Introducción

El Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM), como autoridad técnica y normativa encargada de la generación y gestión de información estratégica sobre recursos naturales, clima y medio ambiente en Colombia, reconoce que la seguridad de la información es un pilar fundamental para garantizar la confiabilidad, integridad, disponibilidad y confidencialidad de los datos que gestiona y divulga.

En este contexto, el presente **Plan de Sensibilización y Entrenamiento en Seguridad de la Información** tiene como objetivo fortalecer la cultura organizacional frente a la protección de la información, mediante la formación continua y la apropiación de buenas prácticas por parte de todos los servidores públicos, contratistas y partes interesadas que intervienen en los procesos institucionales.

Este documento establece los lineamientos, objetivos, estrategias y actividades de capacitación y sensibilización, orientados a prevenir incidentes de seguridad, reducir riesgos, cumplir con la normativa vigente y promover el uso responsable, ético y seguro de los activos de información del IDEAM.

De esta manera, el IDEAM reafirma su compromiso con la mejora continua de su Sistema de Gestión de Seguridad de la Información (SGSI), contribuyendo al fortalecimiento de la confianza de la ciudadanía y de las entidades nacionales e internacionales que dependen de la calidad y protección de la información generada por la institución.

Objetivo

Generar un plan de capacitación, sensibilización y comunicación al interior del IDEAM a nivel de seguridad y privacidad de la información con el fin de fortalecer el conocimiento que permitirán mitigar la materialización de incidentes de seguridad propendiendo así por la integridad, disponibilidad y confidencialidad de los activos de información.

Este plan de capacitación se debe construir e implementar mediante el plan de formación que contempla la estrategia de **Uso y Apropiación** que ha diseñado la oficina de Informática para el IDEAM

Alcance

Aplica para todos los servidores públicos y contratistas del IDEAM

Definiciones

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

Entrenamiento/Capacitación:
Actividades planificadas para desarrollar conocimientos, habilidades y competencias específicas en materia de seguridad de la información, con el fin de garantizar el cumplimiento de políticas, procedimientos y controles establecidos por la institución.

Incidente de Seguridad de la Información:
Evento identificado que compromete o tiene el potencial de comprometer la confidencialidad, integridad o disponibilidad de la información, como accesos no autorizados, pérdida de datos, divulgación indebida o ataques informáticos.

Información Confidencial:
Toda aquella información generada, recibida o custodiada por el IDEAM que, por su naturaleza, debe ser protegida de acuerdo con su nivel de clasificación, incluyendo datos personales, datos sensibles, documentos estratégicos, información técnica y administrativa no divulgable.

Política de Seguridad de la Información:
Documento que establece los principios, lineamientos y directrices que orientan la gestión de la seguridad de la información dentro del IDEAM, alineado a la normativa vigente y estándares internacionales.

Riesgo de Seguridad de la Información:
Posibilidad de que una amenaza explote una vulnerabilidad y cause impacto negativo en los activos de información, afectando la operación, la reputación o el cumplimiento de los objetivos institucionales.

Seguridad de la Información:
Conjunto de medidas, controles y buenas prácticas orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información institucional, previniendo accesos no autorizados, alteraciones, pérdidas o divulgación indebida.

Sensibilización:
Proceso mediante el cual se busca generar conciencia en los funcionarios, contratistas y partes interesadas sobre la importancia de proteger la información, identificar riesgos y aplicar prácticas seguras en su manejo diario.

Siglas
CCOC(Comando Conjunto Cibernético)

Marco Normativo
Ver normograma

Descripción metodológica del tema a desarrollar

De acuerdo a la cadena de seguridad el recurso humano puede llegar a ser el eslabón más débil, por tal motivo es de vital importancia llevar a cabo la construcción y mantenimiento plan de sensibilización, entrenamiento y educación.

El plan de sensibilización tiene como finalidad capacitar y formar a los funcionarios y contratistas del IDEAM con el objetivo de prevenir la materialización de incidentes de seguridad. Los tips o campañas se divulgarán por medio de cartelera digital, correos, intranet y papel tapiz, las áreas involucradas para su creación, aprobación y difusión son las siguientes:

- Área de TI
- Área de Comunicaciones
- Funcionarios y contratistas

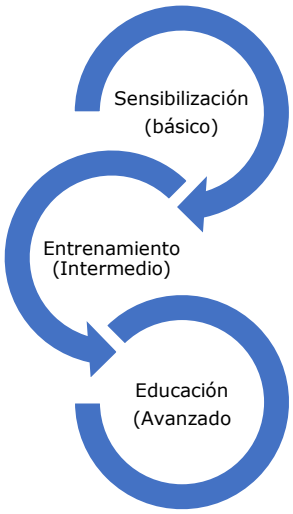
El plan de entrenamiento va dirigido a enseñar y formar de manera presencial con la finalidad de aclarar inquietudes y recibir retroalimentación para poder medir el nivel madurez respecto a las

campañas y tips de seguridad, adicionalmente, al finalizar el entrenamiento es necesario responder un cuestionario para evaluar y confirmar el conocimiento adquirido.

El plan de educación consiste en la preparación del personal experto en seguridad en este caso el Oficial de Seguridad de la información, el cual debe estar contextualizado en los temas de ciberseguridad, Ciberdefensa y amenazas cibernéticas apoyándose de capacitaciones, seminarios, foros, reportes de empresas de seguridad, comunicados del CSIRT, ColCERT o CCOC.

A continuación, se observa una figura el cual entrelaza el plan de sensibilización, entrenamiento y educación:

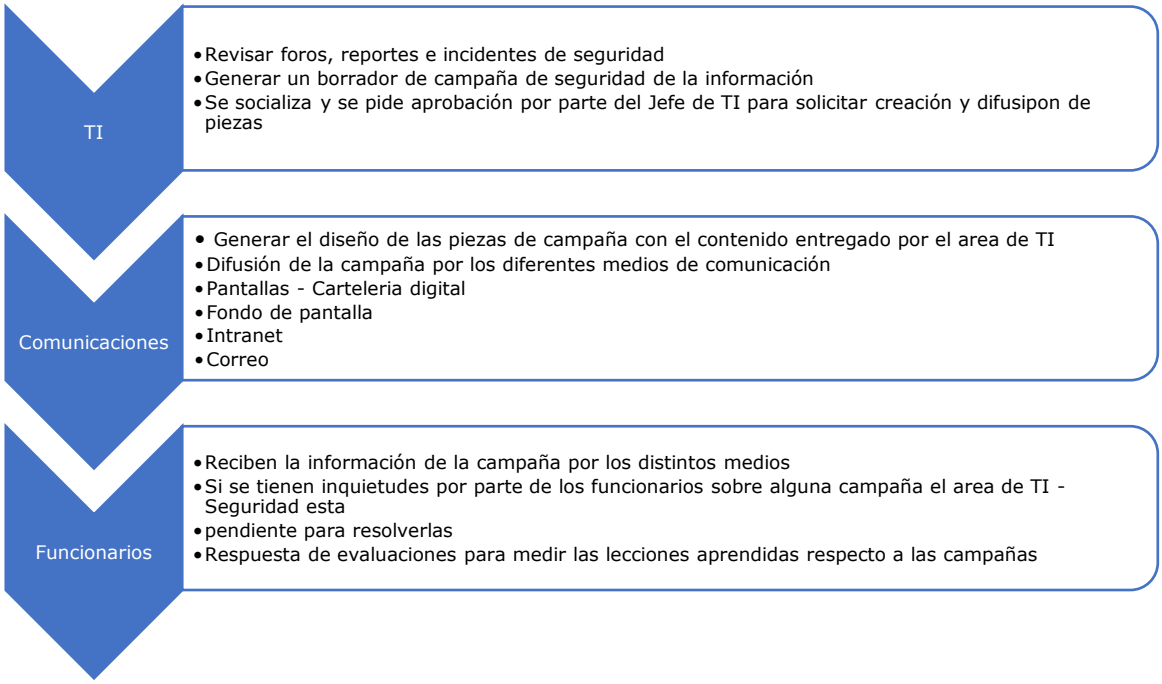
Ilustración 1 Esquema de capacitación



Sensibilización

El siguiente diagrama se observa el flujo donde se identifica las áreas y las actividades a realizas desde su diseño hasta la difusión de las diferentes campañas de seguridad de la información.

Ilustración 2 Esquema de capacitaciones



Para una continua sensibilización de los funcionarios y contratistas se debe generar como mínimo una campaña mensual.

ENTRANAMIENTO

El entrenamiento busca enseñar y fortalecer los conocimientos sobre seguridad de la información, para ello se plantea retomar las campañas realizadas y explicar con mayor detalle de manera presencial, permitiendo que la audiencia pueda expresar sus inquietudes y finalmente al terminar el entrenamiento se realizara una prueba escrita para medir si los funcionarios y contratistas entendieron a cabalidad los explicado o si es necesario reforzar con otro entrenamiento.

Para la fase de entrenamiento se plantea realizar como mínimo una vez al año.

EDUCACIÓN

El Oficial de Seguridad de la Información será el que lidera todos lineamientos de las campañas de sensibilización y entrenamiento e informar con suficiente antelación de la programación de las actividades de sensibilización al Gestor del Dominio de Uso y Apropiación del GAESI para que sean incluidas en el plan de formación de dicho dominio. Adicionalmente los dueños de sistemas y administradores deben tener un alto nivel técnico de seguridad de acuerdo a la relación que tienen con la plataforma que administra, a continuación, se listan los administradores:

- Administrador de seguridad perimetral
- Administrador del Antivirus
- Gestor de los Backups
- Administrador de los sistemas operativos
- Administrador del WSUS
- Los administradores de aplicaciones
- Administrador del Directorio Activo, DHCP y DNS
- Administrador del correo

El oficial de seguridad deberá asistir a todos los eventos o seminarios de CCOC, CSIRT, ColCERT y otros, para su formación permitiendo estar a la vanguardia en Ciberseguridad y Ciberdefensa.

IDENTIFICACIÓN DE ROLES

Para desarrollar el plan de manera apropiada, es necesario la clasificación de roles y sus responsabilidades para cada una de las dependencias o cargos

involucrados, a continuación, se define cada rol y los diferentes objetivos especiales de conocimiento:

Oficial de seguridad	Es el asesor experto en seguridad y quien diseña y ejecuta el plan de capacitación, sensibilización y entrenamiento
Área de comunicaciones	Es el área encargada de generar los diseños de las piezas a difundir por los distintos medios
Líderes de área	Deben conocer y entender las políticas y directivas que forman la base del programa de seguridad, también deben comprender el liderazgo que su rol tiene y que son el ejemplo a seguir
Dueños de sistemas	Deben entender bien las políticas en seguridad, así como también conocer sobre los controles de seguridad y la relación que tiene con los sistemas que manejan
Administradores de sistemas y personal de soporte	Deben tener un buen nivel de preparación a nivel técnico de seguridad (implementación y prácticas de seguridad efectivas) para soportar las operaciones críticas de la Entidad de manera apropiada
Usuarios finales	Requieren de un alto grado de sensibilización sobre la seguridad y las reglas de comportamiento adecuadas con los sistemas que tienen a disposición
Gestor del Dominio de Uso y Apropiación	Profesional del GAESI responsable de consolidar todas las capacitaciones de proyectos TI para su divulgación, socialización y culturización en el IDEAM.

CRONOGRAMA DE ACTIVIDADES DE SESIBILIZACIÓN, ENTRANAMIENTO Y EDUCACIÓN

El cronograma para este plan de capacitaciones es el que se defina en el Plan de formación que contempla la estrategia de **Uso y Apropiación** que ha diseñado la oficina de Informática para el IDEAM, con el cumplimiento de esta estrategia

se da cumplimiento a los lineamientos de Seguridad y privacidad de la información y del dominio de Uso y Apropiación. Las campañas de sensibilización se darán conforme a las nuevas vulnerabilidades o amenazas que se den en su momento o se tipifiquen a nivel internacional, de igual manera se pueden adicionar eventos en el ámbito de educación que generen valor para el fortalecimiento en Ciberseguridad y Ciberdefensa.

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.* Organización Internacional de Normalización.

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.

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

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

Control de cambios

Versión	Fecha	Descripción
01	17/05/2018	creación del documento
02	16/07/2018	Actualización del documento
03	30/11/2018	Actualización del documento
04	11/11/2021	Actualización del documento
05	15/07/2025	Se ajusta código del documento E-SGI-SI-M006 por SGI-M009, se ajusta a imagen institucional