MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

PLAN DE SENSIBILIZACIÓN Y COMUNICACIONES EN SEGURIDAD DE LA INFORMACIÓN

PROCESO

Gestión Estratégica de Tecnologías de la Información

Versión 1

28/12/2022

MADSIG
Sistema Integrado de Gestión

Contenido

1. INTRODUCCIÓN

Este documento describe en forma detallada el plan de sensibilización en seguridad de la información para la vigencia 2022- en el Ministerio de Ambiente y Desarrollo Sostenible (Minambiente) adicionalmente se describe el alcance del programa, actividades y metas a alcanzar.

También se presenta el Plan de Sensibilización para funcionarios y contratistas del Minambiente, relacionado con las temáticas de: (a) políticas de seguridad de la información, (b) procedimientos de seguridad de la información y (c) normas legales que soportan el sistema de gestión de seguridad de la información, (d) Amenazas Informáticas, etc. con el propósito de concientizar a los diferentes colaboradores de la entidad como son funcionarios, contratistas, sobre la importancia de dichos temas, su relación con la ejecución de las actividades diarias y el cumplimiento de la misionalidad de la institución, para garantizar el buen uso y la privacidad de la información.

2. OBJETIVO PRINCIPAL

Realizar la definición de las actividades a ejecutar durante el periodo 2022 necesarias para comunicar y concientizar a los funcionarios y contratistas del Minambiente en la importancia de proteger la información institucional y así impactar y reforzar las buenas prácticas, para el buen uso y la privacidad de la información.

2.1. Objetivos Específicos

- Fortalecer las capacidades institucionales para prevenir y dar respuesta a eventos de seguridad.
- Gestionar mecanismos de sensibilización como charlas, webinar, correos electrónicos y un curso virtual.

3. ALINEACIÓN A LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

El plan de sensibilización en seguridad de la información está alineado con la normativa aplicada para los sistemas de seguridad de la información bajo la norma ISO 27001:2013 y las directrices emitidas por el Ministerio de Tecnologías de la Información y con la política de seguridad de la información en la medida que permite "la participación de los funcionarios, contratistas y terceros en lograr el nivel de cumplimiento adecuado de los lineamientos y requisitos de seguridad de la información".

4. ALCANCE

Dirigido a todos los funcionarios y contratistas del Ministerio de Ambiente y Desarrollo Sostenible se verán beneficiados con este plan de sensibilización al obtener un conocimiento adecuado de cómo manejar con seguridad su información en distintos dispositivos electrónicos.

5. DESCRIPCIÓN

Este numeral muestra la forma bajo la cual se organizan las actividades y los elementos necesarios para realizar las diferentes sensibilizaciones a los funcionarios y contratistas del Minambiente lo cual se muestra en la siguiente

- Determinar los Grupos de Interés: Consiste en definir grupos generales para organizar a los funcionarios, contratistas y la alta gerencia del Minambiente de acuerdo con las funciones u obligaciones que desempeñan y así poder transmitir los mensajes
- Definir la Estrategia de Comunicación: Identificar la forma en la que se desea hacer llegar el mensaje a los diferentes grupos.
- Definir los Canales de Comunicación: Identificar los medios para la divulgación interna, haciendo uso de las herramientas que tiene establecidas actualmente la oficina de comunicaciones de la entidad.
- Plan de Trabajo: Definir la secuencia de actividades para realizar la mejor distribución de los recursos disponibles entre las partes y así llevar a cabo la sensibilización

6. METAS DEL PLAN DE SENSIBILIZACIÓN

El programa de sensibilización en seguridad de la información para la vigencia 2022 tiene como metas principales:

- Comunicar formalmente a toda la entidad la existencia del sistema de gestión de seguridad de la información y sus componentes de apoyo.
- Socializar a todo el personal de la Entidad las políticas de seguridad de la información.
- Socializar los principales procedimientos de seguridad de la información.
- Fomentar la cultura de la seguridad de la información como estrategia de protección de la información institucional.
- Explicar de manera sencilla las normas legales que soportan el sistema de gestión de seguridad de la información.
- Divulgar a todos los funcionarios y contratistas los principales riesgos de seguridad de la información.
- en manera clara en qué consisten diversos tipos de ataques informáticos y cómo controlarlos.
- Comunicar los mecanismos de control dispuestos por la entidad para evitar ataques informáticos.

7. ROLES INVOLUCRADOS

7.1. Directivos

El nivel directivo de Minambiente apoyarán el desarrollo del plan de sensibilización en seguridad de la información mediante acciones como:

conocer y entender los lineamientos y directrices que forman la base para la seguridad de la información, también deben comprender el liderazgo que su rol tiene en la Entidad, ya que son el ejemplo a seguir, por parte de los grupos internos de trabajo y colaboradores en general.

- Autorizar y fomentar en los colaboradores bajo su responsabilidad la participación en las sesiones presenciales o virtuales de sensibilización que se desarrollen durante la vigencia.
- Fomentar la implementación y cumplimiento de las buenas prácticas de seguridad que se divulgarán en la ejecución del plan de sensibilización.
- Participar de acuerdo con su disponibilidad en las actividades del plan de sensibilización.

7.2. Líderes de Procesos

- Coordinar al interior de sus dependencias la participación de los colaboradores en las actividades del plan de sensibilización.
- Participar en las actividades de sensibilización en seguridad programadas de acuerdo con su disponibilidad de tiempo.
- Velar porque en las actividades de sus procesos apliquen las recomendaciones e instrucciones en materia de seguridad que se divulguen en el marco del plan de sensibilización en seguridad de la información.
- Medir la eficacia de los resultados de las actividades de sensibilización en las que participan los colaboradores de sus procesos.
- Identificar y comunicar las necesidades particulares en materia de sensibilización o capacitación en seguridad de la información para su proceso, colaboradores o para la Entidad.

7.3. Responsables de la Seguridad de la Información

- Diseñar el plan de sensibilización en seguridad de la información, teniendo presente la misión de la Entidad y la relevancia que se busca para la cultura de seguridad de la información de la Entidad.
- Identificar las necesidades y las prioridades que tenga la Entidad respecto al tema de sensibilización en seguridad de la información.
- Apoyar la elaboración de las piezas comunicativas, presentaciones, encuestas
- Ejecutar y apoyar las actividades de programa de sensibilización.
- Identificar oportunidades de mejora para la planificación, diseño, implementación y evaluación del programa de sensibilización.

7.4. Administradores de Sistemas de Información y Plataformas

- Participar en las actividades de sensibilización en seguridad de la información de acuerdo con su disponibilidad de tiempo y directrices de los responsables de procesos de la Entidad.
- Identificar los mecanismos que permitan implementar las recomendaciones y buenas prácticas del programa de sensibilización.
- Fomentar la implementación de las buenas prácticas de seguridad de la información propuestas por las campañas de sensibilización.

7.5. Colaboradores del Ministerio de Ambiente y Desarrollo Sostenible

- Participar en las actividades del programa de sensibilización de acuerdo con la coordinación que realice el líder del proceso.
- Identificar formas de implementar en sus actividades diarias las recomendaciones y buenas prácticas del programa de sensibilización.
- Participar en la evaluación de la calidad, impacto y efectividad de las actividades del programa de sensibilización.
- Identificar oportunidades para el mejoramiento del programa de sensibilización, mediante encuestas.

8. ÉSTRATÈGIA DE COMUNICACIONES

Este numeral muestra las consideraciones que se deben tener en cuenta para el desarrollo del presente plan de sensibilización y que permiten articular el desarrollo de las actividades y transmitir los mensajes/información adecuada.

Tabla 1. Estrategias De Comunicación

Estrategia	Descripción
Campaña de Expectativa	Difundir mensajes para estimular el interés y así lograr que las personas quieran obtener más información. Para esto, se debe realizar una comunicación masiva, utilizando los medios digitales como la intranet, el correo institucional del Minambiente, charlas o medios físicos como carteleras.
Participación alta Dirección	Transmitir mensajes de forma directa sobre la importancia/impacto de la seguridad de la información, y como están relacionados con el cumplimiento de los objetivos institucionales, para dar alcance a la política de Gobierno Digital de MinTIC y así comprometerlos con su implementación. por medio de un canal de comunicación directo como una sesión de trabajo conjunta para transmitir la información y atender dudas.
Capacitación en Seguridad de la Información	Realizar sesiones de capacitación de los diferentes funcionarios y contratistas de la entidad en las temáticas abajo descritas.

9. CANALES DE COMUNICACIÓN

A continuación, se describen los canales de comunicación disponibles en la entidad con los cuales se deberán alcanzar los objetivos de los mensajes a trasmitir:

10. AUDIENCIA OBJETIVO

Todos los colaboradores del Minambiente se verán beneficiados con este proyecto al obtener un conocimiento adecuado de cómo manejar con seguridad su información en distintos dispositivos electrónicos.

11. TEMÁTICAS DEL PLAN DE SENSIBILIZACIÓN PLAN DE TRABAJO

A continuación, se presenta el orden secuencial de las actividades y su distribución en el tiempo que se tomarán las capacitaciones, charlas y conferencias durante el año 2022.

A continuación, se relacionan las temáticas a desarrollar en el plan de trabajo.

Conocimiento general del Subsistema de Gestión de Seguridad de la Información, se socializarán conocimientos fundamentales de la seguridad de la información como:

- Concepto de seguridad de la información
- Qué es un riesgo de seguridad de la información
- Cómo está estructurado el sistema de gestión de seguridad de la información
- Quienes son los actores del sistema de gestión de seguridad de la información Conocimiento de las políticas de seguridad de la información
- Explicación de la política general de la seguridad de la información
- Explicación del procedimiento de clasificación y etiquetado de información
- Explicación del procedimiento de Acceso a áreas seguras
- Metodología de gestión de riesgos y su anexo para identificación de riesgos de seguridad Amenazas informáticas
- Phishing
- Rasonware
- Robo de identidad Generalidades sobre regulación en materia de seguridad de la información
- Ley de transparencia y acceso a la información
- Ley de protección de datos personales
- Estrategia de gobierno en línea Atención y respuesta a incidentes de seguridad de la información
- Curso de primeros respondientes en incidentes de seguridad de la información Actividades de sensibilización programadas
- Campaña de sensibilización
- Charlas y conferencias
- Mensajes de correo electrónico informando en que consiste un Phishing, Malware y Rasonware
- Publicaciones en pantallas Materiales y recursos
- Pantallas institucionales.
- Screensavers con mensajes de sensibilización.
- Boletines vía email. Evaluación, Mejora y Seguimiento

12. OBJETIVO

Sensibilizar a los colaboradores de Minambiente en las buenas prácticas que existen en torno a la seguridad de la Información.

13. RESULTADOS ESPERADOS

Se espera generar una cultura con respecto al uso responsable de la información, que se cambien los malos hábitos considerados como inseguros por comportamientos seguros respecto a la protección de la información institucional y de carácter personal. Dentro de las temáticas que se abordarán se contempla:

- Bloqueo de la sesión de trabajo al dejar solo el puesto de trabajo
- Uso de contraseñas seguras
- Mantenimiento del escritorio despejado y la pantalla limpia de información sensible
- Control de acceso a las áreas de almacenamiento y procesamiento de información clasificada y reservada
- Clasificación de la información para su apropiada protección
- Políticas y procedimientos del subsistema de gestión de seguridad de la información

14. LOCALIZACIÓN

Las distintas actividades se disponen para ser realizadas de manera virtual y algunas presenciales conforme a lo establecido por la contingencia nacional Covid-19 a los colaboradores del Minambiente para facilitar el acceso de todos los interesados.

El proyecto se desarrollará en un tiempo de 9 meses para las distintas actividades planeadas, su fecha estimada de inicio es en el mes de marzo hasta noviembre del 2022.

15. ACTIVIDADES DEFINIDAS

- Actividad Escritorio Limpio, por medio de la Alternancia y aleatoriamente se identificarán estaciones de trabajo desatendidas en las cuales se colocará un cartel con imagen de seguridad, se tomará una foto y se publicará en la intranet
- Lanzamiento de una Actividad que genere conciencia y mediante un curso virtual en alianza con FORTINET se envían tips de seguridad, los usuarios deben aprender que los delincuentes también envían mensajes para atacar a los usuarios.

15.1. Charlas – Conferencias

Se propone la realización de las siguientes charlas con duración máximo de 1 hora cada una.

De manera hibrida (virtual, presencial o Hibrida)

- Ley de protección de datos personales
- Escritorio y pantalla limpios
- Formas comunes de ataque informático
- Riesgos de Seguridad de la Información al personal del nivel estratégico
- Identificación, clasificación, actualización y gestión de riesgos de los Activos de Información
- Adopción del Decreto 338 de 2022

15.2. Charlas de sensibilización

Identificación, actualización de activos de información y gestión de riesgos

OBJETIVO: Explicar a todos los colaboradores del Minambiente qué es y para qué sirve la identificación, actualización de los activos de información y la gestión de los riesgos de estos

- **ACTIVIDAD:** Clase Virtual
- **CÓMO:** Exposición
- **TIEMPO:** 45 minutos
- **CUANDO**: Marzo 10 de 2022
- **RESPONSABLE:** Ing. Iván Ontibon (MINTIC)
- **RECURSOS:** Plataforma de Educación Virtual
- **RESULTADOS:** Los participantes podrán explicar cuáles son los beneficios de identificar, actualizar y gestionar los riesgos producto de los activos de información

15.3. Secuestro de información o RASONWARE

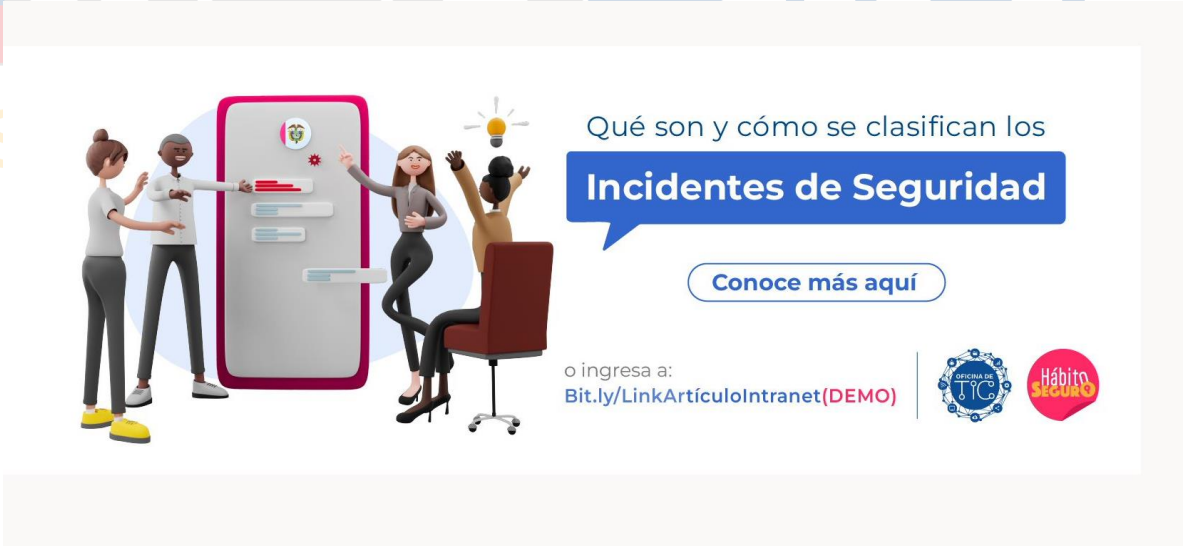
OBJETIVO: Explicar a los colaboradores del Minambiente y entidades adscritas qué es un secuestro de información, experiencia vivida e implicaciones

- **ACTIVIDAD:** Clase Virtual
- **TIEMPO:** 1 hora
- **CUANDO:** abril 22 de 2022
- **RESPONSABLE:** Ing. Juan Manuel Palacio Posada (jefe de TIC del INVIMA)
- **RESULTADOS:** socializar experiencias de entidades del Estado que han sido víctimas de Rasonware

15.4. Riesgos de seguridad de la información dirigida al nivel estratégico

- **OBJETIVO:** Explicar a las directivas del Minambiente, la importancia de conocer, afrontar, mitigar y generar conciencia sobre el tema de riesgos de seguridad de la información
- **ACTIVIDAD:** presencial
- **TIEMPO:** 45 minutos
- **CUANDO:** 25 de mayo de 2022
- **RESPONSABLE:** Ing. Iván Ontibon (MINTIC)
- **RECURSOS:** Salón Colombia, 4 piso del Minambiente
- **RESULTADOS:** sensibilizar a la alta gerencia con respecto a los compromisos al momento de afrontar, mitigar y generar conciencia sobre el tema de riesgos de seguridad de la información.

15.5. Infografía socializada por medio de la Intranet y correo institucional Clasificación delitos informáticos eso fue en junio



15.6. Adopción sobre el Decreto 338 de 2022

Curso Virtual sobre concientización en temas de Seguridad de la Información

- **OBJETIVO:** Sensibilizar a la población del Ministerio en conceptos básicos sobre seguridad de la información
- **ACTIVIDAD:** virtual

- **TIEMPO:** por demanda por módulos
- CUANDO: inicia la 3ra semana de octubre y termina 1ra semana de noviembre de 2022
- **RESPONSABLE:** Equipo de Seguridad de la información y Uso Apropiación de TI
- **RECURSOS:** PLATAFORMA VIRTUAL (FORTINET)
- **RESULTADOS:** Medir el nivel de conocimiento en seguridad de la información de los participantes

15.7. Conocimiento de Dominio A.11.2.9 Política de escritorio limpio y pantalla despejada

- **OBJETIVO:** Explicar a los colaboradores del Minambiente, por qué la importancia bloquear la pantalla del PC cada vez que se levante del puesto y mantener el escritorio limpio de información sensible
- **ACTIVIDAD:** Virtual
- **TIEMPO:** 45 minutos
- **HORA:** 10: 00 AM
- **CUANDO:** 13 de julio de 2022
- **RESPONSABLE:** Ing. Artuz Giovani
- **RECURSOS:** Charla vía TEAMS
- **RESULTADOS:** Los participantes podrán entender. la importancia bloquear la pantalla del PC cada vez que se levante del puesto y mantener el escritorio limpio de información sensible

15.8. Formas comunes de Amenazas y Ataques informáticos

- **OBJETIVO:** explicar a los colaboradores el modus operandi de los ataques informáticos más comunes
- **ACTIVIDAD**: Hibrida
- **TIEMPO:** 45 minutos
- **HORA:** 10: 00 AM
- **CUANDO:** 27 de Julio de 2022
- **RESPONSABLE:** Ing. Arthuz Diaz
- **RECURSOS:** Auditorio Principal del Minambiente y herramienta TEAMS
- **RESULTADOS:** Los participantes podrán conocer cómo se pueden identificar y proteger de los ataques informáticos más comúnmente utilizados.

15.9. Socialización sobre el Decreto 338 y la Resolución 0500

- **OBJETIVO:** explicar a los enlaces de las entidades del sector adscritas y vinculadas, sobre la adopción del decreto 338 y el instrumento de la resolución 0500

- ACTIVIDAD: virtual
- TIEMPO: 45 minutos
- HORA: 11: 00 AM
- CUANDO: 28 de septiembre de 2022
- RESPONSABLE: Ing. Danny Garzón
- RECURSOS: TEAMS

15.10. Socialización sobre conceptos básicos de la Ley protección de datos personales

- **OBJETIVO**: socializar al equipo de la OTIC con apoyo de la Oficina Jurídica, algunos conceptos de la Ley de protección de datos personales
- **ACTIVIDAD:** Virtual
- **TIEMPO:** 45 minutos
- **HORA:** 10: 00 AM
- **CUANDO:** 11 de noviembre de 2022
- **RESPONSABLE:** Ing. René Alvarado
- **RECURSOS:** TEAMS

- Workshop Ruta 22 “Camino Ha SIAC las TIC”
- Tema: Riesgos en la Transformación Digital
- 30 de noviembre
- Conferenciante: Ivan Ontibon, MINTIC

Entre los meses de septiembre (14 y 15) y noviembre (3) del 2022, los funcionarios de la OTIC **Oliver Sanchez** y **René Alvarado** participaron de manera activa en la sensibilización sobre temas generales de la Seguridad de la Información en las jornadas de inducción que el Grupo de Talento Humano programó dirigida a los servidores públicos que se posesionaron producto de la convocatoria de la Comisión Nacional del Servicio Civil.

16. GLOSARIO DE TÉRMINOS

a. **Activo de información:** Cualquier información que tiene valor para la Entidad y para el Sistema de Gestión de Seguridad de la Información. Se consideran también los recursos humanos, tecnológicos que intervienen en el tratamiento directo o indirecto de la información, así como sus procesos y actividades.
b. **Amenazas:** Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.
c. **Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o entidades no autorizados
d. **Control:** Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la entidad que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
e. **Disponibilidad:** Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada.
f. **Gestión de riesgo:** Aplicación sistemática de políticas de gestión procedimientos y prácticas a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión de riesgos.
g. **Incidente de Seguridad de la Información:** Evento no deseado que genera amenaza a la seguridad de la información y que tiene una probabilidad significativa de comprometer a la operatividad de la Entidad
h. **Información:** Cualquier forma de registro de contenidos susceptibles a ser procesados, distribuidos y almacenados, pudiendo estar en formato electrónico, óptico, magnéticos u otro medio de almacenamiento.
i. **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.
j. **Integridad:** Propiedad de precisión y completitud de la información.
k. **Oficial de Seguridad de la Información:** El Oficial de Seguridad de la Información es el responsable del Sistema de Gestión de la Seguridad de la Información (SGSI) y reporta al jefe de la Oficina TIC y al Comité Integrado de Gestión y Desempeño (CIGD).

l. **Colaboradores del Minambiente:** Comprende a los servidores públicos como funcionarios, Contratistas, Personal externos (empresa de vigilancia y personal de servicios generales) designados o asignados bajo Contratación Administrativa de Servicios; y visitantes.

m. **Propietario del activo:** Es el funcionario asignado de garantizar que el activo asignado bajo su responsabilidad esté protegido con los controles definidos en el SGSI y que le apliquen a dicho activo; es el responsable por la afectación de la confidencialidad, integridad y disponibilidad de este, en cualquiera de los procesos que se encuentre involucrado.

n. **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen institucional, etc.) y se pueden aplicar a niveles diferentes (operativo, estratégico, organización).

o. **Seguridad de la Información:** Todas las acciones orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los activos asociados a su tratamiento independiente de la forma en la que la información se encuentre

p. **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.

q. **Sistema de Gestión de la Seguridad de la Información (SGSI):** Es un componente del sistema de gestión de una organización, con base en un enfoque de riesgos, que tiene como función establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. El SGSI está conformado por políticas, procedimientos, directrices, recursos y actividades asociadas, gestionadas por la organización, en la búsqueda de la protección de sus activos de información.

r. **Vulnerabilidad:** Debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad o disponibilidad de dicho activo.

17. DESCRIPCIÓN GENERAL DEL PLAN

17.1. Metas

- El MINAMBIENTE define las siguientes metas a cumplir durante la ejecución del plan de concientización y sensibilización para el Sistema de Gestión de Seguridad de la Información (SGSI):
- Formalizar la comunicación y difusión de la existencia y ejecución de las actividades del SGSI dentro de su alcance.
- Difundir y fomentar una cultura de seguridad de la información para el personal de la institución.

- Dar a conocer las directivas, lineamientos, disposiciones y procedimientos que forman parte del SGSI.
- Socializar con el personal de la institución los principales riesgos de seguridad de la información.
- Prevenir la materialización de los riesgos de seguridad de la información identificados, dando a conocer y explicando al personal de la institución los mecanismos de control establecidos mediante el SGSI.

17.2. Audiencia Objetiva

La implementación y ejecución del presente plan está orientado a comunicar, y sensibilizar el personal (funcionarios y Contratistas), acerca del adecuado manejo de la información institucional y el cumplimiento de las directivas, lineamientos, disposiciones, procedimientos e instrucciones de trabajo establecidos por el SGSI.

El MINAMBIENTE a través del área pertinente, podrán realizar y aplicar encuestas o actividades para recopilar información que permita identificar nuestros públicos objetivos, conocer sus características y perfiles con la finalidad de diseñar y ejecutar estrategias y/o campañas específicas que contribuyan al cumplimiento del presente plan.

Con el fin de orientar de manera efectiva las actividades y estrategias de cumplimiento se han considerado los siguientes roles:

Directivos (as)	Temas relacionados con la normatividad aplicable, generación de conciencia, compromiso y liderazgo con el SGSI.
Personal de Seguridad de la Información	Formación en temas relacionados con la norma de seguridad de la información, ciberseguridad, buenas prácticas de TI y lineamientos de seguridad. Prepararse para gestionar el SGSI

Administradores de sistemas de información, aplicaciones y personal de soporte (OTIC)	Conocer y comprender los lineamientos, procedimientos y controles del SGSI, fortalecer competencias técnicas en seguridad informática y buenas prácticas de TI, todo ello con la finalidad de contar
Usuarios finales	Fortalecer los niveles de concienciación en seguridad de la información, cumplimiento de los lineamientos, controles, recomendaciones y buenas prácticas del SGSI, así como la responsabilidad en el uso de los sistemas y aplicaciones, así como con el manejo de información institucional.