La salud es de todos Minsalud

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL

BOGOTÁ, ENERO DE 2021

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 todos los miembros de la comunidad 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 seguridad de la 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.

Amenaza: Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización [ISO 27000:2014]

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo [ISO 27000:2014].

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [ISO/IEC 27000: 2014]

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada [27000: 2014].

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una amenaza con relación a la probabilidad de ocurrencia.

Identificación del riesgo: Proceso para encontrar, numerar y caracterizar los elementos del riesgo.

Integridad: Propiedad de la información relativa a su exactitud y completitud. [ISO/IEC 27000: 2014]

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.

Tratamiento del riesgo: Selección e implementación de las opciones o acciones apropiadas para ocuparse del riesgo.

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

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.

No obstante, lo anterior se cuenta con el documento soporte **ASIS03 Normatividad Seguridad de la Información** del proceso **ASIC01 Administración del Sistema Integrado de Gestión**, donde se relacionan los requisitos legales aplicables al Sistema de Gestión de Seguridad de la Información.

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

Las políticas del sistema de gestión de seguridad de la información se definen según su orden de importancia en:

Primer Nivel: Corresponde a la Política General del Sistema de Gestión de Seguridad de la información (SGSI), la cual es una directriz global que establece qué y por qué se quiere proteger. Su definición y actualización está alineada con la planeación estratégica de la organización. Establece las responsabilidades generales aplicables a todo el Ministerio en lo que respecta a la temática de Seguridad de la Información.

Tercer Nivel: Corresponde a políticas específicas enfocadas a grupos, servicios o actividades particulares. Su definición y actualización debe reflejar cambios de índole organizacional y tecnológica.

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 óptimo tratamiento de la información, con el desarrollo de actividades relacionadas con el diseño de controles, identificación y gestión de riesgos.

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

1. Contar con plataformas apropiadas que protejan los mecanismos de tratamiento, almacenamiento y comunicación donde están contenidos y soportados los servicios de consulta, registro, validación y realización de trámites del Ministerio de Salud y Protección Social.
2. Fortalecer la cultura y competencias de los servidores públicos de la entidad respecto a la gestión de Seguridad de la Información.
3. Implementar 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 disponibilidad, confidencialidad e integridad de la información del Ministerio de Salud y Protección Social, de acuerdo con los lineamientos establecidos en la regulación legal vigente, normas y buenas practicas nacionales e internacionales para la correcta gestión de riesgos

Los principales objetivos de esta política son:

1. Gestionar los activos de seguridad de la información de la Entidad en cuanto a su identificación, clasificación y protección para preservar su confidencialidad, integridad y disponibilidad.
2. Sensibilizar al personal para lograr servidores públicos competentes y comprometidos con una cultura de seguridad de la información reflejada en la aceptación y aplicación de las directrices de seguridad.
3. Mantener en constante mejora y evaluación el Sistema de Seguridad de la Información, aplicando las acciones consideradas para el sostenimiento del mismo.
4. Afrontar las amenazas y ataques digitales (cibernéticos) de los que es objeto la infraestructura del Ministerio de Salud y Protección Social, mediante la correcta gestión de eventos e incidentes de seguridad de la información.

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 competen al Gobierno nacional y territorial en cuanto a seguridad de la información se refiere.

7. MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El Ministerio de Salud y Protección Social (MSPS) 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 **ASIC01** Administración del Sistema Integrado de Gestión, 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 MSPS; 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 ISO 27001:2013.

8. CUMPLIMIENTO

La Política General del Sistema de Gestión 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 los Sistemas de Información y demás recursos informáticos del Ministerio.

Su incumplimiento significa toda conducta de cualquier miembro del Ministerio que no respete 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 miembros del Ministerio son responsables de acoger e implementar la Política General del Sistema de Gestión 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 4 y 5 del artículo 34 y numerales 16 y 43 del artículo 48 de la ley 734 de 2002.

Artículo 34 Son deberes de todo servidor público:

"… 4. 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."

"… 5. Custodiar y cuidar la documentación 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."

Artículo 48. Son faltas Gravísimas las siguientes:

"…16. 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"

"…43. 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 y en los que se almacene o guarde la misma, o permita 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 a 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.76 Ley 734 de 2002). Las faltas y sanciones son las establecidas en la ley 734 de 2002, conforme al procedimiento constituido para el efecto.

9. ROLES

Usuario: Todo servidor público, proveedor, ente regulador, socios de negocios, y terceros entre otros, que estén involucrados con la información del Ministerio de Salud y Protección Social.

Responsable de Seguridad de la Información: Responsable de planificar, desarrollar, controlar y gestionar las políticas, procedimientos, riesgos y acciones con el fin de mejorar la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad.

10. MEJORA CONTINUA

La política de seguridad de la información 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, cambiosen los procesos, en los objetivos estratégicos del Ministerio, entre otros.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre y Cargo: **Luz Jenny González Peña,** Contratista de la Oficina de Tecnologías de la información y la Comunicación **Edgar Fernando Suárez Mendoza,** Contratista de la Oficina de Tecnologías de la información y la Comunicación **Fecha:** *27 de noviembre de 2020*	**Nombre y Cargo:** **Weimar Pazos Enciso,** Jefe Oficina de Tecnología de la Información y la Comunicación - Líder de Seguridad de la Información **Fecha:** *04 de diciembre de 2020*	**Nombre y Cargo: Comité Institucional de Gestión y Desempeño Acta 01 - 28-01-2021** **Fecha:** *28 de enero de 2021*