



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	2
2. OBJETIVOS.....	2
3.1. Objetivo general	3
3.2. Objetivos específicos.....	3
3. ALCANCE	3
4. TÉRMINOS Y DEFINICIONES	5
5. SIGLAS.....	9
6. MARCO NORMATIVO.....	10
7. MARCO DE ACCIÓN FRENTE AL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	13
8. ROLES Y RESPONSABILIDADES: Revisión de la gestión por el esquema de las líneas de defensa.....	18
9. RECURSOS	20
10. MEDICIÓN	22
11. CONTROL DE CAMBIOS	23



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

1. INTRODUCCIÓN

El presente Plan de tratamiento de riesgos de seguridad y privacidad de la información de la Agencia Presidencial de Cooperación Internacional de Colombia, APC Colombia, establece el marco integral y de acción que serán desarrolladas e implementadas durante la vigencia 2026, con el propósito de identificar, analizar, evaluar y tratar de manera sistemática los riesgos asociados a los activos de información de la Agencia.

Este plan se articula directamente con los procesos institucionales y aplica a todos los recursos tecnológicos y servicios de información que soportan la gestión de la Agencia, en plena conformidad con el Sistema de Gestión de la Seguridad y Privacidad de la Información (SGSPI), adoptado por la Agencia y alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) actualizado mediante la Resolución No. 02277 de 2025 del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC), que modifica el anexo 1 de la Resolución No. 500 de 2021 y la Norma Técnica Colombiana (NTC) ISO/IEC 27001:2022.

Las actividades y los controles definidos, se sustentan en las herramientas institucionales establecidas para la identificación, valoración y tratamiento de activos de información y de riesgos de seguridad y privacidad de la información, guiadas por los lineamientos metodológicos en asociación, con el MSPI y sus guías complementarias.

2. OBJETIVOS

2.1. Objetivo General

Establecer e implementar el Plan de tratamiento de riesgos de seguridad y privacidad de la información en la APC Colombia, mediante la definición, ejecución y seguimiento de acciones y controles orientados a gestionar los riesgos identificados en cada proceso institucional, con



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

el fin de mitigar su impacto, buscando prevenir la ocurrencia de posibles escenarios relacionados con incidentes de seguridad y privacidad de la Información y aquellos de seguridad digital.

2.2. Objetivos Específicos

- Establecer y formalizar las acciones de tratamiento de los riesgos de seguridad y privacidad de la Información identificados en los procesos institucionales, mediante la adopción e implementación de controles orientados a prevenir, mitigar o reducir los impactos asociados a dichos riesgos.
- Verificar y asegurar el cumplimiento y la efectividad de los controles y los planes de tratamiento de riesgos definidos, a través de actividades de seguimiento, evaluación y control, que permitan identificar desviaciones, inconsistencias o incumplimientos y disponer las acciones correctivas y de mejora que correspondan.
- Garantizar una gestión integral y articulada de la seguridad y privacidad de la información en la Agencia, mediante la coordinación de los líderes y responsables de los procesos, la adecuada administración de los activos de información y la prevención de incidentes de seguridad que puedan comprometer la confidencialidad, integridad y disponibilidad de la información.

3. ALCANCE

El presente plan aplica para todos los recursos tecnológicos y servicios de información que soportan la gestión institucional de la APC Colombia, en alineación con sus procesos y los controles definidos en el SGSPI. Este plan tiene como finalidad asegurar la gestión integral, sistemática y coherente de los riesgos de seguridad y privacidad de la información, garantizando la debida protección de los activos de información críticos de la Agencia.



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

4. TÉRMINOS Y DEFINICIONES

Las definiciones son tomadas en gran parte de los lineamientos del MinTIC de la Política de gobierno digital, en especial del Modelo de Seguridad y Privacidad de la Información (MSPI).

- **Acceso a la información pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados (Ley 1712 de 2014, artículo 4).
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la organización (ISO/IEC 27000).
- **Activo de información:** Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos asociados con el manejo de los datos e información misional, operativa y administrativa de la APC Colombia (CONPES 3854 de 20116, acondicionada para la APC Colombia).
- **Aceptación de riesgos:** Decisión formal y documentada mediante la cual la entidad asume un riesgo identificado, cuando este se encuentra dentro de los niveles de tolerancia definidos, sin implementar acciones adicionales de tratamiento.
- **Aliado técnico:** Personal natural o jurídica que según su naturaleza intercambia o es receptor de información con la APC Colombia.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO/IEC 27000).
- **Análisis de riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo (ISO/IEC 27000).



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura (Ley 594 de 2000, artículo 3).
- **Bases de datos personales:** Conjunto organizado de datos personales que sea objeto de tratamiento (Ley 1581 de 2012, artículo
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios, Resolución 2258 de 2009 de la Comisión de Regulación de Comunicaciones (CRC).
- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados, realizado mediante el conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual.
- **Confidencialidad:** se define como aquella información que siendo propiedad de un proceso, área o dependencia no puede ponerse a disposición ni tampoco puede ser revelada a individuos, entidades o procesos no autorizados (Norma ISO/IEC 27000).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad y privacidad de la información por debajo del nivel de riesgo asumido. Control es también utilizado, como sinónimo de



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Consecuencia:** Efecto o resultado derivado de la materialización de un riesgo, que puede afectar: activos de información, procesos, servicios, continuidad operativa o cumplimiento de los objetivos institucionales.
- **Disponibilidad:** indica que la información debe ser accesible y utilizable cuando lo requiera área, dependencia y otra entidad autorizada (Norma ISO/IEC 27000).
- **Datos personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012, artículo 3).
- **Encargado del tratamiento de datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento (Ley 1581 de 2012, artículo 3).
- **Grupos de valor:** Es la forma de presentar a un grupo de personas naturales (ciudadanos) o jurídicas (organizaciones públicas o privadas), a quienes van dirigidos los bienes y/o servicios de una entidad, con características semejantes que tramita, recibe un producto y/o servicio para satisfacer su necesidad, también denominados grupos de interés, públicos de interés, corresponsables u otros, Departamento Administrativo de la Función Pública (DAFP), Glosario del Modelo Integrado de Planeación y Gestión (MIPG), Versión: 03, Fecha: 13/10/2020), como se citó en la Caracterización de partes interesadas y grupos de valor (A-OT-084).
- **Impacto:** Nivel de afectación o daño que puede generar la materialización de un riesgo sobre la entidad, los procesos, activos de información o partes interesadas y grupos de valor.
- **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio,



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014 (Ley 1712 de 2014, artículo 6).

- **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014 (Ley 1712 de 2014, artículo 6).
- **Integridad:** consiste en toda aquella información que debe salvaguardar su exactitud y completitud (Norma ISO/IEC 27000).
- **Ley de habeas data:** Se refiere a la Ley Estatutaria 1266 de 2008. Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.
- **Medida:** Acción, mecanismo o salvaguarda de naturaleza administrativa, técnica o física, destinada a prevenir, reducir, detectar o corregir los riesgos de seguridad y privacidad de la Información.
- **Partes interesadas:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad y privacidad de la información inaceptables e implantar los controles necesarios para proteger la misma (ISO/IEC 27000).
- **Probabilidad:** Grado de posibilidad de ocurrencia de un evento de riesgo, considerando la existencia de amenazas, vulnerabilidades y la efectividad de los controles que han sido implementados.



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

- **Registro nacional de bases de datos:** Directorio público de las bases de datos sujetas a tratamiento que operan en el país (Ley 1581 de 2012, artículo 25).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000).
- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza explote una vulnerabilidad y afecte un activo de información, comprometiendo la confidencialidad, integridad o disponibilidad de la información.
- **Riesgo de seguridad digital:** Posibilidad de afectación negativa sobre los activos de información, los servicios digitales o la operación institucional, derivada del uso, gestión o dependencia de las tecnologías digitales.
- **Riesgo inherente:** Nivel de riesgo existente antes de la aplicación de controles o medidas de tratamiento, determinado a partir de la probabilidad y el impacto identificados.
- **Registro nacional de bases de datos:** Directorio público de las bases de datos sujetas a tratamiento que operan en el país (Ley 1581 de 2012, artículo 25).
- **Riesgo residual:** Nivel de riesgo que permanece después de la implementación de los controles o medidas de tratamiento, el cual debe ser evaluado frente a los criterios de aceptación del riesgo definidos por la entidad.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **Sistema de información:** Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la APC Colombia o de origen externo ya sea adquirido por la Agencia como un producto estándar de mercado o desarrollado para las necesidades de ésta.

- **Terceros:** Personas naturales o personas jurídicas que, relacionados con el SGSPI y los procesos institucionales, son sujetos de acceder, consultar, solicitar, intercambiar, transformar, producir o archivar datos e información institucional, como, por ejemplo: servidores públicos de la APC Colombia u otras entidades públicas, contratistas, entidades privadas, entidades públicas, pasantes, aliados técnicos y ciudadanos.
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento (Ley 1581 de 2012, artículo 3).
- **Tratamiento de datos personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (Ley 1581 de 2012, artículo 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad, deficiencia o ausencia de controles en un activo, proceso o sistema, que puede ser aprovechada por una amenaza y dar lugar a la materialización de un riesgo.

5. SIGLAS

- **APC COLOMBIA:** Agencia Presidencial de Cooperación Internacional de Colombia.
- **CIGD:** Comité Institucional de Gestión y Desempeño.



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

- **CRC:** Comisión de Regulación de Comunicaciones.
- **DAFP:** Departamento Administrativo de la Función Pública.
- **IEC:** Comisión Electrotécnica Internacional (organización que establece normas internacionales para productos y sistemas eléctricos y electrónicos).
- **ISO:** International Organization for Standardization.
- **MinTic:** Ministerio de Tecnologías de la Información y Comunicaciones.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **NTC:** Norma Técnica Colombiana.
- **RNBD:** Registro Nacional de Bases de Datos.
- **SIC:** Superintendencia de Industria y Comercio.
- **SGSPI:** Sistema de gestión de la seguridad de la información.

6. MARCO NORMATIVO

- **Constitución Política de Colombia, artículos 15 y 74**, que consagran el derecho fundamental al habeas data, la protección de la información personal y el acceso a los documentos públicos, en concordancia con los principios de reserva y confidencialidad de la información.
- **Ley 1266 de 2008**, Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales (especialmente datos financieros y crediticios).
- **Ley 1581 de 2012**, Por la cual se dictan disposiciones generales para la protección de datos personales, estableciendo los principios, derechos y obligaciones relacionados con el tratamiento de la información personal.



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

- **Ley 1712 de 2014**, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, que establece criterios de publicidad, reserva y clasificación de la información.
- **Decreto 1377 de 2013**, Reglamenta parcialmente la Ley 1581 de 2012 (autorizaciones, políticas de tratamiento, derechos de los titulares, transferencias internacionales, etc.).
- **Decreto 886 de 2014**, Reglamenta el Registro Nacional de Bases de Datos (RNBD) ante la Superintendencia de Industria y Comercio (SIC).
- **Decreto 103 de 2015**, Por el cual se reglamenta la Ley 1712 de 2014, en lo relacionado con la gestión de la información pública y la clasificación de la información.
- **Decreto 1074 de 2015**, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, que incorpora disposiciones relacionadas con la protección de datos personales.
- **Decreto 1083 de 2015**, Decreto Único Reglamentario del Sector Función Pública, que incorpora lineamientos relacionados con la gestión institucional, el control interno y la administración de riesgos.
- **Decreto 1499 de 2017**, Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Decreto 612 de 2018**, 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.
- **Decreto 1008 de 2018**, Por el cual se establecen los lineamientos generales de la Política de gobierno digital, incluyendo la adopción del MSPI en las entidades públicas.



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

- **Decreto 338 de 2022**, Reglamenta aspectos de seguridad y privacidad en el marco del CSIRT-Gobierno y gestión de incidentes.
- **Conpes 3995 de 2020 (y actualizaciones posteriores)**, Política Nacional de Seguridad Digital (enfocada en gestión de riesgos, resiliencia y respuesta a incidentes).
- **Resolución 1519 de 2020**, Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC), Por la cual se definen los estándares y lineamientos para la implementación de la Política de gobierno digital, incorporando el MSPI, como componente obligatorio.
- **Resolución 500 de 2021**, Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC), establece lineamientos y estándares para la Estrategia de seguridad digital y adopta el Modelo de Seguridad y Privacidad de la Información (MSPI), como habilitador de la Política de gobierno digital. Es el marco principal para la gestión de riesgos de seguridad y privacidad en entidades públicas.
- **Resolución 00460 de 2022**, Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC), Plan Nacional de Infraestructura de Datos (relacionado con seguridad de activos informativos).
- **Norma Técnica Colombiana NTC/ISO/IEC 27001:2022**, Estándar internacional adoptado en Colombia para la implementación de sistemas de gestión de seguridad de la información, utilizado como referente técnico para la gestión de riesgos y controles de seguridad.
- **Norma Técnica Colombiana NTC/ISO/IEC 27005**, Norma de referencia para la gestión de riesgos de seguridad de la información, complementaria a la ISO/IEC 27001.
- **Modelo de Seguridad y Privacidad de la Información (MSPI)**, Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC), marco de referencia para



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

la gestión de la seguridad y privacidad de la información en las entidades públicas, que establece directrices para la identificación, análisis, evaluación y tratamiento de riesgos, alineado con la norma ISO/IEC 27001.

- **Guía para la Gestión Integral del Riesgo en Entidades Públicas**, Versión 7, 2025, Departamento Administrativo de la Función Pública (DAFP).

7. MARCO DE ACCIÓN FRENTE AL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se presenta la tabla que consolida la planificación para el tratamiento de riesgos de seguridad y privacidad de la información.

ÍTEM	ACTIVIDAD	PROCEDIMIENTO	RESPONSABLE	PERÍODO	EVIDENCIA
				Trimestre	
1	Actualización de designación de enlaces del SGSPI.	Memorando por Hermes.	Catorce (14) procesos institucionales Solicitud por el proceso Gestión de tecnologías de la información.	2 y 3	Memorando de respuesta.
2	Entrenamiento y capacitación, frente a la gestión de activos de	No aplica	Proceso Gestión de Tecnologías de la Información.	2 y 3	Presentación y actas de capacitación.



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

ÍTEM	ACTIVIDAD	PROCEDIMIENTO	RESPONSABLE	PERÍODO	EVIDENCIA
				Trimestre	
	información y riesgos de seguridad y privacidad de la información a los catorce (14) procesos institucionales.				
3	Identificación de activos de información: <ul style="list-style-type: none">• Programación y comunicación.• Actualización.• Clasificación.• Valoración.	Aplicación del documento: Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información (A-OT-125).	Procesos institucionales. Programación y comunicación por el proceso Gestión de Tecnologías de la Información.	2 y 3	Inventario de activos de información y gestión de riesgos de seguridad de la información (A-FO-272).
4	Identificación de riesgos de seguridad y privacidad de la información:	Aplicación del documento: Lineamiento metodológico de gestión de activos de información y de	Procesos institucionales. Proceso de Gestión de	2 y 3	Inventario de activos de información y gestión de riesgos de seguridad de



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

ÍTEM	ACTIVIDAD	PROCEDIMIENTO	RESPONSABLE	PERÍODO	EVIDENCIA
				Trimestre	
	<ul style="list-style-type: none">Identificación de causas, riesgos, probabilidad, impacto.Tipificar y valorar el riesgo.Determinar nivel de riesgo inherente.	riesgos de seguridad de la información (A-OT-125).	Tecnologías de la Información.		la información (A-FO-272).
5	Definición del tratamiento del riesgo.	Aplicación del documento: Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información (A-OT-125).	Procesos institucionales.	2 y 3	Inventario de activos de información y gestión de riesgos de seguridad de la información (A-FO-272).
6	Definición de controles sobre riesgos de seguridad y	Aplicación del documento: Lineamiento metodológico de	Procesos institucionales.	2 y 3	Inventario de activos de información y gestión de



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

ÍTEM	ACTIVIDAD	PROCEDIMIENTO	RESPONSABLE	PERÍODO	EVIDENCIA
				Trimestre	
	privacidad de la información: <ul style="list-style-type: none">• Descripción.• Valoración.• Frecuencia.• Documentación.• Determinar riesgo residual.	gestión de activos de información y de riesgos de seguridad de la información (A-OT-125).			riesgos de seguridad de la Información (A-FO-272).
7	Certificación de la gestión de activos de información, riesgos de seguridad y privacidad de la información y declaración de responsabilidad: <ul style="list-style-type: none">• Generar certificados.	Aplicación del documento: Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información (A-OT-125).	Procesos institucionales.	3 y 4	Certificados de gestión de activos y de riesgos.



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

ÍTEM	ACTIVIDAD	PROCEDIMIENTO	RESPONSABLE	PERÍODO	EVIDENCIA
				Trimestre	
8	Seguimiento e implementación de los controles.	Aplicación del documento: Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información (A-OT-125).	Procesos institucionales.	1, 2, 3 y 4	Informe de seguimiento de la implementación de los controles.
9	Evaluación de la efectividad y cobertura de los controles: <ul style="list-style-type: none">• Gestión por el esquema de las líneas de defensa: (tercera línea).• Revisión de la ejecución y/u operación del control.	Aplicación del documento: Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información (A-OT-125).	Procesos institucionales. Proceso Evaluación, Control y Mejoramiento.	2 y 3	Inventario de activos de información y gestión de riesgos de seguridad de la información (A-FO-272).



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

ÍTEM	ACTIVIDAD	PROCEDIMIENTO	RESPONSABLE	PERÍODO	EVIDENCIA
				Trimestre	
	<ul style="list-style-type: none">Revisión de la documentación de evidencias de control.				
10	Publicación en la sede electrónica de la Agencia, el inventario de activos de información.	Aplicación del documento: Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información (A-OT-125).	Proceso Gestión de Tecnologías de la Información. Proceso Gestión de Comunicaciones.	2 y 3 trimestre	URL de publicación.

Fuente: Elaboración del proceso Gestión de tecnologías de la información de la APC Colombia, enero de 2026.

8. ROLES Y RESPONSABILIDADES: Revisión de la gestión por el esquema de las líneas de defensa

El monitoreo y la revisión a la gestión de activos de información y a la gestión de riesgos de seguridad y privacidad de la información, se define acorde con el esquema de las líneas de defensa, en la siguiente tabla:

NO.	LÍNEA	ACCIÓN DE LA OPERACIÓN
-----	-------	------------------------



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

1	Línea estratégica	En este nivel se define el marco general de la gestión de riesgo y se asegura el cumplimiento de los planes de la Agencia.
2	Primera línea de defensa	Esta línea se encarga del mantenimiento efectivo de los activos de información, la gestión de los riesgos asociados, y la implementación de los controles sobre los riesgos de seguridad y privacidad de la información. Por consiguiente, identifica, evalúa, controla y mitiga los riesgos.
3	Segunda línea de defensa	<ul style="list-style-type: none">• Responsable el proceso Gestión de Tecnologías de la Información.• Realizar la planeación y la programación de actividades y acciones para orientar a los procesos institucionales en la ejecución de la gestión de activos de información y de riesgos de seguridad y privacidad de la información en el documento: Plan de seguridad y privacidad de la información (A-OT-101).• Orientar a los procesos institucionales y ofrecer acompañamiento técnico para el desarrollo de las actividades de la gestión de activos de información y la gestión de riesgos de seguridad y privacidad de la información.• Realizar el monitoreo y el seguimiento al cumplimiento de los procesos institucionales frente a la ejecución de actividades de la gestión de activos de información y la gestión de riesgos de seguridad y privacidad de la información, por parte del proceso.



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

		<ul style="list-style-type: none">• Presentar información a la dirección administrativa y financiera, dirección general, y demás instancias de la alta dirección de la Agencia, sobre la gestión de activos de información y de riesgos de seguridad de la información.• Emitir los certificados sobre el número de activos de información, riesgos de seguridad y privacidad de la información y controles, por cada proceso institucional.• Publicar el Inventario de activos de información y de gestión de riesgos de seguridad y privacidad de la información (A-FO-272), en la sede electrónica. Asimismo, en la carpeta red de proceso Gestión de Tecnologías de la Información.• Publicar el documento: Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información (A-OT-125) que, equivalen al Plan de tratamiento de riesgos de seguridad y privacidad de la información de que, trata el Decreto 612 de 2018 <i>“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”</i>.
4	Tercera línea de defensa	A cargo del(a) asesor(a) con funciones de Control Interno y su equipo de trabajo, quienes evalúan de manera independiente y objetiva la efectividad y cobertura de los controles de la 2ª línea de defensa.

Fuente: Adaptado de la Política de gestión del riesgo (A-OT-008) de la APC Colombia.



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

9. RECURSOS

La APC Colombia, dispondrá de los recursos que resulten necesarios y suficientes para la adecuada identificación, análisis, evaluación y tratamiento de los riesgos de seguridad y privacidad de la información, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información bajo su responsabilidad. Así como, la efectiva implementación, operación y mejora continua del SGSPI.

A continuación, se presenta la tabla con la disponibilidad de recursos para el plan de tratamiento de riesgos de seguridad y privacidad de la información.

ÍTEM	RECURSO	VARIABLE
1	Humanos	El proceso Gestión de Tecnologías de la Información, que lidera la gestión de seguridad y privacidad de la información y será responsable de definir e implementar lineamientos metodológicos, frente a la gestión de activos de información y de riesgos de seguridad y privacidad de la información.
2	Técnicos	<ul style="list-style-type: none">Guía para la gestión integral del riesgo en entidades públicas, versión 7 del 2025, emitida por el Departamento Administrativo de la Función Pública (DAFP).Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información, emitido por el proceso Gestión de Tecnologías de la Información de la APC Colombia (A-OT-125).
3	Logísticos	Mesas de trabajo, capacitaciones y jornadas de sensibilización relacionadas con la gestión de activos y de riesgos (salas de reunión, plataformas de videoconferencia institucionales).



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

4	Financieros	Recursos presupuestales necesarios para soportar la implementación, operación y mejora de los controles y acciones definidos en el plan de tratamiento de riesgos de seguridad y privacidad de la información, ya sean adquisición, renovación o fortalecimiento de soluciones tecnológicas de seguridad digital (licenciamiento, suscripciones, mantenimiento y soporte).
---	-------------	--

Fuente: Elaborado por el proceso Gestión de Tecnologías de la Información de la Dirección Administrativa y Financiera de la APC Colombia, enero de 2026.

10. MEDICIÓN

La medición se efectuará con fundamento en un indicador del SGSPI, el cual tiene por objeto determinar el porcentaje de cumplimiento, en la implementación de los controles de seguridad de la información, conforme a aquellos definidos en la matriz de plan de cumplimiento de objetivos del SGSPI, y en concordancia con lo establecido en el respectivo plan de tratamiento de riesgos.

A continuación, se presenta la tabla con la medición para el cumplimiento de la gestión del riesgo.

ÍTEM	INDICADOR	FRECUENCIA DE REVISIÓN
1	Porcentaje de efectividad de los controles implementados de los riesgos de seguridad y privacidad de la información. Formula: $(\text{número de controles efectivos}) / (\text{número total de controles implementados}) \times 100$.	Trimestral.



APC Colombia

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

Código: A-OT-134 | Versión: 01 | Fecha: Febrero 20 de 2026

Fuente: Elaborado por el proceso Gestión de Tecnologías de la Información de la Dirección Administrativa y Financiera de la APC Colombia, enero de 2026.

11. CONTROL DE CAMBIOS

VERSIÓN	CÓDIGO	NOMBRE DEL DOCUMENTO	ACTO/ MECANISMO	DESCRIPCIÓN DEL CAMBIO
1	A-OT-134	Plan de tratamiento de riesgos de seguridad y privacidad de la información.	Brújula, Febrero 20 de 2026	Creación del documento.