Plan de Tratamiento de

Riesgos de Seguridad y Privacidad de la Información

2026

IDEAM

INTRODUCCIÓN

El Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM) reconoce que la información es uno de sus activos más valiosos, ya que sustenta la generación de conocimiento, la toma de decisiones y el cumplimiento de su misión institucional. En este contexto, la gestión adecuada de los riesgos asociados a la seguridad de la información es fundamental para garantizar la continuidad operativa, la confianza de los usuarios y el cumplimiento del marco normativo aplicable.

El Plan de Tratamiento de Riesgos es una herramienta para contribuir a la mitigación de estos, por lo que se realiza análisis, priorizando aquellos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos críticos del Instituto. Este plan se fundamenta en el Modelo de Seguridad y Privacidad de la Información y en las mejores prácticas internacionales, asegurando que las medidas adoptadas sean proporcionales al nivel de riesgo y contribuyan al fortalecimiento del Sistema de Gestión de Seguridad de la Información.

Su aplicación busca minimizar impactos operativos, reputacionales, económicos y legales, garantizando la protección de la información y la infraestructura crítica cibernética que soporta los procesos misionales del Instituto.

1. METODOLOGÍA PARA LA ELABORACIÓN DEL PLAN

La metodología adoptada para el Plan de Tratamiento de Riesgos del IDEAM se fundamenta en el Modelo de Seguridad y Privacidad de la Información del MinTIC, el cual está basado en estándares internacionales como ISO/IEC 27005 (gestión de riesgos de seguridad de la información), ISO/IEC 27001 y las guías del NIST. Este enfoque garantiza que las acciones de tratamiento se realicen de manera sistemática, coherente y alineada con el marco regulatorio vigente.

Los instrumentos de referencia incluyen:

Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas DAFP.

Modelo Integrado de Planeación y Gestión (MIPG).

Marco de Referencia de Arquitectura TI.

Políticas internas de seguridad y privacidad del IDEAM.

2. OBJETIVO

Fortalecer la seguridad y privacidad de la información del IDEAM a través de la implementación el tratamiento de riesgos de seguridad y privacidad de la información alineada con la guía metodológica para la gestión del riesgo del DAFP adoptada por el IDEAM.

3. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, basado en buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Junto con la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información se dan los lineamientos de forma articulada con la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 de seguridad y privacidad de la información en el IDEAM.

El plan de tratamiento de riesgos evaluará las opciones de manejo y tratamiento para los riesgos identificados y evaluados en el análisis de riesgos, cuyos niveles de riesgo para cualquiera de las áreas de impacto resultaron como “Extremo” y “Alto”, en el marco de la operación por procesos de IDEAM y dando alcance al Modelo de Seguridad y Privacidad de la información de MINTIC.

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

Relacionar la normativa aplicable, incluyendo:

- 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 Lineamientos 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 Tratamiento de Riesgos de Seguridad de la Información del IDEAM define las acciones para gestionar los riesgos que pueden afectar la disponibilidad, integridad y confidencialidad de la información hidrológica, meteorológica, climática y ambiental que la entidad produce y administra, garantizando así la continuidad del servicio. El plan consolida los riesgos identificados, establece estrategias de tratamiento, asigna responsables y determina controles para minimizar impactos sobre los activos de información de la entidad.

7.1. Fases de la metodología

7.1.1. Identificación y Análisis del Riesgo

- Se parte del inventario y clasificación de activos críticos, considerando su valor, vulnerabilidades y amenazas.

- Se evalúa el nivel de riesgo mediante criterios de impacto y probabilidad, siguiendo la matriz definida en la Guía de Administración del Riesgo.

7.1.2. Definición de Opciones de Tratamiento

Para cada riesgo identificado, se establecen estrategias de tratamiento:

- Mitigar: Implementar controles para reducir impacto o probabilidad.
- Compartir: Delegar el riesgo a terceros (contratos, seguros).
- Aceptar: Asumir el riesgo cuando es residual y controlado.
- Evitar: Eliminar la causa del riesgo mediante cambios en procesos o tecnología.

7.1.3. Planificación de Controles y Acciones

- Se definen controles técnicos, administrativos y físicos, priorizando según criticidad del riesgo.
- Se asignan responsables, recursos y plazos para la implementación.
- Implementación del Tratamiento
- Ejecución de las acciones definidas en el plan, articuladas con el PETI, el Plan de Seguridad de la Información y el Plan de Acción Institucional.

7.1.4. Monitoreo y evaluación

- Seguimiento periódico del estado de los riesgos y efectividad de los controles.

- Uso de indicadores para medir reducción del riesgo y nivel de madurez del sistema.

7.1.5. Mejora Continua

- Ajuste del plan según resultados, cambios en el contexto o aparición de nuevos riesgos.
- Retroalimentación hacia el ciclo de gestión de riesgos institucional.

7.2. Alineación estratégica

El Plan de tratamiento de riesgos de seguridad de la información se encuentra alineado con el plan de seguridad y privacidad de la información como parte integral del Modelo de seguridad y privacidad de la información (MSPI) así como la coherencia estratégica y operativa en la gestión y protección de los activos institucionales.

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: Gestión 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		

Plan Estratégico Institucional		Modelo Integrado de Planeación y Gestión		Sistema de Gestión Integrado
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		

Fuente: Elaboración Propia

8. MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN – OFICINA DE INFORMATICA.

Tipo de riesgo	Descripción del Riesgo (POSIBILIDAD DE ¿Qué?, ¿Cómo? Y ¿Por qué? "Perdida de" + (Confidencialidad/integridad/disponibilidad) + "debido a" + (Amenaza(s) + Vulnerabilidad(es)) + "afectando" + Activo(s) de información.	Frecuencia	% Probabilidad inherente	Probabilidad inherente	% Impacto inherente	Impacto inherente	Zona de Riesgo inherente	No Control	Dominio	Control Anexo A	Descripción del control
Pérdida de confidencialidad, integridad y disponibilidad	Posibilidad de pérdida de confidencialidad, integridad y disponibilidad por la asignación errada de los derechos de acceso, por error en el uso o abuso de derechos en el activo GAESI-DOCUMENTOS-GENERAL	8760 (Horas/ año)	40%	Baja	20%	Leve	Bajo	1	8. Controles tecnológicos	8.2 Derechos de acceso privilegiados	Coordinador de GAESI, verifica los permisos de acceso y privilegio sobre el repositorio GAESI de SharePoint. El objetivo de detectar si una persona no autorizada tiene acceso, para la inactivación de este.
Pérdida de disponibilidad e integridad	Perdida de integridad y/o disponibilidad por la autenticación de un usuario no autorizado debido a una autenticación débil en GITLAB, que utiliza un único factor de autenticación como es: usuario y contraseña.	8760 (Horas/ año)	60%	Media	80%	Mayor	Alto	1	6. Controles de Personal	6.1 Selección	El administrador de GITLAB, realiza la auditoría de logs dentro del sistema, para verificar trazabilidad, modificaciones, gestión de accesos e identidades. El objetivo del control, es definir el comportamiento, para tener la capacidad de identificar situaciones inusuales y eventos de seguridad de la información que puedan convertirse en incidentes.
Pérdida de disponibilidad e integridad	Posibilidad de pérdida de la Confidencialidad, Integridad y disponibilidad debido a falta de controles de acceso y revisión de permisos a los servicios de red afectando los sistemas de información del IDEAM	8760 (Horas/ año)	80%	Alta	60%	Moderado	Alto	1	8. Controles Tecnológicos	8.3. Restricción de acceso a la información	El jefe y/o supervisor de cada dependencia solicita a la Mesa de Servicio de la Oficina de Informática el acceso del usuario a las herramientas tecnológicas
								2	8. Controles Tecnológicos	8.2. Derechos de acceso privilegiado	El profesional a cargo de la seguridad informática realiza seguimiento a los accesos a la red de la entidad a los proveedores.
Pérdida de disponibilidad	Pérdida de disponibilidad de servicios tecnológicos, por falta de seguimiento al plan de recuperación de desastres debido a Eventos naturales, fallas técnicas, compromiso de las funciones, hardware, software y lugar.	8760 (Horas/ año)	20%	Muy Baja	60%	Moderado	Moderado	1	5. Controles organizacionales	5.30. Preparación de las TIC para la continuidad del negocio	El jefe de la Oficina de informática delega a un responsable de seguridad y privacidad para realizar seguimiento al plan de recuperación de desastres.
Pérdida de disponibilidad	Probabilidad de pérdida de la disponibilidad del Hardware, infraestructura física, redes y comunicaciones, bases de datos y software de backup de la Oficina de Informática, contenida en : Servidores, Clusters, UPS, Aire Acondicionado, Computadores de escritorio y portátiles, equipos de red y seguridad perimetral, debido a afectación en la infraestructura, variación de temperatura, almacenamiento sin protección por copia no controladas lo cual podría ocasionar afectación reputacional y económica por no poder prestar oportunamente los servicios de TI.	8760 (Horas/ año)	80%	Alta	60%	Moderado	Alto	1	8. Controles Tecnológicos	8.13. Copia de seguridad de la información	1. Los especialistas de servidores, aplicaciones y hardware deben verificar que los servicios prestados se encuentren operando con normalidad, en caso contrario se debe realizar el respectivo reporte por medio de la mesa de servicio para su respectiva gestión.
								2	8. Controles Tecnológicos	8.13. Copia de seguridad de la información	2. Los especialistas de servidores y aplicaciones deben verificar que deben verificar que se estén realizando las copias de seguridad de las maquinas que están en la nube-cloud y OnPremise de acuerdo a la periodicidad definida. validar el diligenciamiento de la bitácora de infraestructura, en caso de evidenciar que no se ejecutó el backup programado, se deberá realizar inmediatamente la copia y el escalamiento correspondiente al proveedor de servicio, (como evidencia de esta actividad se tiene bitácora de infraestructura).

Fuente: Elaboración Propia

9. PLAN DE IMPLEMENTACIÓN DEL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de Implementación del Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece un cronograma, para ejecutar las acciones de mitigación identificados en el análisis.

Para garantizar la efectividad del plan y la trazabilidad de las acciones, se implementará un mecanismo de seguimiento, mediante el cual se evalúa el avance de cada actividad, el cumplimiento de los plazos establecidos y la efectividad de los controles aplicados.

Tabla 2 Fase I formalización

FASE I: FORMALIZACION	
DEFINICION Y FORMALIZACION DE MATRIZ DE RIESGOS	
Objetivo	Actividades
Creación y Establecimiento de Matriz de Riesgos de Seguridad a nivel de la Entidad	Realizar la actualización de la metodología, documentación correspondiente.
	Realizar el levantamiento de riesgos de seguridad de la información en base a los activos de información clasificados como críticos.
	Formalización en el sistema de gestión de Calidad - SIG

Fuente: Elaboración Propia

Tabla 3 Fase Identificación

FASE II: IDENTIFICACION	
IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD	
Objetivo	Actividades
Realizar la Actualización de los riesgos de seguridad de la información	Identificación de nuevos riesgos de seguridad y privacidad de la información.
	Realizar la actualización de la matriz de riesgos.
	Implementar controles para seguridad en nube e información personal
	Seguimiento a la efectividad de los controles de los riesgos de seguridad.
	Actualizar el plan de continuidad de la entidad.

Fuente: Elaboración Propia

Tabla 4 Fase Seguimiento

FASE III: SEGUIMIENTO Y MEJORA CONTINUA	
EVALUACION Y MONITOREO DE RIESGOS DE SEGURIDAD	
Objetivo	Actividades
Realizar Seguimiento y monitoreo a los riesgos identificados.	Actualizar procedimientos y lineamientos técnicos sobre la gestión de los riesgos de seguridad de la información.
	Actualizar el plan para la posterior vigencia con las acciones que permitan cerrar las brechas encontradas.

Fuente: Elaboración Propia

9.1. Recomendaciones finales para la implementación del Plan

Para garantizar la efectividad del Plan de Tratamiento de Riesgos de seguridad de la información y su alineación con los objetivos estratégicos del IDEAM, se establecen los siguientes lineamientos operativos:

- **Articulación Interinstitucional y de Procesos**
  Coordinar las acciones de tratamiento con las dependencias responsables del SGSI, TIC, Gestión Documental, Jurídica y líderes de proceso, asegurando coherencia y evitando duplicidades en la implementación de controles.

- **Actualización Periódica del Plan**
  Revisar y ajustar el plan conforme a los resultados del monitoreo, cambios en el contexto organizacional, nuevas amenazas, avances tecnológicos y actualizaciones normativas, garantizando su pertinencia y efectividad.

- **Registro y Evidencia del Avance**
  Documentar todas las acciones de tratamiento en los sistemas institucionales de seguimiento, manteniendo evidencias verificables para auditorías internas y externas.

- **Gestión Dinámica del Riesgo**
  Incorporar la identificación continua de riesgos emergentes y la ejecución de acciones correctivas y preventivas, asegurando la mejora continua del proceso de tratamiento.

- **Integración con el Sistema de Gestión Institucional**

  Alinear las acciones del plan con el SGSI, el PETI, el MIPG y demás componentes del Sistema de Gestión Integrado, garantizando sinergia con los procesos de calidad, control interno y gestión ambiental.

- **Comunicación y Sensibilización Permanente**
  Desarrollar campañas de divulgación y capacitación sobre la gestión de riesgos y los controles implementados, promoviendo la apropiación del plan y fortaleciendo la cultura de seguridad en todos los niveles.

- **Monitoreo y Reporte**

  Establecer mecanismos de seguimiento con indicadores claros y reportes periódicos, asegurando la toma de decisiones informadas y oportunas.

9.2. 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 Plan de Tratamiento de riesgos de seguridad y privacidad de la información 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

10. HOJA DE RUTA

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

Tabla 1 Hoja de Ruta

	2026											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
FASE I												
FASE												

II												
FASE III												

Fuente: Elaboración Propia

11. 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

12. 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
- Plan de Seguridad y Privacidad de la información

13. 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

14. Control de cambios

Versión	Fecha	Descripción
04	27/01/2026	Actualización del documento con actividades para la vigencia 2026