MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL
BOGOTÁ D.C., NOVIEMBRE DE 2024

TABLA DE CONTENIDO

1. OBJETIVO

Cumplir las directrices de las políticas de gestión y desempeño de Gobierno Digital y Seguridad Digital, apoyando el cumplimiento en la norma ISO/IEC 27001 en su versión vigente y demás normatividad aplicable para lograr procesos internos seguros, eficaces y eficientes mediante la identificación, gestión y tratamiento de los riesgos de seguridad y privacidad de la información.

2. ALCANCE DEL DOCUMENTO

Inicia con la definición del contexto estratégico de la Entidad, continúa con el conocimiento del Sistema de Gestión de Seguridad de la Información - SGSI, sus objetivos, políticas generales, controles, gobernabilidad y demás aspectos relevantes, y finaliza con el plan de mantenimiento y continuidad del Sistema de Gestión de Seguridad de la Información.

3. ÁMBITO DE APLICACIÓN

Aplica a todos los procesos del Ministerio de Salud y Protección Social que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información declarado en este documento y 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 de riesgos de seguridad de la información, 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*** *Sistema de Gestión y Mejoramiento Institucional.*
- ***ASIP05*** *Administración del Sistema Integrado de Gestión y MIPG.*
- ***ASIP09*** *Auditoría interna del Sistema Integrado de Gestión.*
- **ASIM02** Manual de Políticas de Seguridad de la Información.
- ***ASIG01*** *Guía para la Administración Integral de riesgos en los procesos.*
- ***ASIS02*** *Declaración de Aplicabilidad.*
- **ASIS03** Normatividad en seguridad de la información y protección de datos personales.
- **ASIS04** Política de Privacidad y Protección de Datos del MSPS.
- **ASIS05** Política general Seguridad de la Información del MSPS.
- **ASIS06** Política de Administración de Riesgos Institucionales.
- ***ASIF21*** *Comprensión de las necesidades y expectativas de las partes interesadas del SGSI.*
- ***ASIF53*** *Matriz de cumplimiento de objetivos de seguridad de la información.*

5. NORMATIVA Y OTROS DOCUMENTOS EXTERNOS

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 y protección de datos personales** del Proceso Sistema de Gestión y Mejoramiento Institucional (ASI), donde se relacionan los requisitos legales aplicables al Sistema de Gestión de Seguridad de la Información - SGSI.

6. DEFINICIONES

Los términos relacionados a continuación están basados y referenciados para efectos del Sistema de Gestión de Seguridad de la Información. Estos términos permitirán una mayor comprensión del presente manual, así como de las dimensiones manejadas a nivel del sistema.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización. [ISO/IEC 27000:2017]

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la 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]

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales. [Ley 1581 de 2012]

Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento. [Ley 1581 de 2012]

Ciberdefensa: Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional. [CONPES 3995 de 2020]

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética. [CONPES 3995 de 2020]
Cibernética: Ciencia de los sistemas de control y comunicación basados en retroalimentación, soportados o impulsados por la computación, particularmente en su relación con los seres vivos y el ser humano. [Universidad La Salle México][1]

[1] https://ingenieria.lasalle.mx/el-concepto-de-cibernetica-en-el-mundo-actual/

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. [CONPES 3995 de 2020]

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. [CONPES 3995 de 2020]

Confidencialidad: propiedad de que la información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados**.** [ISO/IEC 27000:2017]

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. [Ley 1581 de 2012]

Disponibilidad: La disponibilidad, en el contexto de los sistemas de información se refiere a la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto [ISO/IEC 27000:2017]

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento. [Ley 1581 de 2012].

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 27000:2017]

Identificación del riesgo: Proceso para encontrar, reconocer y describir riesgos. [ISO/IEC 27000:2017]

Impacto: El costo para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros p.ej., pérdida de reputación, implicaciones legales. [ISO/IEC 27000:2017]

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

MSPS: Sigla del Ministerio de Salud y Protección Social.

MSPI: Sigla del Modelo de Seguridad y Privacidad de la Información 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: Posibilidad de que ocurra algo. [ISO/IEC 27000:2017]

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos. [Ley 1581 de 2012]

Riesgo: El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización. [ISO/IEC 27000:2017]

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

Titular: Persona natural cuyos datos personales sean objeto de tratamiento. [Ley 1581 de 2012]

Transferencia: La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país. [Decreto 1377 de 2013]

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable. [Decreto 1377 de 2013]

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. [Ley 1581 de 2012]

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles [ISO/IEC 27000:2017]

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. [ISO/IEC 27000:2017]

7. CONTEXTO ESTRATÉGICO

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 planificar, formular, organizar, coordinar, adoptar, dirigir, orientar, ejecutar y evaluar el sistema de salud y protección social, mediante la formulación de políticas, planes y programas, la coordinación sectorial e intersectorial y la articulación, control y vigilancia de los actores de salud que permitan contar con un sistema nacional de salud de calidad, oportuno, accesible, universal, solidario, predictivo y preventivo, participativo, descentralizado e intercultural, obligatorio y sostenible en el tiempo, garantizando el derecho fundamental de la salud y el cuidado de la vida a todas las personas que habitan el territorio colombiano.

7.2 Visión Institucional

El Ministerio de Salud y Protección Social, será reconocido en el 2031 por los habitantes del territorio nacional, los actores del sistema y la comunidad internacional, como la entidad rectora en materia de salud, que garantizará el derecho fundamental de la salud y el cuidado de la vida, mediante la consolidación de un sistema de salud,

preventivo, predictivo, resolutivo, equitativo, solidario, universal, intercultural, accesible, sostenible, eficiente con criterios de calidad y oportunidad.

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 Requisitos, 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 y entes de seguridad nacional que hacen uso de los servicios ofrecidos por el Ministerio de Salud y Protección Social, entre otros.

Para esto, se define como instrumento de apoyo la matriz de necesidades y expectativas de las partes interesadas del SGSI, la cual debe ser actualizada de manera periódica o cada vez que surjan cambios significativos dentro del Sistema de Gestión y Seguridad de la Información. Ver **ASIF21** ***Comprensión de las necesidades y expectativas de las partes interesadas del SGSI*** dentro del Sistema Integrado de Gestión del Ministerio.

7.5 Condiciones de entorno interno y externo

Se determinan las cuestiones internas y externas que pueden generar eventos originando oportunidades o afectando el cumplimiento de la misión y los objetivos de la Institución, en cuanto a la seguridad de la información.

Para esto, se aplica una herramienta de análisis, 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. Lo anterior puede evidenciarse dentro del documento **Contexto Estratégico de Seguridad de la Información** que hace parte del Sistema de Gestión de Seguridad de la Información del Ministerio y el cual se actualiza periódicamente.

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 la seguridad de la información dentro del Ministerio de Salud y Protección Social. Esto aplica a todos los servidores públicos, contratistas y terceros que interactúen y, por el cumplimiento de sus funciones, compartan, utilicen, recolecten, procesen, intercambien, transformen o consulten información de la Entidad.

El Sistema de Gestión de Seguridad de la Información forma parte del Sistema Integrado de Gestión, por lo que su alcance se extiende a los siguientes Procesos dentro del Mapa de Procesos del Ministerio, incluyendo:

- Procesos Estratégicos
  - **ASI** – Sistema de Gestión y Mejoramiento Institucional.
  - **GSC** – Gestión del Servicio al Ciudadano.
- Procesos Misionales
  - **CVS** – Ciclo de Vida y Reingeniería de Sistemas de Información.
- Procesos de Apoyo
  - **ABI** – Administración de Bienes e Insumos.
  - **GTH** – Gestión del Talento Humano.
  - **GST** – Gestión de Soporte a las Tecnologías.
  - **GDO** – Gestión Documental.
  - **GFI** – Gestión Financiera.
  - **GCO** – Gestión de Contratación.
- Procesos de Evaluación
  - **GYP** – Gestión y Prevención de Asuntos Disciplinarios

8.2 Inclusiones y Exclusiones

Para el Ministerio de Salud y Protección Social las inclusiones y exclusiones de controles de seguridad de la información se encuentran identificadas y relacionadas en la Declaración de Aplicabilidad. Ver documento soporte **ASIS02 Declaración de Aplicabilidad**, la cual debe ser revisada y en caso de ser necesario, actualizada anualmente para cumplir la regulación vigente y aplicable.

8.3 Política General del Sistema de Gestión de Seguridad de la Información (SGSI).

La Política General del Sistema de Gestión de Seguridad de la Información que declara el compromiso que tiene la Entidad frente a la protección de la información que genera, almacena y trata, se encuentra dentro del documento **ASIS05 Política General de Seguridad de la Información**, la cual es revisada y evaluada periódicamente para dar cumplimiento a la regulación vigente y aplicable.

8.4 Política de Privacidad y Protección De Datos Personales Del Ministerio De Salud y Protección Social

El Ministerio de Salud y Protección Social, en cumplimiento de la normatividad vigente en materia de privacidad y protección de datos personales, en concordancia con su Sistema Integrado de Gestión (SIG), busca responder a las necesidades y expectativas de los ciudadanos en materia de salud, protección social en salud y protección de datos personales, por lo que cuenta con el documento **ASIS04 Política de Privacidad y Protección de Datos del MSPS**, la cual se integra con los objetivos del SIG y es revisada y evaluada periódicamente para dar cumplimiento a la regulación vigente y aplicable.

8.5 Medición de la eficacia y eficiencia del SGSI

Se mide la eficacia y eficiencia del SGSI mediante la identificación, seguimiento y análisis de indicadores de seguridad de la información para identificar desviaciones que permitan tomar decisiones oportunas en el Ministerio frente a la confidencialidad, integridad y disponibilidad de la información. Ver el documento **ASIF53 Matriz de cumplimiento de objetivos de seguridad de la información** dentro del Sistema Integrado de Gestión del Ministerio.

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 aprobado por la Entidad, donde identifican las dependencias funcionales y estratégicas en cuanto a seguridad de la información. Lo anterior, 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 y eficiente 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 gestión:

Nivel Estratégico

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 nivel está compuesto por el Líder de Seguridad de la Información 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.

Nivel Táctico

Tiene la responsabilidad específica dentro de la gestión en seguridad de la información, principalmente en lo relacionado con la implementación y desarrollo del modelo de seguridad definido.

Este nivel está compuesto por El Grupo de Seguridad de la Información y Protección de Datos Personales de la Oficina de Tecnología de la Información, el Grupo de Soporte Informático y el Grupo de Comunicaciones del Ministerio.

Nivel Operativo

Son los usuarios finales de la información y, por eso, son los responsables de cumplir las políticas, normas, procedimientos y controles establecidos por el Ministerio; los servidores públicos, contratistas y proveedores, y cualquier tercero que acceda a la información de propiedad o custodia del Ministerio.

8.7 Roles y Responsabilidades

El Comité Institucional de Gestión y Desempeño

En consideración a que la orientación respecto de la implementación y operación del Sistema Integrado de Gestión del Ministerio de Salud y Protección Social está a cargo del Comité Institucional de Gestión y Desempeño, siendo la máxima instancia para este efecto,

El Comité Institucional de Gestión y Desempeño, está 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, quien a su vez es el Líder de Seguridad de la Información

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.

Líder seguridad de la Información

El Líder de Seguridad de la Información de la Entidad es responsable del diseño, desarrollo, implantación, mantenimiento y verificación del correcto funcionamiento del Sistema de Gestión de Seguridad de acuerdo con los dominios contenidos en el Modelo de Gestión y Gobierno TI del Marco de Referencia Arquitectura Empresarial:

1. Servicios Tecnológicos

- Liderar la gestión de riesgos de seguridad de la información, privacidad y protección de datos personales sobre la gestión de TI en virtud de los tratamientos de datos que realice el MSPS.
- Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de la información, privacidad y protección de datos personales para la gestión de TI e información con relación al uso adecuado y seguro de los datos.
- Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad sobre la información y los datos personales.
- Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias.
- Apoyar a la alta dirección y los dueños de los procesos misionales dentro del MSPS en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
- Dirigir, solicitar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.

2. Estrategia TI

- Definir y comunicar la estrategia de seguridad de la información, privacidad y protección de datos personales que permita lograr los objetivos del Sistema de Gestión de Seguridad de la Información, y la minimización de los riesgos asociados al uso de la información, a través de servicios tecnológicos.
- Apoyar en la adquisición de bienes y servicios informáticos requeridos para garantizar la seguridad de la información, a través de la definición de requerimientos técnicos y de cumplimiento legal para garantizar la seguridad de la información incluyendo la protección de datos personales.

3. Gobierno TI

- Monitorear y controlar la estrategia de TI con el fin de lograr los objetivos del Sistema de Gestión de Seguridad de la Información, Privacidad y Protección de Datos Personales y la minimización de los riesgos del componente de TI, en relación con el uso y procesamiento de información.
- Gestionar y monitorear la prestación y adquisición de bienes y/o servicios que busquen garantizar la seguridad de la información, incluyendo la protección de datos personales.

4. Sistemas de Información

- Establecer los requerimientos mínimos de seguridad de la información, privacidad y protección de datos personales que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro del MSPS para el procesamiento de la información.
- Garantizar el desarrollo de pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
- Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados.
- Trabajar con la alta dirección y los lideres de procesos misionales dentro del MSPS en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.

5. Información y Datos

- Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados.
- Verificar el cumplimiento de las obligaciones legales y regulatorias del Estado relacionadas con la seguridad de la información.

6. Uso y Apropiación

- Apoyar en el desarrollo de planes de formación y sensibilización en materia de seguridad de la información, privacidad y protección de datos personales, socializando los lineamientos tendientes a garantizar el uso apropiado y seguro, que permita fomentar una cultura de seguridad en la que todos los empleados se sientan responsables de proteger la información y los sistemas del Ministerio.
- Supervisar los resultados del plan de formación y sensibilización para medir el nivel de comprensión y cumplimiento de las políticas de seguridad establecidas para el MSPS, con el fin de identificar oportunidades de mejora.
- Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información, privacidad y protección de datos personales en la implementación de los proyectos de TI.

Líder de Proceso

El servidor público con nivel de Director, Jefe de Oficina o Líder de Proceso es 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 estos. Además, es responsable de los activos de información que se generen en el proceso, asegurando que las decisiones que tome garanticen la confidencialidad, integridad y disponibilidad de la información. Como tal, debe asumir y ejecutar las siguientes responsabilidades frente al Sistema de Gestión de Seguridad de la Información.

- Garantizar que los procesos, procedimientos, actividades, funcionarios, contratistas y proveedores bajo su responsabilidad, cumplan las directrices sobre protección de datos personales y seguridad de la información indicadas por el MSPS.
- 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 de la Información o en su defecto a la Coordinación de Seguridad de la información y Protección de Datos Personales el desempeño de la gestión de seguridad de la información y los planes y proyectos asociados de su proceso.
- Implementar y aplicar controles de seguridad de la información sobre los activos de información.
- Consolidar y hacer seguimiento de las acciones preventivas o correctivas en el proceso.
- Identificar y valorar los activos de información del proceso clasificándolos en niveles de criticidad en términos de su confidencialidad, integridad y disponibilidad.
- Realizar y mantener actualizada la clasificación de los activos de información y la información del proceso de acuerdo con el 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, así mismo proponer planes para su tratamiento (controles de seguridad 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 de su proceso.
- Apoyar las campañas de sensibilización y concientización de seguridad de la información y privacidad de datos personales dentro de su proceso.
- Garantizar la recolección de la información personal solo a través de las herramientas brindadas o avaladas por el MSPS.
- Garantizar que la definición de finalidades para el tratamiento de datos personales y la estructuración de la autorización sea avalada por Líder de Seguridad de la información del Ministerio.
- Garantizar que los soportes de la autorización del tratamiento de datos personales sean debidamente almacenados y estén protegidos ante perdida, daño o modificación, y sean relacionados y tratados como un activo de información.
- Garantizar la constancia de la fecha, hora y medio por la que se capturó la información y del soporte de la autorización del uso y tratamiento de datos personales.
- Garantizar que solo se traten datos personales de acuerdo con las finalidades autorizadas por el titular.
- Garantizar que, durante la transmisión de información personal entre procesos se cuente con los medios técnicos, administrativos y legales idóneos para que la información personal sea confidencial.
- Constatar la pertinencia de los datos personales a entregar y evitar el envío de información innecesaria o que no esté incluida en las finalidades del tratamiento, cuando aquella sea requerida por otras áreas.
- Garantizar la aplicación del criterio de minimización de los datos a recabar, en función de los servicios seleccionados por el usuario.

Administradores de la Plataforma Tecnológica y Sistemas de Información

Son los servidores públicos y contratistas que tienen el conocimiento técnico, habilidades y experiencia para gestionar los sistemas de información, servicios tecnológicos y redes de cómputo, incluyendo el diseño, planeación, configuración, instalación, resolución de problemas y mantenimiento. Son los encargados de implementar en forma activa las normas, estándares, procedimientos y controles, de seguridad de la información.

Sus responsabilidades son las siguientes:

- Gestionar las solicitudes de creación, cancelación y modificación de usuarios y sus respectivos perfiles para los equipos y aplicaciones.
- Mantener actualizada una lista usuarios con permisos de acceso a los equipos y sistemas de información bajo su responsabilidad.
- Cumplir con los requerimientos de seguridad de la información establecidos para la operación y administración de los sistemas de información y recursos de tecnología.
- Analizar e informar por los medios establecidos al Líder de Seguridad de la Información y/o Coordinación de Seguridad de la Información y Protección de Datos Personales, cualquier evento que atente contra la seguridad de la información.
- Mantenerse actualizado con respecto 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.
- Establecer los procedimientos técnicos necesarios para garantizar que las bases de datos y repositorios de información personal no se puedan acceder, manipularse o alterarse por terceros, sin autorización.
- Garantizar que se generen copias de respaldo de las bases de datos, las cuales deben tener las mismas medidas de seguridad que la información original.
- Establecer un procedimiento de archivo, custodia y eliminación de información.
- Garantizar la aplicación de medidas técnicas superiores para el acceso a las bases de datos o repositorios de información personal.

Oficina de Control Interno

Oficina encargada de la evaluación y verificación que las actividades, operaciones y actuaciones del Ministerio, así como la administración de los recursos de información, se realicen de acuerdo con 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.
- Verificar la aplicación de las recomendaciones relacionadas con controles de seguridad de la información identificados 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 y a la Coordinación de Seguridad de la Información y Protección de Datos Personales 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.

Grupos de Gestión, Ejecución y Liquidación Contractual

- Garantizar que las elaboraciones de contratos cumplan los requisitos necesarios en materia de seguridad de la información y protección de datos personales y se recauden las autorizaciones de contratistas cuando sean personas naturales.
- Garantizar que el relacionamiento con encargados del tratamiento de dados personales esté regido por un contrato y/o convenios, almacenados en físico o digital, que garantice la entrega, uso y devolución de la información de acuerdo con las políticas de transmisión de datos personales.

Usuarios

Servidores públicos, contratistas y 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.

Sus responsabilidades son las siguientes:

- Conocer y cumplir las políticas, procedimientos, guías, instructivos y demás controles de seguridad de la información, privacidad y protección de datos personales.
- Conocer y cumplir los requisitos legales y regulatorios que debe aplicar el Ministerio, de acuerdo con su misión en materia de seguridad de la información, privacidad y protección de datos personales.
- 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, impartidas por el Grupo de Seguridad de la Información y Protección de Datos Personales en conjunto con la Subdirección de Gestión del Talento Humano.
- Reportar los incidentes o eventos de seguridad de la información detectados, de acuerdo con los lineamientos establecidos por el Ministerio.
- Informar a los Líderes de Proceso, Líder de Seguridad de la Información y Coordinación de Seguridad de la Información y Protección de Datos Personales, 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 ante un acceso no autorizado por parte de un tercero.
- Controlar los requisitos de seguridad de la información en contratos con terceros y en relación con las partes interesadas.
- Responder por la seguridad de la información de los activos de información que tiene bajo su custodia.
- No deshabilitar ni alterar los controles de seguridad de la información implementados por el Ministerio de Salud y Protección Social
- Proteger las cuentas de acceso, privilegios y contraseñas asociadas, evitando compartirlas con otros usuarios.
- Utilizar los controles de seguridad física determinados por el Ministerio para salvaguardar la seguridad de la información.

- 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 se encuentran identificados en cada Proceso que hace parte del Sistema Integrado de Gestión del Ministerio. Por lo tanto, los procesos del Ministerio de Salud y Protección Social son sometidos a 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 con la **Política de Administración de Riesgos Institucionales – ASIS06** y 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 de seguridad produzca resultados comparables y reproducibles con el objetivo de que el Ministerio pueda contar con una trazabilidad y monitoreo de la gestión de riesgos de seguridad de la información.

8.9 Auditoría Interna

Los procesos del Ministerio de Salud y Protección Social son sometidos a revisión en jornadas de Auditoría Interna, con el fin de determinar el cumplimiento de los requisitos establecidos para el Sistema de Gestión de Seguridad de la Información. El Ministerio cuenta con un procedimiento detallado con el ciclo de planificación, establecimiento e implementación de un ciclo de auditoría interna, considerando los requisitos que atañen general y específicamente a un Proceso. Ver **ASIP09 - 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, la cual debe ser llevada a cabo por lo menos una vez al año para garantizar el correcto funcionamiento del sistema de gestión. Para la Revisión por la Dirección se hará seguimiento como mínimo, a la siguiente información de entrada:

1. Estado de las acciones provenientes de revisiones previas.
2. Cambios externos e internos que sean relevantes para el Sistema de Gestión de Seguridad de la Información.
3. Cambios en las necesidades y expectativas de las partes interesadas frente al Sistema de Gestión de Seguridad de la Información.
4. No conformidades y acciones correctivas, y sus tendencias.
5. Resultados obtenidos mediante indicadores de seguridad de la información, y sus tendencias.
6. Resultados de las auditorías y su tendencia.
7. Cumplimiento de los objetivos de seguridad de la información, y sus tendencias.

8. Acciones de seguimiento de revisiones previas efectuadas por la Dirección.
9. Retroalimentación con las partes interesadas.
10. Resultados de la gestión realizada sobre los riesgos en seguridad de la información identificados en la Entidad.
11. Recomendaciones para la mejora continua.

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 estratégico Sistema de Gestión y Mejoramiento Institucional, ubicado en la Intranet de la Entidad.

Estas políticas definen y orientan la conducta de los servidores públicos, contratistas y terceros sobre la información generada, obtenida y procesada por la Entidad. Ver documento **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 revisará y de ser necesario se actualizará por lo menos una (1) vez cada año o cuando se presenten cambios significativos en el Ministerio o según 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, cambios en los objetivos estratégicos del Ministerio, cambios en la normatividad, entre otros.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre y Cargo: **Jeison Joann Walteros López,** Contratista del Grupo de Seguridad de la Información y Protección de Datos personales. **Edgar Fernando Suárez Mendoza,** Contratista del Grupo de Seguridad de la Información y Protección de Datos personales. **Jorge Fernando Bejarano Lobo**, Contratista del Grupo de Seguridad de la Información y Protección de Datos personales. **Víctor Alfonso Parrado Rodríguez,** Profesional Especializado del Grupo de Infraestructura de TI de la OTIC **Fecha:** *23 de octubre de 2024*	**Nombre y Cargo:** **Jorge Eliecer González Díaz,** Coordinador Grupo Seguridad de la Información y Protección de Datos Personales. **Fecha:** *18 de noviembre de 2024*	**Nombre y Cargo:** **Jorge Eliécer González Díaz,** Jefe Oficina de Tecnología de la Información y la Comunicación (E) – Líder de Seguridad de la Información. **Fecha:** *26 de noviembre de 2024*