MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

# Manual de Seguridad de la Información

**PROCESO**

**Gestión Estratégica de Tecnologías de la Información**

**Versión 4**

**18/05/2023**

MADSIG
Sistema Integrado de Gestión

## CONTENIDO

## 1. INTRODUCCIÓN

El aumento de los incidentes de seguridad de la información en las entidades, pueden llegar a generar pérdidas financieras, de imagen, información y datos, así como a la generación de reprocesos administrativos, es por lo anterior, que se crea la necesidad de implementar, mantener y mejorar de manera continua, un Sistema de Gestión de Seguridad de la Información (SGSI) donde se diseñen, documenten, implementen y monitoreen controles basados en una gestión de riesgos que minimice el impacto o la probabilidad de ocurrencia de estos, y cuya finalidad sea mantenerlos en niveles aceptables para la entidad.

Este manual recopila los lineamientos generales de seguridad de la información definidas por el Ministerio de Ambiente y Desarrollo Sostenible, Minambiente; las cuales constituyen los pilares para el desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI).

El Ministerio de Ambiente y Desarrollo Sostenible decide establecer, implementar, hacer seguimiento, mantener y mejorar un SGSI; por ello es necesario construir un manual de seguridad de la información que consolide la normatividad, alcance, política, grupo operativo y la metodología de gestión de riesgo del SGSI.

## 2. OBJETIVO DEL DOCUMENTO

Proporcionar y comunicar a las partes interesadas los lineamientos de Seguridad de la Información que deben ser aplicados por parte de todos los colaboradores de Ministerio de Ambiente y Desarrollo Sostenible, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad, tomando como referencia la Norma ISO/IEC 27001:2013 y su anexo A.

## 3. ALCANCE

Aplica para la protección de los activos de información del Ministerio de Ambiente y Desarrollo Sostenible ubicado en la sede de Bogotá, Calle 37 No. 8 – 40, de acuerdo con la versión vigente de la declaración de aplicabilidad.

## 4. NORMATIVIDAD

La norma internacional ISO/IEC 27001:2013 contiene los estándares para implementar la gestión de la seguridad de la información permitiendo el aseguramiento, la confidencialidad e integridad de los datos, así como de los sistemas que la procesan basándose en la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

En este sentido el marco de referencia normativo lo estipulan las leyes: 1753 de 2015 por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "*Todos por un nuevo país*". En su art. 159 que modifica el art. 227 de la ley 1450 del 2011 "Obligatoriedad de suministro de información. Para el desarrollo de los planes, programas y proyectos incluidos en el Plan Nacional de Desarrollo y en general para el ejercicio de las funciones públicas, las entidades públicas y los particulares que ejerzan funciones públicas pondrán a disposición de las entidades públicas que así lo soliciten, la información que generen obtenga, adquieran, controlen y administren, en cumplimiento y ejercicio de su objeto misional. El uso y reutilización de esta información deberá garantizar la observancia de los principios, normas de conformidad con lo dispuesto en las Leyes 1581 del 2012 Protección de datos personales y la ley 1712 del 2014 por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, así como las demás normas que regulan la materia. Además, el suministro de la información será gratuito, y Las entidades públicas propenderán por la integración de los sistemas de información para el ejercicio eficiente y adecuado de la función pública."



También los decretos 1078 del 2015 por medio del cual se expide "*El Decreto Único Reglamentario del Sector de Tecnologías de la información y las comunicaciones*" en su título 9 "*Políticas y Lineamientos de Tecnologías de la Información*", el Decreto 1499 del 2017 por medio del cual se modifica el Decreto 1083 del 2015 Decreto único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la ley 1753 del 2015" en su capítulo 2 "*Políticas de Gestión y Desempeño institucional* en su art. 2.2.22.2.1 que hace referencia a las "*Políticas de Gestión y Desempeño Institucional*" dentro de las cuales se encuentran numeral "11. Gobierno Digital, antes Gobierno en línea, 12. Seguridad Digital". Y los últimos el Decreto 1413 del 2017 en su título 17 establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales y el Decreto 612 del 2018 en su numeral "2.2.22.3.14 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 que deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año:

- Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- Plan de Seguridad y Privacidad de la Información

Adicionalmente, el documento CONPES 3701 del 2011 brinda los lineamientos de política para ciberseguridad y ciberdefensa, que busca fortalecer las capacidades del estado para afrontar las diferentes amenazas y mitigar el impacto de las mismas, y el documento CONPES 3854 del 2017 de la Política de seguridad digital, establece nuevos lineamientos y directrices sobre el tema teniendo en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación.

## 5. TÉRMINOS Y DEFINICIONES

Establecer las normas que se deben cumplir en cuanto a la clasificación, manejo y etiquetado de la información, con el fin de asegurar que reciba el nivel de protección adecuado de la información de MINAMBIENTE.

**Aceptación del Riesgo**: Decisión informada de asumir un riesgo en particular. [ISO/IEC 27000:2018]

**Activo:** Cualquier cosa que tenga valor para la organización. [ISO/IEC 13335-1:2004].

**Activo de Información**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, hardware, software, sistemas de información, edificios, personas, imagen, etc.) que tenga valor para el Ministerio de Ambiente y Desarrollo Sostenible.

**Amenazas**: Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización. [ISO/IEC 27000:2018].

**Análisis del riesgo**: Proceso de comprender la naturaleza del riesgo y determina el nivel de riesgo. [ISO/IEC 27000:2018]. Busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.

**Comunicación y consulta del riesgo**: Conjunto de procesos continuos e iterativos que una

organización realiza para proporcionar, compartir u obtener información, y para entablar un diálogo con las partes interesadas sobre la gestión del riesgo. [ISO/IEC 27000:2018].

**Confidencialidad**: Propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos. [ISO/IEC 27000:2018].

**Control**: Medida que modifica el riesgo. [ISO/IEC 27000:2018]. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

**Disponibilidad**: Propiedad de ser accesible y utilizable a la demanda por una entidad autorizada. [ISO/IEC 27000:2018].

**Estimación del riesgo**: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

**Evaluación del riesgo**: Proceso de comparar los resultados del análisis de riesgo con criterios de riesgo para determinar si el nivel de riesgo o magnitud es aceptable o tolerable. [ISO/IEC 27000:2018].

**Evento**: Aparición o cambio de un conjunto particular de circunstancias. [ISO/IEC 27000:2018].



**Eventos en seguridad de la información**: Ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o el fracaso de los controles, o una situación previamente desconocida que puede ser la pertinente a seguridad. [ISO/IEC 27000:2018].

**Gestión de Incidentes de Seguridad de la Información**: Procesos para detectar, informar, evaluar, responder, tratar, y aprender de los incidentes de seguridad de la información. [ISO/IEC 27000:2018].

**Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización con relación al riesgo. [ISO/IEC 27000:2018].

**Identificación del riesgo**: Proceso para encontrar, reconocer y describir los riesgos. [ISO/IEC 27000:2018].

**Impacto**: Cambio adverso en el nivel de los objetivos del negocio logrado.

**Incidente en seguridad de la información**: Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la organización y amenaza la seguridad de la información. [ISO/IEC 27000:2018].

**Integridad**: Propiedad de exactitud y completitud. [ISO/IEC 27000:2018].

**Nivel de Riesgo**: Magnitud del riesgo expresada en términos de la combinación del impacto y la probabilidad. [ISO/IEC 27000:2018].

**Política**: Intenciones y direcciones de una organización como se expresan formalmente por la Alta Dirección. [ISO/IEC 27000:2018].

**Probabilidad**: Posibilidad de que algo suceda. [ISO/IEC 27000:2018].

**Propietario del riesgo**: Persona o entidad con la responsabilidad y autoridad para gestionar un riesgo. [ISO/IEC 27000:2018].

**Riesgo**: Efecto en la incertidumbre de los objetivos [ISO/IEC 27000:2018].

**Riesgo residual**: Riesgo restante después del tratamiento del riesgo. [ISO/IEC 27000:2018].



**Tratamiento del riesgo**: Proceso de modificar el riesgo. [ISO/IEC 27000:2018].

**Valoración del riesgo**: Proceso general de identificación, análisis y evaluación de riesgos. [ISO/IEC 27000:2018].

**Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas. [ISO/IEC 27000:2018].

## 6. GRUPO OPERATIVO DE SEGURIDAD DE LA INFORMACIÓN

El grupo operativo de seguridad de la información se encarga de definir el alcance, gestionar, planificar, controlar y verificar los procesos del SGSI. El grupo operativo es primordial en la implementación del SGSI ya que es el ente que regula cualquier cambio dentro del sistema de gestión, siempre apuntando a una mejora continua.

Las funciones del grupo operativo son las siguientes:

- Revisar periódicamente el estado general de la seguridad de la información, mínimo una vez al año.
- Revisar y monitorear los incidentes de seguridad de la información.
- Revisar, actualizar y escalar a la Alta Dirección las políticas de seguridad de la información del SGSI.
- Realizar otras actividades de alto nivel (p. ej. Estrategias, planes, proyectos, entre otros) relacionadas con la seguridad de la información.
- Establecer proyectos especiales para la identificación de amenazas potenciales.
- Evaluar la eficacia de las medidas tomadas.
- Elaborar un plan de formación y sensibilización en seguridad de la información.
- Presupuestar los recursos necesarios.
- Planificar auditorías internas periódicas del SGSI.
- Concertar las medidas o controles de seguridad en el procesamiento de la información.
- Validar jurídicamente las medidas o controles a implantar.
- Reportar al Comité Institucional de Gestión y Desempeño sobre eventos e incidentes de seguridad y el estado general de seguridad de la información.

El documento M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información, relaciona la matriz de roles y responsabilidades de los integrantes del grupo operativo de la seguridad de la información.

# 7. POLÍTICAS DEL SGSI

## 7.1. Política General del SGSI

En cumplimiento de su objeto misional, el cual es definir la política Nacional Ambiental y promover la recuperación, conservación, protección, ordenamiento, manejo, uso y aprovechamiento de los recursos naturales renovables, al fin de asegurar el desarrollo sostenible y garantizar el derecho de todos los ciudadanos a gozar y heredar de un ambiente sano; el Ministerio se compromete a definir y establecer un Sistema de Gestión de la Seguridad de la Información para garantizar los requerimientos de las partes interesadas, haciendo un uso eficiente de sus recursos y preservar la confidencialidad, integridad y disponibilidad de la información, bajo un enfoque de prevención de riesgos, mejora continua y autocontrol en los procesos y en la prestación de los servicios, con el apoyo de un equipo humano competente y comprometido.

Como objetivos específicos para el cumplimiento de la Política y del objetivo estratégico del SGSI se tiene:

- Establecer políticas específicas para proteger la confidencialidad, integridad y disponibilidad de la información de la Ministerio.
- Socializar a través del documento MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN M-E-GET-04, las políticas específicas y lineamientos de seguridad de la Información aplicables al Ministerio.
- Crear una cultura de aseguramiento de los activos de información en el Ministerio a través de ejercicios de socialización y capacitación de las políticas y lineamientos definidos en este y otros manuales.
- Definir lineamientos de Seguridad de la Información por medio de su implementación promoviendo la mejora continua.
- Orientar a los funcionarios y dependencias sobre las definiciones de política, lineamientos y demás controles de seguridad establecidos en el Ministerio

Las revisiones de la Política de Seguridad de la Información del Ministerio de Ambiente y Desarrollo Sostenible, al considerarse una política integrada, será revisada bajo la periodicidad definida por el Sistema Integrado de Gestión o cuando se presenten cambios significativos en el Ministerio tales como:

- Objetivos tanto del Sistema de Gestión de Seguridad de la información, como en el cumplimento de los objetivos misionales de MINAMBIENTE o cambios en los procesos relacionados.
- Cambios en la tecnología.
- Condiciones contractuales, regulatorias o legales.