Plan de Tratamiento de Riesgos de Seguridad Digital (PTR-SD)

AÑO 2026

TABLA DE CONTENIDO

INTRODUCCIÓN 3
OBJETIVO 3
MARCO NORMATIVO 3
ANALISIS DE CONTEXTO 4
CONTEXTO ESTRATEGICO 6
RIESGOS Y CONTROLES 7
PROCESO DE FORMULACIÓN 8
CRONOGRAMA 9
SEGUIMIENTO Y CONTROL 10
ROLES Y RESPONSABILIDAD 10
COMUNICACIÓN Y DIVULGACIÓN 12
GESTION DEL CONOCIMIENTO 12
ANEXOS 13
TABLA DE RENTENCIÓN DOCUMENTAL 13
CONTROL DE CAMBIOS 13

INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad Digital (PTR-SD) de RTVC para la vigencia 2026 se elabora con el propósito de establecer, de manera institucional, las acciones necesarias para tratar los riesgos de seguridad digital que pueden afectar la confidencialidad, integridad y disponibilidad de la información y de los servicios tecnológicos que soportan los procesos misionales y de apoyo de la entidad.

Este plan se realiza en el marco del fortalecimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) y del componente de Gestión del Riesgo y Control Interno, teniendo en cuenta los lineamientos aplicables para entidades públicas definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y el Departamento Administrativo de la Función Pública (DAFP), así como los resultados de diagnósticos, auditorías y análisis institucionales que evidencian brechas y necesidades de mejora en materia de seguridad digital.

El objeto central del PTR-SD es priorizar y organizar los tratamientos (acciones y controles) que permitan reducir los niveles de riesgo a rangos aceptables, asegurar la continuidad de la operación y fortalecer la confianza en el uso del entorno digital en RTVC durante la vigencia 2026.

Para su elaboración se tuvo en cuenta que el presente plan constituye la base institucional para la identificación, análisis y alineación de los riesgos de seguridad digital de RTVC, los cuales serán gestionados y tratados de manera progresiva durante la vigencia 2026. En este sentido, el plan considera como insumos iniciales la matriz institucional de riesgos, las capacidades y recursos disponibles, la dependencia de terceros y proveedores tecnológicos, y los compromisos institucionales asociados a la estrategia de Gobierno Digital.

OBJETIVO

Orientar y priorizar el tratamiento de los riesgos de seguridad digital en Radio Televisión Nacional de Colombia – RTVC durante la vigencia 2026, mediante la definición de acciones institucionales que contribuyan a reducir la probabilidad y el impacto de eventos que puedan afectar la confidencialidad, integridad y disponibilidad de la información y de los servicios tecnológicos que soportan los procesos de la entidad.

MARCO NORMATIVO

El Plan Institucional de Tratamiento de Riesgos de Seguridad Digital de Radio Televisión Nacional de Colombia – RTVC se formula en cumplimiento del marco normativo y de política pública aplicable a las entidades públicas en materia de gestión del riesgo, seguridad digital, protección de la información y Gobierno Digital.

Las normas y documentos de referencia que se relacionan a continuación constituyen el fundamento para la definición, implementación y seguimiento de las acciones previstas en el presente plan, y orientan la gestión institucional del riesgo de seguridad digital, en concordancia con los principios de planeación, control interno y mejora continua.

Tabla 1 Normatividad aplicable

Norma	Descripción
Decreto 1499 de 2017	Adopta el Modelo Integrado de Planeación y Gestión – MIPG.
Decreto 612 de 2018	Establece directrices para la integración de los planes institucionales y estratégicos al Plan de Acción de las entidades del Estado.
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 338 de 2022	Define lineamientos para fortalecer la gobernanza de la seguridad digital.
Decreto 767 de 2022	Establece los lineamientos generales de la Política de Gobierno Digital.
Resolución 500 de 2021 – MinTIC	Define los lineamientos para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital.
Guía DAFP	Guía para la administración del riesgo en la gestión, corrupción y seguridad digital en entidades públicas.
ISO 31000:2018	Norma internacional de referencia para la gestión del riesgo, utilizada como marco de apoyo conceptual para la identificación, análisis, evaluación y tratamiento de riesgos.

Fuente: *Elaboración propia – Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD) RTVC 2026, con base en la normatividad vigente aplicable en materia de seguridad digital, gestión del riesgo y planeación institucional, y en los lineamientos del MinTIC y el Departamento Administrativo de la Función Pública (DAFP).*

ANALISIS DE CONTEXTO

Para la formulación del Plan Institucional de Tratamiento de Riesgos de Seguridad Digital de Radio Televisión Nacional de Colombia – RTVC se realizó un análisis del contexto interno y externo, con el fin de identificar y recopilar información relevante sobre los factores que influyen en la gestión de los riesgos de seguridad digital y en el cumplimiento de los objetivos del plan durante la vigencia 2026.

Contexto externo

RTVC, en su calidad de entidad pública y sistema de medios públicos, desarrolla su gestión en un entorno caracterizado por una alta dependencia de las tecnologías de la información para el desarrollo de sus procesos, así como por el uso creciente de servicios tecnológicos y plataformas digitales para la prestación de servicios institucionales.

Desde el componente normativo y de política pública, se tuvieron en cuenta los lineamientos vigentes en materia de seguridad digital y Gobierno Digital aplicables a las entidades del Estado, los cuales establecen la necesidad de fortalecer de manera progresiva la gestión de los riesgos asociados a la información y a los servicios digitales.

En el ámbito tecnológico, se identificó una mayor exposición al riesgo derivada de la digitalización de procesos, la interoperabilidad de plataformas, el uso de infraestructuras tecnológicas compartidas y la dependencia de terceros y proveedores externos, lo cual amplía la superficie de exposición al riesgo y aumenta la probabilidad de afectaciones a la confidencialidad, integridad y disponibilidad de la información institucional.

Estas condiciones externas hacen necesario que RTVC adopte un enfoque preventivo y progresivo para el tratamiento de los riesgos de seguridad digital, alineado con sus capacidades institucionales y con los lineamientos definidos para las entidades públicas.

Contexto interno y estado inicial de la gestión del riesgo

Desde el contexto interno, la gestión de riesgos de seguridad digital en RTVC se encuentra en una etapa inicial de fortalecimiento, lo que representa una oportunidad institucional para estructurar y consolidar de manera progresiva este componente fundamental del Modelo de Seguridad y Privacidad de la Información (MSPI).

Los diagnósticos y auditorías internas realizados han evidenciado la necesidad de fortalecer la identificación de los riesgos de seguridad digital, así como de avanzar en la consolidación de una matriz integral de activos y riesgos aplicable a los diferentes procesos de la entidad.

En este sentido, RTVC se encuentra en proceso de fortalecimiento de sus prácticas de administración del riesgo, en concordancia con los lineamientos del Departamento Administrativo de la Función Pública y el enfoque de mejora continua del MSPI.

Adicionalmente, recientemente se adelantó un ejercicio de auditoría al Modelo de Seguridad y Privacidad de la Información (MSPI), cuyos resultados constituyen un insumo relevante para la identificación de oportunidades de mejora en la gestión institucional de la seguridad digital. En este marco, el presente plan se articula con las acciones de fortalecimiento derivadas de la implementación del MSPI, particularmente en lo relacionado con la consolidación de la gestión de riesgos como elemento transversal del modelo.

Tendencias, oportunidades y amenazas

El análisis del contexto permitió identificar como tendencia el incremento de la exposición a riesgos de seguridad digital asociado a la digitalización de procesos y a la dependencia tecnológica. Como oportunidad, se reconoce la posibilidad de fortalecer la gestión institucional del riesgo mediante la articulación del presente plan con el MSPI, el Modelo Integrado de Planeación y Gestión (MIPG) y los procesos de planeación y control interno. Finalmente, se identifican amenazas asociadas a la materialización de riesgos de seguridad

digital que podrían generar impactos operativos, reputacionales y afectar la continuidad de los servicios institucionales si no se gestionan de manera oportuna.

Con base en este contexto, el Plan Institucional de Tratamiento de Riesgos de Seguridad Digital para la vigencia 2026 se orienta a fortalecer progresivamente la identificación y el tratamiento de los riesgos, estableciendo una base sólida para el avance en la madurez de la gestión de la seguridad digital en RTVC.

CONTEXTO ESTRATEGICO

El Plan Institucional de Tratamiento de Riesgos de Seguridad Digital de Radio Televisión Nacional de Colombia – RTVC se articula con la Plataforma Estratégica Institucional 2023-2026, en la medida en que contribuye al fortalecimiento de las capacidades institucionales para la protección de la información, la continuidad de la operación y el cumplimiento de los objetivos estratégicos de la entidad.

El plan se alinea con la visión institucional de RTVC, orientada a garantizar la prestación confiable y oportuna de los servicios como sistema de medios públicos, reconociendo que la gestión adecuada de los riesgos de seguridad digital es un habilitador transversal para el logro de los objetivos misionales y estratégicos. En este sentido, el tratamiento de los riesgos de seguridad digital aporta a la sostenibilidad de los procesos, a la protección de los activos de información y al fortalecimiento de la confianza en el uso del entorno digital.

Así mismo, el presente plan se articula con las políticas del Modelo Integrado de Planeación y Gestión (MIPG), en particular con aquellas relacionadas con la gestión del riesgo, el control interno y el uso y aprovechamiento de las tecnologías de la información, aportando al fortalecimiento de la planeación institucional y a la toma de decisiones informadas frente a los riesgos que pueden afectar la operación de la entidad.

Desde el enfoque de procesos, el Plan Institucional de Tratamiento de Riesgos de Seguridad Digital tiene un impacto transversal sobre el mapa de procesos de RTVC, incidiendo tanto en los procesos misionales como en los procesos estratégicos y de apoyo, al establecer lineamientos y acciones para el tratamiento de riesgos asociados a la información y a los servicios tecnológicos que los soportan.

De esta manera, el plan se constituye en un instrumento de articulación estratégica que contribuye a la implementación del MSPI, al fortalecimiento del MIPG y al cumplimiento de los objetivos institucionales definidos para la vigencia 2023-2026.

RIESGOS Y CONTROLES

En esta sección se relacionan los riesgos de seguridad digital identificados para el Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD), así como los controles y consecuencias asociados, en coherencia con el estado actual de madurez de la entidad y con el enfoque de fortalecimiento progresivo definido para la vigencia 2026.
Los riesgos aquí descritos se centran en aspectos institucionales relacionados con la identificación, ejecución, seguimiento y apropiación de los tratamientos de riesgos de seguridad digital, y se encuentran alineados con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la gestión del riesgo institucional.

Tabla 2: Riesgos asociados

Riesgo	Control	Consecuencia
R1. Identificación incompleta de los riesgos de seguridad digital en los procesos institucionales, lo que puede limitar la definición de tratamientos adecuados y oportunos.	• Fortalecimiento progresivo del proceso institucional de identificación de riesgos de seguridad digital. • Articulación de la identificación de riesgos con la matriz institucional de activos y riesgos. • Acompañamiento a los procesos para la identificación de riesgos de seguridad digital.	• Riesgos no tratados o tratados de manera inadecuada. • Exposición a incidentes no previstos.
R2. Limitaciones en capacidades institucionales (recursos, roles o nivel de madurez) para ejecutar de manera efectiva los tratamientos de riesgos de seguridad digital definidos.	• Priorización de tratamientos de acuerdo con criticidad y capacidades institucionales. • Definición clara de roles y responsabilidades. • Planeación gradual del fortalecimiento de capacidades.	• Ejecución parcial o tardía de los tratamientos. • Persistencia de riesgos críticos. • Avances limitados en la madurez del MSPI.
R3. Falta de seguimiento a los tratamientos de riesgos de seguridad digital, lo que puede impedir la identificación oportuna de desviaciones y oportunidades de mejora.	• Definición de mecanismos de seguimiento e indicadores del PTR-SD. • Revisión periódica del avance de los tratamientos. • Reporte de resultados la coordinación de TI	• Desconocimiento del estado real de los riesgos. • Ausencia de mejora continua. • Debilidades evidenciadas en auditorías.

R4. Debilidades en la cultura institucional de seguridad digital, que pueden afectar la efectividad de los tratamientos de riesgos definidos en el plan.	• Inclusión de acciones de sensibilización y divulgación asociadas al PTR-SD. • • Comunicación clara de responsabilidades en seguridad digital. • Articulación con programas institucionales de formación.	• Baja apropiación de los tratamientos definidos. • Incremento de errores humanos. • Limitaciones para consolidar una cultura de seguridad digital.

Fuente: Elaboración propia – Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD) RTVC 2026, con base en el análisis del contexto institucional, los resultados del Diagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) 2025 y los lineamientos del MinTIC y el Departamento Administrativo de la Función Pública (DAFP).

***Nota:** Los riesgos y controles aquí relacionados corresponden al alcance del Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD) y constituyen una referencia general para orientar las acciones de tratamiento durante la vigencia 2026. Su desarrollo detallado, seguimiento y actualización se realizará de manera articulada con los instrumentos institucionales de gestión del riesgo y con los planes de tratamiento que se definan en el marco del MSPI.*

PROCESO DE FORMULACIÓN

El Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD) de Radio Televisión Nacional de Colombia – RTVC para la vigencia 2026 fue formulado a partir del análisis del contexto institucional y del estado actual de la gestión del riesgo en la entidad, con el propósito de fortalecer de manera progresiva la identificación, el tratamiento y el seguimiento de los riesgos específicos asociados a la seguridad digital, en el marco del Modelo de Seguridad y Privacidad de la Información (MSPI).

Durante el proceso de formulación se tuvieron en cuenta los resultados de diagnósticos institucionales, ejercicios de autoevaluación y auditorías relacionadas con el MSPI, así como la revisión de los instrumentos de planeación y gestión vigentes. Estos insumos permitieron identificar brechas y oportunidades de mejora, especialmente en la incorporación sistemática de los riesgos de seguridad digital dentro de la gestión institucional del riesgo.

Así mismo, el plan fue formulado considerando el nivel de madurez actual de la entidad, las capacidades institucionales disponibles en términos de recursos, roles y responsabilidades, y la necesidad de articular las acciones de tratamiento con el Modelo Integrado de Planeación y Gestión (MIPG), garantizando un enfoque realista, gradual y alineado con la planeación institucional.

Situación actual

RTVC cuenta con un esquema de gestión del riesgo institucional en el que se han identificado riesgos asociados a los procesos y a la gestión organizacional. Sin embargo, la incorporación de los riesgos específicos de seguridad digital dentro de este esquema se encuentra en una etapa inicial de fortalecimiento.

La identificación de riesgos se ha realizado de manera general, lo que evidencia la necesidad de profundizar en el análisis de los riesgos asociados a la confidencialidad, integridad y disponibilidad de la información y de los servicios tecnológicos que soportan los procesos institucionales. Así mismo, se identifican oportunidades de mejora relacionadas con la estandarización de prácticas entre los procesos, la ejecución oportuna

de los tratamientos definidos, el seguimiento sistemático de las acciones y el fortalecimiento de la cultura institucional en materia de seguridad digital.

Si bien la entidad presenta avances en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), se requiere consolidar la gestión de riesgos de seguridad digital como un componente transversal, articulado con la gestión del riesgo institucional y con los procesos de planeación y control.

Situación deseada

Para la vigencia 2026, RTVC proyecta fortalecer de manera progresiva la gestión de los riesgos de seguridad digital mediante la implementación del Plan Institucional de Tratamiento de Riesgos de Seguridad Digital como instrumento orientador para la identificación, priorización, ejecución y seguimiento de los tratamientos de riesgo.

La situación deseada contempla una identificación más clara y homogénea de los riesgos de seguridad digital entre los procesos institucionales, tratamientos priorizados de acuerdo con la criticidad y las capacidades de la entidad, mecanismos de seguimiento definidos y una mayor apropiación institucional de la seguridad digital como componente transversal del MSPI.

Con la implementación del presente plan, se espera reducir la exposición a eventos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, avanzar en la madurez de la gestión de riesgos de seguridad digital y fortalecer la capacidad institucional para prevenir, detectar y responder a incidentes de seguridad digital.

CRONOGRAMA

Tabla 3: Cronograma de actividades 2026

No.	Categoría / Componente	Actividad	Fecha inicial	Fecha final
1	Planeación	Socialización del Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD) con los líderes de proceso	Febrero 2026	Marzo 2026
2	Identificación de riesgos	Fortalecimiento del proceso de identificación de riesgos de seguridad digital en los procesos institucionales	Marzo 2026	Junio 2026
3	Identificación de riesgos	Articulación de los riesgos de seguridad digital con la matriz institucional de activos y riesgos	Abril 2026	Julio 2026
4	Tratamiento del riesgo	Definición y priorización de los tratamientos de riesgos de seguridad digital conforme a la criticidad y capacidades institucionales	Mayo 2026	Agosto 2026
5	Implementación	Ejecución gradual de los tratamientos de riesgos de seguridad digital definidos en el plan	Junio 2026	Noviembre 2026
6	Seguimiento y control	Definición e implementación de mecanismos de seguimiento e indicadores del PTR-SD	Julio 2026	Septiembre 2026

No.	Categoría / Componente	Actividad	Fecha inicial	Fecha final
7	Seguimiento y control	Seguimiento periódico al avance del Plan Institucional de Tratamiento de Riesgos de Seguridad Digital	Agosto 2026	Diciembre 2026
8	Mejora continua	Evaluación del avance del PTR-SD y definición de acciones de mejora para la siguiente vigencia	Noviembre 2026	Diciembre 2026

***Fuente**: Elaboración propia – Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD) RTVC 2026, en articulación con el Plan de Acción Institucional y los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG).*

SEGUIMIENTO Y CONTROL

El seguimiento y control del Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD) de RTVC para la vigencia 2026 se realizará con el propósito de verificar el avance en la ejecución de las actividades definidas, evaluar la implementación de los tratamientos de riesgo y apoyar la mejora continua de la gestión de riesgos de seguridad digital en la entidad.

Indicador asociado

Tabla 4: Ficha del indicador del plan

Nombre del indicador	Frecuencia	Meta	Tipología
Avance del Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD)	Semestral	≥ 90 %	Eficacia

Mecanismos de seguimiento

El seguimiento del Plan Institucional de Tratamiento de Riesgos de Seguridad Digital se llevará a cabo mediante los siguientes mecanismos:

- Elaboración de informes periódicos de avance del PTR-SD por parte de la Coordinación de Tecnologías de la Información.
- Revisión del cumplimiento de las actividades definidas en el cronograma del plan.
- Seguimiento a los tratamientos de riesgos de seguridad digital definidos y su estado de implementación.

ROLES Y RESPONSABILIDAD

Para la correcta ejecución, seguimiento y control del Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD) de RTVC para la vigencia 2026, se definen los

siguientes roles y responsabilidades, en concordancia con el Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo de Seguridad y Privacidad de la Información (MSPI):

Tabla 5 Roles y Responsabilidades

Roles	Responsabilidades
Alta Dirección / Comité Institucional de Gestión y Desempeño (CIGD)	• Aprobar el Plan Institucional de Tratamiento de Riesgos de Seguridad Digital y sus actualizaciones. • Orientar la toma de decisiones estratégicas frente a la gestión de riesgos de seguridad digital • Conocer los avances y resultados del PTR-SD en el marco del seguimiento institucional.
Primera Línea de Defensa – Procesos y Dependencias de RTVC	• Participar en la identificación de los riesgos de seguridad digital asociados a sus procesos. • Implementar los tratamientos de riesgos de seguridad digital definidos en el PTR-SD que les correspondan. • Reportar avances, dificultades y evidencias de ejecución. • Aplicar los lineamientos y controles de seguridad digital definidos por la entidad. • Contribuir al fortalecimiento de la cultura institucional de seguridad digital.
Segunda Línea de Defensa – Coordinación de Tecnologías de la Información	• Liderar la implementación del Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD). • Brindar acompañamiento técnico a los procesos para la identificación, tratamiento y seguimiento de los riesgos de seguridad digital. • Articular el PTR-SD con el Modelo de Seguridad y Privacidad de la Información (MSPI). • Consolidar los avances, indicadores y reportes de seguimiento del plan. • Coordinar la definición y priorización de tratamientos de riesgo conforme a la criticidad y capacidades institucionales.
Apoyo técnico – Especialista de Seguridad Digital	• Brindar acompañamiento técnico y metodológico para la gestión de riesgos de seguridad digital. • Apoyar la identificación, análisis y seguimiento de los riesgos definidos en el PTR-SD. • Asesorar a los líderes de proceso en la implementación de los tratamientos de riesgo. • Apoyar la consolidación de información y evidencias requeridas para el seguimiento del plan y del MSPI.
Seguimiento institucional – Proceso de Planeación	• Realizar el seguimiento institucional al PTR-SD conforme a los lineamientos del MIPG y del Plan de Acción Institucional. • Consolidar y validar los reportes de avance del plan. • Presentar los resultados del seguimiento a las instancias correspondientes. • Articular el PTR-SD con los demás planes institucionales de la

	entidad.

Fuente: *Elaboración propia – Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD) RTVC 2026, alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) y el Modelo Integrado de Planeación y Gestión (MIPG).*

COMUNICACIÓN Y DIVULGACIÓN

El Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD) de RTVC para la vigencia 2026 será comunicado y divulgado con el fin de garantizar su conocimiento, apropiación y correcta implementación por parte de los actores involucrados.

La comunicación del plan estará orientada principalmente a los líderes de proceso y a las áreas responsables de la ejecución de las actividades definidas, asegurando que conozcan el alcance del PTR-SD, sus objetivos, las responsabilidades asociadas y la importancia de la gestión de los riesgos de seguridad digital como componente transversal de la entidad.

La divulgación del plan se realizará a través de los canales institucionales definidos por RTVC, en articulación con la Coordinación de Tecnologías de la Información y el proceso de Planeación, y podrá incluir socializaciones, circulares internas, conforme a los lineamientos de gestión documental y transparencia.

Estas acciones de comunicación y divulgación permitirán fortalecer la cultura institucional de seguridad digital y apoyar la ejecución efectiva del PTR-SD durante la vigencia 2026.

GESTION DEL CONOCIMIENTO

La gestión del conocimiento en el marco del Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD) de RTVC se orienta a garantizar que la información, las buenas prácticas, las lecciones aprendidas y las experiencias generadas durante la identificación, tratamiento, seguimiento y control de los riesgos de seguridad digital sean registradas, organizadas y reutilizadas de manera sistemática.

Este enfoque permite fortalecer la capacidad institucional para gestionar los riesgos de seguridad digital de forma progresiva, asegurar la continuidad de la operación y apoyar la toma de decisiones informadas, contribuyendo al fortalecimiento del Modelo de Seguridad y Privacidad de la Información (MSPI).

Así mismo, la gestión del conocimiento asociada al PTR-SD se articula con los principios del Modelo Integrado de Planeación y Gestión (MIPG), promoviendo la mejora continua de la gestión del riesgo y la consolidación de prácticas institucionales en materia de seguridad digital.

ANEXOS

El Plan Institucional de Tratamiento de Riesgos de Seguridad Digital (PTR-SD) de RTVC para la vigencia 2026 contempla la generación progresiva de documentos e insumos de soporte, los cuales se desarrollarán en el marco de la ejecución del plan y conforme al avance de las actividades definidas.

En este sentido, los anexos asociados al PTR-SD no se incluyen en la presente versión del documento, dado que su elaboración se realizará durante la vigencia 2026 como resultado de los procesos de identificación, tratamiento y seguimiento de los riesgos de seguridad digital.

Los documentos que se generen como soporte del plan serán gestionados y conservados de acuerdo con los lineamientos institucionales de gestión documental y estarán disponibles para los procesos de seguimiento, control y auditoría cuando aplique.

VIGENCIA

Este plan se define para la vigencia 2026 y fue aprobado en sesión de Comité Institucional de Gestión y Desempeño el 27 de enero de 2026.

TABLA DE RENTENCIÓN DOCUMENTAL

Código Serie	Código Subserie	Nombre Serie	Nombre Subserie
430.36	430.36.09	PLANES	Plan Seguridad y Privacidad de la Información

CONTROL DE CAMBIOS

Versión	Descripción de ajuste	Área Productora	Fecha de Aprobación
01	Creación del documento para la vigencia 2026. Se ajusta el enfoque del plan como instrumento institucional, se redefine el alcance y se incorporan componentes de análisis de contexto, roles y responsabilidades, seguimiento, comunicación, gestión del conocimiento y cronograma, en alineación con el MSPI, el MIPG y los lineamientos vigentes del MinTIC y el DAFP.	Coordinación de Tecnologías de la Información	27/01/2026

01	Se realiza nuevamente el cargue del documento, se incluye encabezado, se ajusta código, logo, se incluye control de cambios, así mismo dando cumplimiento a los lineamientos del manual de marca. V2 y la Guía de Administración de Información Documentada SIG.	Coordinación de Planeación	05/10/2026