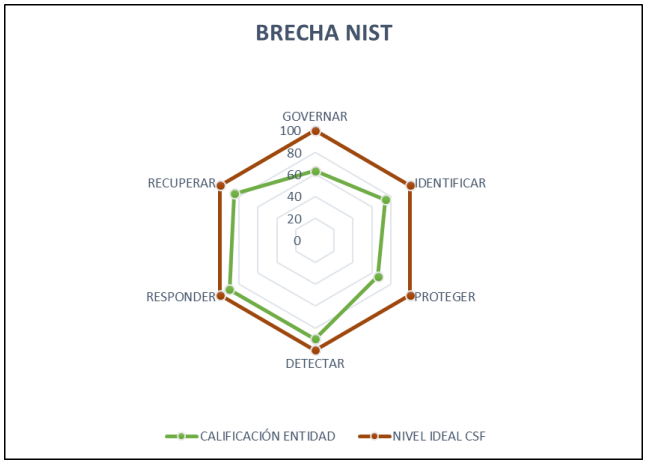
Ilustración 3: Brechas ISO 27001:2022 autodiagnóstico



Fuente: Elaboración Propia

Y un 78% de avance en el nivel de madurez respecto a NIST 800

Ilustración 4: Brechas NIST diagnóstico de seguridad



Fuente: Elaboración Propia

El SGSI del IDEAM presenta un nivel Gestionado con fortalezas notables en seguridad física, gestión de incidentes, cumplimiento, detección y respuesta. Las prioridades para cerrar brechas se concentran en el gobierno y documentación del Sistema de gestión para el modelo de

seguridad y privacidad de la información con la gestión de riesgos institucional, seguridad en la nube, la gestión de identidades y accesos, protección, etiquetado y anonimización de datos, prevención de fuga de datos y plan de continuidad de negocio. Avanzando en estas líneas, la entidad puede llevar su madurez a Optimizado durante la vigencia 2026.

9. ANALISIS DE BRECHAS

Con el propósito de robustecer el Modelo de Seguridad y Privacidad de la Información, se propone la actualización e implementación de controles avanzados que permitan alcanzar un nivel de madurez optimizado y alineado con los estándares del MSPI. En este marco, se presentan las siguientes estrategias, orientadas a mejorar la postura de seguridad institucional, fortalecer la resiliencia operativa y garantizar la protección integral de los activos de información.

9.1. Gobierno y alineación del sistema de gestión de seguridad de la información

Gobierno y alineación del Sistema de Gestión de Seguridad de la Información (SGSI), orientadas a la transición hacia el nuevo Modelo de Seguridad y Privacidad de la Información versión 2025 basado en ISO 27001:2022. Esta estrategia incluye la unificación de la Política General y la definición del alcance oficial del SGSI mediante acto administrativo, la actualización del MSPI 2025 y la garantía de coherencia documental en resoluciones, manuales, procedimientos y Declaración de Aplicabilidad (SoA), cerrando hallazgos para completar el ciclo PHVA.

9.2. Gestión de riesgos institucionales

Gestión integral de riesgos orientada a consolidar los riesgos institucionales de seguridad de la información, mediante la formulación y valoración de riesgos y oportunidades en todos los procesos, la actualización y publicación del Plan de Tratamiento en su versión vigente y la implementación de mecanismos de seguimiento periódico a través de tableros de control. Esta estrategia busca garantizar la trazabilidad de decisiones, priorizar acciones y fortalecer la capacidad de respuesta ante incidentes, cerrando brechas relacionadas con la ausencia de riesgos consolidados, planes desactualizados y evaluaciones periódicas incompletas.

9.3. Protección de datos personales y privacidad

Protección integral de la información y datos personales mediante la implementación de esquemas de clasificación y etiquetado, la definición de responsables y encargados de bases con datos personales, y la adecuación de políticas de retención y eliminación segura. Esta estrategia también contempla la incorporación de mecanismos de anonimización, enmascaramiento y cifrado de información, garantizando el cumplimiento normativo y la mitigación de riesgos asociados a la fuga o uso indebido de información sensible.

9.4. Seguridad en la nube e IAM

Fortalecimiento de la seguridad en entornos de nube mediante la formalización de una política específica para el uso de servicios en la nube,

la definición de responsabilidades compartidas y la implementación de controles robustos de gestión de identidades y accesos. Esto incluye autenticación multifactor, revisión periódica de privilegios, registro de actividades críticas y documentación de riesgos asociados a entornos cloud, complementados con controles compensatorios que aseguren la integridad y disponibilidad de los servicios.

9.5. Continuidad y resiliencia (BCP/DRP/BIA)

Gestionar de continuidad de servicios críticos mediante la formalización y actualización del Análisis de Impacto en el Negocio (BIA), el Plan de Continuidad (BCP) y el Plan de Recuperación ante Desastres (DRP), verificando su articulación con la gestión de incidentes y la ejecución de pruebas periódicas tanto simuladas como técnicas. Esta estrategia busca reducir el impacto ante eventos disruptivos, para tener recuperación oportuna de servicios esenciales.

9.6. Personas, cultura y trabajo remoto/BYOD

Fortalecimiento de la cultura organizacional, documentación sobre el trabajo remoto y dispositivos propios BYOD mediante la documentación de una política que contemple cifrado, borrado remoto y cadena de custodia para activos fuera de las instalaciones, el refuerzo de acuerdos de confidencialidad y el desarrollo de campañas de concientización periódicas orientadas a la prevención de incidentes, phishing y manejo seguro de la información. Estas medidas buscan reducir riesgos humanos y garantizar la protección de activos en entornos no controlados.

9.7. Operaciones y tecnología (vulnerabilidades y código seguro)

Fortalecimiento de la seguridad operativa y tecnológica mediante la gestión de vulnerabilidades con escaneo de seguridad. Esta estrategia también incluye la estandarización de procesos de sanitización y borrado seguro antes de la reutilización o disposición final de equipos, asegurando la protección de la información en todo su ciclo de vida.

10. PLAN DE IMPLEMENTACIÓN

El Plan de Seguridad y Privacidad de la información para la vigencia 2026 y en concordancia con el Modelo de Seguridad y Privacidad de la Información contempla el siguiente cronograma el cual tendrá un seguimiento cuatrimestral.

Tabla 1 Cronograma fase de preparación

FASE 0: PREPARACION **ACTUALIZACIÓN Y PUBLICACION DE PLANES**	
Objetivo	Actividades
Actualización y Publicación de planes del SGSI.	Realizar la actualización de los planes de: - Plan de seguridad y privacidad de la información - Plan de comunicación y sensibilización de TI.
	Realizar la publicación de planes en el portal web de la entidad.

Fuente: Elaboración Propia

Tabla 2 Cronograma fase de Diagnóstico

FASE I: DIAGNOSTICO	
ANÁLISIS GAP ISO 27001 y MSPI	
Objetivo	**Actividades**
Análisis GAP (análisis de brecha) frente a la normatividad vigente y MSPI	Realizar un análisis GAP o de brecha al SGSI, siguiendo como marco de referencia la norma ISO 27001 y la normatividad e instrumento definida por el Ministerio de Tecnologías de la Información.

Fuente: Elaboración Propia

Tabla 3 Cronograma fase de Planificación

FASE II: PLANIFICACION **DISEÑO DE CONTROLES TECNICOS Y ADMINSITRATIVOS**	
Identificar y/o Diseñar los controles técnicos y administrativos para cerrar las brechas identificadas en la fase de diagnóstico y de acuerdo con la	Establecer plan de trabajo para cerrar las brechas encontradas en el diagnóstico inicial.
	Realizar la planeación de las actividades de: - Gobierno y alineación del sistema de gestión de seguridad de la información - Actualización de riesgos de seguridad de la información - Controles para protección de datos personales y privacidad. - Controles para seguridad en la nube e IAM

normatividad vigente.	- Actualización de los controles de continuidad y resiliencia (BCP/BIA/DRP) - Controles para personas, cultura y trabajo remoto/BYOD - Controles para operaciones y tecnología (Vulnerabilidades y código seguro)

Fuente: Elaboración propia

Tabla 4 Cronograma fase de Implementación

FASE III: IMPLEMENTACION CONTROLES Y SENSIBILIZACION	
Objetivo	**Actividades**
Implementación de controles de acuerdo con la normatividad vigente y la sensibilización y capacitación en temas de seguridad	Implementación de controles: - Actualización de políticas, alcance del SGSI, declaración de aplicabilidad, procedimientos y formatos.
	- Realizar la actualización de los activos de información con todas las áreas de la entidad y gestionando los riesgos institucionales.
	- Implementar controles para la seguridad en la nube y el doble factor de autenticación.
	- Realizar la actualización de los documentos DRP/BCP/BIA con los procesos estratégicos de la entidad.

FASE III: IMPLEMENTACION	
	- Implementar controles para los dispositivos personales.
	- Realizar ejercicios de escaneo de vulnerabilidades a los sistemas de información y código fuente
	- Realizar actividades de capacitación y campañas de seguridad de acuerdo con el plan de sensibilización de TI.

Fuente: Elaboración Propia

Tabla 5 Cronograma fase de Evaluación

FASE IV: EVALUACION **AUDITORIA INTERNA SGSI**	
Objetivo	**Actividades**
Identificar los niveles de cumplimento en la entidad y la identificación de vulnerabilidades	Realizar auditorías internas a los sistemas de información
	Realizar auditorías a procesos y procedimientos de la entidad

Fuente: Elaboración Propia

Tabla 6 Cronograma fase de mejora continua

FASE V: MEJORA CONTINUA **IDENTIFICACION DE OPORTUNIDADES DE MEJORA** **Objetivo**	**Actividades**
Identificar las acciones de mejora en el SGSI	Realizar la medición de los controles implementados hasta la vigencia.
	Realizar una evaluación que permita medir el conocimiento asimilado por los funcionarios capacitados en temas de seguridad informática.
	Realizar el levantamiento de brechas para incluir en los planes estratégicos de la posterior vigencia.

Fuente: Elaboración Propia

10.1. Recomendaciones Finales para la implementación del Plan

Para garantizar la efectividad del Plan de Seguridad y Privacidad de la Información y su alineación con los objetivos estratégicos del IDEAM, se recomienda adoptar los siguientes lineamientos operativos:

- Coordinación de interdependencias: Asegurar la articulación entre las áreas responsables del SGSI, TIC, Gestión Documental, Jurídica y líderes de proceso, evitando duplicidades y garantizando la coherencia en la ejecución de actividades.

- Actualización periódica: Revisar y ajustar el Plan conforme a las orientaciones del DAFP, la normatividad vigente y los cambios en el Modelo Integrado de Planeación y Gestión (MIPG), asegurando su pertinencia frente a nuevas amenazas y regulaciones.

- Registro oportuno del avance: Documentar el progreso de cada actividad en los sistemas institucionales de seguimiento,

manteniendo evidencias verificables para auditorías internas y externas.

- Gestión de riesgos y acciones de mejora: Incorporar la identificación continua de riesgos emergentes y la ejecución de acciones correctivas y preventivas, garantizando la mejora continua del SGSI.

- Alineación con el Sistema de Gestión Integrado: Integrar las acciones del Plan con los componentes del SGI y los objetivos estratégicos institucionales, asegurando sinergia con los procesos de calidad, control interno y gestión ambiental.

- Comunicación y sensibilización permanente: Mantener campañas de divulgación y capacitación para asegurar la apropiación del Plan por parte de todos los actores involucrados, fortaleciendo la cultura de seguridad.

- Monitoreo y reporte a la alta dirección: Establecer mecanismos de seguimiento con indicadores claros y reportes periódicos al Comité de Dirección, para garantizar la toma de decisiones informadas y oportunas.

10.2. Sistema De Monitoreo Y Evaluación Del Plan

Nombre del Indicador	Fórmula de cálculo	Responsable	Meta anual	Unidad de medida	Meta cuatrimestre I	Meta cuatrimestre II	Meta cuatrimestre III	Código línea PAI o Nombre Ind. Gestión
Porcentaje de avance en el cumplimiento del PESI 2026	((Actividades ejecutadas / Total de Actividades planificadas) ×100)	Jefe de Oficina de Informática Coordinador Grupo GAESI	100%	Número de actividades	Cumplimiento del 33.3% de las actividades establecidos en todo el plan	Cumplimiento del 33.3% de las actividades establecidos en todo el plan.	Cumplimiento del 33.3% de las actividades establecidos en todo el plan	INFO2026-1 , INFO2026-2, INFO2026-3

Fuente: Elaboración Propia

11. HOJA DE RUTA

Para cada una de las fases planteadas para la vigencia 2026 se establecen las fechas de culminación de esta.

Tabla 7 Hoja de ruta 2026

FASES	2026											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago.	Sep.	Oct	Nov	Dic
FASE 0												
FASE I												
FASE II												
FASE III												
FASE IV												
FASE V												

Fuente: Elaboración Propia

12. COMUNICACIÓN Y DIFUSIÓN

ESTRATEGIA	MEDICIÓN
La estrategia de comunicación es a través de las actividades programadas en el plan de comunicación y sensibilización de TI.	El monitoreo del plan es a través de seguimiento mensual del cumplimiento de las actividades programadas

Fuente: Elaboración Propia

13. DOCUMENTOS RELACIONADOS EN EL SGI

Dentro de los documentos relacionados con el Plan estratégico de seguridad de la información se encuentran:

- Plan de comunicación y sensibilización de TI.
- Plan estratégico de tecnologías y comunicaciones PETI

14. BIBLIOGRAFÍA

- Modelo de seguridad y privacidad de la información MSPI de MinTIC versión 2025
- Plantillas de Gobierno digital MinTIC
- ISO 27001 versión 2022
- NIST 800 53 cybersecurity framework

15. CONTROL DE CAMBIOS

Versión	Fecha	Descripción
04	30/01/2026	Actualización del documento con actividades para la vigencia 2026