MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD EN LA INFORMACIÓN

MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL
BOGOTÁ, ENERO DE 2021

TABLA DE CONTENIDO

1. OBJETIVO

Dar cumplimiento a lo establecido en las directrices indicadas en las políticas de gestión y desempeño de Gobierno Digital y de Seguridad Digital, apoyando el cumplimiento en la norma ISO/IEC 27001:2013 y demás normatividad que le aplique, con el fin de lograr procesos internos seguros y eficientes a través de la identificación, gestión y tratamiento de los riesgos.

2. ALCANCE DEL DOCUMENTO

Inicia con la definición del contexto estratégico de la entidad, continúa con la comprensión del sistema de gestión de seguridad de la información sus objetivos, políticas generales, controles, exclusiones, gobernabilidad y demás aspectos relevantes y finaliza con el plan de mantenimiento y continuidad del Sistema de Gestion de Seguridad de la Información.

3. ÁMBITO DE APLICACIÓN

Aplica a todos los Procesos del Ministerio de Salud y Protección Social que hacen uso de la información y de las herramientas tecnológicas que puedan ser vulnerables en cuanto a su confidencialidad, integridad y disponibilidad o frente a la materialización del riesgo y que de alguna manera impidan cumplir con el objeto misional del direccionamiento del sistema de salud y protección social en salud.

4. DOCUMENTOS ASOCIADOS

- **ASIC01** Administración del Sistema Integrado de Gestión.
- **ASIP04** Administración del Sistema de Gestión de Seguridad de la Información.
- **ASIM02** Manual de Políticas de Seguridad de la Información
- **ASIG01** Guía para la Administración Integral de riesgos en los procesos.
- **ASIG02** Guía para la medición de la eficacia del SGSI.
- **ASIG03** Guía para el levantamiento y valoración de activos de seguridad información.
- **ASIG04** Guía para el uso y protección de firmas electrónicas.
- **ASIG05** Gestión Incidentes Seguridad Información.
- **ASIS02** Declaración de Aplicabilidad.
- **ASIS04** Política de Privacidad y confidencialidad del MSPS.
- **ASIS05** Política general Seguridad de la Información.
- **ASIS06** Política de Administración de Riesgos Institucionales.
- **ASIM02** Manual de políticas de seguridad de la información.
- **ASIF21** Comprensión de las necesidades y expectativas de las partes interesadas del SGSI.

5. NORMATIVA Y OTROS DOCUMENTOS EXTERNOS

El marco legislativo y regulatorio en el cual se circunscribe el Subsistema 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.

6. DEFINICIONES

Los términos relacionados a continuación están basados y referenciados para efectos del Sistema de Gestión de Seguridad de la Información, ya que muchos de ellos son citados directamente de la norma ISO/IEC 27000:2014. Estos términos permitirán una mayor comprensión del presente manual, así como de las dimensiones manejadas a nivel de sistema.

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, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000:2014).

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

Ciberdefensa: Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Cibernética: Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas. (Academia de la Lengua Española).

Ciberdelito / Delito Cibernético: Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

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

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y tratamiento de riesgos. [ISO/IEC 27000:2014].

Identificación del riesgo: Proceso para encontrar, reconocer y describir riesgos. [ISO/IEC 27000:2014].

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

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

MSPS: Sigla del Ministerio de Salud y Protección Social.

MSPI: Sigla del Modelo de seguridad y privacidad establecido por el MINTIC en el marco de la estrategia de Gobierno Digital.

OTIC: Sigla de la Oficina de Tecnología de la Información y la Comunicación perteneciente al Ministerio de Salud y Protección Social.

Probabilidad: Frecuencia o factibilidad de ocurrencia del Riesgo.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. [ISO/IEC 27000:2014].

SGSI: Sigla del Sistema de Gestión de Seguridad de la Información.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles [ISO/IEC 27000:2014].

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

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y los recursos que la soportan.

7. CONTEXTO ESTRATÉGICO INTERNO Y EXTERNO

7.1. Misión Institucional

El Ministerio de Salud y Protección Social es una entidad pública del nivel central del Gobierno Nacional y cabeza del sector salud, encargada de conocer, dirigir, evaluar y orientar el sistema de seguridad social en salud, mediante la formulación de políticas, planes y programas, la coordinación intersectorial y la articulación de actores de salud con el fin de mejorar la calidad, oportunidad, accesibilidad de los servicios de salud y sostenibilidad del sistema, incrementando los niveles de satisfacción de los pacientes, familias, comunidades y habitantes del territorio nacional.

7.2 Visión Institucional

El Ministerio de Salud y Protección Social, será reconocida en el 2031 por los habitantes del territorio nacional y los actores del sistema como la entidad rectora en materia de salud, que ha mejorado los niveles de calidad, oportunidad y accesibilidad a los servicios de salud y la sostenibilidad del sistema.

7.3 Objetivos de la Entidad

El Ministerio de Salud y Protección Social tendrá como objetivos, dentro del marco de sus competencias, formular, adoptar, dirigir, coordinar, ejecutar y evaluar la política pública en materia de salud, salud pública, y promoción social en salud, y participar en la formulación de las políticas en materia de pensiones, beneficios económicos periódicos y riesgos profesionales, lo cual se desarrollará a través de la institucionalidad que comprende el sector administrativo.

El Ministerio de Salud y Protección Social dirigirá, orientará, coordinará y evaluará el Sistema General de Seguridad Social en Salud y el Sistema General de Riesgos Profesionales, en lo de su competencia, adicionalmente formulará establecerá y definirá los lineamientos relacionados con los sistemas de información de la Protección Social.

7.4 Necesidades y Expectativas de las Partes Interesadas

Para el alcance del SGSI, el Ministerio establece como partes interesadas la Alta Dirección, líderes de proceso, servidores públicos, entes de control, ciudadanos, entidades adscritas, entidades del sector, personas naturales y jurídicas, organizaciones Internacionales, entes de seguridad nacional que hacen uso de los servicios ofrecidos por el Ministerio de Salud y Protección Social.

Dentro de las partes interesadas se debe definir la dimensión en la que se encuentre cada una de las partes, para esto se definió como instrumento de apoyo la matriz de necesidades y expectativas de las partes interesadas del SGSI, la cual debe ser actualizada de manera periódica y cada vez que se requiera. Ver **ASIF21** Comprensión de las necesidades y expectativas de las partes interesadas del SGSI.

7.5 Condiciones de entorno interno y externo

Se determinaron las cuestiones internas y externas que pueden generar eventos originando oportunidades o afectando negativamente el cumplimiento de la misión y los objetivos de una institución.

Para esto se aplica una herramienta de análisis generalmente aceptada, denominada matriz FODA, realizando un análisis del entorno y el ambiente organizacional, identificando dos categorías: a) factores externos (amenazas y oportunidades), siendo las primeras, las situaciones que pueden atentar contra un desempeño institucional, b) factores internos (debilidades y fortalezas), siendo las primeras, las falencias institucionales que le obstaculizan o imposibilitan el desempeño eficiente, eficaz y efectivo, y las segundas las potencialidades con que cuenta la organización para su desarrollo. Las situaciones pueden ser:

Entorno interno:

FORTALEZAS (F)	DEBILIDADES (D)
Experiencia, independencia y capacidades técnicas del talento humano	Ineficiencia en la aplicación de controles en procesos administrativos.
Certificaciones Obtenidas En Normas Técnicas: Calidad, Seguridad de la Información, Seguridad y Salud en el Trabajo, OSHAS.	Débil articulación entre dependencias.
Sistema de información SISPRO, datos sectoriales, encuestas y estudios para la toma de decisiones.	Incertidumbre en la continuidad del talento humano (servidores públicos y contratistas).
Rectoría del sector y coordinación con el resto de entidades (sector salud, territoriales).	Frecuentes recortes presupuestales.
Reconocimientos institucionales (entorno laboral saludable, gobierno digital, atención al ciudadano, adecuada ejecución presupuestal, fenecimiento de la cuenta fiscal por parte de la Contraloría General de la República).	Restricciones en la contratación por ley de garantías electorales.
Nueva entidad Administradora de los Recursos del Sistema General de Seguridad Social en Salud (ADRES).	Dificultades en el seguimiento a la gestión y en la apropiación de la cultura de rendición de cuentas.
Finalización de procesos de liquidación en el sector.	Desconocimiento de la misión institucional y del sistema de salud por parte de algunos servidores públicos y contratistas.
Percepción fuerte de la importancia de la temática de Seguridad de la Información a nivel directivo.	Baja apropiación de la temática de seguridad de la información al interior del Ministerio (Proceso de Cambio Cultural en los servidores públicos).
Cumplimiento de los indicadores de Seguridad de la Información.	Falta de conciencia para evitar la entrega de información personal (Prevención de la Ingeniería Social).
	Integración de los diferentes sistemas al Sistema Integrado de Gestión de manera no articulada.
	Talento humano con baja capacitación en la temática del SGSI.
	Falta definición de las funciones del Responsable de Seguridad de la Información.

Entorno Externo

OPORTUNIDADES (O)	AMENAZAS (A)
Consolidación del nuevo Modelo Integrado de Planeación y Gestión – MIPG.	Afectación en la continuidad de las estrategias contempladas en el actual plan de desarrollo en lo referente a la entidad.
Instrumentos definidos en el marco de la transparencia y la rendición de cuentas.	Entorno político (elecciones).
Reconocimiento del sistema de salud colombiano.	Movimientos sociales.
Ingreso del país a la OCDE.	Deficiente crecimiento económico y generación de empleo formal.
Implementación de nueva normatividad e instrumentos en el sistema de salud (Ley Estatutaria en Salud, mecanismo de exclusiones, Modelo Integrado de Atención en Salud-MIAS, aplicativo MIPRES).	Baja percepción sobre los logros y el manejo de los recursos del sector.
Aplicación de las directrices de MinTic para la implementación de la seguridad digital en las entidades del orden nacional.	Ataques informáticos externos a la infraestructura del MSPS.
Promover la coordinación interinstitucional con el CSIRT de gobierno, COLCERT.	Cambios sustanciales para la adopción del Modelo Integrado de Planeación y Gestión – MIPG.

Ilustración 1. Matriz DOFA para Seguridad de la Información

7.6 Requisitos Generales y Normativos de Seguridad de las Partes Interesadas

Dar cumplimiento a toda la normatividad vigente y asociada dentro de los documentos del SGSI tales como el manual, los procedimientos y demás documentos desarrollados por el Ministerio para la gestión del SGSI, y que se encuentran alineados y acordes con lo establecido por la norma ISO/IEC 27001:2013 y al Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno Digital. Ver documento soporte **ASIS03** Normatividad Seguridad de la Información.

8. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL

8.1 Alcance del SGSI

Se definen las instancias y responsabilidades del Sistema de gestión de seguridad de la información, incluyendo la definición de los objetivos, políticas, planes de trabajo y metodologías que permitan mantener y retroalimentar al Sistema de Gestión de Seguridad de la Información – SGSI en el Ministerio.

El Sistema de Gestión de Seguridad de la Información hace parte del Sistema Integrado de Gestión, el cual está compuesto de 27 procesos integrados dentro del Mapa de Procesos del Ministerio así:

- Estratégicos (7 Procesos)
- Misionales (9 Procesos)
- Apoyo (9 Procesos)
- Evaluación (2)

8.2 Exclusiones

Para el Ministerio de Salud y Protección Social las exclusiones de seguridad de la información se encuentran identificadas y relacionadas en la Declaración de Aplicabilidad. Ver documento soporte **ASIS02** Declaración de aplicabilidad.

8.3 Infraestructura - Instalaciones físicas

El alcance del Sistema de Gestión de Seguridad de la Información en términos de ubicación, dentro del marco de los procesos incluidos en el numeral 8.1, operan en las instalaciones del Ministerio de Salud y Protección Social y en el centro de datos externo del proveedor de servicios contratado a través de los acuerdos marco de precios de Colombia Compra Eficiente para centro de datos Nube Privada II.

8.4 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.

Objetivos de Seguridad de la Información.

El Ministerio ha establecido los siguientes objetivos.

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.

8.5 Medición de la eficacia del SGSI

Se mide la eficacia del SGSI a través de la Identificación, seguimiento y análisis de indicadores de seguridad con el fin de identificar desviaciones o tendencias que permitan la toma de decisiones oportunas en el Ministerio frente a la confidencialidad, integridad y disponibilidad de la información. Ver **ASIG02** Guía para la medición de la eficacia del SGSI.

8.6 Estructura y Gobierno de Seguridad de la Información

La estructura y gobierno de seguridad de la información del Ministerio de Salud y Protección Social corresponde al esquema definido y aprobado por la entidad, en donde se identifican las dependencias funcionales y estratégicas en términos de seguridad de la información para la Entidad. Esta estructura define los roles y responsabilidades. Adicionalmente permite alinear la gestión de seguridad de la información con la misión y los objetivos del Ministerio.

El propósito del gobierno de seguridad de la información es:

- Alinear la estrategia de la seguridad de la información con la Misión para soportar los objetivos institucionales.
- Establecer un enfoque basado en riesgos para la gestión de seguridad de la información, mediante la ejecución de medidas apropiadas para mitigar los riesgos y reducir el impacto potencial en los recursos de información a niveles aceptables.
- Implementar una gestión eficaz de controles para la gestión de seguridad de la información.
- Medir, dirigir y monitorear la gestión de seguridad de la información.
- Proteger la información en todos los tipos, incluyendo: papel, digital, voz.
- Fomentar buena conducta de las personas en el uso de la información.

Para la implementación eficaz de la gestión en seguridad de la información se tienen establecidos los siguientes niveles de responsabilidad y autoridad:

Nivel Estratégico

Es el grupo encargado de definir la estrategia de seguridad de la información para el Ministerio, definir y aprobar las Políticas de Seguridad de la Información, aprobar los proyectos de seguridad, establecer las prioridades para su desarrollo, y revisar la implementación y la eficacia de las medidas adoptadas.

Este grupo lo compone el líder de seguridad y el Comité Institucional de Gestión y Desempeño, de manera que las decisiones y proyectos que se definan cuente con su aval y sean acordes a los objetivos estratégicos.

La Alta Dirección demuestra su compromiso a través de:

- La revisión y aprobación de la Política General de Seguridad y Privacidad de la Información.
- El fomento y la promoción activa de una cultura de seguridad de la información dentro del Ministerio.
- La asignación de los recursos adecuados para implementar y mantener las políticas, así como la gestión de seguridad de la información.

Nivel Táctico

Son grupos que tienen responsabilidades específicas dentro de la gestión en seguridad de la información, principalmente en lo relacionado con la implementación y desarrollo del modelo de seguridad definido. Los principales integrantes de este grupo corresponden a los servidores públicos de la Oficina de Tecnología de la Información y las Comunicaciones del Ministerio.

Nivel Operativo

Son los usuarios finales de la información y por tal razón son los responsables de cumplir las políticas, normas, procedimientos y controles establecidos por el Ministerio, este grupo lo componen servidores públicos, contratistas, proveedores, así como cualquier tercero que acceda a la información de propiedad o en custodia del MINISTERIO.

8.7 Roles y Responsabilidades

El Comité Institucional de Gestion y Desempeño: estará integrado por:

1. El Secretario General, quien lo presidirá;
2. El Viceministro de Salud Pública y Prestación de Servicios o por quien designe;
3. El Viceministro de Protección Social o por quien designe;
4. El Jefe de la Oficina Asesora de Planeación;
5. El Subdirector de Gestión del Talento Humano;
6. El Subdirector Administrativo;
7. El Subdirector Financiero; y,

8. El Jefe de la Oficina de Tecnología de la Información y la Comunicación.

El Comité Institucional de Gestión y Desempeño, tendrá las funciones definidas en el literal D "En relación con el Sistema de Gestión de Seguridad de la Información (SGSI), la política de Seguridad Digital y la Privacidad y Protección de Datos" del artículo 12 de la resolución 2363 de 2018.

Dueño/Líder del Proceso

Es el servidor público responsable de la correcta ejecución de las actividades (*Distribuidas entre diferentes áreas funcionales)* de los procesos a su cargo y de gestionar el mejoramiento continuo de éstos.

Responsable de los activos de información que utilicen y generen en su gestión diaria, de tal forma que las decisiones que tomen garanticen la confidencialidad, privacidad, integridad y disponibilidad de la información.

Responsabilidades

Dentro de las responsabilidades directas del Dueño o Líder del Proceso, se encuentran:

- Verificar el cumplimiento de la legislación y normatividad de seguridad de la información en su proceso.
- Participar en la identificación de los proyectos y planes de mejoramiento de seguridad de la información asociados a la gestión de riesgo sobre la información de su proceso.
- Reportar al Líder de Seguridad el desempeño de la gestión de seguridad de la información y los planes y proyectos asociados de su proceso.
- Verificar la implementación y aplicación de controles.
- Verificar la aplicación del proceso de gestión de incidentes de seguridad de la información.
- Consolidar y hacer seguimiento de las acciones preventivas o correctivas en el proceso.
- Identificar y valorar los activos de información y la información más importante del proceso en términos de su confidencialidad, privacidad, integridad y disponibilidad.
- Realizar y mantener actualizada la clasificación de los activos de información y la información del proceso de acuerdo al esquema de clasificación definido por el Ministerio.
- Definir y autorizar los criterios y niveles de acceso a la información de los servidores públicos o contratistas del proceso o área.
- Asignar el etiquetado pertinente a los activos de información y la información del proceso, conforme a los lineamientos dados por el Ministerio.
- Identificar y evaluar los riesgos de seguridad de la información del proceso y sus activos de información asociados, así mismo proponer planes para su tratamiento (controles de seguridad de la información).
- Verificar la aplicación del tratamiento de riesgos estipulado de acuerdo a la clasificación de la información.
- Asegurar la implementación, operación y mantenimiento de los controles de seguridad de la información aplicados a los activos de información y la información del proceso.

Administradores de la Plataforma Tecnológica y Sistemas de Información

Son los servidores públicos que tienen el conocimiento técnico, habilidades y experiencia para gestionar todos los aspectos de una red de cómputo, incluyendo el diseño, planeamiento, configuración, instalación, resolución de problemas y mantenimiento. Se encargan de implementar en forma activa las normas, estándares y procedimientos, para brindar un nivel apropiado de seguridad de la información.

Responsabilidades:

Sus responsabilidades son las siguientes:

- Gestionar todas las solicitudes de creación, baja y modificación de usuarios y sus respectivos perfiles para los equipos y aplicaciones.
- Mantener actualizada una lista de todos los usuarios con permisos de acceso a los equipos y sistemas de información bajo su responsabilidad.
- Cumplir con los requerimientos de seguridad informática establecidos para la operación y administración de los sistemas de información y recursos de tecnología.
- Analizar e informar por los medios establecidos, cualquier evento que atente contra la seguridad de la información.
- Mantenerse actualizado con respecto a nuevas amenazas, posibles ataques y riesgos que pueden afectar los equipos y/o sistemas de información bajo su responsabilidad.
- Implementar y velar por una adecuada operación de los lineamientos (Normas y estándares), mecanismos, herramientas y procedimientos de seguridad en la plataforma tecnológica que soporta los procesos.

Oficina de Control interno

Grupo encargado de la evaluación y verificación de que las actividades, operaciones y actuaciones del Ministerio, así como la administración de los recursos de información, se realicen de acuerdo a la legislación y normatividad vigente dentro de las políticas establecidas y en atención a los objetivos institucionales.

- Realizar revisiones independientes sobre el cumplimiento de las políticas, procedimientos, guías y controles definidos por el Ministerio.
- Proporcionar una evidencia objetiva al Líder de Seguridad de la Información, sobre la eficacia con la que el Ministerio evalúa y gestiona sus riesgos de seguridad de la información, incluida la forma en la que funcionan y son aplicados los controles para mitigar los riesgos.
- Identificar la necesidad de controles y proporcionar la base para que los mecanismos de monitoreo sean establecidos.
- Verificar la aplicación de las recomendaciones relacionadas con controles de seguridad identificadas en los informes de auditoría interna para determinar si los procesos han ejecutado los planes de acción adecuadamente.

- Informar y alertar al Líder de Seguridad de la Información sobre las desviaciones que puedan presentarse en la ejecución de los planes de acción que impacten directamente en la gestión de riesgos, el cumplimiento regulatorio y/o de políticas de seguridad.

Usuarios

Servidores públicos, contratistas o proveedores, que tienen acceso a los activos de información, usan los servicios de procesamiento de información y son responsables de cumplir las políticas de seguridad de la información.

Responsabilidades:

Sus responsabilidades son las siguientes:

- Conocer y cumplir las políticas, procedimientos, guías, instructivos y demás controles de seguridad de la información.
- Conocer y cumplir los requisitos legales y regulatorios que debe aplicar el Ministerio, de acuerdo a la misión.
- Utilizar los activos de información y la información sólo para el cumplimiento de sus funciones.
- Participar activamente en las charlas, talleres y capacitaciones sobre seguridad de la información.
- Reportar los incidentes o eventos de seguridad de la información detectados, de acuerdo a lo establecido en la guía **ASIG05** Gestión Incidentes Seguridad Información.
- Informar a los Líderes de Proceso y/o el Líder de Seguridad, sobre cualquier exposición a un riesgo de seguridad, ya sea real o potencial.
- Tomar las medidas necesarias e inmediatas para no exponer la información Confidencial y Privada a un acceso no autorizado por parte de un tercero.
- Controlar los requisitos de seguridad de la información en contratos con terceros y en la relación con las partes interesadas.
- Responder por la seguridad de la información que tiene bajo su custodia.
- No deshabilitar los controles de seguridad en su estación de trabajo, ni buscar opciones para evitar su cumplimiento (firewall, antivirus, cifrado).
- Proteger las cuentas de acceso, privilegios y contraseñas asociadas, evitando compartirlas con otros usuarios.
- Utilizar los controles de seguridad física de forma apropiada, como mantener cerradas las puertas que tengan control de acceso, validar que los proveedores se registren y sean acompañados al lugar que se dirigen, y no prestar la tarjeta de proximidad.
- Colaborar en las investigaciones de eventos y/o incidentes de seguridad que se presenten y estén relacionadas con la actividad de sus usuarios individuales.

8.8 Gestión de Riesgos de Seguridad de la Información

La gestión de riesgos es la columna vertebral de la gestión de seguridad de la información y permite a la Institución identificar sus necesidades para proteger sus activos de información y establecer los controles adecuados para mitigar dichos riesgos.

Los activos de información del SGSI del Ministerio se encuentran identificados en el inventario de activos de información de cada proceso ubicados en el sistema integrado de gestión institucional.

Por lo tanto, los procesos del Ministerio de Salud y Protección Social, son sometidos a un proceso de análisis y valoración de riesgos de seguridad de la información, que incluye su tratamiento y los criterios de aceptación del riesgo para identificar los niveles de riesgo aceptable.

La gestión de riesgos de seguridad de la información, se lleva a cabo de acuerdo a la "Guía para la administración integral de riesgos en los Procesos - **ASIG01**. Esta metodología está documentada y aprobada, permitiendo asegurar que la evaluación de riesgos produzca resultados comparables y reproducibles con el objetivo de que el Ministerio pueda contar con una trazabilidad y monitoreo de la gestión de riesgos en los procesos.

8.9 Auditoría interna

Los procesos del Ministerio de Salud y Protección Social son sometidos a revisión en jornadas de Auditoria Interna, con el fin de determinar el cumplimiento de los requisitos establecidos por la norma ISO 27001:2013 y los requisitos establecidos para el Sistema de Seguridad de la Información. El Ministerio cuenta con un procedimiento detallado con el ciclo de planificación, establecimiento e implementación de un ciclo auditor, considerando los requisitos que atañen general y específicamente a un proceso. Para ello, en cada formato ASIF01 caracterización, el proceso contiene los requisitos de norma ISO 270011:2013, que son compatibles con el objetivo y alcance respecto al sistema, y así hacer una revisión detallada del cumplimiento de estos. Adicional, se cuenta con equipos de personas capacitadas en principios y técnicas de auditoria que apoyan el buen desarrollo de las auditorías. Para profundizar más en las actividades de la auditoria interna de calidad, se cuenta con el procedimiento **MACP04** - Auditoría Interna del Sistema Integrado de Gestión.

8.10 Revisión por la Dirección

La revisión por la alta dirección del SGSI está incluida en la comprobación que se aplica al Sistema Integrado de Gestión del Ministerio. Para la Revisión por la Dirección se hará seguimiento a la siguiente información de entrada:

1. Resultados de las auditorías.
2. Estado de las acciones correctivas y preventivas.
3. Acciones de seguimiento de revisiones previas efectuadas por la dirección.
4. Cambios que podría afectar al Sistema de Gestión de Seguridad de la Información.
5. Recomendaciones para la mejora.
6. Resultados de la gestión realizada sobre los riesgos en seguridad de la información identificados en la entidad.
7. Resultados obtenidos mediante indicadores de seguridad de la información implementados de acuerdo con la "Guía para la medición de la eficacia del SGSI - **ASIG02".**

8.11 Políticas específicas de Seguridad de la Información

El Ministerio ha establecido políticas específicas de seguridad de la información, las cuales se encuentran disponibles para consulta en la documentación del Proceso de Administración del Sistema Integrado de Gestión Institucional, ubicada en la Intranet.

Estas políticas definen y orientan la conducta de los servidores públicos, contratistas o terceros sobre la información generada, obtenida, procesada por la Entidad. Ver: **ASIS04** Política de Privacidad y confidencialidad del MSPS, **ASIS05** Política general Seguridad de la Información, **ASIS06** Política de Administración de Riesgos Institucionales y **ASIM02** Manual de políticas de seguridad de la información.

9. MEJORA CONTINUA

Este Manual 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.

La entidad ha establecido el procedimiento **MACP03** Planes de Mejora, y la Guía **MACG02** Planes de Mejora, el cual tiene como fin orientar el emprendimiento de acciones para evitar la recurrencia de no conformidades. Con el fin de llevar el control de las acciones definidas se cuenta con la matriz **MACF05** Registro y control de planes de mejora, la cual contiene la información sobre todas las acciones que se han formulado hasta la fecha, las fuentes que originaron las no conformidades, el proceso al que pertenecen, la descripción de las no conformidades, las causas que las originaron, el responsable de ejecutarlas, el tipo de acción, las fechas en que se van a ejecutar, y su estado. Adicional a las acciones para evitar la no conformidad y acción correctiva, se definen actividades para administrar los riesgos de seguridad digital, las cuales se convierten en acciones preventivas.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre y Cargo: Jorge Eliecer Gonzalez Diaz, Profesional Especializado de la Oficina de Tecnología de la Información y la Comunicación y **Edgar Fernando Suarez Mendoza,** Contratista de la Oficina de Tecnología de la Información y la Comunicación **Fecha:** *23 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:** *30 de noviembre de 2020*	**Nombre y Cargo: Comité Institucional de Gestión y Desempeño Acta No.1 - 28-01-2021** **Fecha:** *28 de enero de 2021*