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 y Protección de Datos Personales

---

Seguridad de la información. Plan de Gestión de Riesgos 2026

Elaborado por: José Alexander Parra González, contratista
José Eduardo Pérez Altamar, contratista
Julio Cesar Benavides Carranza, contratista

Grupo Seguridad de la Información y Protección de Datos Personales

2026

Contenido

Resumen Ejecutivo

El Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información del Ministerio de Salud y Protección Social para el año 2026, 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 datos sensibles y críticos y que por lo tanto exige un adecuado tratamiento de los riesgos inherentes a la gestión de la información que procesa, almacena, recolecta y gestiona . 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 de Seguridad y Privacidad de la Información (MSPI) 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 de Salud y Protección Social (MSPS), 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 productos y servicios 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 27000:2018]
- Integridad: Propiedad de la información relativa a su exactitud y completitud. [ISO/IEC 27000:2018]
- Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada [ISO/IEC 27000:2018]
- 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 27000:2018]

Objetivo General

Ejecutar las acciones concretas, planeadas y aprobadas para mitigar amenazas, cuyo propósito es asegurar que el tratamiento del riesgo (reducir, aceptar evitar, y compartir) se ejecute mediante la aplicación y seguimiento de controles específicos, asignando responsables y plazos definidos.

Este Plan actúa como una hoja de ruta operativa para el grupo de Seguridad de la Información y Protección Dados Personales, lo cual garantiza que los riesgos de seguridad de la información se reduzcan a un nivel aceptable para el Ministerio de Salud y Protección Social, protegiendo así la integridad, confidencialidad y disponibilidad de los activos críticos de manera verificable y estructurada.

Objetivos específicos

1. Revisar y evaluar los activos de información críticos para el MSPS, 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 materialización de los riesgos en los sistemas de información, aplicativos en 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 para el año 2026, abarca los procesos 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 darle tratamiento, evaluar y mitigar los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y continuidad operativa de la información de 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.

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 adopta -proceso de transición- la guía del DAFP Guía para la Gestión Integral del Riesgo en Entidades Públicas versión 7-2025, en su 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 de Seguridad y Privacidad de la Información del Ministerio de las Tecnologías y las comunicaciones y estándares internacionales de referencia como la ISO/IEC 27001:2022 para la gestión de la seguridad de la información y la 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, debidamente alineado con el Modelo de Seguridad y Privacidad de la Información definido por MinTic. La misma 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] Esta metodología es un enfoque basado en el ciclo de vida de la gestión de riesgos de la Guía para la Gestión Integral del Riesgo en Entidades Públicas versión 7-2025, 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.

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.

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 evaluarán 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 2027

Indicador	Meta	Frecuencia
Eventos e Incidentes de seguridad de la información gestionados por el personal responsable dentro del MSPS	80%	trimestral
Porcentaje de evaluación de impacto y entendimiento de las sensibilizaciones de seguridad de la información realizadas sobre funcionarios y contratistas del MSPS	75%	semestral
Escenarios de Recuperación de Desastres (DRP) probados de acuerdo con el cronograma establecido en el Plan de Continuidad de Negocio del MSPS	100%	anual
Porcentaje de riesgos identificados en los procesos que hacen parte del alcance del SGSI	90%	anual
Nivel de actualización de la matriz de activos identificados para cada proceso, de acuerdo con el nivel de criticidad.	100%	anual

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	Enero 2026	Documento inicial	Grupo Seguridad de la Información e Innovación

Versión	Fecha	Cambio Realizado	Responsable
1.0	Febrero 2026	Revisión al Plan De Gestión De Riesgos De Seguridad De La Información	Grupo Seguridad de la Información e Innovación
1.1	Marzo 2026	Ajustes al Plan De Gestión De Riesgos De Seguridad De La Información	Grupo Seguridad de la Información e Innovación
1.1	Abril 2026	Revisión del Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información	OAPES
1.1	Abril 2026	Aprobación del Plan De Gestión De Riesgos De Seguridad De La Información	Líder Grupo Seguridad de la Información e Innovación
1.2	Enero 2027	Revisión y actualización anual	Grupo de Seguridad de la información y Protección de Datos Personales

Plan de trabajo: Actividades y Tiempos

Este plan contempla las actividades a desarrollar, en el cronograma de trabajo que se ejecutará desde enero de 2026 a enero de 2027, del cual se dispondrá de evidencias en el aplicativo MiGestion en el módulo de SGSI.

Se debe realizar trimestralmente un análisis en cada Proceso Certificado en la ISO 27001:2022, con el fin de entender la naturaleza de los riesgos y determinar su nivel de criticidad, en esta fase se realiza la valoración del impacto en los activos digitales, las amenazas y las vulnerabilidades, en esta etapa de valoración de impacto se deben medir las consecuencias para el Ministerio, si algún riesgo llega a materializarse.

Análisis de Riesgos y valoración de impacto

Actividad	Responsable	Fecha de Inicio	Fecha de Cierre	Evidencia en MiGestión
2. Análisis de riesgos y valoración de impacto 2026-1.	Líder de Proceso	abr-26	abr-26	gestión de riesgos
2.1. Análisis de riesgos y valoración de impacto 2026-2.	Líder de Proceso	jul-26	jul-26	gestión de riesgos
2.2. Análisis de riesgos y valoración de impacto 2026-3.	Líder de Proceso	oct-26	oct-26	gestión de riesgos
2.3. Análisis de riesgos y valoración de impacto 2026-4.	Líder de Proceso	ene-27	ene-27	gestión de riesgos

Evaluación de la gestión a los riesgos digitales

Actividad	Responsable	Fecha de Inicio	Fecha de Cierre	Evidencia en MiGestión
1. Seguimiento a la gestión de riesgos de seguridad de la información 2026-1.	Grupo Seguridad de la Información y Protección de Datos Personales	abr-26	abr-26	Informe de análisis de riesgos

1.2. Seguimiento a la gestión de riesgos de seguridad de la información 2026-2.	Grupo Seguridad de la Información y Protección de Datos Personales	jul-26	jul-26	Informe de análisis de riesgos
1.3. Seguimiento a la gestión de riesgos de seguridad de la información 2026-3.	Grupo Seguridad de la Información y Protección de Datos Personales	oct-26	oct-26	informe de análisis de riesgos
1.4. Seguimiento a la gestión de riesgos de seguridad de la información 2026-4.	Grupo Seguridad de la Información y Protección de Datos Personales	ene-27	ene-27	Informe de análisis de riesgos
4. Evaluación final y cierre de gestión de riesgos de seguridad de la información 2026	Grupo Seguridad de la Información y Protección de Datos Personales	ene-27	ene-27	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 colaboradores del Ministerio estén constantemente actualizados sobre nuevas amenazas, vulnerabilidades y mejores prácticas, esto fortalecerá la respuesta ante incidentes.

- 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.

- 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 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.

Conclusiones

Este PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN del Ministerio de Salud y Protección Social para 2026, presenta un enfoque integral y actualizado para la gestión de riesgos, alineado con estándares internacionales como ISO/IEC 27001:2022 e ISO 31000:2018, y sustentado en las políticas y guías institucionales. El plan cubre todo el ciclo de vida de los riesgos, desde su identificación y valoración hasta el tratamiento, monitoreo y mejora continua, abarcando tanto activos digitales como físicos y asegurando la resiliencia operativa frente a amenazas cibernéticas y operacionales. Se definen los roles y responsabilidades en tres líneas de defensa, lo que facilita la supervisión y la mejora constante del sistema de gestión. Además, incorpora indicadores de desempeño y revisiones periódicas para garantizar la efectividad y adaptación del plan ante cambios tecnológicos y normativos. Este documento identifica oportunidades de mejora relevantes, como el fortalecimiento de la capacitación en ciberseguridad, la adopción de inteligencia artificial para la evaluación de riesgos, el refuerzo de auditorías a proveedores externos y la colaboración del equipo de seguridad con control interno en la gestión de incidentes y reporte de los monitoreos a los riesgos.

Por último, este plan posiciona al Ministerio en un nivel avanzado de madurez en la gestión de riesgos, con una visión proactiva y adaptativa que responde a los desafíos actuales de la transformación digital y la protección de datos sensibles.