DOCUMENTO SOPORTE DE POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL					
Naturaleza del proceso:	**Estratégico**	**Código:**	**ASIS05**	**Versión:**	**05**

SGSI
Sistema de Gestión de Seguridad de la Información

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL

Ministerio de Salud y Protección Social

BOGOTÁ D.C., NOVIEMBRE DE 2023

TABLA DE CONTENIDO

1. OBJETIVO

Proteger, conservar y asegurar la información del Ministerio de Salud y Protección Social y las herramientas tecnológicas utilizadas para su generación, procesamiento y disposición, con el fin de preservar la confidencialidad, integridad y disponibilidad frente amenazas, deliberadas o accidentales y posibles vulnerabilidades.

2. ALCANCE

Esta política establece los criterios y comportamientos que deben seguir todas las partes interesadas sobre la seguridad de la información del Ministerio de Salud y Protección Social (servidores públicos, contratistas y terceros, entre otros) para preservar la seguridad de la información en la Entidad.

3. GLOSARIO

- **Activos de información:** Bases de datos, documentación física y digital, software, hardware, equipos de comunicación, servicios informáticos y de comunicaciones, infraestructura (iluminación, energía, aire acondicionado, etc.) y las personas (son quienes generan, transmiten y destruyen información) asociados(as) a seguridad de la información. [ISO/IEC 27000: 2017]

- **Amenaza:** Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización [ISO/IEC 27000: 2017]

- **Análisis del riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo [ISO/IEC 27000: 2017]

- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [ISO/IEC 27000: 2017]

- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada [ISO/IEC 27000: 2017]

- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una amenaza con relación a la probabilidad de [ISO/IEC 27000: 2017]

- **Identificación del riesgo:** Proceso para encontrar, numerar y caracterizar los elementos del riesgo. [ISO/IEC 27000: 2017]

- **Integridad:** Propiedad de la información relativa a su exactitud y completitud. [ISO/IEC 27000: 2017]

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias [ISO/IEC 27000: 2017]

- **Tratamiento del riesgo:** Selección e implementación de las opciones o acciones apropiadas para ocuparse del riesgo. [ISO/IEC 27000: 2017]

- **Vulnerabilidad:** La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas consecuencias [ISO/IEC 27000: 2017]

- **MSPS**: Ministerio de Salud y Protección Social

4. MARCO LEGAL

El marco legislativo y regulatorio en el cual se circunscribe el Sistema de Gestión de la Seguridad de la Información del Ministerio de Salud y Protección Social incluye las leyes, decretos, resoluciones y demás normas relevantes en aspectos relacionados con seguridad y privacidad de la información.

Dado lo anterior, se cuenta con el documento soporte **ASIS03 Normatividad en Seguridad de la Información**, donde se relacionan los requisitos legales aplicables al Sistema de Gestión de Seguridad de la Información del Ministerio.

5. INTRODUCCIÓN

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración del Ministerio de Salud y Protección Social con respecto a la protección de los activos de información (servidores públicos, información, procesos, infraestructura tecnológica, entre otros), a la implementación del Sistema de Gestión de Seguridad de la Información y al apoyo, generación y publicación de sus políticas, procedimientos, guías y formatos.

El Ministerio debe contar con plataformas tecnológicas apropiadas que protejan los mecanismos de tratamiento, almacenamiento y comunicación donde están contenidos y soportados sus servicios de consulta, registro, validación y realización de trámites del Sistema General de Seguridad Social en Salud (SGSSS) de Colombia, contando con personal competente y comprometido con una cultura de seguridad de la información reflejada en la aceptación y aplicación de las directrices establecidas.

Con la implementación de políticas en seguridad de la información, este Ministerio busca dar cumplimiento a disposiciones legales y regulatorias emitidas por los diferentes organismos estatales y contar con una metodología de gestión de riesgos de seguridad de la información como herramienta para actuar proactivamente ante la presencia de situaciones que puedan afectar la seguridad de los procesos del Ministerio.

6. POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI).

El Ministerio de Salud y Protección Social asume el compromiso de implementar y mantener el Sistema de Gestión de Seguridad de la Información, destacando la importancia de una gestión adecuada de la información y el fortalecimiento de la confianza en el cumplimiento del deber institucional, cuyo objetivo es la formulación, adopción, implementación, y seguimiento de las políticas, regulaciones, reglamentaciones, planes, programas y proyectos del Sector Salud y Protección Social.

Esta política aplica a toda la Entidad, sus servidores públicos, contratistas y terceros del Ministerio y la ciudadanía en general, buscando la protección de los activos de seguridad de la información, a través del cumplimiento de los requisitos legales e institucionales, así como de los lineamientos para el tratamiento de la información, con el desarrollo de actividades relacionadas con el diseño de controles, identificación y gestión de riesgos de seguridad.

La Política General de Seguridad de la Información estará determinada por las siguientes premisas:

1. Aplicar la seguridad y privacidad para toda la información y los datos personales que reposan en bases de datos y/o archivos manuales, automatizadas que se encuentren en poder del Ministerio de Salud y Protección Social, de los servidores públicos, contratistas, proveedores, operadores, terceros, ciudadanos en general y todas aquellas personas naturales o jurídicas que tengan algún tipo de relación con la entidad y que, de conformidad con la normativa vigente, sean objeto de tratamiento. Se exceptúan de este alcance los casos referenciados en el artículo 2 de la Ley Estatutaria 1581 de 2012 y las normas que lo modifiquen, deroguen o subroguen.

2. Contar con plataformas apropiadas que protejan los mecanismos de tratamiento, almacenamiento y comunicación de la información y los datos personales y donde están contenidos y soportados los servicios de consulta, registro, validación y realización de trámites del Ministerio de Salud y Protección Social.

3. Garantizar que el uso de la información y los datos personales se realice bajo las medidas de seguridad apropiadas a fin de evitar que se presenten usos no acordes a la normatividad o perdidas de confidencialidad, integridad y disponibilidad sobre los mismos.

El incumplimiento a la Política General de Seguridad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa del Ministerio incluyendo lo establecido en las normas que apliquen a nivel Gobierno Nacional y territorial en cuanto a seguridad de la información se refiere.

7. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos de seguridad de la información son:

1. Gestionar los activos de información, salvaguardando la información de estos ante cualquier incidente que pueda provocar su destrucción, divulgación, indisponibilidad o uso no compartido.

2. Gestionar los riesgos de seguridad de la información aplicando los controles necesarios para cada situación, garantizando la sostenibilidad de las operaciones.

3. Fortalecer la cultura de seguridad de la información, brindando concientización y sensibilización permanente a cada colaborador, para enfrentar proactiva y reactivamente las amenazas a las que se exponen en el manejo diario de la información propia y de terceros.

4. Establecer mecanismos que permitan mantener la seguridad de la información durante una interrupción de la infraestructura tecnológica que soporta la operación de los servicios ofrecidos por la Entidad.

5. Gestionar los eventos e incidentes de seguridad de la información, fortaleciendo la capacidad del Ministerio para hacer frente a las amenazas y ataques informáticos.

8. MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El Ministerio de Salud y Protección Social determina la información como un activo de alta importancia para la Entidad, el cual permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, generando la necesidad de implementar reglas y medidas que permitan identificar los riesgos y proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información, razón por la cual el Ministerio establece el documento de políticas de seguridad de la información

denominado **ASIM02 Manual de políticas de seguridad de la información** del Proceso **ASI** - Sistema de Gestión y Mejoramiento Institucional, las cuales deben ser adoptadas por los servidores públicos, proveedores, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con el Ministerio; estas políticas se encuentran enfocadas al cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma NTC ISO/IEC 27001 en su versión vigente.

9. CUMPLIMIENTO

La Política General de Seguridad de la Información es mandataria a todo nivel, por lo tanto, debe ser cumplida por los servidores públicos, contratistas y terceros que interactúen con lo mencionado en el presente documento.

Su incumplimiento significa toda conducta de cualquier miembro definido en el alcance de este documento que no acate las políticas. Entre los ejemplos de incumplimiento se incluyen, sin limitarse a ellos:

a) Los servidores públicos que sean negligentes en la aplicación de medidas de seguridad de la información y control dentro de la organización.
b) Una acción o inacción por parte de un servidor público que contribuye a la violación de las normas orientadas al buen uso de la información.
c) Un servidor público que no resuelve o remite inmediatamente a una autoridad superior los problemas de seguridad de la información que sean detectados.
d) Los servidores públicos que no tomen las medidas correspondientes ante una queja o un incidente de seguridad de la información.

Todos los definidos en el alcance de este documento son responsables de acoger e implementar la Política General de Seguridad de la Información y demás políticas y documentos que son referenciados en este documento y sus complementarios. El incumplimiento de los documentos en referencia, para los servidores públicos constituye falta disciplinaria conforme a lo señalado en los numerales 5, 6 y 22 del artículo 38 y numerales 4 y 5 del artículo 62 de la ley 1952 de 2019.

Artículo 38 Son deberes de todo servidor público:

"… 5. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos."

"… 6. Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos."

"… 22. Vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a que han sido destinados".

Artículo 62. Son faltas Gravísimas las siguientes:

"…4. Atentar, con cualquier propósito, contra la inviolabilidad de la correspondencia y demás formas de comunicación, u obtener información o recaudar prueba con desconocimiento de los derechos y garantías constitucionales y legales".

"…5. Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas."
Los contratistas, consultores y terceros que estén involucrados en incidentes de incumplimiento pueden ver terminado su contrato de acuerdo con las condiciones que en él se han establecido.

Si por alguna razón, estas Políticas no cubren algún caso en concreto, se deberá consultar al Grupo de Seguridad de la Información y Protección de Datos Personales - GSIPSP de la OTIC quien emitirá su concepto o disposición al respecto previa consulta de las áreas del Ministerio que haya lugar, según sea el caso.

La competencia para realizar la investigación disciplinaria es de la Oficina de Control Interno Disciplinario (art.83 Ley 1952 de 2019). Las faltas y sanciones son las establecidas en la ley 1952 de 2019, conforme al procedimiento constituido para el efecto.

10. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades para la administración y funcionamiento del Sistema de Gestión de Seguridad de la Información se encuentran de manera explícita dentro del documento **ASIM04 Manual del sistema de seguridad de la información** el cual se alinea a la presente Política General de Seguridad de la información y es revisado y evaluado periódicamente.

11. MEJORA CONTINUA

La política general de seguridad de la información del MSPS es de aplicación inmediata y continua, desde el momento de su divulgación y socialización dentro del Ministerio. Este documento se actualizará por lo menos una (1) vez cada dos (2) años o cuando se presenten cambios significativos en el Ministerio o las directrices gubernamentales que sean aplicables en cada caso. En las revisiones se tendrán en cuenta factores como: Incidentes de seguridad, nuevas vulnerabilidades detectadas, cambios dentro de la infraestructura organizacional o tecnológica, cambios en los procesos, en los objetivos estratégicos del Ministerio, entre otros.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre y Cargo: **Edgar Fernando Suárez Mendoza,** Contratista del Grupo de Seguridad de la Información y Protección de Datos personales **Fecha:** *18 de octubre de 2023*	**Nombre y Cargo:** **Henry Díaz Dussan,** Jefe Oficina de Tecnología de la Información y la Comunicación – Líder de Seguridad de la Información **y Jorge Eliecer González Díaz,** Coordinador Grupo de Seguridad de la Información y Protección de Datos Personales **Fecha:** *20 de octubre de 2023*	**Nombre y Cargo:** **Comité Institucional de Gestión y Desempeño 08-11-2023** Acta No. 3 de 2023 **Fecha:** *08 de noviembre de 2023*