



Plan de Sensibilización y Comunicación en Seguridad de la Información 2024

Proceso
Gestión Estratégica de
Tecnologías de la Información
Versión 1
31/01/2024

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	Plan de Sensibilización y Comunicación en Seguridad de la Información	 Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 31/01/2024	Código: DS-E-GET-34

CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVO GENERAL	4
3. OBJETIVOS ESPECÍFICOS	4
4. ALCANCE	4
5. DEFINICIONES.....	4
6. MARCO LEGAL	5
7. GRUPOS DE INTERES.....	6
8. CANALES DE COMUNICACIÓN Y DIVULGACIÓN	7
9. IMPLEMENTACIÓN DEL PLAN DE SENSIBILIZACIÓN.....	8
10. CRONOGRAMA DE SENSIBILIZACIÓN PARA LA VIGENCIA 2024.....	8
11. ENCUESTA DE PERCEPCIÓN DE LA CULTURA DE SEGURIDAD DE LA INFORMACIÓN.....	9
12. MONITOREO Y MEJORA CONTINUA DEL PLAN	9
13. INDICADOR DE CUMPLIMIENTO DEL PLAN	10



SC-2000142



SA-2000143

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	Plan de Sensibilización y Comunicación en Seguridad de la Información	
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 31/01/2024	Código: DS-E-GET-34

1. INTRODUCCIÓN

El continuo crecimiento y evolución de las tecnologías de la información y las comunicaciones han permitido mejorar de manera significativa el crecimiento, desarrollo de las actividades propias de las Entidades públicas como de la empresa privada. En el mismo sentido de avance en los entornos digitales, se han masificado las vulnerabilidades y amenazas que afectan tanto a la tecnología como a los usuarios, por esta razón se requiere generar la cultura de sensibilización en materia de seguridad de la información, cuyo objetivo es socializar y generar conciencia en el recurso humano que apoya las funciones y operaciones del Ministerio, para fortalecer las debilidades y gestar buenas prácticas de seguridad de la información que se deben tener en cuenta o implementar en cada una de las instancias de la Entidad.

Cuando se habla de seguridad y privacidad de la información, es necesario que exista un trabajo articulado entre procesos, recursos tecnológicos, medidas de seguridad y personas, con el propósito de proteger la información institucional, reduciendo de esta forma la posibilidad de materialización de riesgos de seguridad de la información a los que día a día están expuestos los datos, información sin importar el medio en que se encuentre, aplicativos, medios de comunicación, redes sociales y demás entornos en los cuales se genere, transforme, almacene y divulgue.

Por lo anterior, se requiere definir y ejecutar el Plan de Sensibilización de Seguridad de la Información, el cual no se enfoca únicamente en el aseguramiento de plataformas e implementación de controles técnicos, sino que, involucra de forma directa al talento humano que conforma la Entidad, toda vez que, son el eslabón más débil del ciclo de seguridad de la información, teniendo en cuenta que, por más medidas, lineamientos, políticas, controles y dispositivos de seguridad que se implementen, si las personas hacen mal uso o caso omiso de los mismos, es aquí en donde se pueden explotar vulnerabilidades, que pueden conllevar a la materialización de riesgos, pérdida de información, y posible afectación de la reputación del Ministerio y como consecuencia la pérdida de confianza por parte de los interesados.

En tal sentido, el presente documento va dirigido a todos los colaboradores del Ministerio de Ambiente y Desarrollo Sostenible (Ambiente), buscando fortalecer el conocimiento de las Políticas Específicas de Seguridad de la Información, buenas prácticas de seguridad, divulgación de alertas, engaños, nuevos ataques cibernéticos y de esta forma generar conocimiento previo en caso de enfrentar amenazas, eventos e incidentes de seguridad de la información que atenten contra la seguridad y privacidad de la misma, en el ámbito institucional y cotidiano.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	Plan de Sensibilización y Comunicación en Seguridad de la Información	
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 31/01/2024	Código: DS-E-GET-34

2. OBJETIVO GENERAL

Establecer la estrategia, metodología y actividades de sensibilización y entrenamiento para fortalecer la cultura organizacional de Seguridad y Privacidad de la Información del Ministerio de Ambiente y Desarrollo Sostenible, contribuyendo a la apropiación de conceptos que se derivan de la preservación, confidencialidad, integridad y disponibilidad de la Información.

3. OBJETIVOS ESPECÍFICOS

- Definir los temas y actividades para las sensibilizaciones y entrenamiento en seguridad de la información y datos personales.
- Divulgar las políticas específicas de seguridad de la información.
- Dar a conocer a los diferentes grupos de interés sus roles y responsabilidades frente a la seguridad y privacidad de la información.
- Fortalecer las capacidades institucionales de respuesta y reacción ante incidentes de seguridad de la información.
- Implementar diferentes mecanismos de sensibilización como charlas, correos electrónicos, fondos de pantalla, carteleras y otras dinámicas para divulgar contenido de seguridad de la información.
- Fomentar el compromiso de los colaboradores de la Entidad respecto a las actividades y requerimientos del Sistema de Gestión de Seguridad de la Información – SGSI.
- Divulgar y socializar las principales amenazas cibernéticas, como medida preventiva para reducir la materialización de riesgos que puedan afectar la seguridad de la Información.
- Generar mecanismos para realizar mayor cobertura en el Ministerio.

4. ALCANCE

El Plan de Sensibilización y Comunicación de Seguridad de la Información aplica a todos los directivos, colaboradores, contratistas y demás partes interesadas del Ministerio de Ambiente y Desarrollo Sostenible, por lo cual se requiere de su participación en el desarrollo de las actividades previstas en el plan.

5. DEFINICIONES

Amenazas: Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	Plan de Sensibilización y Comunicación en Seguridad de la Información	 Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 31/01/2024	Código: DS-E-GET-34

Confidencialidad: Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o Entidades no autorizados

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.

Disponibilidad: Propiedad de ser accesible y utilizable ante la demanda de una Entidad autorizada.

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.

Incidentes 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

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.

Integridad: Propiedad de precisión y completitud de la información.

Colaboradores del Ministerio: 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.

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). m. 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 n. 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.

6. MARCO LEGAL

Directiva Presidencial 02: Febrero 24 de 2022, “Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC)”.



SC-2000142



SA-2000143

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	Plan de Sensibilización y Comunicación en Seguridad de la Información	 Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 31/01/2024	Código: DS-E-GET-34

Decreto 338: Marzo 8 de 2022, "Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".

Resolución 746: Marzo 11 de 2022, "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".

Decreto 767: Mayo 16 de 2022, "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Resolución 500: Marzo 10 de 2021, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".

Resolución 1519: Agosto 24 de 2020, "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".

Decreto 612: Abril 4 de 2018, "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado".

Decreto 886: Mayo 13 de 2014, "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos".

Decreto 1377: Junio 23 de 2013, "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".

Ley 1581: Octubre 17 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013".

7. GRUPOS DE INTERES

- Directivos: Ministro(a) Viceministros, Secretario General, Directores, Subdirectores, Jefes de Oficina y Coordinadores de Grupo.
- Equipo TIC (Infraestructura, Seguridad Perimetral, Desarrollo, Bases de datos, Sistemas de Información y Mesa de ayuda)
- Equipo de Seguridad de la Información.



SC-2000142



SA-2000143

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	Plan de Sensibilización y Comunicación en Seguridad de la Información	
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 31/01/2024	Código: DS-E-GET-34

- Procesos, Oficinas, Dependencias y Grupos Internos
- Colaboradores del Ministerio (funcionarios, contratistas)

8. CANALES DE COMUNICACIÓN Y DIVULGACIÓN

A continuación, se describen los canales de comunicación disponibles en la Entidad, con los cuales se contribuye a alcanzar los objetivos de la información que se va a divulgar:

Intranet: publicación de las presentaciones de las charlas de seguridad de la información realizadas, boletines y grabaciones de las sesiones.

Correos Masivos: a través de la cuenta de Comunicaciones, se dará a conocer a toda la Entidad los temas de seguridad de la información.

Boletines del Seguridad de la Información y Ciberseguridad: se remitirán boletines informativos por correo masivo para divulgar noticias, recomendaciones, buenas prácticas de seguridad, vulnerabilidades que afecten la Infraestructura tecnológica, e información relevante para los colaboradores del Ministerio, proveniente de las autoridades competentes como el Equipo de respuesta a incidentes de seguridad informática - CSIRT de Gobierno, Policía, entre otros medios oficiales.

Enlace o link a sesiones de charlas virtuales: se programarán en el calendario por parte del equipo de Seguridad de la Información o con el apoyo de Comunicaciones en los boletines informativos.

Charlas presenciales: se apoyarán espacios como las jornadas de inducción y reinducción para los funcionarios, en las cuales el Grupo de Talento Humano requiera el apoyo del equipo de Seguridad de la Información participando o realizando sesiones presenciales o virtuales según sea el caso para las diferentes áreas de la Entidad.

Eslogan de las piezas comunicativas: La Oficina de la Tecnologías de la Información y Comunicación - OTIC, divulgará el Eslogan "**LA SEGURIDAD DE LA INFORMACIÓN ES RESPONSABILIDAD DE TODOS**", el cual permitirá tener una mayor apropiación y sentido de pertenencia por parte de los colaboradores del Ministerio.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	Plan de Sensibilización y Comunicación en Seguridad de la Información	 Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 31/01/2024	Código: DS-E-GET-34

9. IMPLEMENTACIÓN DEL PLAN DE SENSIBILIZACIÓN

Con las sesiones de sensibilización y comunicación se busca divulgar políticas, lineamientos, buenas prácticas de Seguridad y Privacidad de la Información y demás temas de interés en materia de seguridad, dirigido a los colaboradores de la Entidad. La estrategia de divulgación del presente Plan, se realizará haciendo uso de los medios de comunicación institucionales, para lograr llegar a la mayor cantidad de funcionarios, contratistas y demás partes interesadas en el Ministerio; en las cuales se comunicará la importancia de la seguridad de la información, su cuidado y adecuado tratamiento.

10. CRONOGRAMA DE SENSIBILIZACIÓN PARA LA VIGENCIA 2024

Tema para socializar	Dirigido a	Medio Ejecución	Responsable	Escenario	Fecha
Registro Nacional de Bases de Datos Personales	Directivos, Jefes de Oficina, Coordinadores, Funcionarios y contratistas	Charlas de sensibilización, y socialización	Equipo de Seguridad de la Información	Reporte y Registro Nacional de Bases de Datos Personales	Febrero Marzo
Boletines de Seguridad de la Información	Funcionarios y contratistas	Correo masivo	Equipo de Seguridad de la Información	Correo electrónico	Trimestral o cuando se requiera
Activos de información	Funcionarios y contratistas	Charlas de sensibilización, y socialización	Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Marzo Abril
Gestión de Riesgos de seguridad de la información	Funcionarios y contratistas	Charlas de sensibilización, y socialización	Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Julio / septiembre
Manual de Políticas Específicas de Seguridad de la información y/o Política de Datos Personales	Funcionarios y contratistas	Charlas de sensibilización, y socialización	Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Mayo Noviembre
Gestión de Incidentes de Seguridad de la Información	Funcionarios y contratistas	Charlas de sensibilización, y socialización	Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Junio Septiembre



SC-2000142



SA-2000143

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	Plan de Sensibilización y Comunicación en Seguridad de la Información		
	Proceso: Gestión Estratégica de Tecnologías de la Información		
Versión: 1	Vigencia: 31/01/2024		Código: DS-E-GET-34

Charlas por demanda de temas de seguridad de la información	Funcionarios y contratistas	Charlas de sensibilización, y socialización	Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Cuando se requiera
Fondos de pantalla con tips de seguridad o información de actualidad	Directivos, Jefes de Oficina, Coordinadores, Funcionarios y contratistas	Piezas comunicativas	Equipo de Seguridad de la Información	Pantallas de las estaciones de trabajo	Trimestral o cuando se requiera
Charlas de seguridad de la información, con panelistas externos al Ministerio u otras entidades	Funcionarios y contratistas	Charlas de sensibilización, y socialización	Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	1 (una) por semestre

11. ENCUESTA DE PERCEPCIÓN DE LA CULTURA DE SEGURIDAD DE LA INFORMACIÓN

Como actividad complementaria a la divulgación de la información y actividades del Plan de Sensibilización y Comunicación en Seguridad de la Información, propiciando la cultura de seguridad y privacidad del Ministerio. El Equipo de seguridad de la Información, aplicará encuestas aleatorias que servirán como instrumento de medición y percepción de la información comunicada, así como la importancia y comprensión de la misma.

12. MONITOREO Y MEJORA CONTINUA DEL PLAN

Con el objetivo de evidenciar la ejecución de las actividades del Plan de Sensibilización y Comunicación en Seguridad de la Información, se dispondrá de los siguientes soportes:

- Encuestas o evaluaciones (aleatorias) de los conocimientos adquiridos en seguridad de la información y datos personales. (PDF)
- Presentaciones o piezas de comunicativas.
- Listados de asistencia de colaboradores que asistieron a las sensibilizaciones. (XLS, PDF o Pantallazos)



SC-2000142



SA-2000143

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	Plan de Sensibilización y Comunicación en Seguridad de la Información	 Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 31/01/2024	Código: DS-E-GET-34

13. INDICADOR DE CUMPLIMIENTO DEL PLAN

Como indicador clave para la cobertura del Plan de Sensibilización y Comunicación en Seguridad de la Información en el Ministerio, se define el siguiente:

Nombre del Indicador:	Cobertura del Plan de Sensibilización y Comunicación del SGSI
Formula del Indicador:	(No. colaboradores asistentes a las sesiones de sensibilización / No. de colaboradores propuestos en el semestre dentro del plan de sensibilización) * 100%
Responsable del Indicador:	Jefe Oficina TIC
Utilidad del Indicador:	Realizar el seguimiento de cobertura a las sesiones de entrenamiento o sensibilización del SGSI

