1. Introducción

Enfoque del IDEAM
El Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM), consciente de los riesgos que pueden afectar la operación y continuidad de su plataforma tecnológica, ha decidido estructurar, implementar y mantener un Plan de Recuperación de Desastres (DRP). Este plan tiene como propósito identificar la infraestructura tecnológica, tanto física como lógica. Los servicios locales y en la nube, el talento humano involucrado y los riesgos de tipo catastrófico, con el fin de establecer estrategias que permitan reducir los tiempos de recuperación y garantizar la continuidad operativa del proceso de Gestión de Tecnología y Seguridad de la Información.

La continuidad de las operaciones debe estar alineada con el Modelo de Seguridad y Privacidad de la Información, así como con la Guía 10 del MinTIC, orientada a la preparación de las TIC para la continuidad del negocio, y la Guía 11, que establece los lineamientos para la realización del Análisis de Impacto al Negocio (BIA), en este caso con un enfoque tecnológico.

Adicionalmente, se tendrán en cuenta los lineamientos establecidos en la norma ISO 24762, que proporciona pautas para la recuperación de servicios de tecnología de la información y comunicaciones ante desastres, así como la NIST SP 800-34, guía de planificación de contingencias para sistemas de información. Todo esto en el marco de la gestión de riesgos, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información institucional, mitigando posibles impactos negativos sobre los activos de información del IDEAM.

Este enfoque se fundamenta en estándares internacionales como la ISO 31000 (gestión de riesgos), la ISO 27005 (gestión de riesgos de seguridad de la información), la Guía 5 de MinTIC sobre clasificación de activos, y en el diseño de controles para entidades públicas. Asimismo, se articula con lo dispuesto en el Decreto 1008 de 2018, que establece los lineamientos generales de la Política de Gobierno Digital, incluyendo los habilitadores transversales: Seguridad de la Información, Arquitectura de TI y Servicios Ciudadanos Digitales.

En línea con la evolución de esta política, el Decreto 767 de 2022 refuerza el compromiso del Estado con la transformación digital, buscando mejorar la calidad de vida de los ciudadanos y la competitividad del país. Este decreto promueve el uso ágil, sencillo y útil de la tecnología, en un entorno seguro y responsable, y define cinco elementos clave para la implementación de la Política de Gobierno Digital:

- Gobernanza,
- Innovación Pública Digital,
- Habilitadores,
- Líneas de acción
- Iniciativas dinamizadoras.

Finalmente, se incorpora lo establecido en la Resolución Interna 063 de 2025, mediante la cual el IDEAM adopta su Política General de Seguridad y Privacidad de la Información, Seguridad Digital y los lineamientos para el uso adecuado de la información institucional.

2. Objetivos

2.1. Objetivo General

Brindar la continuidad de las operaciones esenciales del servicio y la protección de los activos tecnológicos del Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM), mediante la definición de actividades, roles y responsabilidades que permitan mantener la operatividad de la infraestructura tecnológica ante la ocurrencia de desastres, interrupciones mayores o eventos contingentes. Este plan busca asegurar una respuesta oportuna y una recuperación eficaz, minimizando los tiempos de inactividad a través de procedimientos ágiles y efectivos, y protegiendo los activos de información institucional.

2.2. Objetivos Específicos

- Asegurar la recuperación de los servicios tecnológicos prestados por el IDEAM dentro de los márgenes de tiempo tolerables, garantizando la continuidad de las operaciones críticas.
- Establecer un plan de respuesta ante desastres que defina claramente las acciones a seguir en caso de eventos disruptivos, asegurando la protección de los activos tecnológicos y la continuidad del servicio.
- Minimizar los impactos negativos mediante el fortalecimiento de la resiliencia operativa, a través de evaluaciones periódicas de riesgos y vulnerabilidades que permitan anticipar y mitigar posibles interrupciones.
- Entrenar al personal del IDEAM en la ejecución del plan de respuesta ante desastres, promoviendo una actuación coordinada, eficiente y oportuna en situaciones de crisis.

- Reducir los tiempos de toma de decisiones durante la fase de recuperación posterior a un incidente que afecte la continuidad del proceso de Gestión de Tecnología y Seguridad de la Información.
- Implementar medidas preventivas y de mitigación que disminuyan la probabilidad de ocurrencia de desastres y su impacto sobre las operaciones y activos tecnológicos del IDEAM.
- Cumplir con los requerimientos legales y regulatorios aplicables, así como con las expectativas de las partes interesadas.
- Mantener la seguridad de la información antes, durante y después de cualquier evento que pueda comprometer la confidencialidad, integridad o disponibilidad de los datos institucionales.

3. Alcance

Las actividades establecidas en este plan se encuentran en el marco de las responsabilidades de la Oficina de Tecnología del IDEAM, y abarcan los siguientes aspectos:

- Responsables de los procesos críticos.
- Infraestructura y servicios de Tecnología de la Información.
- Recuperación de servicios tecnológicos priorizados, incluyendo aplicaciones, comunicaciones, infraestructura y sistemas de información.
- Activos de información asociados al proceso de Gestión de Tecnología de la Información y comunicaciones, con impacto transversal en toda la entidad.

4. Definiciones

4.1 Definiciones

- Activación: Declaración de que los acuerdos de la entidad para la continuidad del negocio deben implementarse para asegurar la entrega de productos o servicios clave.
- Activo de información: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocio de la entidad y que, en consecuencia, debe ser protegido. Esto incluye bases de datos, archivos, sistemas de información, documentación física y digital, infraestructura tecnológica y el conocimiento de los funcionarios.

- Análisis de riesgos: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo asociado a los activos de información. Este proceso implica la identificación de vulnerabilidades, la evaluación de la probabilidad e impacto de las amenazas, y la determinación del nivel de riesgo resultante.
- Continuidad del negocio: Capacidad de la entidad para mantener la entrega de productos o servicios a niveles predefinidos aceptables después de un evento perjudicial.
- Desastre: Problema o evento no planificado que interrumpe los procesos de negocio por un período de tiempo superior a lo que la entidad puede soportar sin sufrir perjuicios considerables.
- Evento: Ocurrencia o cambio de un conjunto particular de circunstancias.
- Incidente: Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción en la calidad de ese servicio.
- Impacto: Consecuencia de la materialización de una amenaza sobre un activo.
- Plataforma tecnológica crítica: Servicios, sistemas de información, servidores, bases de datos, sistemas de almacenamiento y respaldo, equipos y enlaces de comunicación que son esenciales para soportar los procesos, operaciones y servicios de la entidad.
- Riesgo: El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

Siglas

- **BIA:** Análisis de Impacto en el Negocio (Business Impact Analysis).
- **CCOCI:** Comando Conjunto Cibernético
- **ColCERT:** Grupo de Respuestas a Emergencias Cibernéticas de Colombia.
- **CSIRT Gobierno:** Equipo de Respuesta a Incidentes de Seguridad Informática del gobierno de Colombia.
- **CSIRT PONAL:** Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional.
- **DOFA:** Debilidades, Oportunidades, Fortalezas y Amenazas.

- **DRP:** Plan de recuperación de desastres (Disaster recovery plan).
- **IDEAM:** Instituto de Hidrología, Meteorología y Estudios Ambientales.
- **ISO/IEC:** Organización Internacional de Normalización / Comisión Electrotécnica Internacional.
- **MinTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **SIG:** Sistema Integrado de Gestión.
- **SGSI:** Sistema de Gestión de la Seguridad de la Información.
- **TI:** Tecnologías de la Información.
- **TIC:** Tecnologías de la Información y las Comunicaciones.

5. Marco normativo

Ver normograma

6. Política del Plan de Recuperación de Desastres (DRP)

El IDEAM adelanta las acciones necesarias para asegurar que las funciones esenciales del proceso de Gestión de Tecnología de la Información y Comunicaciones para que continúen operando ante cualquier contingencia que afecte parcial o totalmente su plataforma tecnológica y recursos asociados.

7. Roles y Responsabilidades

Información confidencial

Organigrama DRP

Ilustración 1: Organigrama DRP IDEAM

Información Confidencial

Fuente: Creación propia del IDEAM

8. Responsables

Tabla 1: Equipo DRP

Información Confidencial

Fuente: Creación propia del IDEAM

9. Activación del plan de recuperación de desastres Responsabilidades antes, durante y después

Información Confidencial

10. Responsabilidades antes, durante y después

11. Plan de Comunicaciones

Información Confidencial

12. Contexto del proceso de Gestión de Tecnología de la Información y comunicaciones

Información Confidencial

13. Usuarios del proceso

Información Confidencial

14. Acuerdo de nivel de servicio (SLA - OLA)

Información Confidencial

15. Gestión de recuperación de desastres

Información Confidencial

16. Escenarios de desastres

Información Confidencial

17. Infraestructura, servicios y sistemas de información de tecnológica crítica

Información Confidencial

18. Aplicaciones y servicios organizados por criticidad

Información Confidencial

19. Infraestructura críticos relacionados con la recuperación

Información Confidencial

20. Bases de datos

Información Confidencial

21. Proveedores

Información Confidencial

22. Topología de red

Información Confidencial

23. Actividades de notificación, evaluación y activación del DRP

Información Confidencial

24. Notificación del evento y/o incidente

Información Confidencial

25. Evaluación del evento y/o incidente

Información Confidencial

26. Requerimientos mínimos

Información Confidencial

27. Retorno a la normalidad

Información Confidencial

28. Pruebas

El plan de recuperación de desastres (DRP) debe ser probado al menos una vez al año, para proteger el principio de independencia las pruebas pueden ser ejecutadas o supervisadas por un tercero que no haya participado en la formulación del documento o sea responsable del activo a auditar. Se debe definir cuales pruebas se van a ejecutar durante la vigencia de acuerdo con las pruebas establecidas en el registro del documento Formato Pruebas DRP.

Relación de confidencialidad

El Plan de recuperación de desastres se tiene el detalle de la topología de red, infraestructura, hardware y software crítico, proveedores e información que puede ayudarle a un ciberdelincuente para la ejecución de un ataque cibernético proporcionándole rutas específicas, criticidad de servicios e información que

debe protegerse y que está cubierta bajo la siguiente exclusión de la Ley 1712 del 2014

29. Documentos relacionados en el SIG

GTI-F019 Formato pruebas DRP

30. Control de cambios

Versión	Fecha	Descripción
01	01/06/2017	Creación del Documento
02	21/07/2017	Actualización del documento
03	20/06/2018	Actualización del documento dentro del SGI
04	12/08/2019	Actualización del documento dentro del SGI
05	06/07/2024	Actualización del documento dentro del SGI
06	10/12/2020	Actualización del documento dentro del SGI
07	22/11/2021	Actualización del documento dentro del SGI

08	15/07/2025	Se realiza actualización código de e-sgi-m004 a SGI-M008 y se actualiza imagen institucional.
09	28/07/2025	Ajusta en la definición del cronograma, responsables, usuarios, acuerdos de servicios,