MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

PLAN DE SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN – 2023

PROCESO

Gestión Estratégica de Tecnologías de la Información

Versión 2

31/03/2023

MADSIG
Sistema Integrado de Gestión

TABLA DE CONTENIDO

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, frente a debilidades y buenas prácticas de seguridad 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 la información del Ministerio.

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 ciudadanos.

En tal sentido, el presente documento va dirigido a todos los colaboradores del Ministerio de Ambiente y Desarrollo Sostenible (Minambiente), 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, tanto en el ámbito institucional como en el personal.

2. OBJETIVO GENERAL

Establecer la estrategia 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 preservación de la confidencialidad, integridad y disponibilidad de la Información.

2.1. 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 funcionarios y contratistas 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 mecanismos de sensibilización como charlas, correos electrónicos, fondos de pantalla, carteleras y demás 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.

3. ALCANCE

El Plan de Sensibilización y Comunicación de Seguridad de la Información aplica a todos los colaboradores del Ministerio de Ambiente y Desarrollo Sostenible.

4. ROLES Y RESPONSABILIDADES

ROLES	RESPONSABILIDADES
ALTA DIRECCIÓN: Ministra (o), Viceministros, Secretario General, Directores, Subdirectores, Jefes de Oficina.	Es su deber conocer, entender y aplicar la reglamentación del orden Nacional y Territorial, que fundamentan legalmente el

	Sistema de Gestión de Seguridad de la Información. Apoyar y comprometerse con el cumplimiento de las políticas de seguridad de la información y apoyar los procesos de sensibilización y entrenamiento en este sentido.
RESPONSABLE DE SEGURIDAD: Equipo de Seguridad de la Información	Asesorar en políticas y medidas de seguridad, recomendaciones y buenas prácticas.
PROPIETARIOS DE LA INFORMACIÓN: Líderes de procesos	Adoptar e implementar las políticas de seguridad, controles, y la relación que tienen con sus sistemas e interacción con otros procesos.
COLABORADORES (Funcionarios, Contratistas y Terceros)	Requieren de un alto grado de sensibilización y entrenamiento sobre la seguridad de la información y su reglamentación, para el uso correcto de los sistemas de información. Y protección de los activos de información

MADSIG Sistema Integrado de Gestión

4.1. DIRECTIVOS

El nivel directivo de Minambiente avala y respalda 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, patrocinadores de la importancia de la protección de la información y se comprometen a promover una cultura de seguridad en la entidad.
- 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.
- Deben asegurarse de que todos los colaboradores estén al tanto de las políticas y procedimientos relacionados con la seguridad de la información. Deben comunicar claramente las consecuencias de no seguir estas normas y la importancia de cumplirlas para proteger la información de la entidad y partes interesadas; fomentando 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 y liderar el plan.

4.2. LÍDERES / RESPONSABLES 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 en su proceso.
- Deben asegurarse de que los colaboradores tengan acceso sólo a la información necesaria para desempeñar sus funciones y que sepan cómo manejar adecuadamente la información confidencial.
- Asegurarse que las actividades de sus procesos adopten y apliquen las recomendaciones e instrucciones en materia de seguridad que se divulguen en el marco del plan de sensibilización en seguridad de la información.
- Identificar y comunicar las necesidades particulares en materia de sensibilización o entrenamiento en seguridad de la información para su proceso, colaboradores o para la Entidad.

4.3. RESPONSABLE 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.
- Realizar una evaluación constante del plan de sensibilización y comunicación de la seguridad de la información y formular los ajustes necesarios para garantizar su efectividad.
- Apoyar la elaboración de las piezas comunicativas, presentaciones y encuestas; que deben comunicar claramente las causas y efectos de la explotación de las vulnerabilidades, la importancia de cumplir las políticas para proteger la información de la entidad y los interesados.
- Ejecutar y apoyar las actividades del plan de sensibilización.
- Identificar oportunidades de mejora para la planificación, diseño, implementación y evaluación del plan de sensibilización.

4.4. PROPIETARIOS DE LA INFORMACIÓN

- Participar en las actividades de sensibilización en seguridad de la información de acuerdo con el cronograma y directrices de los responsables de procesos de la Entidad.
- Identificar las vulnerabilidades de los aplicativos, sistemas de información, accesos y usos de la data y de los mecanismos que permitan implementar las recomendaciones y buenas prácticas del plan de sensibilización.
- Fomentar la implementación de las buenas prácticas de seguridad de la información propuestas por las campañas de sensibilización.
- Realizar el monitoreo sobre los logs, incidentes y otros que minimicen la explotación de las vulnerabilidades de forma proactiva y no reactiva.

4.5. COLABORADORES DEL MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

- Participar en las actividades del plan 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 plan de sensibilización.
- Los funcionarios y contratistas deben estar conscientes de las amenazas y saber cómo reconocer y reportar cualquier actividad sospechosa o inusual.
- Participar en la evaluación de la calidad, impacto y efectividad de las actividades del plan de sensibilización.
- Identificar oportunidades para el mejoramiento del plan de sensibilización, mediante encuestas.

5. CANALES DE COMUNICACIÓN DE LA INFORMACIÓN

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: se propone publicar algunos temas tratados en las charlas del SGSI, boletines emitidos por el CSIRT de Gobierno, por la Policía Nacional, videos de seguridad, entre otros.

Correos Masivos: a través del Grupo de Comunicaciones, se propone dar a conocer a toda la Entidad temas detallados como:

- Boletines del CSIRT de Gobierno y de la Policía, conforme sean recibidos en el Ministerio.

- Correos de recomendaciones de buenas prácticas de seguridad y tipos de ataques.

Charlas virtuales: se generarán charlas virtuales mediante herramientas colaborativas tecnológicas definidas por el Minambiente.

- Enlace o link a sesiones de charlas virtuales programadas a través del equipo de Seguridad de la Información de la Oficina de Tecnologías de la Información y Comunicaciones – OTIC.

Charlas presenciales: se aprovecharán espacios como las jornadas de inducción y reinducción que organiza el Grupo de Talento Humano para los funcionarios, el equipo de Seguridad de la Información realizará la programación de sesiones presenciales para las diferentes áreas de la Entidad.

Eslogan de las piezas comunicativas: Se propone a través de la Oficina de la Tecnologías de la Información y Comunicación - OTIC, la divulgación del Eslogan **"LA SEGURIDAD DE LA INFORMACIÓN ES RESPONSABILIDAD DE TODOS",** el cual permitirá tener una mayor apropiación entre funcionarios, contratistas y terceros.

6. IMPLEMENTACIÓN DEL PLAN DE SENSIBILIZACIÓN

Con las sesiones de sensibilización y entrenamiento se busca divulgar las políticas, lineamientos, y buenas prácticas de Seguridad y Privacidad de la Información en la Entidad. La estrategia de difusión del Plan, se realizará mediante diferentes medios de comunicación para lograr llegar a la mayor cantidad de funcionarios y contratistas del Ministerio, mediante el envío de correos masivos, publicaciones en la intranet o carteleras digitales, además se realizarán sesiones o charlas virtuales y/o presenciales de sensibilización en las que se establecerá la importancia del cuidado y tratamiento de la información empleando casos prácticos y cotidianos de fácil entendimiento para las diferentes audiencias (grupos de interés).

6.1. CRONOGRAMA JORNADAS DE SENSIBILIZACIÓN PARA LA VIGENCIA 2023

¿Qué información se va a comunicar?	¿A quiénes?	Forma de Ejecutarla	Responsable	Escenario	Fecha
Reporte y Registro Nacional de Bases de Datos Personales	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Andrés Cadena, Contratista - OTIC Equipo de Seguridad de la Información	Sesiones virtuales	Febrero (1) Marzo (1)

¿Qué información se va a comunicar?	¿A quiénes?	Forma de Ejecutarla	Responsable	Escenario	Fecha
Activos de información Roles y Responsabilidades	Directivos	Charlas de sensibilización, socialización y/o entrenamiento	Liliana Perilla Profesional Especializado - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Marzo (1)
Seguridad de la información e identificación y clasificación de activos de información	Comunicaciones	Charlas de sensibilización, socialización y/o entrenamiento	Oliver Sánchez Técnico - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Marzo (1)
Identificación de Activos de información	Funcionarios y contratista del Equipo de Seguridad de la Información	Charlas de sensibilización, socialización y/o entrenamiento	Andrés Cadena - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Marzo (1)
Identificación de Activos de información	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Andrés Cadena, Liliana Perilla - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Abril (1) Julio (1)
Carga de evidencias en los informes de los colaboradores de la OTIC	Funcionarios y contratistas OTIC	Charlas de sensibilización, socialización y/o entrenamiento	Andrés Cadena, Contratista - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Abril (1)
Gestión de Riesgos de seguridad de la información	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Liliana Perilla Profesional Especializado - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Julio (1) Septiembre (1)
Manual de políticas específicas de seguridad de la información	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	René Alvarado Profesional Especializado - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Abril (1) Septiembre (1)
Beneficios del Doble Factor de Autenticación	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Carlos Centeno Técnico - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Mayo (1)
Malware	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Carlos Centeno Técnico - OTIC Equipo de Seguridad de la Información	Pieza comunicativa Sesiones virtuales o presenciales	Mayo (1)

MADSIG Sistema Integrado de Gestión

¿Qué información se va a comunicar?	¿A quiénes?	Forma de Ejecutarla	Responsable	Escenario	Fecha
Escritorio limpio y pantalla desatendida	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	René Alvarado Profesional Especializado - OTIC Equipo de Seguridad de la Información	Pieza comunicativa Sesiones virtuales o presenciales	Junio (1)
Suplantación de identidad o marca - registro abusivo de nombre de dominio	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Oliver Sánchez Técnico - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Junio (1)
Ataques informáticos	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Oliver Sánchez Técnico - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Julio (1)
Gestión de Seguridad en Redes Sociales	Comunicaciones	Charlas de sensibilización, socialización y/o entrenamiento	René Alvarado Profesional Especializado - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Julio (1)
Uso de contraseñas seguras	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	René Alvarado Profesional Especializado - OTIC Equipo de Seguridad de la Información	Pieza comunicativa Sesiones virtuales o presenciales	Agosto (1)
Control de acceso a redes	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Liliana Perilla Profesional Especializado - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Agosto (1)
Simulacro controlado de Phishing	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Andrés Cadena, Contratista - OTIC Equipo de Seguridad de la Información	Correo Electrónico	Septiembre (1)
Gestión de incidentes	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Oliver Sánchez Técnico - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Septiembre (1)
Uso adecuado del drive	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Liliana Perilla Profesional Especializado - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Octubre (1)

MADSIG Sistema Integrado de Gestión

¿Qué información se va a comunicar?	¿A quiénes?	Forma de Ejecutarla	Responsable	Escenario	Fecha
Uso Apropiado de Internet	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Carlos Centeno Técnico - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Octubre (1)
Vishing – Smishing – Whaling. Pautas para reconocer un sitio o mensaje de Phishing	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	René Alvarado Profesional Especializado - OTIC Equipo de Seguridad de la Información	Pieza comunicativa Sesiones virtuales o presenciales	Noviembre (1)
Gestión de Seguridad en Redes Sociales	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Oliver Sánchez Técnico - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Noviembre (1)
Suplantación de identidad o marca - registro abusivo de nombre de dominio	Funcionarios y contratistas	Charlas de sensibilización, socialización y/o entrenamiento	Liliana Perilla Profesional Especializado - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Diciembre (1)
Control de acceso a redes	Infraestructura OTIC	Charlas de sensibilización, socialización y/o entrenamiento	Oliver Sánchez Técnico - OTIC Equipo de Seguridad de la Información	Sesiones virtuales o presenciales	Diciembre (1)

MADSIG Sistema Integrado de Gestión

6.2. 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 y la identificación de necesidades para la apropiación de la cultura de seguridad y privacidad del Ministerio, el Equipo de seguridad de la Información, aplicará encuestas que servirán como instrumento de medición de la percepción de la información comunicada, así como la importancia y comprensión de la misma, de igual forma a nivel de encuesta se recolectará información sobre temas de interés de los funcionarios y contratistas para incluirlos en futuras charlas.

6.3. Monitoreo del Programa

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:

- Listados de asistencia
- Encuestas o evaluaciones de percepción de la cultura de seguridad y de los conocimientos adquiridos en seguridad de la información y datos personales.
- Presentaciones o piezas de comunicativas.
- Seguimiento de colaboradores que asistieron a las sensibilizaciones.

6.4. 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	Objetivo	Fórmula
Cobertura **(Colaboradores)**	Identificar el alcance del Plan: **Primer semestre** – 80 funcionarios y/o contratistas **Segundo semestre** – 80 funcionarios y/o contratistas	(Número de colaboradores asistentes a las sesiones de entrenamiento o sensibilización) / (Número de colaboradores propuestos en el semestre) * 100

6.5. Mejora Continua

Se propone realizar por lo menos una reunión con la jefe de la OTIC, y conforme los resultados consignados en los resultados de las encuesta de percepción presentados por el equipo de Seguridad de la Información, tomar decisiones en cuanto a posibles mejoras al Plan de Sensibilización y Comunicación en Seguridad de la Información, en la cual se considere recursos económicos destinados a la contratación de actividades tercerizadas, panelistas o premios a nivel de incentivos

para las personas que demuestren mayor nivel de compromiso y adquisición de conocimientos de acuerdo a las encuestas de percepción.

7. NORMATIVIDAD Y DOCUMENTOS ASOCIADOS

- **Ley 1581 de 2012**, "Por la cual se dictan disposiciones generales para la protección de datos personales". Esta Ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma[1].

  Principios Rectores previstos en la Ley 1581, consagrados en el artículo 4:

  a) **Principio de veracidad**: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
  b) **Principio de acceso y circulación restringida**: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente Ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley.
     Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la Ley.
  c) **Principio de seguridad:** La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente Ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
  d) **Principio de confidencialidad:** Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos

1 Ley 1581 de 2012, artículo 1.

personales cuando ello corresponda al desarrollo de las actividades autorizadas en la Ley y en los términos de la misma.

- **Ley 1712 de 2014**, "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones". El objeto de esta Ley es, regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información[2].

- **Norma NTC ISO/IEC 27001:2013**, es una norma colombiana que hace posible que las organizaciones aseguren la confidencialidad y al mismo tiempo la integridad de toda la información que tengan. La versión internacional de la norma que está vigente es la Norma ISO 27001:2013 y es el referente mundial a la hora de implementar un Sistema de Gestión de Seguridad de la Información.

- Generalidades del Marco de Referencia de Arquitectura Empresarial (AE) para la gestión de TI[3], Este Marco de Referencia, es el instrumento principal para implementar la Arquitectura TI en Colombia y habilitar la Estrategia de Gobierno Electrónico del Estado Colombiano, con el cual las entidades públicas direccionan la forma de cómo perciben, usan y proyectan las Tecnologías de Información y las Comunicaciones -TIC. El objetivo principal del Ministerio de Tecnologías de la Información y las Comunicaciones con estas tres herramientas, la Estrategia, la Arquitectura y el Marco, es apoyar a las instituciones en la eficacia de la gestión de Tecnologías de la Información (TI).

  El Marco de Referencia de (AE) en su dominio de Información, cuenta con principios rectores que se relacionan con el presente Plan, dentro de los cuales se encuentra la Seguridad de la información, en la cual se define que el Marco de Referencia de AE para la Gestión de TI debe asegurar la incorporación de mecanismos de seguridad de la información en cada uno de los dominios.

2 Ley 1712 de 2014, artículo 1.

3 G.GEN.01 Generalidades del Marco de Referencia de Arquitectura Empresarial (AE) para la gestión de TI, V.1.3, 2017. MINTIC.

8. GLOSARIO DE TÉRMINOS

a. **Amenazas:** Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.
b. **Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o Entidades no autorizados
c. **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.
d. **Disponibilidad:** Propiedad de ser accesible y utilizable ante la demanda de una Entidad autorizada.
e. **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.
f. **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
g. **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.
h. **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.
i. **Integridad:** Propiedad de precisión y completitud de la información.
j. **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.
k. **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.
l. **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.

o. **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.

p. **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.

MADSIG Sistema Integrado de Gestión