Igualdad

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

Francia Elena Márquez Mina
Ministra de Igualdad y Equidad

Ligia Galvis Amaya
Jefe Oficina de Tecnologías de la Información

Juan Diego Mallama C.
Luz Amparo Gantiva R.
Nelson Alberto Gutiérrez P.
Carlos Fredy Rey C.
Andrés Felipe Rodríguez G.
Oficina de Tecnologías de la Información - Grupo de Transformación Digital

Edwin Sánchez R.
Natalia Bayona A.
Rafael Coronado B.
Joan Daniel Barragán R.
Santiago Andrés Díaz M
Kevin Santiago Sabogal H.
Iván Andrés Cardona M.
Oficina de Tecnologías de la Información - Grupo Servicios Tecnológicos

Estructuración visual del documento realizada por: Oficina Asesora de Planeación

Fecha de Aprobación Versión 1: 30-01-2025

Contenido

1. Presentación

El Plan de Tratamiento de Riesgos del Ministerio de Igualdad y Equidad - MIE tiene como propósito establecer medidas efectivas para mitigar los riesgos identificados en el análisis institucional, como la pérdida de confidencialidad, integridad y disponibilidad de los activos de información. Estas acciones buscan garantizar la seguridad y la privacidad de la información, minimizando incertidumbres que puedan afectar el cumplimiento de los objetivos estratégicos del **MIE**.

Este plan se diseña con el fin de evaluar y priorizar las acciones necesarias para abordar los riesgos de seguridad y privacidad de la información presentes en los procesos de la entidad. Estas acciones se organizan en actividades, detallando responsables y fechas de ejecución, asegurando su implementación durante la vigencia del plan.

La definición de estas actividades se fundamenta en el análisis de riesgos, en las necesidades particulares del Ministerio y en el contexto de sus procesos, enfocado en su misión de promover la equidad y la igualdad; el plan proporciona herramientas para identificar las características de los riesgos y trazar los pasos necesarios para ejecutar las medidas de mitigación de manera efectiva y alineada con los valores institucionales. En ese contexto, el plan de tratamiento de riesgos contempla estrategias específicas para identificar, analizar, mitigar y monitorear los riesgos relacionados con la seguridad y privacidad de la información, priorizando la protección de la información vinculada a los enfoques de derechos, género, diferencial, étnico-racial e interseccional, considerando la sensibilidad de los datos que impactan directamente en la vida de las poblaciones históricamente discriminadas o marginadas. El tratamiento de riesgos incluirá controles técnicos, administrativos y legales que aseguren el cumplimiento de las normativas aplicables, así como mecanismos de auditoría y revisión

periódica, lo que permitirá, a través de seguimientos basados en indicadores de gestión y desempeño, evaluar continuamente el impacto de las medidas adoptadas en la reducción de los riesgos identificados. Tales indicadores, articulados con las funciones del MIE, permitirán medir la efectividad de los controles, identificar brechas, y proponer mejoras para garantizar la seguridad y privacidad de la información en todos los niveles. Las recomendaciones para el sistema de indicadores incluirán criterios claros de evaluación, periodicidad de análisis, responsables del seguimiento, y acciones correctivas para atender desviaciones, asegurando que el tratamiento de riesgos respalde los objetivos del MIE.

2. Introducción

El Plan de Tratamiento de Riesgos del **Ministerio de Igualdad y Equidad** busca fomentar una cultura preventiva que permita la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos asociados a la seguridad y privacidad de la información, seguridad digital y la continuidad operativa de los servicios tecnológicos. Este enfoque estratégico está orientado a reducir las afectaciones que puedan comprometer el cumplimiento de los objetivos institucionales, especialmente aquellos relacionados con la equidad, la inclusión social y la transformación digital como herramientas para el desarrollo y la igualdad.

Para garantizar una gestión objetiva y efectiva de los riesgos, este plan establece acciones que permiten mitigar situaciones que podrían impactar negativamente en la misión del Ministerio. Entre los riesgos abordados se incluyen interrupciones operativas, vulnerabilidades digitales y amenazas a la confidencialidad, integridad y disponibilidad de los activos de información.

El plan se desarrolla en coherencia con los lineamientos establecidos en documentos normativos clave, como el Documento CONPES 3995 de 2020,

Resolución 500 de 2021 y el Decreto Único Reglamentario 1078 de 2015, que incluye disposiciones sobre seguridad y privacidad de la información. Asimismo, adopta las mejores prácticas internacionales como las normas ISO 27001, junto con las guías del **Modelo Integrado de Planeación y Gestión (MIPG)**, garantizando estándares de calidad y cumplimiento normativo en la administración del riesgo.

En línea con el Decreto 612 de 2018, este documento se actualiza para fortalecer el Plan de Tratamiento de Riesgos al interior del Ministerio, integrando las recomendaciones del Comité del Modelo Integrado de Gestión (MIG).

3. Definiciones[1]

Riesgo: Efecto que se causa sobre los objetivos de las entidades debido a eventos potenciales. Esto incluye la posibilidad de pérdidas por deficiencias en recursos humanos, procesos, tecnología, infraestructura o acontecimientos externos.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza explote una vulnerabilidad, causando pérdida o daño en un activo de información. Combina la probabilidad del evento y sus consecuencias.

Riesgo Fiscal: Efecto dañoso sobre los recursos públicos, bienes o intereses patrimoniales de naturaleza pública a causa de un evento potencial.

Gestión del Riesgo Fiscal: Conjunto de actividades que las entidades deben desarrollar para identificar, valorar, prevenir y mitigar los riesgos fiscales sobre bienes, recursos o intereses patrimoniales públicos.

[1] Tomado de Guía para la administración del riesgo y el diseño de controles en entidades públicas - DAFP Versión 6

Gestor Público: Persona que participa directa o indirectamente en la administración de bienes, recursos o intereses patrimoniales de naturaleza pública. Esto incluye contratistas, interventores y supervisores, entre otros.

Bien Público: Comprende bienes muebles e inmuebles de propiedad pública destinados al uso público o a la prestación de servicios públicos. Incluye bienes de uso público, como calles y parques, y bienes fiscales, como edificios y equipos.

Causa Raíz: Es el evento o acción que, al presentarse, genera directamente un efecto dañoso sobre bienes, recursos o intereses patrimoniales públicos. Es la causa principal que, si no ocurre, el daño no se materializa.

Control: Medida implementada para reducir o mitigar un riesgo. Puede ser preventivo, correctivo o detectivo, según el contexto.

Riesgo Inherente: Nivel de riesgo propio de la actividad antes de aplicar controles, calculado como la combinación de probabilidad e impacto del riesgo.

Nivel de Riesgo: Valor determinado al combinar la probabilidad de ocurrencia de un evento dañino y el impacto de dicho evento en la capacidad institucional para alcanzar los objetivos.

Confidencialidad: Propiedad de la información que garantiza que no sea accesible ni divulgada a individuos, entidades o procesos no autorizados. Es un pilar clave en la seguridad de la información.

Integridad: Propiedad que asegura que la información es exacta, completa y confiable, evitando modificaciones no autorizadas.

Disponibilidad: Propiedad de la información que garantiza su accesibilidad y usabilidad cuando sea requerida por una entidad autorizada.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una amenaza para causar un impacto negativo en la información o los procesos.

Activo de Información: Elemento utilizado por la organización en su entorno digital, como aplicaciones, servicios web, hardware, redes y datos físicos o digitales.

4. Objetivos

- ✓ Definir y apropiar políticas de seguridad que permitan preservar la confidencialidad, disponibilidad y autenticidad de la información institucional.
- ✓ Garantizar el cumplimiento de los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas aplicables a la seguridad y privacidad de la información.
- ✓ Identificar y gestionar los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad operativa.
- ✓ Promover y fortalecer el conocimiento interno relacionado con la gestión de riesgos asociados a la seguridad y privacidad de la información, la seguridad digital y la continuidad de la operación de los servicios.

5. Alcance

El fin principal es implementar una gestión eficiente de riesgos en las áreas de seguridad y privacidad de la información, seguridad digital y continuidad operativa, asegurando la integración de buenas prácticas en los procesos de la entidad. Esto permitirá prevenir incidentes que puedan comprometer los objetivos institucionales y facilitar la toma de decisiones informadas.

1. **Lineamientos Generales para la Gestión de Riesgos**

- **Identificación y Análisis**: Establecer criterios para reconocer y evaluar los riesgos que puedan afectar la seguridad de la información y la continuidad de los servicios.
- **Tratamiento y Monitoreo**: Diseñar e implementar medidas correctivas y preventivas, asegurando un seguimiento constante de los riesgos tratados.
- **Evaluación y Mejora Continua**: Revisar periódicamente los riesgos y las estrategias implementadas para garantizar su efectividad y alineación con los objetivos institucionales.

2. Plan de Tratamiento de Riesgos

Este plan priorizará los riesgos clasificados como Moderados, Altos y Extremos, conforme a los lineamientos del Ministerio de TIC. Los riesgos en niveles inferiores serán aceptados bajo las políticas de tolerancia al riesgo de la entidad.

3. Adopción de Buenas Prácticas

Integrar estándares reconocidos internacionalmente como ISO 27001 (Seguridad de la Información) en los procesos de gestión, fortaleciendo la capacidad del Ministerio para enfrentar amenazas y proteger sus activos de acuerdo con el nivel de madurez de acuerdo con el instrumento de autoevaluación MSPI.

4. Cumplimiento Normativo

Asegurar la conformidad con los requisitos legales y regulatorios vigentes en materia de protección de la información y continuidad operativa, garantizando la integridad de los procesos.

5. Cultura de Seguridad

Fomentar una cultura organizacional basada en la seguridad y privacidad de la información, promoviendo la sensibilización continua de todos los colaboradores.

6. Marco Referencial

6.1. Política de Administración de Riesgos

El **Ministerio de Igualdad y Equidad**, en el marco de su compromiso con la promoción de la equidad, la inclusión y la garantía de derechos, establece esta política de administración de riesgos como parte de su Modelo Integrado de Gestión. Su propósito es implementar medidas de prevención, monitoreo y seguimiento que permitan mitigar riesgos en las actividades y procesos relacionados con la ejecución de políticas, planes, programas y estrategias destinados a reducir las desigualdades, proteger los derechos humanos y promover la justicia social.

Esta política busca prevenir situaciones que puedan afectar:

- La transparencia y ética institucional.
- La seguridad y privacidad de la información.
- La continuidad operativa de los servicios tecnológicos para la población.
- La gestión de recursos destinados a programas sociales.
- Los aspectos seguridad informática y de la información en la ejecución de proyectos.

El Ministerio prioriza el cumplimiento de sus objetivos institucionales, asegurando el uso eficiente de los recursos y una atención integral a los grupos de interés, especialmente aquellos de especial protección constitucional. Por lo

cual, atiende las políticas públicas y las directrices establecidas, especialmente las que contiene el CONPES 4089 de 2022 sobre el Plan Nacional de Política Criminal 2022 – 2025 en el sentido de fortalecer el uso de las tecnológicas de información que permitan apoyar la efectividad de la implementación de una política criminal, facilitando la articulación del MIE con las entidades que participan en las etapas de investigación y juzgamiento que ya han incluido en sus lineamientos, objetivos y direccionamientos internos, el uso de herramientas tecnológicas, métodos y modelos de análisis de datos y de información geoespacial y georreferencial, uso de fuentes tecnológicas externas como las cámaras de los sistemas de vigilancia, implementación del expediente electrónico, y el desarrollo de audiencias virtuales, entre otros. No obstante, el CONPES evidencia que las entidades que han adoptado estas tecnologías han tenido poca efectividad en el uso de herramientas que pueden apoyar en la aplicación de la justicia, por la falta de articulación entre entidades y la constante mutación de la criminalidad, lo que exige la articulación de los datos de las diferentes entidades, el desarrollo de análisis, sistemas de información y herramientas que faciliten la gestión de las actividades de investigación. Por ello, el CONPES establece en la Línea de acción 7. *"Fortalecer los sistemas de información y analítica de datos, así como, la gestión institucional y del conocimiento, para la disrupción de las organizaciones criminales en los territorios"*.

Por otro lado, el Ministerio de Justicia y del Derecho con apoyo de la Policía Nacional, Procuraduría General de la Nación y la Fiscalía General de la Nación, diseñará una estrategia interinstitucional que incorpore la utilización de herramientas tecnológicas de intercambio de información, para la disrupción de estructuras delincuenciales dedicadas al uso de menores para la comisión de delitos y violencia sexual. La naturaleza del documento CONPES 4089 de 2022 como Política Criminal, tiene por objetivo fortalecer la acción del Estado para prevenir delitos, visibilizar y perseguir violaciones especialmente las basadas en género y proteger los derechos de los colombianos. Uno de los lineamientos que impacta directamente el MIE en el documento CONPES, es el de coordinar la elaboración de un análisis criminológico sobre el efecto de las sanciones

impuestas a los adolescentes, que sirva de base para la generación de estrategias de prevención de la reiteración en el delito, de acuerdo con la información que sea reportada por el Instituto Colombiano de Bienestar Familiar y la Policía Nacional.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del MIE se fundamentará en un marco de referencia, que incorpore las normativas nacionales, estándares internacionales y lineamientos de transformación digital establecidos en el CONPES 4089 de 2022, la Ley 2297 de 2023, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los nuevos estándares internacionales como ISO/IEC 27001:2022. Este marco permitirá al MIE alinear sus controles de seguridad con las mejores prácticas y garantizar la protección de los datos sensibles de las poblaciones vulnerables.

La implementación de tecnologías emergentes como inteligencia artificial (IA) y Blockchain se realizará bajo principios éticos y responsables. Estas tecnologías serán evaluadas en términos de impacto en la privacidad y seguridad de la información. La protección de datos sensibles se priorizará a través de la adopción de herramientas tecnológicas y estrategias para gestionar de forma segura los datos relacionados con poblaciones históricamente marginadas, en cumplimiento con las nuevas exigencias regulatorias.

En concordancia con la Ley 2297 de 2023 se implementarán herramientas tecnológicas de gestión específicas para la protección de datos sensibles y evaluaciones periódicas de riesgos y controles asociados al manejo de información en entornos digitales. Así mismo se realizará un seguimiento periódico al Modelo de Seguridad y Privacidad de la Información (MSPI), de manera que se implementen nuevas técnicas que permitan afrontar los nuevos desafíos frente a la gestión de seguridad y privacidad de la información, tales como:

- Gestión de riesgos en entornos Cloud: Se implementarán controles específicos para garantizar la seguridad en la adopción de servicios en la

nube, incluyendo la evaluación de proveedores y la protección de datos almacenados y procesados en estos entornos.

- Desafíos frente al desarrollo de actividades tele presenciales: Se adoptarán medidas como el uso de redes seguras, autenticación multifactor y cifrado de extremo a extremo para mitigar riesgos asociados al trabajo remoto.
- Modelo Zero Trust: Se aplicará un enfoque basado en la confianza mínima, asegurando que cada acceso a los sistemas de información o herramientas tecnológicas sea validado rigurosamente, independientemente de la ubicación del usuario o dispositivo.
- Continuidad del negocio: Se integrarán planes de continuidad adaptados a los nuevos riesgos, asegurando la recuperación rápida y segura ante incidentes de seguridad.

Frente a las nuevas tecnologías que serán implementadas, el MIE adoptará las recomendaciones del estándar ISO/IEC 27001:2022 que introduce prácticas avanzadas para la gestión de riesgos de seguridad de la información, como:

- Controles contra Ransomware: Políticas de respaldo, segmentación de redes y monitoreo proactivo para prevenir ataques de Ransomware.
- Seguridad en servicios Cloud: Estrategias específicas para proteger datos almacenados en la nube y garantizar el cumplimiento de los acuerdos de nivel de servicio (SLA).
- Gestión de riesgos en la cadena de suministro digital: Evaluación continua de riesgos asociados a terceros y proveedores tecnológicos.
- Protección contra amenazas avanzadas persistentes (APT): Implementación de tecnologías como detección avanzada de amenazas y análisis de comportamiento para prevenir ataques sofisticados.

Este marco será revisado y actualizado de forma periódica para garantizar su vigencia y efectividad, en función de los cambios tecnológicos, normativos y de contexto operativo del Ministerio.

6.2. Objetivo de la Política

Establecer lineamientos claros para gestionar los riesgos asociados a seguridad y privacidad de la información, seguridad digital y continuidad operativa de los servicios (riesgos de interrupción) en el marco de la misión del Ministerio. Esto incluye prevenir la materialización de riesgos que puedan comprometer la equidad, la protección de derechos y la atención a poblaciones en situación de desigualdad.

El enfoque de la política está orientado a:

- Asegurar decisiones oportunas y fundamentadas.
- Minimizar efectos adversos en las operaciones institucionales.
- Garantizar la sostenibilidad y continuidad de los compromisos con los grupos de interés.

6.3. Tratamiento de los Riesgos

La gestión de riesgos es una responsabilidad compartida, liderada por la oficina de tecnologías de la información, e incluye las siguientes categorías:

1. **Aceptar el Riesgo:**

Los riesgos bajos pueden ser aceptados, siempre bajo seguimiento continuo.

Nota: Ningún riesgo asociado a corrupción será aceptado.

2. **Reducir el Riesgo**:

Implementar medidas o controles que disminuyan la probabilidad, el impacto o ambos, asegurando la eficiencia en el uso de recursos.

3. **Evitar el Riesgo**:

Suspender o no iniciar actividades que generen riesgos inaceptables o que puedan comprometer los derechos de los sujetos de especial protección constitucional.

4. **Compartir el Riesgo**:

Transferir o compartir una parte del riesgo mediante seguros o alianzas estratégicas, sin transferir la responsabilidad sobre el mismo.

6.4. Gestión de Riesgos de Seguridad, Privacidad y Continuidad Operacional

El Ministerio se compromete a:

1. **Identificar y analizar riesgos** que puedan impactar los procesos destinados a la equidad, la inclusión y la justicia social.
2. **Tratar y monitorear las amenazas** que afecten la información, la operación de servicios y la protección de recursos.
3. **Alinear las estrategias de gestión de riesgos** con los objetivos institucionales, asegurando que los niveles de riesgo aceptados sean acordes con la misión de proteger y garantizar los derechos de la población.

7. Metodología

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016). [2]

La clasificación de activos de información del MIE establecerá la forma adecuada de uso de los activos que posee la entidad, de cómo deberán ser utilizados, los roles y responsabilidades que tienen los funcionarios sobre los mismos y el nivel de clasificación de la información que cada activo tendrá.

El inventario y clasificación de activos pretende identificar plenamente los documentos, bases de datos, sistemas de información, infraestructura tecnológica y personas que tienen valor para la entidad, por lo cual se debe elaborar y mantener un inventario de los mismos, que identifique además el propietario, su clasificación en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada, etiquetado y manipulado de la información, asimismo se asignaran los criterios y niveles de clasificación que permitan determinar el valor del activo de acuerdo con su criterio de confidencialidad, integridad y disponibilidad establecido, cruzado con su nivel de clasificación alta, media o baja, siendo nivel de clasificación alta si cumple con al menos dos de estos criterios, clasificación, media si cumple uno de los criterios o al menos uno de los niveles es medio y baja si en la clasificación de todos sus niveles es baja, esto con el fin identificar qué activos deben ser tratados de manera prioritaria.

La gestión de activos del MIE estará alineada con el Dominio 8, Gestión de Activos del anexo A de la norma ISO 27001:2013, y la guía de controles del

[2] Tomado de https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150516:Guia-de-gestion-de-riesgos. Guía No. 7.

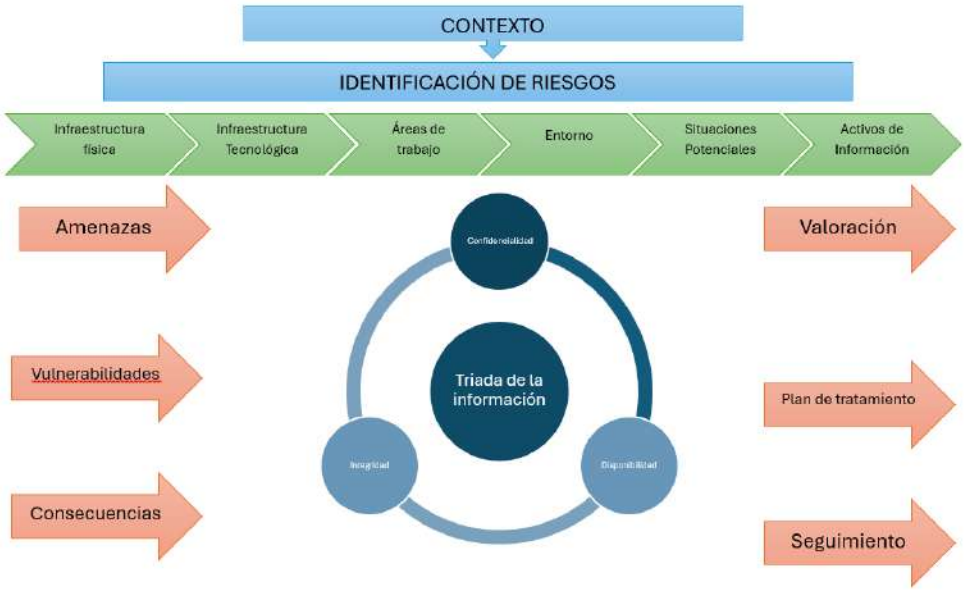
modelo de seguridad y privacidad de la información que contempla los siguientes criterios:

- Inventario de activos: Se identificarán y se creará un inventario de activos asociados con la información y las instalaciones de procesamiento, y se mantendrá un inventario de estos activos.
- Propiedad de los activos: Los activos mantenidos en el inventario tendrán asignado un propietario.
- Uso aceptable de los activos: Se identificarán, documentarán e implementarán reglas para el uso aceptable de información y activos asociados e instalaciones de procesamiento de información.
- Devolución de activos: Todos los funcionarios, contratistas y terceros deberán devolver los activos que se encuentren a su cargo al desvincularse de la entidad o al término del contrato.
- Clasificación de la información: La información se clasificará en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o la modificación no autorizada.
- Etiquetado de la información: Se desarrollará e implementará un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la entidad.
- Manejo de activos: Se desarrollarán e implementarán procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la entidad.

Esta metodología estará respaldada por la política y el manual de políticas de seguridad y privacidad de la información del MIE. Adicionalmente se llevarán a cabo actividades que permitan afianzar y resguardar los activos de información y la seguridad de la red perimetral y los servicios en nube desde la protección física de los recursos tecnológicos, hasta los servicios suministrados por proveedores de tecnologías en nube.

Actividades	Tareas	Responsable de la tarea	Fecha inicio	Fecha fin
Cifrado de discos	Aplicar técnicas de cifrado, para proteger la información almacenada en los discos duros de almacenamiento de los equipos de cómputo y servidores de la Entidad.	Oficina de Tecnologías de la Información	2/01/2025	20/12/2025
Doble factor de autenticación	Aplicar el doble factor de autenticación para los sistemas de información publicados en Internet	Oficina de Tecnologías de la Información	2/01/2025	20/12/2025
Monitoreo a la infraestructura crítica de TI	Implementar, monitorear y hacer seguimiento al sistema de monitoreo sobre la infraestructura crítica de TI.	Oficina de Tecnologías de la Información	2/01/2025	20/12/2025
Implementación de políticas de seguridad a nivel de red perimetral	Implementar soluciones de seguridad perimetral que permitan mitigar las principales amenazas cibernéticas.	Oficina de Tecnologías de la Información	2/01/2025	20/12/2025
Sensibilización	Socialización del código de ética e integridad	Subdirección de Talento Humano	2/01/2025	20/12/2025
Documentación y monitoreo de ANS	Definir, documentar y monitorear el cumplimiento de los ANS internos y realizar seguimiento al cumplimiento por parte de proveedores de servicios de TI.	Oficina de Tecnologías de la Información	2/01/2025	20/12/2025

7.1. Desarrollo metodológico[3]



Fuente: Elaboración Propia

Establecimiento del Contexto

El contexto abarca los aspectos externos, internos y específicos del proceso que deben considerarse para gestionar los riesgos relacionados con seguridad y privacidad de la información, seguridad digital y continuidad de los servicios (riesgos de interrupción) del Ministerio de Igualdad y Equidad. Este análisis permite identificar las causas potenciales de los riesgos y las áreas que podrían verse afectadas.

La definición del contexto seguirá las metodologías planteadas por MinTIC, enfocándose en garantizar que los procesos operen de forma segura y alineada con los objetivos de inclusión, equidad y justicia social.

Identificación del Riesgo

La identificación de riesgos se realiza considerando:

- Infraestructura física, áreas de trabajo y entorno en general.

[3] MIG-TIC-MA-008 Lineamientos para la administración de riesgos – sección 10.3 Administración de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios.

- Activos de información asociados a los procesos, evaluando su criticidad y atributos como confidencialidad, integridad y disponibilidad.
- La falta de controles o vulnerabilidades puede ser explotada por amenazas, resultando en incidentes que impacten los objetivos institucionales. Por ello, se registran en el mapa de riesgos los siguientes elementos:
- Triada de la información afectada (confidencialidad, integridad, disponibilidad).
- Dueño del riesgo (líder del proceso).
- Activo de información comprometido, amenazas, vulnerabilidades y consecuencias.
- El inventario de activos, valorado según la criticidad y clasificación de la información, sirve de base para esta identificación. La metodología incluye el uso de herramientas como el catálogo de amenazas y vulnerabilidades definido en los Lineamientos para la gestión del riesgo en entidades públicas, validado en mesas de trabajo con los diferentes procesos de la entidad.

Valoración del Riesgo

La valoración se realiza siguiendo la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP. Este análisis incluye:

- Identificación de amenazas, vulnerabilidades y consecuencias.
- Determinación del nivel de riesgo inherente mediante la evaluación de probabilidad e impacto.
- Relación de los riesgos con controles basados en la Norma ISO 27001:2013, evaluando variables como:
  - Responsable del control.
  - Tipo de control (preventivo, detectivo, correctivo).
  - Implementación (manual o automática).
  - Periodicidad y evidencia de ejecución.
  - Los controles transversales se establecen de manera conjunta cuando el custodio del activo pertenece a un proceso diferente o a un tercero,

garantizando la adecuada protección y continuidad de los activos de información esenciales para la misión del Ministerio.

Definición y Aprobación de Mapas de Riesgos y Planes de Tratamiento

Finalizadas las etapas de identificación y valoración, los líderes de procesos, con apoyo de gestores, deben formalizar la aprobación de mapas de riesgos y planes de tratamiento; estos se centrarán en mitigar los riesgos con niveles residuales Moderados, Altos o Extremos. El proceso de formalización se realiza mediante la aprobación por parte del comité de gestión y desempeño previa validación por parte de la oficina asesora de planeación.

Materialización del Riesgo

En caso de materialización:

Se reportará siguiendo el procedimiento establecido para la gestión de incidentes de seguridad y privacidad de la información.

El riesgo será reanalizado, actualizando su nivel en el mapa correspondiente.

Si el riesgo no estaba identificado, se procederá a su registro y análisis para evitar futuros incidentes.

7.2. Oportunidad de mejora

El **Ministerio de Igualdad y Equidad** no debe limitarse únicamente a la identificación y gestión de riesgos. Como parte de su compromiso con la equidad, la inclusión y el cumplimiento de sus objetivos institucionales, este análisis debe ser también una herramienta estratégica para identificar oportunidades.

Una **oportunidad** se entiende como la consecuencia positiva que puede surgir del tratamiento de un riesgo. Al implementar controles efectivos y medidas preventivas, es posible no solo mitigar amenazas, sino también fortalecer procesos, optimizar recursos y generar beneficios adicionales para la entidad y sus grupos de interés.

Integración del Enfoque de Oportunidades

1. Detección de Oportunidades

Durante la etapa de análisis de riesgos, se debe evaluar cómo los resultados del tratamiento del riesgo pueden generar ventajas estratégicas, tales como:

- Mayor eficiencia en los procesos operativos.
- Incremento en la confianza de los grupos de interés.
- Potenciación de la capacidad institucional para alcanzar los objetivos estratégicos.

2. Transformación del Riesgo en Valor Agregado

Al abordar un riesgo, la identificación de oportunidades permite:

- Innovar en los procesos de gestión y operación.
- Mejorar la resiliencia institucional frente a futuros desafíos.
- Fortalecer la cultura organizacional basada en la proactividad y el aprendizaje continuo.

3. Gestión y Monitoreo de Oportunidades

Las oportunidades identificadas deben integrarse en los planes de tratamiento de riesgos y ser monitoreadas como parte del ciclo de mejora continua. Esto asegura que el Ministerio no solo reduzca los riesgos, sino que también maximice su impacto positivo en la misión institucional.

8. Recursos

RECURSOS	VARIABLE
Humanos	Grupos Internos de Trabajo de la OTI - Servicios Tecnológicos y Transformación Digital
	Encargado de seguridad informática y de la información
	Líderes y gestores de procesos

<table>
<tr><td></td><td colspan="3">Dimensión de Seguridad informática de la Oficina de TI</td></tr>
<tr><td></td><td colspan="3">Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT (Al interior del Ministerio: Mesa Técnica para la gestión de la seguridad).</td></tr>
<tr><td rowspan="2">Técnicos</td><td colspan="3">Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del DAFP</td></tr>
<tr><td colspan="3">Herramienta para la gestión de riesgos (Matriz de Riesgos SGSPI)</td></tr>
<tr><td>Logísticos</td><td colspan="3">Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.</td></tr>
<tr><td rowspan="3">Financieros</td><td colspan="3">Recursos para la adquisición de conocimiento, recursos humanos, técnicos.</td></tr>
<tr><td>Iniciativa</td><td>Proyecto</td><td>Presupuesto</td></tr>
<tr><td>Fortalecimiento de las capacidades institucionales para la seguridad y Privacidad de la Información</td><td>Fortalecimiento institucional para la superación de brechas de desigualdad e inequidad a nivel nacional.</td><td>$1.164.500.000,00</td></tr>
</table>

Nota: La ejecución de las actividades y proyectos establecidos en este plan está sujeta a la disponibilidad presupuestal del Ministerio de Igualdad y Equidad. En caso de presentarse recortes presupuestales o reasignación de recursos por prioridades institucionales, se documentará mediante informes técnicos el impacto sobre el cumplimiento de las actividades programadas y se realizarán los ajustes pertinentes al plan, previa aprobación del Comité Institucional de Gestión y Desempeño.

9. Medición

La mesa técnica para la gestión de seguridad del **Ministerio de Igualdad y Equidad** es la encargada de realizar el monitoreo y seguimiento de los riesgos relacionados con Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción)**.**

Responsabilidades de la mesa técnica para la gestión de seguridad

1. **Revisión Periódica**: Supervisar los riesgos aprobados por los procesos, así como los controles y planes de tratamiento, siguiendo las periodicidades y fechas de cumplimiento establecidas.
2. **Validación de Resultados**: Confirmar la efectividad de los seguimientos realizados y garantizar el registro de los soportes correspondientes a los controles definidos.

Reporte de Cumplimiento

- Los enlaces de TI de las dependencias deben reportar el cumplimiento de sus planes de tratamiento y controles, asegurando que la información esté debidamente soportada.
- Los profesionales del área de Seguridad y Privacidad de la Información revisan y validan estos reportes para garantizar su coherencia y precisión.

Medición del Nivel de Implementación

La oficina de Tecnologías de la Información proyectará los formatos de indicadores de gestión para su revisión y aprobación, los cuales permitirán realizar un seguimiento sistemático a los indicadores establecidos y evaluar los niveles de cumplimiento respecto a los objetivos organizacionales. Los formatos contarán con una descripción clara del indicador, la fórmula de cálculo, el valor objetivo, el rango de tolerancia, la periodicidad de medición, el responsable de su monitoreo, las fuentes de datos utilizadas y los planes de acción en caso de desviaciones. Además, se incluirá un espacio para registrar los resultados históricos, análisis de tendencias y observaciones relevantes, con el propósito de facilitar la toma de decisiones basadas en información confiable como fuente origen de la Oficina de Tecnologías de la Información.

- Se utilizarán los indicadores establecidos en la matriz de riesgos para medir el **nivel de implementación de los controles** destinados a mitigar los riesgos identificados.

- Estos indicadores determinarán el porcentaje de ejecución de los controles definidos en los sistemas de gestión de la entidad, asegurando que los esfuerzos para mitigar riesgos estén alineados con los objetivos institucionales.

10. Control de cambios

Fecha	Versión	Descripción
20 de diciembre de 2024	1.0.	Creación

11. Referencias

- ✓ Manual de Gobierno Digital
- ✓ Autodiagnóstico MSPI 2024
- ✓ Matriz Gobierno Digital 2020
- ✓ Anexo A del estándar ISO/IEC 27001:2013
- ✓ Las principales nueve (9) amenazas de ciberseguridad https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

Ministerio de
Igualdad y Equidad