# PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Revisado y aprobado por: Jorge Eliecer González Díaz

Coordinador Grupo de Seguridad de la Información e Innovación

---

## Seguridad de la información. Plan de Gestión de Riesgos 2025

Elaborado por: José Alexander Parra González, contratista
Barnard Stith Bejarano Rengifo, contratista
John Yimmy Campo Rosero, contratista
Jorge Fernando Bejarano Lobo, contratista
José Eduardo Pérez Altamar, contratista

Grupo Seguridad de la Información e Innovación - 2025

# Contenido



## Resumen Ejecutivo

El Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información del Ministerio de Salud y protección Social, tiene como propósito establecer un marco metodológico integral y sistemático para la identificación, evaluación, análisis, tratamiento y monitoreo continuo de los riesgos asociados a la confidencialidad, integridad y disponibilidad de la información. Este plan garantiza que los procesos de gestión de riesgos se encuentren alineados con los principios clave de la seguridad de la información, abordando de manera eficaz las amenazas y vulnerabilidades presentes en los sistemas y servicios del Ministerio.

El desarrollo y la implementación de este plan se sustenta en la Política de Administración de Riesgos Institucionales (ASIS06) y en la Guía para la Administración Integral de Riesgos en los Procesos (ASIG01). Asimismo, su ejecución se basa en normas internacionales y mejores prácticas reconocidas, como las establecidas en la ISO/IEC 27001:2022 para la gestión de seguridad de la información y la ISO 31000:2018 para la gestión de riesgos. Esto asegura la protección óptima de los activos digitales del Ministerio y refuerza la confianza en la gestión de la información, mitigando los riesgos y adaptándose de manera proactiva a las amenazas emergentes.

## Introducción

La seguridad de la información constituye un componente fundamental en todas las entidades públicas, particularmente en entidades como el Ministerio de Salud y Protección Social, que maneja un alto volumen de información sensible y crítica y que por lo tanto exige un adecuado tratamiento de los riesgos inherentes a la gestión de datos personales. Frente al aumento exponencial de las amenazas cibernéticas y la creciente complejidad de los riesgos asociados con la transformación digital, el Plan de Gestión de Riesgos de Seguridad

de la Información tiene como objetivo mitigar los riesgos inherentes a la seguridad digital, fortalecer los controles internos y garantizar la continuidad operativa de los sistemas de información del Ministerio.

El presente documento establece un marco metodológico estructurado y claro para la gestión de riesgos, fundamentado en mejores prácticas internacionales y alineado con los lineamientos derivados del Modelo se Seguridad y Privacidad de la Información expedido por el Ministerio de las Tecnologías de la Información y las Comunicaciones. Su objetivo principal es garantizar la protección efectiva de los activos digitales del Ministerio, promoviendo la adecuada gestión de riesgos de seguridad y privacidad de la información en el marco del uso de tecnologías de información que soportan los servicios misionales y de apoyo de la entidad.

A través de la implementación de este plan, el Ministerio no solo busca proteger los activos de información, sino también fomentar una cultura organizacional orientada a la prevención y a la mejora continua en la gestión de riesgos de seguridad de la información.

## Definiciones

- Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [ISO/IEC 27000:2017]
- Integridad: Propiedad de la información relativa a su exactitud y completitud. [ISO/IEC 27000:2017]
- Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada [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]

## Objetivo General

Establecer una metodología integral, de gestión de riesgos de seguridad y privacidad de la información que permita identificar, evaluar, mitigar y monitorear continuamente los riesgos cibernéticos, digitales y operativos, garantizando la protección de los activos digitales y facilitando la articulación con otras acciones orientadas a promover la continuidad de los servicios misionales y de apoyo, ante amenazas emergentes.

## Objetivos específicos

1. Revisar y evaluar los activos de información críticos para el Ministerio, a fin de comprender su valor y la exposición a riesgos potenciales que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

2. Evaluar los riesgos asociados a la seguridad y privacidad de la información, de conformidad con las metodologías definidas para el efecto, con el fin de identificar amenazas y vulnerabilidades, y determinar el impacto y la probabilidad de los riesgos en los sistemas de información del Ministerio.

3. Implementar controles de seguridad preventivos, detectivos y correctivos que permitan reducir la probabilidad de materialización de los riesgos y mitigar los impactos de las amenazas identificadas.

4. Monitorear de manera continua y periódica la efectividad de los controles de seguridad implementados, garantizando su adecuación a las necesidades del Ministerio y su capacidad para enfrentar los riesgos emergentes en un entorno digital en constante cambio.

## Alcance

El Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información del Ministerio de Salud y Protección Social abarca inicialmente los procesos certificados y, de manera progresiva, se integrarán los demás componentes del Sistema Integrado de Gestión (SIG) certificados, cubriendo de manera integral la gestión de riesgos asociados a los sistemas de información, redes de comunicación, infraestructura tecnológica y bases de datos, procesos operativos, físicos entre otros. Este plan tiene como propósito identificar, evaluar y mitigar los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y continuidad operativa de la información y los activos digitales y físicos del Ministerio, a lo largo de su ciclo de vida, desde la captura, almacenamiento y procesamiento, hasta su transmisión y disposición final. Incluye tanto los sistemas y aplicaciones utilizadas para la gestión administrativa y operativa como las redes internas y externas que soportan la conectividad y el intercambio de datos, así como los dispositivos de hardware y software que componen la infraestructura tecnológica. Asimismo, abarca los repositorios de datos, tanto estructurados como no estructurados, que contienen información crítica y sensible.

Este enfoque asegura que el Ministerio mantenga un entorno de gestión de la información resiliente frente a amenazas cibernéticas y operacionales, garantizando la seguridad y privacidad de la información, así como procurar la continuidad de los servicios prestados a la ciudadanía.

## Marco Referencial

El Ministerio de Salud y Protección Social ha adoptado la Política de Administración de Riesgos Institucionales (ASIS06), la cual establece las directrices fundamentales para la identificación, análisis, tratamiento y monitoreo de los riesgos en todos los procesos de la entidad. Esta política garantiza un enfoque estructurado, sistemático

y proactivo en la gestión de riesgos de seguridad y privacidad de la información, orientado a mitigar las amenazas y vulnerabilidades que puedan comprometer el cumplimiento de los objetivos estratégicos del Ministerio.

La política se complementa con la Guía para la Administración Integral de Riesgos en los Procesos (ASIG01), que proporciona una metodología detallada para la gestión integral de riesgos. Esta guía permite realizar una evaluación sistemática de los riesgos de seguridad y privacidad de la información y la implementación de controles adecuados para cada fase del ciclo de vida del riesgo, asegurando la cobertura efectiva de todos los aspectos organizacionales y operativos.

Asimismo, el Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información se alinea con el Modelo se Seguridad y Privacidad de la Información del Ministerio de las Tecnologías y las comunicaciones y estándares internacionales de referencia como ISO/IEC 27001:2022 para la gestión de la seguridad de la información y ISO 31000:2018 para la gestión de riesgos de seguridad y privacidad de la información, estos marcos proporcionan un conjunto de mejores prácticas globales, permitiendo la adopción de un enfoque sólido y escalable para gestionar los riesgos relacionados con la información y la tecnología.

## Metodología[1]

La metodología de gestión de riesgos de seguridad y privacidad de la información adoptada en el Plan de Gestión de Riesgos del Ministerio de Salud y Protección Social tiene un enfoque integral y continúo basado en las mejores prácticas internacionales y la normatividad vigente, como la ISO 31000:2018 y la ISO/IEC 27001:2022, debidamente alineado con el Modelo se Seguridad y Privacidad de la Información adoptado por MinTic. Esta metodología está diseñada para identificar, evaluar, tratar y monitorear los riesgos asociados a los activos de información, garantizando la protección de estos frente a amenazas y vulnerabilidades.

La implementación del plan se realiza a través de un ciclo de gestión estructurado, compuesto por las siguientes fases:

1. Establecimiento del Contexto y Políticas de Gestión de Riesgos: Definición del contexto estratégico y organizacional en el que se gestionan los riesgos, alineado con la Guía para la Administración Integral de Riesgos en los Procesos (ASIG01), y las directrices del Ministerio. En esta fase se establecen las bases para el enfoque de gestión de riesgos y se definen las políticas de tratamiento de riesgos.

[1] Esta metodología es un enfoque basado en el ciclo de vida de la gestión de riesgos, alineado con los estándares internacionales ISO 31000:2018 para la gestión de riesgos y ISO/IEC 27001:2022 para la seguridad de la información. La metodología se enfoca en un proceso iterativo, continuo y flexible, que permite adaptar la gestión de riesgos a las necesidades y condiciones cambiantes del Ministerio, asegurando que la protección de los activos digitales y la continuidad operativa sean gestionadas de manera efectiva a largo plazo.

2. Identificación de Riesgos: En esta fase se identifican los activos de información críticos y los riesgos asociados, incluyendo amenazas, vulnerabilidades y los posibles impactos sobre la confidencialidad, integridad y disponibilidad de la información.

3. Análisis de Riesgos: Se realiza un análisis detallado de los riesgos identificados para comprender su naturaleza y las posibles consecuencias de su materialización, se tiene en cuenta para este análisis, las causas, los efectos y las probabilidades de ocurrencia.

4. Valoración de Riesgos: Los riesgos identificados y analizados se valoran en función de su probabilidad de ocurrencia y el impacto potencial, utilizando un enfoque cualitativo o cuantitativo, según corresponda, esta fase permite priorizar los riesgos en función de su gravedad.

5. Tratamiento de Riesgos (Manejo del Riesgo): Con base en la valoración, se desarrollan estrategias para mitigar o eliminar los riesgos, implementando controles preventivos, y correctivos, este proceso también puede implicar la transferencia o aceptación del riesgo, dependiendo de los resultados de la valoración.

6. Implementación de Controles y Medidas de Mitigación: En esta fase se llevan a cabo las acciones concretas para implementar los controles y las medidas de mitigación acordadas en la fase anterior. Este paso incluye la actualización de políticas, procedimientos y tecnología para asegurar la protección de los activos.

7. Monitoreo y Seguimiento de Riesgos: Se establece un sistema de monitoreo continuo para verificar la efectividad de los controles implementados, así como para identificar posibles cambios en el entorno de riesgos, el monitoreo asegura que las medidas de tratamiento sigan siendo efectivas a lo largo del tiempo.

8. Revisión y Mejora Continua: Con base en el monitoreo y los resultados obtenidos, se realiza una revisión periódica del proceso de gestión de riesgos, esta fase permite realizar ajustes y mejoras en el plan, en función de la evolución de los riesgos, nuevas amenazas o cambios en el contexto organizacional.

9. Cierre de la Gestión del Riesgo: Una vez que los riesgos han sido tratados y controlados adecuadamente, y tras verificar que no se requieren más acciones inmediatas, se procede al cierre formal del riesgo. Sin embargo, este proceso es dinámico y puede reabrirse si surgen nuevos riesgos o condiciones.

10. Documentación y Reporte: Durante todo el proceso de gestión de riesgos, se garantiza la documentación completa de cada fase, incluyendo la evaluación de riesgos, los controles implementados y el seguimiento de los resultados. Esta documentación se utiliza para la toma de decisiones y para cumplir con los requisitos de auditoría y cumplimiento.

## Recursos

Siguiendo el esquema de Líneas de Defensa (ASIS06), los responsables de la gestión de riesgos son:

Línea Estratégica (Gobierno y Supervisión): Alta Dirección y Comité de Control Interno son responsables de establecer la visión estratégica de la seguridad de la información, definir el nivel de riesgo y garantizar que las iniciativas de seguridad estén alineadas con los objetivos organizacionales.

Primera Línea (Gestión y Operación de Controles): Equipos operativos, administradores de sistemas y responsables de seguridad tecnológica implementan y operan los controles de seguridad en el día a día. Incluye a usuarios estratégicos, quienes aplican las políticas de seguridad en sus funciones diarias.

Segunda Línea (Supervisión y Coordinación del Riesgo): Directivos y coordinadores de gestión de riesgos supervisan y evalúan el cumplimiento de los controles de seguridad, asegurando que los riesgos sean identificados y tratados de manera eficaz.

Equipos de cumplimiento y normatividad verifican la adhesión a regulaciones, estándares y mejores prácticas de seguridad.

Tercera Línea (Auditoría y Aseguramiento Independiente): Oficina de Control Interno y Auditoría Independiente realizan evaluaciones objetivas sobre la efectividad del sistema de gestión de riesgos y los controles de seguridad, proporcionando recomendaciones para la mejora continua.

Este esquema garantiza una gestión de riesgos estructurada, permitiendo la identificación temprana de amenazas, el monitoreo de controles y la evaluación independiente de la seguridad de la organización.

## Indicadores de Monitoreo

Se establecerán los siguientes indicadores clave de desempeño (KPIs) para evaluar de manera objetiva la efectividad del Plan de Gestión de Riesgos de Seguridad y privacidad de la Información. Estos indicadores permitirán monitorear el cumplimiento de los objetivos, identificar áreas de mejora y garantizar la alineación con las mejores prácticas y marcos normativos aplicables para medir la efectividad del plan a 31 de enero de 2026:

| Indicador | Meta | Frecuencia |
|---|---|---|
| Gestionar los riesgos de seguridad de la información aplicando los controles necesarios para cada situación | >95% | Anual |
| Número de auditorías de seguridad realizadas (Interna, Externa, Proveedores) | 2 auditorías | Anual |
| Cumplimiento del cronograma de gestión de riesgos | 100% | Trimestral |

## Control de cambios

El Plan de Gestión de Riesgos será revisado anualmente y actualizado según la evolución de los riesgos, los avances tecnológicos y los cambios en el marco normativo y regulatorio. Esta revisión garantizará su efectividad y alineación con las mejores prácticas internacionales, permitiendo una respuesta proactiva ante nuevas amenazas y la mejora continua en la protección de los activos de información del Ministerio de Salud y Protección Social.

| Versión | Fecha | Cambio Realizado | Responsable |
|---|---|---|---|
| 1.0 | Febrero 2025 | Documento inicial | Grupo Seguridad de la Información e Innovación |
| 1.0 | Marzo 2025 | Revisión al Plan De Gestión De Riesgos De Seguridad De La Información | Grupo Seguridad de la Información e Innovación |
| 1.1 | Marzo 2025 | Ajustes al Plan De Gestión De Riesgos De Seguridad De La Información | Grupo Seguridad de la Información e Innovación |
| 1.1 | Abril 2025 | Revisión del Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información | OAPES |
| 1.1 | Abril 2025 | Aprobación del Plan De Gestión De Riesgos De Seguridad De La Información | Líder Grupo Seguridad de la Información e Innovación |

| Versión | Fecha | Cambio Realizado | Responsable |
|---|---|---|---|
| 1.2 | Enero 2026 | Revisión y actualización anual | Comité de Control Interno |

## Plan de trabajo: Actividades y Tiempos

Este plan contempla las actividades a desarrollar, en el cronograma de trabajo que se ejecutará desde febrero de 2025 a enero de 2026, con evidencias en MiGestion.

| Actividad | Responsable | Fecha de Inicio | Fecha de Cierre | Evidencia en MiGestión |
|---|---|---|---|---|
| **1. Seguimiento y actualización de la guía ADMINISTRACIÓN INTEGRAL DE RIESGOS EN LOS PROCESOS (ASIG01)** | OAPES - Grupo Seguridad de la Información e Innovación. | Febrero 2025 | Febrero 2025 | Acta de revisión de política |
| **2. Seguimiento a la gestión de riesgos de seguridad de la información 2025-1.** | Líderes de proceso y Grupo Seguridad de la Información e Innovación. | Abril 2025 | Abril 2025 | gestión de riesgos |
| **2.1. Seguimiento a la gestión de riesgos de seguridad de la información 2025-2.** | Líderes de proceso y Grupo Seguridad de la Información e Innovación. | Julio 2025 | Julio 2025 | gestión de riesgos |
| **2.2. Seguimiento a la gestión de riesgos de seguridad de la información 2025-3.** | Líderes de proceso y Grupo Seguridad de la Información e Innovación. | Octubre 2025 | Octubre 2025 | gestión de riesgos |
| **2.3. Seguimiento a la gestión de riesgos de seguridad de la información 2025-4.** | Líderes de proceso y Grupo Seguridad de la Información e Innovación. | Enero 2026 | Enero 2026 | gestión de riesgos |
| **3. Análisis de riesgos y valoración de impacto 2025-1.** | Grupo Seguridad de la Información e Innovación | Abril 2025 | Abril 2025 | Informe de análisis de riesgos |

| Actividad | Responsable | Fecha de Inicio | Fecha de Cierre | Evidencia en MiGestión |
|---|---|---|---|---|
| **3.1. Análisis de riesgos y valoración de impacto 2025-2.** | Grupo Seguridad de la Información e Innovación | Julio 2025 | Julio 2025 | Informe de análisis de riesgos |
| **3.2. Análisis de riesgos y valoración de impacto 2025-3.** | Grupo Seguridad de la Información e Innovación | Octubre 2025 | Octubre 2025 | informe de análisis de riesgos |
| **3.3. Análisis de riesgos y valoración de impacto 2025-4.** | Grupo Seguridad de la Información e Innovación | Enero 2026 | Enero 2026 | Informe de análisis de riesgos |
| **4. Evaluación final y cierre de gestión de riesgos de seguridad de la información 2025** | Grupo Seguridad de la Información e Innovación y Oficina de Planeación | Enero 2026 | Enero 2026 | Informe de cierre anual |

## Oportunidades de Mejora

Optimización de la Capacitación Continua en Ciberseguridad: expandir y diversificar los programas de formación en ciberseguridad. Asegurarse de que todos los empleados, no solo el personal de la OTIC, esté constantemente actualizado sobre nuevas amenazas, vulnerabilidades y mejores prácticas, esto fortalecerá la respuesta ante incidentes. Podría considerarse la implementación de simulacros de ataques cibernéticos para entrenar a todo el personal de la OTIC en un entorno controlado.

Mejora de la Evaluación de Riesgos mediante Inteligencia Artificial y Análisis Predictivo: Si bien el plan incluye un análisis de riesgos detallado, la adopción de tecnologías avanzadas, como inteligencia artificial (IA) y análisis predictivo, puede mejorar significativamente la precisión en la identificación y valoración de riesgos. La IA puede ayudar a prever amenazas emergentes con base en patrones de comportamiento de usuarios y sistemas, permitiendo una respuesta más ágil y proactiva.

Automatización del Monitoreo y Respuesta a Incidentes de Seguridad: mejorar la eficiencia en la respuesta ante eventos e incidentes mediante la automatización del reporte. Implementar en MiGestion la herramienta que alerte para que se tome medidas inmediatas en caso de incidentes críticos, esto podría reducir el tiempo de respuesta, mejorando la protección frente a amenazas.

Fortalecimiento del Control y Auditoría de Proveedores Externos: A medida que se amplía el uso de servicios y tecnologías externas (por ejemplo, almacenamiento en la nube), es esencial que los controles y auditorías de los proveedores externos sean más rigurosos. Realizar auditorías periódicas sobre los proveedores que

gestionan datos sensibles del Ministerio contribuirá a asegurar que se cumplan los estándares de seguridad y protección establecidos en el plan.

Inclusión de Evaluaciones de Impacto Regulares en la Continuidad del Negocio: realizar evaluaciones periódicas de impacto en la continuidad del negocio en escenarios de crisis cibernéticas o de infraestructura. Esto fortalecería la capacidad del Ministerio para mantener operaciones críticas durante incidentes graves y garantizar la mínima interrupción en los servicios a la ciudadanía.

Refuerzo en la Gestión de Riesgos en los Procesos de Innovación: incluir un enfoque específico de gestión de riesgos para los procesos de innovación. Evaluar los riesgos asociados con la implementación de nuevas herramientas tecnológicas ayudará a anticipar vulnerabilidades antes de que sean implementadas en los sistemas operativos del Ministerio.

Mejora en la Integración de las Áreas de Control Interno y Seguridad de la Información: la mejora en la integración de los equipos de seguridad de la información y control interno puede facilitar una mejor alineación de los procesos de auditoría y gestión de riesgos. Crear flujos de comunicación más ágiles y establecer procesos conjuntos garantizaría una supervisión más efectiva de todas las actividades relacionadas con la seguridad de la información.