Igualdad

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

MINISTERIO DE IGUALDAD Y EQUIDAD

Juan Carlos Florián Silva
Persona Ministra de Igualdad y Equidad

Guillermo Cadena Ronderos
Jefe Oficina de Tecnologías de la Información

Juan de Jesús Aponte Buitrago
Oficina de Tecnologías de la Información

Juan Diego Mallama
Oficina de Tecnologías de la Información – Grupo de Gobierno Digital

Edwin Sánchez
Oficina de Tecnologías de la Información – Grupo de Servicios Tecnológicos

Fecha de Aprobación Versión 2: xx de enero de 2026

Contenido

El Plan de Tratamiento de Riesgos 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 **Ministerio de Igualdad y Equidad**.

Dicho plan se diseña con el fin de evaluar y priorizar las acciones necesarias para abordar los riesgos 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.

1. Introducción

El Plan de Tratamiento de Riesgos del Ministerio de Igualdad y Equidad establece las actividades que permita la identificar, analizar, evaluar y monitorear los riesgos de seguridad de la información. 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.

El plan se desarrolla alineado con la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 del DAFP 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).

2. 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.

3. Objetivos

- ✓ Establecer las actividades para Identificar y gestionar los riesgos de seguridad y privacidad de la información.
- ✓ Promover y fortalecer el conocimiento interno relacionado con la gestión de riesgos asociados a la seguridad y privacidad de la información.
- ✓ Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas en materia de seguridad y privacidad de la información

4. 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.

5. Desarrollo del Plan

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]

Estrategia	Objetivo	Actividades
Actualización metodológica de gestión de riesgos	Actualizar los documentos e instrumentos de gestión de riesgos	• Formalizar GE_A-PO-001 Política de Administración de Riesgos con los componentes de Seguridad de la información

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

Estrategia	Objetivo	Actividades
	de seguridad de la información fortaleciendo el componente de seguridad de la información alineado a las actualizaciones normativas y procedimentales	• Formalizar GE_A-GU-001 Guía de Administración de Riesgos con los componentes de Seguridad de la información
		• Formalizar GE_A-PR-003 Procedimiento de Gestión de Administración de Riesgos Institucionales
		• Actualizar y socializar el formato de matriz de riesgos de seguridad de la información
Identificación y evaluación de riesgos de Seguridad de la Información	Gestionar los riesgos de seguridad de la información mediante la identificación, el análisis de probabilidad e impacto, y la valoración de los controles o el establecimiento de planes de acción.	• Desarrollar mesas de trabajo con los procesos para la Identificación/actualización y clasificación del inventario de activos de información
		• Identificar y evaluar los riesgos de seguridad de la información en todos los procesos de la entidad
		• Gestionar y hacer seguimiento de eventos, incidentes y vulnerabilidades de seguridad de la información

6. Aprobación

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de gestión y desempeño institucional con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Juan de Jesús Aponte Buitrago **Cargo:** Contratista Dirección General	Nombre: Edwin Sánchez Cargo: Coordinador Grupo Interno Servicios tecnológicos – OTI Nombre: Juan Diego Mallama Cargo: Coordinador Grupo Interno Transformación Digital – OTI	Nombre: Guillermo Cadena Cargo: jefe Oficina de tecnologías de la Información - OTI Fecha: 09-01-2026

7. Control de cambios

Fecha	Versión	Descripción
30-01-2025	1.0.	Creación
XX-01-2026	2.0.	Actualización

Ministerio de
Igualdad y Equidad