Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Ministerio de las Culturas, las Artes y los Saberes.

2026

"Se consideran copias controladas los documentos que se encuentran vigentes en ISOLUCIÓN"

Contenido

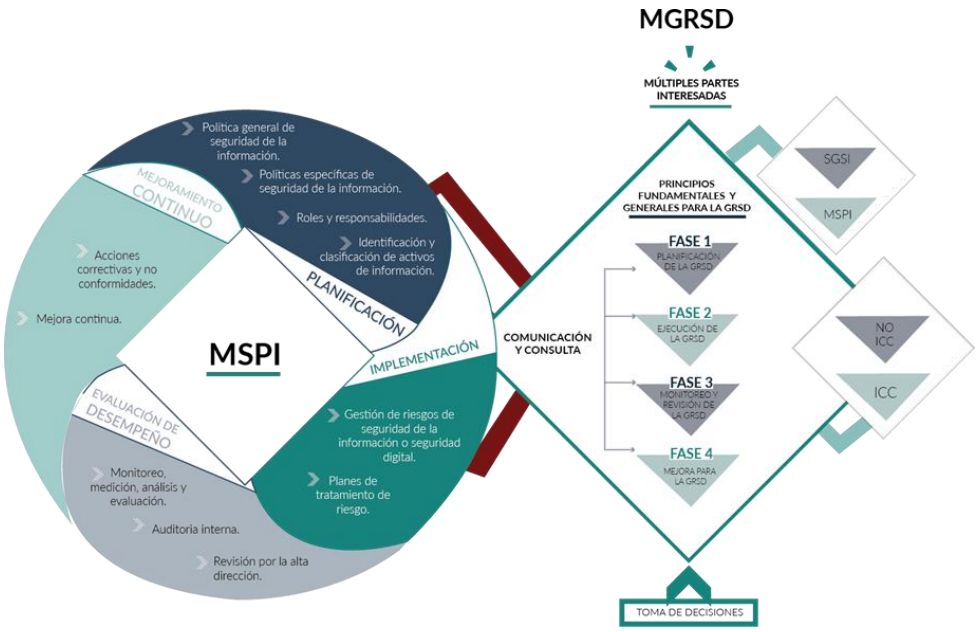
1. INTRODUCCIÓN 3
2. OBJETIVO 4
OBJETIVOS ESPECÍFICOS 4
3. ALCANCE 4
4. CONTEXTO INSTITUCIONAL 5
POLÍTICA DE ADMINISTRACIÓN DEL RIESGO 5
5. REFERENCIAS 8
6. OPERACIÓN DE LA GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN 9
Estado de la gestión de riesgos de seguridad y privacidad de la información – Vigencia 2025 11
7. ESTRATEGIAS 13

1. INTRODUCCIÓN

La gestión de la seguridad y privacidad de la información constituye un habilitador para la continuidad y confiabilidad de los servicios del Ministerio de las Culturas, las Artes y los Saberes. En este contexto, el presente Plan de Tratamiento de Riesgos se formula como un instrumento operativo para identificar, evaluar y tratar de manera progresiva los riesgos asociados a los activos de información, de acuerdo con su nivel de criticidad y con la capacidad técnica, operativa y presupuestal de la Entidad.

El plan se fundamenta en los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Administración del Riesgo institucional y la norma ISO/IEC 27001:2022, priorizando la protección de la confidencialidad, integridad y disponibilidad de la información que soporta los procesos misionales, estratégicos y de apoyo.

Se detalla a continuación las áreas del MSPI donde se integrará y aplicará de manera directa el Modelo de Gestión de Riesgos de Seguridad de la Información:



2. OBJETIVO

Definir las estrategias para identificar, evaluar y mitigar los riesgos asociados a la seguridad de la información, asegurando así la protección y resiliencia de los activos de información de la Entidad.

OBJETIVOS ESPECÍFICOS

- Proteger y reducir el riesgo asociado a los activos de información.
- Asignar los controles para cada uno de los riesgos identificados que ayuden a la mitigación del riesgo; así como su plan de implementación.
- Realizar seguimiento de los planes de manejo para el tratamiento de los riesgos identificados.

3. ALCANCE

La gestión de riesgos de seguridad de la información es aplicable y sin excepción para todos los procesos y áreas que, durante la identificación y

actualización de sus activos de información, determinen un nivel de criticidad alto. Sin embargo, los líderes de cada área tienen la autonomía de evaluar y decidir sobre la generación de riesgos asociados a sus activos, incluso si estos no son clasificados como de alta criticidad. Esta flexibilidad permite una gestión de riesgos más adaptada y efectiva, alineada con las necesidades y particularidades de cada área institucional.

4. CONTEXTO INSTITUCIONAL

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Alta Dirección del Ministerio de las Culturas, las Artes y los Saberes se encuentra comprometida con la administración integral del riesgo como un eje estratégico para garantizar el cumplimiento de la misionalidad institucional y la consecución de los objetivos estratégicos. Este compromiso se materializa a través del fortalecimiento de directrices orientadas a identificar, analizar, evaluar y tratar los riesgos, con el fin de evitar, prevenir, asumir, reducir, compartir o transferir aquellos eventos que puedan generar efectos adversos para la Entidad, así como potenciar las oportunidades que contribuyan al mejoramiento continuo del Sistema Integrado de Gestión Institucional, en concordancia con el Modelo Integrado de Planeación y Gestión – MIPG.

En este marco, el Ministerio gestiona de manera integral las amenazas externas y debilidades internas que puedan afectar sus procesos, productos y servicios, incluyendo los riesgos de gestión, fiscales, de corrupción, de lavado de activos, financiación del terrorismo y proliferación de armas (LA/FT/PA), así como los riesgos de seguridad de la información, mediante el monitoreo periódico de la eficacia y efectividad de los controles establecidos. El seguimiento a esta gestión se realiza a través del esquema de líneas de defensa definido en la Política de Administración del Riesgo y es evaluado por la Oficina de Control Interno, en el marco del Comité Institucional de Coordinación de Control

Interno, conforme a los lineamientos del MIPG.

En coherencia con lo anterior, la gestión de los riesgos de seguridad de la información se concibe como un componente transversal de la administración del riesgo institucional y como un habilitador para la protección de los activos de información del Ministerio, garantizando la confidencialidad, integridad y disponibilidad de la información. Para este propósito, la identificación, análisis, valoración y tratamiento de los riesgos digitales se realiza tomando como insumo los activos de información de cada proceso y su clasificación de acuerdo con su nivel de criticidad, en articulación con el Subsistema de Gestión de Seguridad de la Información (SGSI) y los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI.

En desarrollo de la Política de Administración del Riesgo, el Ministerio establece las siguientes directrices aplicables al Plan de Tratamiento de Riesgos de Seguridad de la Información:

- La administración del riesgo se gestiona bajo los principios de legalidad, oportunidad y valor público, y se reconoce como un elemento clave para la planeación estratégica institucional.

- Se consideran factores de riesgo todos aquellos eventos que puedan afectar la calidad de los productos, servicios y trámites de la Entidad, así como la satisfacción de los ciudadanos, usuarios y grupos de valor.

- Se prioriza la gestión de los riesgos derivados del incumplimiento normativo, de posibles afectaciones patrimoniales, sanciones de los entes de control, fallos judiciales, daños antijurídicos y compromisos éticos, incluidos aquellos asociados a la información y a los servicios digitales.

- La Alta Dirección garantiza la asignación de los recursos necesarios

para la gestión del riesgo, promoviendo la participación de los servidores públicos, la comunicación permanente y el seguimiento a las acciones de mejora definidas en los planes de tratamiento.

- En la formulación e implementación de nuevas políticas, proyectos, productos y servicios, se aplica de manera obligatoria la metodología institucional de administración del riesgo, con el fin de identificar, evaluar y establecer controles preventivos que eviten la materialización de riesgos o permitan la gestión de oportunidades.

- Para los riesgos de seguridad de la información, se exige su articulación con los activos de información, la definición de controles técnicos, administrativos y organizacionales, y la incorporación de planes de tratamiento orientados a minimizar su impacto y probabilidad.

- El monitoreo y seguimiento de los mapas de riesgos y de los controles asociados a la seguridad de la información será responsabilidad de los líderes de proceso, en coordinación con las instancias de la segunda y tercera línea de defensa, conforme al ciclo de control institucional.

De esta manera, el Plan de Tratamiento de Riesgos de Seguridad de la Información se articula directamente con la Política de Administración del Riesgo del Ministerio, asegurando que los riesgos digitales sean gestionados de forma sistemática, coherente y alineada con los objetivos estratégicos de la Entidad, fortaleciendo la cultura de control, la toma de decisiones informada y la protección de la información como activo estratégico institucional.

5. REFERENCIAS

Normativa	Entidad	Descripción
Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP es la Versión 7	Departamento Administrativo de Función Pública	Metodología para la gestión integral del riesgo
Resolución 02277 de 2025	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
Resolución 460 de 2022	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno digital, y se dictan los lineamientos generales para su implementación.
Resolución 500 de2021	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Decreto 620 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Resolución 1519 de 2020.	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos

Normativa	Entidad	Descripción
Directiva 002 de 2020	Presidencia de la Republica	Medidas para atender la contingencia generada por el covid-19, a partir uso de las tecnologías la información y las telecomunicaciones - TIC
CONPES 3995 de 2020.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política Nacional de Confianza y Seguridad Digital.
Decreto 612 de 2018	Presidencia de la Republica	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado
Ley 1581 de 2012	Congreso de Colombia	Se dictan disposiciones generales para la protección de datos personales

6. OPERACIÓN DE LA GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

La gestión de los riesgos de seguridad de la información en el Ministerio de las Culturas, las Artes y los Saberes se desarrolla bajo una metodología institucional estandarizada, alineada con los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG, el Modelo de Seguridad y Privacidad de la Información – MSPI y la Política de Administración del Riesgo de la Entidad.

Para tal efecto, se adoptan como referentes metodológicos la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" del Departamento Administrativo de la Función

Pública (DAFP) y la "Guía de orientación para la gestión de riesgos de seguridad digital" del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), incorporando las buenas prácticas vigentes en gestión de riesgos de seguridad de la información.

La operación de la gestión del riesgo se fundamenta en un enfoque basado en activos de información, mediante el cual se identifican, analizan, evalúan y tratan los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información que soporta los procesos misionales, estratégicos y de apoyo de la Entidad. Este enfoque permite priorizar los riesgos de acuerdo con la criticidad de los activos, su nivel de exposición y el impacto potencial sobre la continuidad del servicio, la protección de los datos personales, el cumplimiento normativo y la confianza institucional.
El proceso operativo de gestión del riesgo en seguridad de la información se estructura en las siguientes fases:

- Identificación: reconocimiento de amenazas, vulnerabilidades y eventos de riesgo asociados a los activos de información, considerando el contexto interno y externo de la Entidad, los cambios tecnológicos, los incidentes ocurridos y las amenazas emergentes.

- Análisis y evaluación: valoración de los riesgos en términos de probabilidad e impacto, determinando el nivel de riesgo inherente y residual conforme a los criterios institucionales de aceptación y tolerancia.

- Tratamiento: definición e implementación de controles administrativos, técnicos y organizacionales orientados a evitar, reducir, transferir o aceptar los riesgos, mediante planes de tratamiento formalmente documentados y priorizados.

- Monitoreo y seguimiento: verificación periódica de la efectividad de los controles implementados, la evolución del

nivel de riesgo residual y el avance de los planes de tratamiento, en coherencia con el ciclo de control institucional y el esquema de líneas de defensa.

Esta operación se articula de manera directa con los procedimientos de gestión de incidentes de seguridad de la información, de forma que los eventos materializados retroalimentan la identificación de nuevos riesgos, el ajuste de controles y la actualización de los planes de tratamiento, garantizando un enfoque de mejora continua.

En consecuencia, la gestión del riesgo de seguridad de la información no se concibe como un ejercicio aislado, sino como un componente transversal de la gestión institucional, integrado a la planeación estratégica, a la administración de los activos de información y a los procesos de control y evaluación, asegurando una respuesta oportuna frente a amenazas, el cumplimiento de los lineamientos normativos vigentes y el fortalecimiento de la postura de seguridad digital del Ministerio.

Estado de la gestión de riesgos de seguridad y privacidad de la información – Vigencia 2025

Durante la vigencia 2025, el Ministerio de las Culturas, las Artes y los Saberes adelantó la gestión de los riesgos de seguridad y privacidad de la información de manera articulada con la Política de Administración del Riesgo institucional, el Modelo Integrado de Planeación y Gestión (MIPG) y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).

Con base en el reporte institucional de riesgos, se identificaron y gestionaron 21 riesgos clasificados como riesgos de Seguridad de la Información, asociados a activos de información de diferentes procesos misionales, estratégicos y de apoyo de la Entidad. Estos riesgos se encuentran en etapa de seguimiento de controles, lo que evidencia que cuentan con medidas de tratamiento definidas y se

encuentran bajo monitoreo permanente por parte de los responsables de proceso.

Los riesgos identificados están relacionados principalmente con posibles afectaciones a la disponibilidad, integridad y confidencialidad de la información, derivadas de eventos como fallas en plataformas tecnológicas, indisponibilidad de servicios, uso inadecuado de credenciales, ausencia o debilidad de respaldos de información, y dependencias tecnológicas críticas para la operación institucional.

Desde el punto de vista organizacional, los riesgos de seguridad de la información se distribuyen en diversos procesos institucionales, destacándose aquellos asociados a la gestión tecnológica y a los procesos misionales que dependen de manera directa de los servicios de información y de las plataformas digitales para la prestación de sus servicios.
La gestión de estos riesgos durante la vigencia 2025 se enfocó en:

- La aplicación de controles técnicos, administrativos y organizacionales.
- El seguimiento periódico a la efectividad de los controles establecidos.
- La articulación con los procedimientos de gestión de incidentes de seguridad de la información.
- La retroalimentación del análisis de riesgos a partir de eventos materializados y lecciones aprendidas.

El presente Plan de Tratamiento de Riesgos 2026 da continuidad a la gestión adelantada en 2025, priorizando acciones viables, medibles y alineadas con las capacidades institucionales. Sus estrategias se orientan al fortalecimiento progresivo de los controles existentes, al

cierre de brechas críticas y a la reducción gradual del nivel de riesgo residual, en coherencia con el contexto organizacional y los recursos disponibles.

7. ESTRATEGIAS

Eje	Identificación de Riesgos de Seguridad y Privacidad de la Información
Actividad	Identificar los riesgos asociados a los activos de información con criticidad alta o aquellos que los lideres definan, considerando amenazas, vulnerabilidades, impactos y escenarios de materialización, con base en la metodología institucional de gestión del riesgo.
Producto	Riesgos de seguridad y privacidad de la información. Registrados en ISOLUCION
Tiempo estimado	2 meses (marzo - abril 2026)
Responsable	Líderes de proceso, con apoyo del Oficial de Seguridad de la Información

Eje	Análisis y Evaluación del Riesgo
Actividad	Valorar la probabilidad e impacto de los riesgos identificados, priorizando aquellos con mayor nivel de exposición, conforme a los criterios de aceptación definidos por la Entidad.
Producto	Riesgos de seguridad y privacidad de la información. Registrados en ISOLUCION
Tiempo estimado	2 meses (marzo - abril 2026)
Responsable	Líderes de proceso, con apoyo del Oficial de Seguridad de la Información

Eje	Tratamiento del Riesgo
Actividad	Definir e implementar las opciones de tratamiento para los riesgos priorizados (mitigar, aceptar, transferir o evitar), mediante la selección y aplicación de controles administrativos, técnicos y físicos alineados con el MSPI e ISO/IEC 27002:2022.
Producto	Riesgos de seguridad y privacidad de la información. Registrados en ISOLUCION
Tiempo estimado	2 meses (marzo - abril 2026)
Responsable	Líderes de proceso, con apoyo del Oficial de Seguridad de la Información

Eje	Monitoreo y Revisión del Riesgo
Actividad	Realizar seguimiento periódico al estado de los riesgos tratados, a la eficacia de los controles implementados y a los cambios en el contexto institucional, ajustando el plan cuando sea necesario.
Producto	Informes de seguimiento y matriz de riesgos actualizada.
Tiempo estimado	Actividad permanente durante la vigencia 2026
Responsable	Segunda línea de defensa