PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2026

TABLA DE CONTENIDO

1. GENERALIDADES DEL PLAN INSTITUCIONAL 3
   1.1. Introducción 3
   1.2. Alcance 4
   1.3. Objetivos 5
   1.3.1. Objetivo general 5
   2.1 Objetivos específicos 5
2. CONTEXTO ESTRATÉGICO 6
3. DESCRIPCIÓN DEL PLAN 8
4. CRONOGRAMA DE SEGUIMIENTO Y EVALUACIÓN 10

1. GENERALIDADES DEL PLAN INSTITUCIONAL

1.1. Introducción

El Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información del Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas-IPSE se desarrolla con el propósito de gestionar de manera integral los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad, privacidad y resiliencia de los activos de información institucionales. Este plan constituye un instrumento fundamental y se articula directamente con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), los requisitos del Gobierno Digital y las obligaciones normativas emanadas del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

En su construcción se adopta plenamente la nueva Guía para la Gestión Integral del Riesgo-Versión 7 del Departamento Administrativo de la Función Pública, la cual establece un enfoque unificado, moderno y transversal para la gestión institucional del riesgo en las entidades públicas de Colombia. Esta guía, consolidada en el documento Guía para la Gestión Integral de Riesgos en Entidades Públicas-Versión 7, introduce una visión más amplia, preventiva y estratégica del riesgo, integrando componentes de transparencia, anticorrupción, seguridad de la información, continuidad del negocio, gestión tecnológica y control interno, permitiendo que las entidades avancen hacia modelos de madurez superiores en la toma de decisiones basadas en riesgo.

La guía enfatiza la importancia de comprender el contexto institucional, identificar riesgos internos y externos, evaluar amenazas emergentes, diseñar controles proporcionales, fortalecer la cultura organizacional y garantizar la trazabilidad del proceso mediante mecanismos de evaluación y seguimiento. De este modo, el plan incorpora un enfoque integral que articula riesgos tecnológicos, operativos, reputacionales, regulatorios y humanos, alineándose con las exigencias del MSPI, el Sistema Integrado de Gestión (SIG), el MIPG y las directrices estratégicas del IPSE.

Este plan se alinea al MANUAL DE GESTIÓN DE RIESGOS - IPSE- ME-M01, donde se formula también en coherencia con los requerimientos establecidos en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026-IPSE, en el cual se reconoce que la protección de la información y la gestión del riesgo digital constituyen factores críticos para asegurar la continuidad operativa y la estabilidad institucional en las zonas no interconectadas.

Finalmente El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información 2026 se formula como un plan institucional integrante del Plan de Acción Anual, en el marco del Decreto 612 de 2018, y se articula con el Plan Estratégico Institucional y las dimensiones y políticas de MIPG.

1.2. Alcance

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del IPSE aplica a todos los procesos misionales, estratégicos y de apoyo que administran, generan, procesan o custodian activos de información dentro de la entidad. Su alcance comprende la identificación, análisis, valoración y tratamiento de los riesgos asociados a la seguridad digital, la privacidad de los datos, la continuidad operativa y la protección de la infraestructura tecnológica, en coherencia con los lineamientos establecidos en el MANUAL DE GESTIÓN DE RIESGOS - IPSE- ME-M01.

El plan incluye actividades relacionadas con el riesgo en sistemas de información, plataformas tecnológicas, servicios en la nube, proveedores estratégicos, talento humano, así como los riesgos emergentes derivados del avance tecnológico y del contexto institucional. Su implementación abarca a todos los servidores públicos, contratistas y terceros que intervienen en el ciclo de vida de la información, garantizando que los controles definidos se apliquen de manera transversal en toda la entidad, conforme a las disposiciones del IPSE y a las orientaciones del modelo MSPI.

1.3. Objetivos

1.3.1. Objetivo general

Gestionar de manera integral los riesgos que puedan afectar la seguridad y privacidad de la información del IPSE, mediante la identificación, valoración y tratamiento de riesgos, incluidos los emergentes en coherencia con el Modelo de Seguridad y Privacidad de la Información (MSPI) y los lineamientos del MANUAL DE GESTIÓN DE RIESGOS - IPSE- ME-M01 garantizando la protección de los activos de información y la continuidad operativa institucional.

2.1 Objetivos específicos

1. Identificar, analizar y valorar de manera sistemática los riesgos relacionados con la Seguridad y Privacidad de la Información, la Seguridad Digital y la Continuidad de la Operación, incluyendo riesgos de interrupción y riesgos emergentes, considerando el contexto estratégico, tecnológico y organizacional de la entidad.

2. Definir, priorizar y aplicar lineamientos, controles y acciones de tratamiento que permitan gestionar integralmente los riesgos identificados, asegurando la protección de la integridad, confidencialidad, disponibilidad, privacidad, trazabilidad y autenticidad de la información, como soporte directo al cumplimiento de la misión, visión y objetivos estratégicos del IPSE.

3. Implementar un proceso de gestión de riesgos alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI), para la gestión de riesgos, y el enfoque de gestión integral definido por la Función Pública, garantizando que los riesgos emergentes, tecnológicos, digitales y operativos sean controlados, mitigados o transferidos de forma eficaz.

4. Fortalecer las capacidades institucionales mediante la apropiación de conocimientos, metodologías, herramientas y buenas prácticas relacionadas con la gestión de riesgos en Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, promoviendo una cultura organizacional consciente, preventiva y orientada a la mejora continua

2. CONTEXTO ESTRATÉGICO

2.1 Proceso de Gestión de Riesgos de Seguridad de la Información

El flujo corresponde a una secuencia metodológica para identificar, analizar, valorar y controlar los riesgos asociados a la Seguridad de la Información. El proceso se desarrolla de manera lógica y progresiva, avanzando desde la identificación del riesgo hasta la valoración de los controles implementados. La secuencia se puede describir así:

1. Identificación de los riesgos clave y su relación con los objetivos
En esta etapa se identifican los riesgos que pueden afectar el cumplimiento de los objetivos institucionales. Incluye: detección de amenazas, eventos de riesgo, vulnerabilidades y escenarios relevantes.

2. Identificación de áreas de impacto
Una vez identificado el riesgo, se determina qué áreas o dimensiones se verían afectadas (operativa, tecnológica, reputacional, legal, financiera, etc.).

3. Identificación de áreas de factores de riesgo
Aquí se analizan los factores internos y externos que pueden generar, incrementar o detonar el riesgo. Ejemplos: fallas humanas, debilidades de control, proveedores, condiciones del entorno, tecnologías críticas.

4. Descripción del riesgo
Se elabora una definición clara y completa del riesgo, incluyendo el evento, la causa y la posible consecuencia. Esto permite estandarizar la comprensión del riesgo en toda la organización.

5. Determinar la probabilidad
Se evalúa la probabilidad de ocurrencia del riesgo con base en criterios definidos por la entidad: historial, frecuencia, nivel de exposición, debilidades del entorno, etc.

6. Estructura para la descripción del control
Se documentan los controles existentes, especificando:

- tipo de control,
- responsable,
- mecanismo de funcionamiento,
- evidencia de aplicación,
- periodicidad.

Esta fase permite conocer el nivel de mitigación actual.

7. Valoración de controles
Finalmente, se analiza la efectividad real de los controles identificados, evaluando si reducen adecuadamente la probabilidad o el impacto del riesgo. Esto permite identificar brechas de control y proponer controles adicionales o mejoras.

Este flujo es consistente con enfoques de gestión de riesgos basados en MSPI, ISO 31000, ISO 27005 y lineamientos sectoriales.

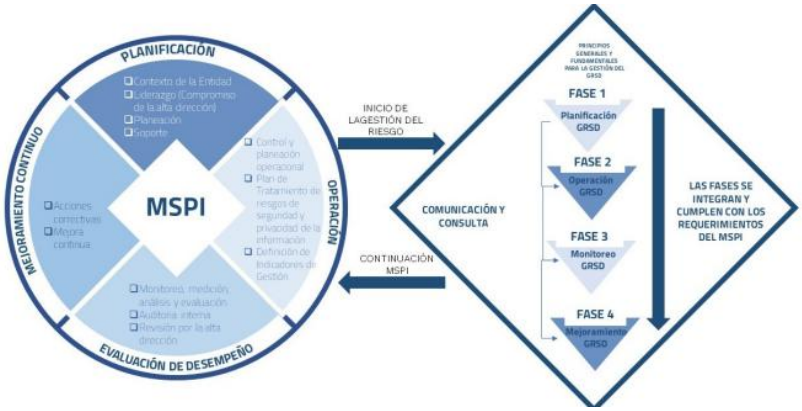
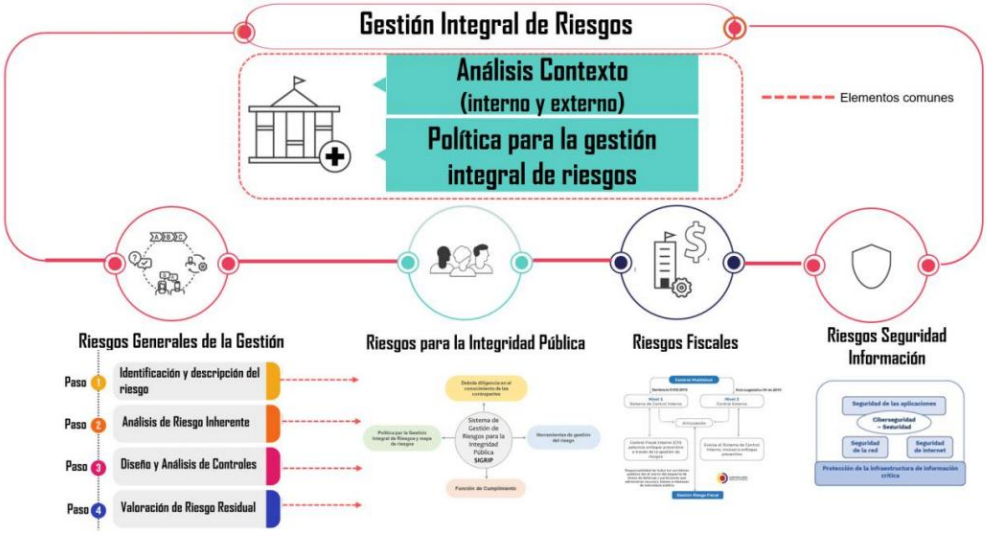


Ilustración 1 Interacción MSPI - Modelo Gestión de Riesgo de seguridad de la información

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Figura 13 Articulación ámbitos gestión del riesgo



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

3. DESCRIPCIÓN DEL PLAN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información constituye el instrumento operativo mediante el cual el IPSE gestiona los riesgos que amenazan los activos de información, siguiendo un proceso estructurado basado en el ciclo metodológico del Modelo de Seguridad y Privacidad de la Información (MSPI) y las directrices institucionales vigentes. Este plan traduce los resultados del análisis de riesgos en acciones concretas de mitigación, reducción, transferencia o aceptación del riesgo, garantizando la continuidad de los servicios tecnológicos y la protección de la información crítica de la entidad.

Este enfoque técnico permite consolidar un tratamiento del riesgo coherente, verificable y alineado con los estándares de seguridad digital, garantizando que los riesgos identificados sean atendidos mediante acciones medibles, oportunas y orientadas a la continuidad de la operación y la protección de los activos de información del IPSE.

IPSE	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Periodo Enero - Diciembre 2026

	• Actividad	• Entregable	1	2	3	4	5	6	7	8	9	10	11	12	Responsable	
Consolidar y actualizar la Matriz de Valoración de Riesgos	Tomar los riesgos identificados y valorados en el requisito 7.3.2, verificando probabilidad, impacto, controles existentes y nivel de riesgo residual.	Requisito MSPI : 7.3.2													Gestion de TICs	
Definir la estrategia de tratamiento para cada riesgo	Para cada riesgo clasificado como Alto o Crítico, determinar si la acción será: Reducir Transferir Evitar Aceptar (con justificación) Sustento: Requisito MSPI 7.3.3	Requisito MSPI : 7.3.3													Gestion de TICs	
Diseñar los controles y acciones de tratamiento	Construir las acciones, controles y medidas necesarias para disminuir el nivel del riesgo a un valor aceptable. Debe incluir: Control propuesto Objetivo del control Responsable Recursos Tiempo estimado	Matriz de Controles													Gestion de TICs	
Elaborar el Plan de Tratamiento de Riesgos consolidado	Unificar en un solo documento todos los riesgos, controles, recursos, fechas y responsables, dejando una matriz estructurada y trazable frente a 7.3.3. Sustento: Entregable "Plan de Tratamiento de Riesgos de Seguridad de la Información" registrado en el cronograma MSPI	Matriz de Controles													Gestion de TICs	
Socializar y obtener aprobación de líderes de proceso	Presentar los riesgos y sus planes de tratamiento a los responsables de cada proceso para validar viabilidad, ajustar acciones y obtener aprobación formal	Matriz de riesgos y sus planes de tratamiento a los responsables de cada proceso													Gestion de TICs	
Escalar al Comité Institucional de Gestión y Desempeño (CIGD)	Los riesgos cuyo tratamiento requiera recursos adicionales, mayor tiempo o cambios estructurales deben ser escalados al CIGD para priorización y aprobación. Sustento: La operación del MSPI 8.1 y 8.2	Matriz de Riesgos que requieran recursos adicionales													Gestion de TICs	
Implementar los controles definidos para riesgos Altos/Críticos	Ejecutar las acciones aprobadas (técnicas, administrativas, físicas), dejando evidencia: SOC/SIEM Gestión de vulnerabilidades (SDI 225) Gestión de incidentes (SDI 220–223) Endurecimiento	Documentación que evidencia la Gestión													Gestion de TICs	
Registrar evidencias de implementación	Consolidar logs, pantallazos, reportes, configuraciones, actas, entregables técnicos como prueba verificable del control implementado. Sustento: En FURAG y MSPI se exige evidencia como comprobación de implementación de controles.	Documentación que evidencia la Gestión													Gestion de TICs	
Evaluar la eficacia de los controles aplicados	Medir el resultado de los controles aplicados usando indicadores definidos en 8.3 del MSPI: reducción de impacto reducción de probabilidad cumplimiento de SLA tiempo de atención de incidentes estado de vulnerabilidades Sustento: Requisito 8.3 – Indicadores de madurez y desempeño del MSPI	Matriz de Indicadores													Gestion de TICs	
Revaloración del riesgo residual	Después de implementados los controles, recalcular probabilidad/impacto para obtener el riesgo residual y compararlo con los criterios de aceptación. Sustento: Actividad 8.2 exige "información documentada de los resultados obtenidos	información documentada de los resultados obtenidos													Gestion de TICs	
Consolidar reporte anual del PTR y alimentar el ciclo de mejoramiento	Elaborar informe con todas las actividades ejecutadas, resultados de efectividad, riesgos mitigados, controles implementados y acciones 2027. Sustento: Requisito 10.1 – Oportunidades de mejora del MSPI	Reporte consolidado													Gestion de TICs	

4. CRONOGRAMA DE SEGUIMIENTO Y EVALUACIÓN

Se realizará un seguimiento y evaluación continua del Plan de Tratamiento de Seguridad y Privacidad de la Información conforme al Plan de Acción Institucional 2026, asegurando la mejora continua y el cumplimiento de los objetivos establecidos.

PLANES DE ACCIÓN OPERATIVOS INSTITUCIONALES 2026					PROGRAMACIÓN TRIMESTRAL 2026						
OBJETIVO ESTRATÉGICO /PROCESO	PROYECTO DE INVERSIÓN	PLAN DE ACCIÓN	ACTIVIDAD A DESARROLAR	DOCUMENTO SOPORTE/ PRODUCTO DE LA ACTIVIDAD	RESPONSABLE DE ACTIVIDAD	RECURSOS PRESUPUESTALES	META DE LA ACTIVIDAD ANUAL	PRIMER TRIMESTRE	SEGUNDO TRIMESTRE	TERCER TRIMESTRE	CUARTO TRIMESTRE
Gestionar estratégicamente las necesidades de innovación en tecnología, seguridad y operatividad que requiera la entidad, con el fin de apoyar el cumplimiento de los objetivos institucionales en el marco de la estrategia de Gobierno Digital, a través del Plan Estratégico de Tecnologías de la Información (PETI).	PROCESO INTERNO	Gestionar la infraestructura tecnológica (Azure, onprimise y oracle)	Seguimiento y control al cronograma de trabajo acorde a obligaciones contractuales	Matriz de seguimiento y cumplimiento de actividades	Heider Suarez/ Ricardo Mendez	Recursos Humanos	4	1	1	1	1
		Gestionar la seguridad de la información	Seguimiento y control del cronograma Plan de Seguridad y Privacidad de la Información (Incluye riesgos)	Anexo detallado del cronograma	Heider Suarez/ Ricardo Mendez	Recursos Humanos	4	1	1	1	1
		Apropiar recursos tecnológicos	Sensibilización mediante piezas comunicativas para el uso y apropiación de recursos tecnológicos (SIGIPSE, SIGEAPP, APIPSE Moodle	Cumplimiento del cronograma (Matriz)	Heider Suarez/ Ricardo Mendez	Recursos Humanos	4	1	1	1	1
		Gestionar Políticas de MIPG	Implementación de las políticas de MIPG aplicadas al TSI	Documento de autodiagnóstico del MIPG (entregado primer trimestre) Plan de acción (iniciado	Heider Suarez/ Ricardo Mendez	Recursos Humanos	4	1	1	1	1
OBJETIVO ESTRATEGICO 3 Promover la transformación institucional para optimizar la eficiencia operativa y administrativa		Hoja de Ruta sectorial TSI 2026	Gestionar el cumplimiento de requerimientos del sector minero energético	Hoja de ruta actualizada	Heider Suarez/ Ricardo Mendez	Recursos Humanos	3		1	1	1
		Seguimiento y control contractual	Gestionar softw are Kactus, ADA, ControlDoc y SGI) con seguimiento y control	Matriz Consolidada orden de pago	Heider Suarez/ Ricardo Mendez/ Diana Paola Monteegro	Recursos Humanos	4	1	1	1	1

Es importante garantizar la adecuada articulación del documento señalado en el numeral 3, *Descripción del Plan*, se articula directamente con el Plan de Seguridad de la Información 2026 de manera que su desarrollo y posterior seguimiento se realicen conforme al Plan de Acción institucional. Dicho seguimiento se ejecutará con base en la actividad de control descrita en el Plan de Acción 2026, la cual fue definida para realizar el correspondiente monitoreo y verificación de su cumplimiento.

https://ipse.gov.co/mapa-del-sitio/transparencia-ipse/planeacion/plan-de-accion/

5. CONTROL DE CAMBIOS

Versión	Fecha	Naturaleza del cambio
01	20-01-2023	Actualización del documento por cambio de vigencia.
02	20-01-2024	Actualización del documento por cambio de vigencia.
03	20-01-2025	Actualización del documento por cambio de vigencia.
04	20-01-2026	Actualización del documento por cambio de vigencia.

	Elaboró:	Revisó:	Aprobó:
Nombre:	**Ricardo Méndez Barco**	**Heider Rafael Suarez Pacheco**	**Comité de Gestión y Desempeño Institucional**
Cargo:	**Profesional Especializado Grado 14**	**Coordinador Grupo de Tecnologías y Sistemas de Información**	