Introducción

El Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM) es la entidad responsable de generar, consolidar y administrar información técnica, científica y ambiental de carácter estratégico para la toma de decisiones en materia de recursos naturales, clima y ambiente en Colombia. La naturaleza de su misión implica gestionar grandes volúmenes de información, parte de la cual es sensible, confidencial y de interés público, por lo que su adecuada protección es fundamental para garantizar la confianza de la ciudadanía, el Estado y la comunidad internacional.

En este contexto, el **Reglamento Interno de Seguridad de la Información** establece los principios, normas, procedimientos y responsabilidades que deben observar los servidores públicos, contratistas y colaboradores del IDEAM para salvaguardar la confidencialidad, integridad, disponibilidad y uso adecuado de la información institucional y de los activos tecnológicos que la soportan.

Este reglamento se fundamenta en la normativa nacional vigente, como la Ley 1581 de 2012 de Protección de Datos Personales, la Ley 1273 de 2009 sobre delitos informáticos, las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y los estándares internacionales de gestión de la seguridad de la información (ISO/IEC 27001), adoptados por la institución para fortalecer su Sistema de Gestión de Seguridad de la Información (SGSI).

El IDEAM, mediante la aplicación de este reglamento, busca promover una cultura organizacional basada en la responsabilidad, la prevención de riesgos, el uso seguro de la información y la mejora continua de los procesos asociados a la seguridad digital, en concordancia con sus principios de legalidad, transparencia y servicio al país.

Objetivo

Establecer los principios, criterios y requerimientos de Seguridad de la Información que garantice la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce y conserva mediante el uso de las tecnologías de información, dando a conocer a los funcionarios, contratistas, practicantes y terceros la necesidad de que exista una responsabilidad en el manejo y custodia de los activos de información en todas las dependencias del instituto.

Alcance

El presente reglamento será de aplicación a todas las áreas, procesos y dependencias del Instituto, siendo este de obligatorio cumplimiento, conforme a la política de seguridad y privacidad de la información y regirá a partir de la oficialización del mismo.

Definiciones

Activo de Información:
Cualquier recurso que contenga información de valor para el IDEAM, incluyendo documentos físicos y digitales, bases de datos, sistemas informáticos, redes, equipos tecnológicos y medios de almacenamiento.

Confidencialidad:
Principio de la seguridad de la información que garantiza que los datos solo sean accesibles por personas autorizadas.

Disponibilidad:
Principio que asegura que la información y los activos asociados estén accesibles y utilizables cuando se requieran por usuarios autorizados.

Incidente de Seguridad de la Información:
Evento o situación que afecta o puede afectar negativamente la confidencialidad, integridad o disponibilidad de la información institucional (p. ej., pérdida de datos, acceso no autorizado, ataque informático).

Integridad:
Principio que garantiza la exactitud y completitud de la información y sus métodos de procesamiento.

Política de Seguridad de la Información:
Documento institucional que establece los lineamientos generales y compromisos para proteger la información, en coherencia con la normativa aplicable y los estándares internacionales.

Protección de Datos Personales:
Conjunto de principios, normas y procedimientos orientados a garantizar que el tratamiento de los datos personales se realice respetando los derechos fundamentales de los titulares, conforme a la Ley 1581 de 2012.

Responsable del Tratamiento:
Persona natural o jurídica, pública o privada, que por sí misma o en asocio con

otros, decide sobre la base de datos y/o el tratamiento de los datos personales (IDEAM).

Sensibilización:
Acción de informar y motivar a los funcionarios y contratistas sobre la importancia de aplicar buenas prácticas de seguridad de la información en sus actividades diarias.

Usuario Autorizado:
Persona que, por su función o relación contractual con el IDEAM, tiene permiso para acceder, procesar o custodiar información institucional bajo los principios de seguridad definidos.

Siglas
No Aplica

Marco Normativo
Ver Normograma

Descripción metodológica del tema a desarrollar
Dentro del marco normativo de acuerdo a los lineamientos del gobierno nacional y las normas vigentes que se emplean para el SGSI, Sistema de gestión de seguridad de la información en el IDEAM, se tendrá en cuenta el presente documento para el correcto desarrollo del sistema, permitiendo parametrizar los diferentes lineamientos relacionados con la protección de la información, siendo esta un bien del Instituto.

1. Todo funcionario, contratista, practicante y tercero que preste servicios al IDEAM, deberá conocer la política de seguridad y privacidad de la información y las políticas de seguridad que se encuentran en el plan de seguridad de la información del instituto.

2. Todo funcionario, contratista, practicante y tercero que preste servicios al IDEAM, deben firmar el documento de acuerdo de confidencialidad, orientado a la no-divulgación de la información sensible. De comprobarse que un funcionario divulgó y/o sustrajo información confidencial para bien propio y/o bien de un tercero, se procederá a tomar las acciones respectivas. Ante una violación de este acuerdo se deberá notificar al interventor del contrato y/o jefe inmediato para tomar las acciones respectivas de acuerdo a la gravedad del incidente presentado.

3. Todo funcionario, contratista, practicantes y tercero que preste servicios al IDEAM, una vez finalizado el contrato correspondiente, debe cumplirse con la no divulgación de información confidencial de la organización. En caso de

comprobar que se ha hecho pública la información por cuenta del ex-empleado o ex-contratista se procederá a realizar las acciones legales a que haya lugar.

4. Los funcionarios, contratistas y terceros que presten servicios al Instituto y que hagan uso de los recursos de TI de la entidad tanto de hardware como se software tales como: computadores, portátiles, PDAs, correos, bases de datos etc., deben acogerse al reglamento al acuerdo de uso de activos de información (acceso páginas Web no autorizadas, instalación de aplicaciones en el equipo, cambios en la configuración por defecto, etc.). En caso que se demuestre su incumplimiento, se procederá a ejecutar las acciones legales establecidas.

5. Todos los funcionarios, contratistas y terceros que presten servicios al Instituto y requieren hacer algún cambio dentro de la configuración del equipo de cómputo asignado por la oficina de informática, se debe solicitar mediante mesa de servicio por parte del jefe directo de la dependencia al jefe de la oficina informática o quien haga sus veces, dando a conocer el motivo o justificación por el cual se hace necesaria la petición.

6. Todos los funcionarios, contratistas y terceros que presten servicios al IDEAM, deberán devolver los activos de información del Instituto en el momento de la terminación del contrato correspondiente y deberá entregar su bandeja de ORFEO sin ningún documento pendiente al jefe inmediato y/o interventor del contrato.

7. Todos los funcionarios, contratistas y terceros que presten servicios al IDEAM, utilizarán de manera razonable, eficiente y responsable las redes corporativas y equipos informáticos que se encuentren en cualquier oficina o dependencia, en la cual se desarrolle la actividad para la cual fue contratado. Si estos medios tecnológicos son dispuestos para otra actividad fuera de la contratada, se procederá a ejecutar las acciones legales establecidas.

8. Todos los lineamientos que se disponen en el presente reglamento, así como la política de seguridad y privacidad de la información y las políticas que lo soportan en el plan de seguridad de la información serán de estricto cumplimiento.

Documentos relacionados en el SGI

No aplica

Bibliografía

ISO/IEC 27001:2022. *Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información — Requisitos.*

ISO/IEC 27002:2022. *Tecnología de la información — Código de prácticas para controles de seguridad de la información.*

Manual para la Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). Ministerio de Tecnologías de la Información y las Comunicaciones — MinTIC, Colombia.

Guía de Seguridad de la Información para Entidades Públicas. Agencia Nacional Digital – MinTIC, Colombia.

Política de Gobierno Digital. Departamento Administrativo de la Función Pública y Ministerio de Tecnologías de la Información y las Comunicaciones.

Control de cambios

VERSIÓN	FECHA	DESCRIPCIÓN
1	23/12/2016	Creación del documento
2	05/04/2018	Se actualiza versión y codificación para cumplimiento con el decreto 415
3	15/07/2025	Se actualiza código E-SGI-SI-M001 por SGI-M010, se ajusta imagen institucional