Instituto Nacional de Metrología de Colombia

Plan de Tratamiento de Riesgos de Seguridad de la Información (PTRSI)

2024-2026

OIDT

Bogotá, Enero de 2026

INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad de la Información (PTRSI) es el instrumento mediante el cual la entidad define y ejecuta las acciones necesarias para tratar los riesgos identificados que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional. Este plan se formula en coherencia con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC, la Política de Gobierno Digital y las buenas prácticas establecidas en la norma ISO/IEC 27001:2022.

El PTRSI constituye un componente esencial del Sistema de Seguridad y Privacidad de la Información (SSPI), permitiendo priorizar, implementar y hacer seguimiento a los controles de seguridad requeridos para reducir los riesgos a niveles aceptables, de acuerdo con el apetito y la tolerancia al riesgo definidos por la entidad.

1. OBJETIVO GENERAL

Definir e implementar las acciones de tratamiento necesarias para mitigar, aceptar, transferir o evitar los riesgos de seguridad de la información identificados, garantizando la protección adecuada de la información institucional y el cumplimiento de los lineamientos del MSPI del MinTIC.

1.1. OBJETIVOS ESPECÍFICOS

- Priorizar los riesgos de seguridad de la información con base en su nivel de criticidad.
- Definir controles técnicos, administrativos y organizacionales para el tratamiento de los riesgos.
- Asignar responsables y plazos para la implementación de los tratamientos definidos.
- Realizar seguimiento y evaluación periódica al estado de los riesgos tratados.
- Asegurar la articulación del tratamiento de riesgos con el SIG y la planeación institucional.

2. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad de la Información aplica a todos los riesgos de seguridad de la información identificados y valorados en el marco del MSPI, asociados a los activos de información, procesos, sistemas de información, infraestructuras tecnológicas, servicios digitales, servidores públicos, contratistas y terceros que tengan acceso, manejo o custodia de información institucional.

El alcance del PTRSI es coherente con el alcance definido para el Sistema de Seguridad y Privacidad de la Información y se articula con el Sistema Integrado de Gestión (SIG).

3. ABREVIATURAS O SÍMBOLOS

- **CIGD:** Comité Institucional de Gestión y Desempeño
- **ISO:** International Organization for Standardization
- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **PESI:** Plan Estratégico de Seguridad y Privacidad de la Información
- **PTRSI:** Plan de Tratamiento de Riesgos de Seguridad de la Información
- **SGSI:** Sistema de Gestión de Seguridad de la Información
- **SIG:** Sistema Integrado de Gestión
- **SSPI:** Sistema de Seguridad y Privacidad de la Información
- **TIC:** Tecnologías de la Información y las Comunicaciones

4. DEFINICIONES

- **Activo de información:** Cualquier información, sistema, recurso tecnológico o soporte que tenga valor para la entidad y cuya pérdida, alteración o divulgación no autorizada pueda generar impactos negativos.

- **Apetito al riesgo:** Nivel de riesgo que la entidad está dispuesta a aceptar para el cumplimiento de sus objetivos estratégicos.

- **Control de seguridad:** Medida administrativa, técnica u organizacional implementada para modificar un riesgo de seguridad de la información.

- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza explote una vulnerabilidad y cause impactos sobre la confidencialidad, integridad, disponibilidad o privacidad de la información.

- **Riesgo residual:** Nivel de riesgo que permanece después de aplicar los controles de tratamiento.

- **Tratamiento del riesgo:** Proceso de selección e implementación de medidas para mitigar, aceptar, transferir o evitar un riesgo.

5. MARCO NORMATIVO

- Decreto 1078 de 2015
- Ley 1581 de 2012 y normas complementarias
- Política de Gobierno Digital
- Modelo de Seguridad y Privacidad de la Información – MSPI (MinTIC)
- ISO/IEC 27001:2022
- ISO/IEC 27005:2022 (gestión del riesgo)
- Lineamientos de gestión del riesgo del DAFP

6. ENFOQUE METODOLÓGICO

El tratamiento de riesgos se realiza conforme a la metodología institucional de gestión de riesgos de seguridad de la información, alineada con el MSPI, la ISO/IEC 27005 y los lineamientos del DAFP, considerando las siguientes etapas:

1. Identificación de riesgos
2. Análisis y valoración de riesgos
3. Evaluación y priorización
4. Definición de opciones de tratamiento
5. Implementación de controles
6. Seguimiento y revisión

7. CRITERIOS PARA EL TRATAMIENTO DEL RIESGO

Las opciones de tratamiento de los riesgos de seguridad de la información incluyen:

- **Mitigar:** Implementar controles para reducir la probabilidad o el impacto del riesgo.
- **Aceptar:** Asumir el riesgo residual cuando se encuentre dentro del nivel aceptable definido por la entidad.
- **Transferir:** Compartir el riesgo con terceros (seguros, contratos, acuerdos).
- **Evitar:** Eliminar la actividad que genera el riesgo.

La selección del tratamiento se realiza considerando el nivel de riesgo, el costo-beneficio, la viabilidad técnica y el impacto institucional.

8. LÍNEAS DE ACCIÓN DEL PTRSI

a. Fortalecimiento de controles estratégicos

Priorización e implementación de controles críticos definidos en el MSPI y la ISO/IEC 27001, enfocados en activos de información de alto impacto y riesgos con mayor nivel de criticidad.

b. Tratamiento operativo de riesgos priorizados

Ejecución de planes de tratamiento con responsables, plazos y recursos definidos, asegurando la reducción progresiva del riesgo residual.

c. Integración con la gestión institucional

Articulación del tratamiento de riesgos con el SIG, la planeación institucional y los procesos de control interno.

d. Seguimiento y control directivo

Monitoreo periódico del estado de los riesgos tratados, mediante indicadores, reportes ejecutivos y presentación de resultados a la Alta Dirección y al CIGD.

9. ROLES Y RESPONSABILIDADES

- **Comité Institucional de Gestión y Desempeño (CIGD):** Aprobar el Plan de Tratamiento de Riesgos y realizar seguimiento estratégico.
- **Alta Dirección:** Definir el apetito al riesgo y garantizar los recursos necesarios.
- **CISO / Responsable de Seguridad de la Información:** Coordinar la definición, implementación y seguimiento del PTRSI.
- **Responsables de proceso y de activos:** Ejecutar las acciones de tratamiento asignadas.

- **Oficina TIC:** Implementar controles tecnológicos definidos en el plan.

10. SEGUIMIENTO Y MONITOREO

El seguimiento al PTRSI se realiza de manera periódica mediante:

- Revisión del estado de implementación de los controles.
- Medición del riesgo residual.
- Reportes de avance al Comité de Seguridad de la Información y al CIGD.
- Articulación con auditorías internas y externas.

11. ACTIVIDADES Y CRONOGRAMA:

Se han definido unas actividades programadas para cada eje; esto con el fin de lograr posicionar el SGSI a nivel estratégico u táctico y a su vez contribuir en su implementación y mejoramiento continuo en la vigencia 2024-2026. Para poder visibilizar las actividades se cuenta con el Plan de Tratamiento de Riesgos de Seguridad de la Información y la gestión del cambio por parte de la OAP, el cual se adjunta al presente documento.

12. ASIGNACIÓN PRESUPUESTAL PARA LA VIGENCIA 2026

Se han asignado recursos para garantizar la eficacia del SGSI y el MSPI, los cuales se relacionan a continuación:

AÑO 2026		
Ítem	**Proyecto**	**Inversión**
1	Implementación de backups fuera de sitio	$94.281.134
2	Soporte NAC, SIEM, inteligencia de amenazas y SOC	$575.647.349
3	Servicio de Ethical hacking	$ 20.125. 000

4	Servicios profesionales para articular en el sistema integrado de gestión (SIG) el sistema de gestión de seguridad y privacidad de la información,	$ 84.588.504
Total		**$ 754.516.987**

13. ANEXOS

- Plan de Tratamiento de Riesgos de Seguridad de la Información
- Gestión del Cambio – Gestión de Riesgos

_____

Alejandra Villabón Aldana
Responsable SGSI.
Fecha: 2026-01- 21