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 y que se establece en el documento denominado "**E-GI-G004 GUÍA ESTRATEGÍA USO Y APROPIACIÓN**" el cual se encuentra publicado en el macroproceso estratégico de TI "Gestión de Tecnología de Información y comunicaciones.".

GLOSARIO:

- **Sensibilización:** Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.
- **Entrenamiento:** Proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas a su cargo.
- **Política:** Declaraciones de alto nivel que expresan los objetivos a cumplir de la entidad respecto a algún tema en particular.
- **Ingeniería Social:** Tipo de ataque de seguridad en la cual un individuo manipula al otro con el fin de obtener información que puede ser utilizada para acceder a un sistema no autorizado, sustraer dinero o incluso suplantar la identidad de la víctima.
- **CSIRT(Computer Security Incident Response Team):** Es el equipo de respuesta a incidentes el cual coordina las actividades para la recuperación en el menor tiempo posible generando el menor, para impacto,
- **ColCERT(Grupo de Respuesta a Emergencia Cibernéticas de Colombia):** son los responsables de la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional.
- **CCOC(Comando Conjunto Cibernético):** es una unidad creada con la finalidad de atender todas las amenazas cibernéticas a nivel nacional al estado, al gobierno y fuerzas militares.

PLAN DE SENSIBILIZACIÓN, ENTRENAMIENTO Y EDUCACIÓN

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:

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.

TI

- Revisar foros, reportes e incidentes de seguridad
- Generar un borrador de campaña de seguridad de la información
- Se socializa y se pide aprobación por parte del Jefe de TI para solicitar creación y difusipon de piezas

Comunicaciones

- Generar el diseño de las piezas de campaña con el contenido entregado por el area de TI
- Difusión de la campaña por los diferentes medios de comunicación
  - Pantallas - Carteleria digital
  - Fondo de pantalla
  - Intranet
  - Correo

Funcionarios

- Reciben la información de la campaña por los distintos medios
- Si se tienen inquietudes por parte de los funcionarios sobre alguna campaña el area de TI - Seguridad esta pendiente para resolverlas
- Respuesta de evaluaciones para medir las lecciones aprendidas respecto a las campañas

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 plataformaque 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 y que se establece en el documento denominado "**E-GI-G004 GUÍA ESTRATEGÍA USO Y APROPIACIÓN**" el cual se encuentra publicado en el macroproceso estratégico de TI "Gestión de Tecnología de Información y comunicaciones." 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 deeducación que generen valor para el fortalecimiento en Ciberseguridad y Ciberdefensa.

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

Elaboró:	Revisó:	Aprobó:
		
Harbey Martínez Guerrero CISO IMPRECTICS - IDEAM	**Eduardo Ramírez Acosta** Coordinador GAESI Oficina de Informática	**Alicia Barón Leguizamón** Jefa Oficina de Informática