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

Ministerio de las Culturas, las Artes y los Saberes.

2025

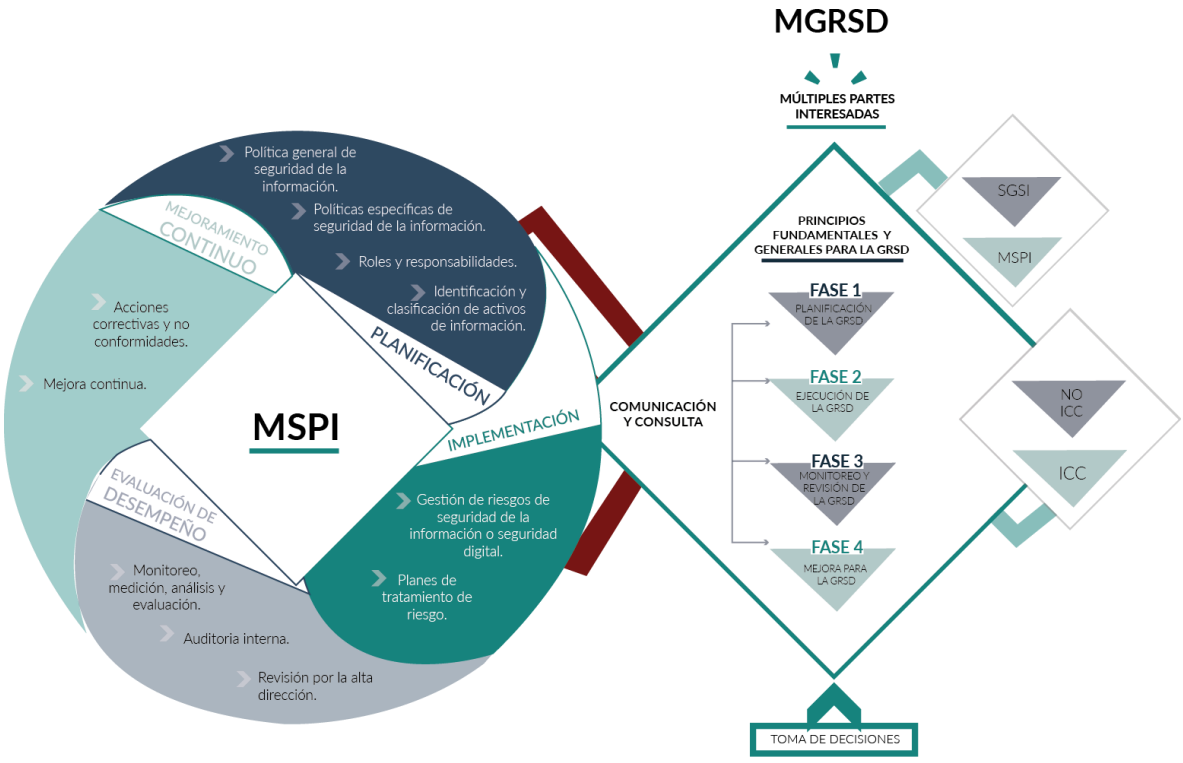
Contenido

1. INTRODUCCIÓN

La gestión efectiva de la seguridad y privacidad de la información es hoy en día un factor clave para el éxito y la continuidad operativa de cualquier entidad. Con el propósito de enfrentar los riesgos relacionados con estos aspectos de manera eficiente, hemos desarrollado un plan de tratamiento de riesgos. Este plan se fundamenta en las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI) y se alinea con nuestra política organizacional de gestión de riesgos.

Implementar este plan facilitará la identificación, evaluación y manejo proactivo de los riesgos, garantizando así la integridad, confidencialidad y disponibilidad de la información institucional. Se enfoca no solo en la tecnología, sino también en los procesos organizacionales y el componente humano.

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. OBJETIVOS

OBJETIVO GENERAL

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. 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 de riesgos, a través del fortalecimiento de directrices que permiten gestionar, evitar, prevenir, asumir, reducir, compartir o transferir los riesgos que pueden implicar efectos negativos en la Entidad, tanto como aquellos que permiten aprovechar, potenciar, operar y/o aumentar las oportunidades de mejorar la eficacia del Sistema Integrado de Gestión Institucional.

Así mismo, se gestionan de manera integral las amenazas externas y debilidades internas, los riesgos de calidad para los productos y servicios, los riesgos de seguridad de la información y los posibles actos que se deriven de los riesgos de corrupción, mediante el monitoreo periódico a la eficacia y efectividad de los controles establecidos por los procesos. El seguimiento a esta gestión es realizado por la Oficina de Control Interno y publicado conforme a los requerimientos legales vigentes para la toma decisiones por parte de la Alta Dirección.

En su compromiso con la promoción de los riesgos positivos, entendidos como oportunidades externas o fortalezas internas que permiten orientar y alinear los riesgos con los objetivos estratégicos y dar cumplimiento a la normatividad legal vigente; la Alta Dirección vela por la superación de sus capacidades internas en relación con el contexto interno y externo que afecta sus prioridades.

En concordancia con lo mencionado, se establecen las siguientes directrices:

- La Administración del Riesgo es gestionado basándose en el concepto de oportunidad, legalidad y como un asunto clave para el éxito de su planeación estratégica.

- La Administración del Riesgo considera como un factor de riesgo, todo aquello que afecte la calidad de los productos, servicios y trámites de la Entidad e impacta la satisfacción de los ciudadanos, usuarios y/o beneficiarios.

- La Administración del Riesgo para la entidad considera los efectos del incumplimiento de la legislación vigente y desarrollo jurisprudencial que puedan conllevar a detrimento patrimonial, multas, hallazgos de los entes de control, tutelas, fallos judiciales en contra y cualquier evento de daño antijurídico, de ética pública y compromiso ante la comunidad.

- La Alta Dirección determinará los recursos necesarios para la gestión del riesgo, propiciando espacios de participación de los colaboradores, un proceso permanente de comunicación, revisión, seguimiento y control a las acciones de mejora para el tratamiento de los riesgos.

- En la implementación de una nueva política cultural, así como en el diseño y/o desarrollo de nuevos productos y servicios se deberá tener en cuenta la metodología establecida en el P-OPL-013 Procedimiento de Administración del Riesgo, a fin de que el responsable del proceso actúe de manera preventiva, realizando la respectiva identificación, análisis, evaluación y establecimiento de controles que prevengan la materialización del riesgo o la potenciación de oportunidades.

- Para la identificación y tratamiento de los riesgos de seguridad de la información o riesgos digitales, se debe tomar como insumo los activos de información de cada proceso y su clasificación en términos de nivel de criticidad.

- Los riesgos transversales serán monitoreados y gestionados por los procesos que tienen en su propósito las cuestiones o eventos a mitigar o potenciar, sin embargo, por su carácter transversal los procesos afectados tendrán la oportunidad de manifestar sus consideraciones y opiniones en la construcción de los mapas, en la gestión de los controles, en el monitoreo y en el seguimiento.

- El monitoreo de los mapas de riesgos y la implementación de los controles se realizará por parte de los líderes de cada proceso y/o

proyecto, conforme el ciclo de control aprobado en el marco de este documento en su capítulo final.

- Se tendrá en cuenta para los Riesgos con nivel de riesgo residual diferente de bajo, la implementación de los planes de tratamiento a los riesgos, acorde con los lineamientos definidos por MINTIC.

4. ALCANCE

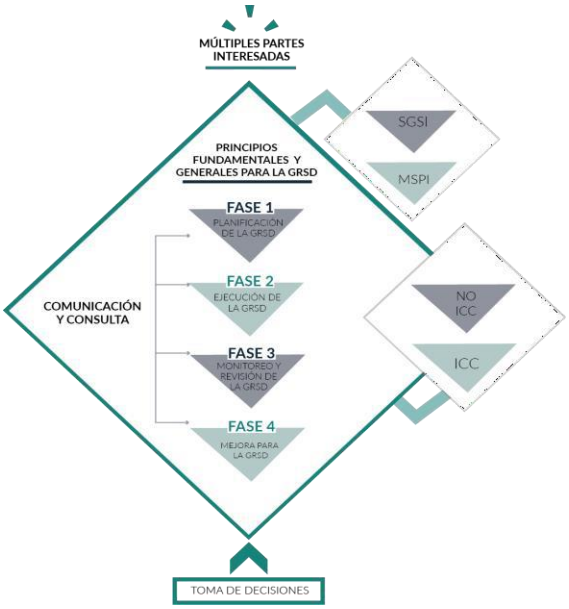
La gestión de riesgos de seguridad de la información es aplicable y sin excepción para todos los procesos y áreas que, durante la identificación y actualización de sus activos de información, determinen un nivel de criticidad alto. Sin embargo, los líderes de cada área tienen la autonomía de evaluar 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.

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

A continuación, se relaciona la metodología adoptada para la gestión de riesgos de seguridad de la información en la entidad, basándose en dos recursos fundamentales: la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" del Departamento Administrativo de la Función Pública (DAFP), actualizada en noviembre de 2022, y la "Guía de orientación para la gestión de riesgos de seguridad digital" del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Este plan sigue las fases metodológicas y se alinea con la Política de Administración de Riesgos institucional. Esta alineación se extiende desde

la identificación estratégica de riesgos de seguridad digital hasta la implementación y monitoreo efectivo de las acciones de gestión de riesgos.



6. ESTRATEGIAS

LÍNEA DE ACCIÓN	ACTIVIDADES
Identificación, consolidación de riesgos de seguridad de la información y seguridad digital	Identificar, analizar y evaluar los riesgos de aquellos activos de información con criticidad alta
	Establecer controles y planes de tratamiento sobre los riesgos
	Aceptar y aprobar los riesgos identificados por cada uno de los lideres de área
	Estructurar las carpetas para almacenamiento de las evidencias reportadas en los seguimientos.

Seguimiento planes de tratamiento	Realizar seguimiento a los planes de manejo de riesgo de seguridad de la información establecidos por cada uno de los lideres de las áreas, con sus respectivas evidencias.
Documentación de controles	Declaración de aplicabilidad

7. REFERENCIAS

Normatividad	Entidad	Descripción
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 de 2021	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
Resolución 2893 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPA, y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado colombiano.

Normatividad	Entidad	Descripción
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
CONPES 3854 de 2016.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política de Seguridad Digital del Estado Colombiano
Decreto 1078 de 2015	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Ley 1712 de 2014	Presidencia de la Republica	Ley de transparencia y el derecho a la información pública nacional
Ley 1581 de 2012	Congreso de Colombia	Se dictan disposiciones generales para la protección de datos personales
CONPES 3701 de 2011.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Lineamientos de Política para Ciberseguridad y Ciberdefensa.