 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	<p>PROCEDIMIENTO GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</p>	Código: E-SGI-SI-P001
		Versión: 04
		Fecha: 10/04/2018
		Página: 1 de 6

1. OBJETIVO

El objetivo del procedimiento es establecer las actividades tendientes a garantizar una efectiva administración de la Política de Seguridad de la Información del Instituto de Hidrología, Meteorología y Estudios Ambientales - IDEAM junto con sus respectivos roles, responsables y responsabilidades.

El documento de Política de Seguridad de la Información comprende Políticas, Normas y Procedimientos, Instructivos, por lo que se debe contemplar cualquier cambio en ellos con el fin que sea documentación viva y que responda a las necesidades de seguridad de la información del Instituto.

2. ALCANCE

En este procedimiento se tratará todo lo que tiene que ver con la Administración de la Política, desde su creación hasta su posible eliminación.

3. NORMATIVIDAD

Ver Normograma.

4. DEFINICIONES

- **Administración de Riesgos:** Es el proceso de medir las amenazas y vulnerabilidades (a través del análisis y evaluación del riesgo), determinando y verificando controles compensatorios apropiados para los requerimientos del Instituto y su costo.

- **Confidencialidad:** Aseguramiento de que la información es accesible sólo para quienes están autorizados.

- **Delitos Informáticos:** Son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático.

El "delito informático" puede comprender tanto aquellas conductas que recaen sobre herramientas informáticas propiamente tales, llámense programas, ordenadores, etc.; como aquellas que valiéndose de estos medios lesionan otros intereses jurídicamente tutelados como son la intimidad, el patrimonio económico, la fe pública, etc.

- **Disponibilidad:** Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando se requiera.


- **Entes de Control:** Son las Entidades encargadas de ejercer control sobre los ciudadanos o las corporaciones distritales o nacionales, por ejemplo. Procuraduría General de la Nación, Personería Distrital, etc.

- **Entes Judiciales:** Entidades que son autoridad Judicial a nivel Distrital o Nacional, por ejemplo. Fiscalía General de la Nación.

- **Estándares de Seguridad:** Es un documento que describe la implantación de una guía para un componente específico de hardware, software o infraestructura. Son productos, procedimientos y métricas aprobadas, que definen en detalle cómo serán implementadas las Políticas de Seguridad de Activos de Información para un ambiente en particular, teniendo en cuenta las fortalezas y debilidades de las características de seguridad disponibles.

- **Evaluación y Análisis de Riesgo:** El proceso de analizar un ambiente objetivo y las relaciones de sus atributos de riesgo relacionados. El análisis debe identificar vulnerabilidades y amenazas las cuales deben asociarse con los activos afectados, identificar el impacto y la naturaleza de resultados no deseados e identificar y evaluar las medidas para administrar el riesgo.

- **Habeas data:** Habeas Data significa "que tengas los datos" ó "que vengan los datos", es decir, tomar conocimiento de datos propios en poder de otro. Aparece a finales del siglo XX como la acción más eficaz de protección del derecho a la intimidad frente al poder de los archivos de entidades públicas y privadas que recogen datos e informaciones sobre las personas, no los actualizan y hacen uso indebido de los mismos, en perjuicio de tales personas. La ley 1266 de 2008, o ley de habeas data, permite a las personas,

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	<p>PROCEDIMIENTO GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</p>	Código: E-SGI-SI-P001
		Versión: 04
		Fecha: 10/04/2018
		Página: 2 de 6

conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas, teniendo en cuenta lo establecido en el Artículo 15 de la Constitución Política de Colombia.

Integridad. Salvaguardia de la exactitud y completitud de la información y sus métodos de procesamiento.

Ley de Delitos Informáticos. La Ley 1273 de 2009 es la ley por medio de la cual se crea un nuevo bien jurídico tutelado llamado “de la protección de la información y de los datos”, y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

- **OSI.** Oficial de Seguridad de la Información.

- **Política:** Declaración general de principios que presenta la posición de la administración para una área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías. Las políticas deben ser pocas (número pequeño), deben ser apoyadas y aprobadas por la dirección del instituto y deben ofrecer direccionamiento a toda la organización o a un conjunto importante de funcionarios. Por definición, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.

- **Procedimiento:** Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar algo, para el propósito de este documento es la seguridad relacionada a dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el encargado del proceso o del sistema.

- **Política de Seguridad.** Es un documento de nivel general que describe los diversos requerimientos de orden legal, reglamentario y operacional y los objetivos del Programa de Seguridad. La Política de Seguridad de la Información constituye un precepto para todas las entidades, dependencias y/o funcionarios del IDEAM respecto al cumplimiento de las guías y los estándares en que se reglamenta. Son de largo plazo.

- **Seguridad de la información.** Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Servidores Públicos.** Todas aquellas personas que están vinculadas al IDEAM en planta, contratistas de prestación de servicios, etc.


- **SGSI.** Sistema de Gestión de Seguridad de la Información.

5. POLÍTICAS DE OPERACIÓN

✓ Este procedimiento de Gestión de la Seguridad de la Información y Mecanismos de Seguridad de la Información involucra a todos los funcionarios, administradores o responsables de componentes tecnológicos, Oficina de Informática, responsables de seguridad de la información.

6. DESARROLLO

Ver anexo flujograma (Numeral 8)

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PROCEDIMIENTO GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código: E-SGI-SI-P001
		Versión: 04
		Fecha: 10/04/2018
		Página: 3 de 6

IMPLEMENTACIÓN

Fase de implementación en esta fase la política es comunicada, acatada o no cumplida (excepción)

No.	ACTIVIDAD	RESPONSABLE	REGISTRO	PUNTOS DE CONTROL	TIEMPOS DE ACTIVIDAD
1	COMUNICACIÓN: Crear el instrumento y estrategia de comunicación requisitos para difundir la política.	Oficial de Seguridad Jefe Oficina Informática	Documento, Cartelera, Correo electrónico, Pagina web, taller, etc.		N/A
2	CUMPLIMIENTO: Adelantar implementación de la política haciendo uso de las herramientas tecnológicas que se requieran. En el evento en que se requieran servicios especializados para la implementación se podrá apoyar en servicios contratados	En controles tecnológicos: Funcionarios Oficina Informática Dueños/Responsables de Procesos.	Control de seguimiento		N/A
3	EXCEPCIONES: Realizar las gestiones necesarias para la implementación de actividades no viables inicialmente.	Funcionarios Oficina Informática Dueños/Responsables de proceso Comité de Dirección de la Información	Control de seguimiento		N/A

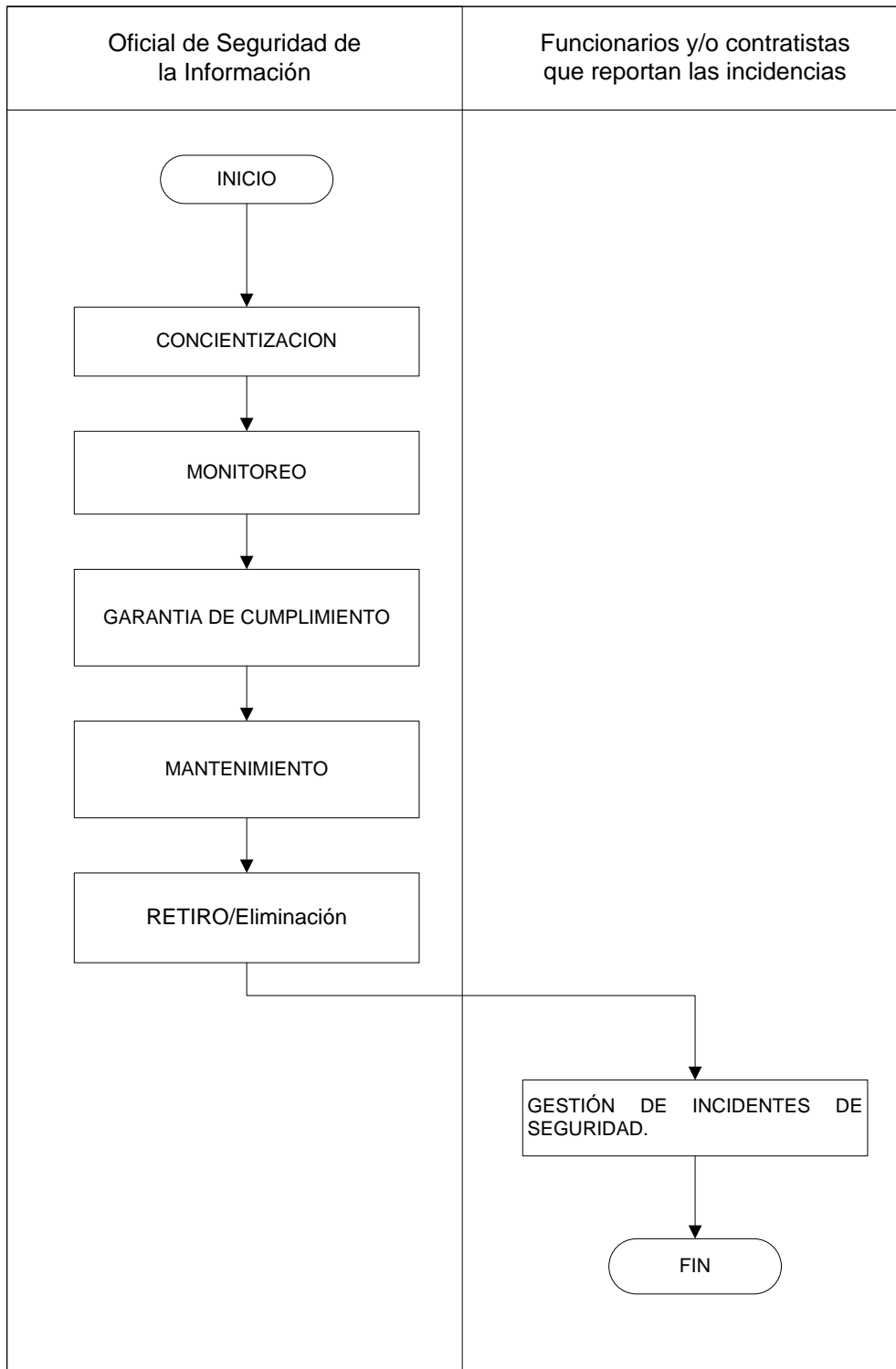
MANTENIMIENTO

Descripción: Los usuarios deben ser conscientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla).

No.	ACTIVIDAD	RESPONSABLE	REGISTRO	PUNTOS DE CONTROL	TIEMPOS DE ACTIVIDAD
1	CONCIERTIZACION: Garantizar la concientización continua de la política	Oficial de Seguridad de la Información. Comité de Dirección de la Información	Control de actas o listas de asistencia		N/A

2	<p>MONITOREO: Realizar seguimiento y reporte del cumplimiento de la política.</p> <p>Realizar las observaciones de las políticas que le aplican a las dependencias y a quienes cobijan esas políticas.</p>	<p>A nivel de modelo de gestión: Oficial de Seguridad.</p> <p>A nivel de controles TI: Funcionarios Oficina Informática</p> <p>Funcionarios y Contratistas del Ideam</p>	Control de seguimiento		N/A
3	<p>GARANTIA DE CUMPLIMIENTO : Afrontar contravenciones a la política de acuerdo a la normatividad vigente.</p> <p>Adelantar las acciones correctivas requeridas para restituir el cumplimiento de la política.</p>	<p>Oficial de Seguridad</p> <p>Dueños/Responsables de procesos.</p>	Control de seguimiento		N/A
4	<p>MANTENIMIENTO: Asegurar que la política esté actualizada.</p> <p>Garantizar la vigencia y la integridad de la política-</p> <p>Tendencias de cambio (en tecnología, procesos, personas, la organización, entre otros.) recomendando y coordinando modificaciones resultado de los cambios</p>	<p>Oficial de Seguridad</p> <p>Comité de Dirección de la Información.</p>	Control de seguimiento		N/A
5	<p>RETIRO/Eliminación: Prescindir de la política cuando no se necesita más.</p> <p>Después de que la política ha cumplido su finalidad y no es necesaria debe ser retirada</p>	Oficial de Seguridad	Control de seguimiento		N/A
6	<p>GESTIÓN DE INCIDENTES DE SEGURIDAD.</p> <p>Los funcionarios y/o contratistas deben reportar a través de la Mesa de Ayuda las incidencias relacionadas con seguridad de la información, siguiendo el <i>Instructivo gestión de incidentes</i></p>	Funcionarios y/o contratistas que reportan las incidencias	Formato para reporte de incidentes de seguridad		N/A

7. ANEXO FLUJOGRAMA



	PROCEDIMIENTO GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código: E-SGI-SI-P001
		Versión: 04
		Fecha: 10/04/2018
		Página: 6 de 6

8. HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
01	06/03/2013	Creación del Procedimiento.
02	28/11/2014	Actualización de los puntos de control de las actividades e inclusión de la actividad de Gestion de Incidentes de Seguridad. Nuevo formato de Procedimiento, en Normatividad se remite al Normograma del Proceso. Adicionalmente se hizo cambio de Condiciones generales pasó a ser Políticas de Operación.
03	23/11/2017	Se actualiza, versión y codificación para cumplimiento con el decreto 415.
04	10/04/2018	Actualización del documento.

ELABORÓ: Luis Alejandro Pinilla Oficial de Seguridad de la Información	REVISÓ: Eduardo Ramirez Acosta Profesional Especializado Oficina Informática	APROBÓ: Leonardo Gádenas Chitiva Jefe Oficina Informática
--	---	---