PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

AÑO 2026

TABLA DE CONTENIDO

INTRODUCCIÓN 3
OBJETIVO 3
OBJETIVOS ESPECÍFICOS 3
ALCANCE 4
MARCO NORMATIVO 5
ANALISIS DE CONTEXTO 6
Resultados Consolidados del Diagnóstico del MSPI 7
Resultados por Fases del MSPI 7
CONTEXTO ESTRATEGICO 8
RIESGOS Y CONTROLES 9
PROCESO DE FORMULACIÓN 12
PORTAFOLIO DE PROYECTOS Y PRODUCTOS ESPERADOS 15
CRONOGRAMA 16
SEGUIMIENTO Y CONTROL 18
ROLES Y RESPONSABILIDAD 19
COMUNICACIÓN Y DIVULGACIÓN 20
GESTION DEL CONOCIMIENTO 20
VIGENCIA 21
ANEXOS 21
TABLA DE RENTENCIÓN DOCUMENTAL 21
CONTROL DE CAMBIOS 21

INTRODUCCIÓN

La Radio Televisión Nacional de Colombia – RTVC reconoce que la información es un activo estratégico y esencial para el cumplimiento de su misión, la prestación del servicio público de comunicación y la generación de contenidos confiables para la ciudadanía. En este contexto, la seguridad digital constituye un pilar fundamental para proteger los procesos institucionales, garantizar la continuidad operativa y fortalecer la confianza en los servicios y plataformas administradas por la entidad.

El presente Plan Estratégico de Seguridad y Privacidad de la Información (PESI) se formula con el propósito de orientar, planificar y fortalecer la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en RTVC. Su objeto central es establecer el marco estratégico y las acciones necesarias para consolidar un Sistema de Gestión de Seguridad de la Información (SGSI) sostenible, alineado con las políticas nacionales de seguridad digital, los lineamientos del Ministerio TIC y las mejores prácticas internacionales, como la norma ISO/IEC 27001:2022.

El PESI incorpora los resultados del diagnóstico actualizado del MSPI, los cuales permiten identificar el nivel de madurez del modelo, las brechas existentes, los controles priorizados y las oportunidades de mejora que deben desarrollarse durante la vigencia. Con base en esta evaluación, el plan orienta acciones estratégicas que incrementan la capacidad institucional para gestionar los riesgos digitales y proteger los activos de información frente a amenazas internas y externas.

Este plan establece una ruta estratégica basada en el ciclo PHVA (Planear, Hacer, Verificar y Actuar), mediante la cual se definen acciones orientadas a fortalecer los controles de seguridad, mejorar la gestión del riesgo, desarrollar capacidades institucionales, promover la cultura de seguridad digital y asegurar una implementación gradual y sostenida del MSPI.

A través de este enfoque proactivo, RTVC busca garantizar la confidencialidad, integridad y disponibilidad de la información, promover la mejora continua y adaptarse a las exigencias del entorno digital, contribuyendo al fortalecimiento de la confianza ciudadana en el marco de la Política Pública de Gobierno Digital.

OBJETIVO

Establecer las directrices estratégicas para fortalecer la gestión de la seguridad de la información y la seguridad digital en RTVC – Sistema de Medios Públicos, mediante la implementación progresiva del Modelo de Seguridad y Privacidad de la Información (MSPI). Lo anterior con el fin de garantizar la protección de los activos de información, la gestión integral de riesgos, la continuidad de los servicios tecnológicos y la consolidación de una cultura organizacional orientada a la seguridad digital.

OBJETIVOS ESPECÍFICOS

- Fortalecer la gobernanza de la seguridad de la información, asegurando la definición clara de roles, responsabilidades y mecanismos de coordinación necesarios para la implementación efectiva del MSPI en todos los procesos institucionales.
- Implementar, actualizar y mejorar los controles administrativos, físicos y tecnológicos necesarios para mitigar los riesgos asociados a la confidencialidad, integridad, disponibilidad y privacidad de la información administrada por RTVC.

- Gestionar los riesgos de seguridad digital, mediante la identificación, análisis, valoración, tratamiento y seguimiento continuo de amenazas, vulnerabilidades y eventos que puedan afectar los activos de información.

- Fortalecer la continuidad y resiliencia de los servicios tecnológicos, mediante el desarrollo de capacidades institucionales para la prevención, respuesta, recuperación y operación ante incidentes de seguridad, fallas técnicas o interrupciones del servicio.

- Promover una cultura institucional de seguridad digital, mediante programas de sensibilización, capacitación y apropiación de buenas prácticas dirigidos a servidores públicos, contratistas y terceros con acceso a la información.

- Asegurar el cumplimiento del marco normativo aplicable, incluyendo las disposiciones de protección de datos personales, seguridad digital, Gobierno Digital, MSPI, ISO/IEC 27001:2022 y demás lineamientos regulatorios internos y externos.

- Monitorear y evaluar el desempeño del MSPI, a través de indicadores, auditorías internas y externas, revisiones por la dirección y mecanismos de seguimiento que garanticen la mejora continua del modelo.

- Mejorar los procesos, procedimientos y lineamientos de seguridad digital, garantizando su actualización continua y su coherencia con los objetivos institucionales y con los requisitos del SGSI/MSPI.

ALCANCE

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) busca establecer los fundamentos necesarios para el desarrollo gradual y sostenible de la seguridad digital en RTVC - Sistema de Medios Públicos. Su alcance prioriza la identificación y protección de los activos de información, la gestión integral de riesgos y la definición de políticas, roles y responsabilidades que permitan avanzar hacia un modelo de gestión estructurado, progresivo y maduro.

Para la vigencia 2026, el PESI centra su alcance en los procesos misionales de RTVC, con énfasis en la gestión de contenidos digitales, la operación de plataformas, la infraestructura

tecnológica y los componentes asociados a la seguridad de la información, por ser estos los que concentran los activos más críticos de la entidad.
En esta etapa, la estrategia de seguridad digital se focaliza especialmente en:

- La gestión y operación de plataformas digitales, sitios web y servicios asociados.
- La gestión tecnológica, infraestructura audiovisual e infraestructura TI que soporta el servicio público de comunicación.
- Los procesos de soporte operativo relacionados con la continuidad del servicio y la disponibilidad de las plataformas institucionales.

El PESI abarca los componentes esenciales que soportan la gestión de la seguridad digital, con especial atención en:

- El fortalecimiento de la cultura organizacional en materia de seguridad digital.
- La creación, actualización y formalización de documentos base (políticas, procedimientos, lineamientos y estándares).
- La identificación de vulnerabilidades, riesgos y brechas que puedan afectar la información institucional.
- La planificación de controles, proyectos y acciones prioritarias para el fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI/MSPI).

A medida que RTVC avance en la madurez de su Sistema de Gestión de Seguridad de la Información (SGSI), el alcance del PESI se ampliará de forma progresiva para incorporar nuevas áreas, servicios, procesos y controles, conforme a:

- Los resultados del diagnóstico de madurez institucional.
- Las prioridades derivadas de la gestión del riesgo.
- Los lineamientos actualizados del MSPI y de la Política de Gobierno Digital.
- La disponibilidad de recursos humanos, tecnológicos y presupuestales.

MARCO NORMATIVO

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) se fundamenta en el marco normativo nacional e internacional que regula la protección de los datos, la gestión del riesgo, la seguridad digital y los lineamientos para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en entidades públicas. Este marco orienta la estructura, operación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) de RTVC.

A continuación, se presenta la normatividad aplicable:

Tabla 1 Normatividad aplicable

NORMA	DESCRIPCIÓN
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector TIC, que consolida la normativa sobre tecnologías de la información, Gobierno Digital y seguridad digital.
Decreto 612 de 2018	Establece directrices para la integración de los planes institucionales y estratégicos al Plan de Acción, incluyendo el PESI como instrumento obligatorio de gestión.
CONPES 3995 de 2020	Adopta la Política Nacional de Confianza y Seguridad Digital, que define los lineamientos estratégicos de ciberseguridad para el país.
Resolución 500 de 2021 (MinTIC)	Define los lineamientos para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la gestión de riesgos y la atención de incidentes de seguridad digital.
Decreto 338 de 2022	Establece el Modelo de Gobernanza de la Seguridad Digital para fortalecer la articulación interinstitucional en materia de ciberseguridad.
Decreto 767 de 2022	Reglamenta la Política de Gobierno Digital, orientada al fortalecimiento de la transformación digital del Estado.
Resolución 02277 del 3 de junio de 2025 (MinTIC)	Actualiza los lineamientos del MSPI, incorpora la versión 2022 de la norma ISO/IEC 27001, define criterios de madurez del SGSI y establece su articulación con la Política de Gobierno Digital y el MIPG.
ISO/IEC 27001:2022	Norma internacional para el establecimiento, implementación, mantenimiento y mejora continua de los Sistemas de Gestión de Seguridad de la Información (SGSI).
NIST Cybersecurity Framework 2.0 (2024)	Marco internacional de referencia para la gestión del riesgo de ciberseguridad, aplicable a organizaciones públicas y privadas.
Política Nacional de Seguridad Digital 2023–2030	Establece las estrategias, metas e instrumentos para fortalecer la resiliencia, confianza y soberanía digital del Estado colombiano.

ANALISIS DE CONTEXTO

El análisis de contexto del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) permite comprender la situación actual de RTVC en materia de seguridad digital, identificar los factores internos y externos que influyen en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y orientar la toma de decisiones estratégicas para la vigencia 2026.

Este análisis se basa principalmente en los resultados del diagnóstico oficial del MSPI realizado en la vigencia 2025, el cual evaluó el nivel de madurez de la entidad en cada uno de los componentes definidos por el modelo. Asimismo, integra elementos institucionales derivados del sistema de planeación, la gestión del riesgo, la normatividad aplicable y las condiciones operativas que pueden impactar la seguridad de la información.

Resultados Consolidados del Diagnóstico del MSPI

El diagnóstico institucional evidenció un nivel de madurez global del 50,1%, lo que ubica a RTVC en un nivel intermedio de implementación. Los resultados por componente fueron los siguientes:

Tabla 2 Resultados Generales del Diagnóstico

Componente MSPI	Resultado (%)	Interpretación
Madurez Global	50,1 %	Nivel Intermedio
Personas	70,0 %	Implementación Sólida
Organizacionales	52,4 %	Maduros Parcialmente
Tecnológicos	57,1 %	Nivel Medio
Físicos	38,6 %	Brechas Críticas
Cláusulas del Sistema	34,0 %	Gobernanza Insuficiente

Fuente: Oficina de Control Interno – Informe de Auditoría MSPI 2025.

Estos resultados muestran que RTVC presenta avances importantes en el componente de personas, niveles intermedios en controles organizacionales y tecnológicos, y brechas críticas en las cláusulas del sistema y en la seguridad física.

Resultados por Fases del MSPI

El diagnóstico también evaluó la madurez institucional conforme a las fases de implementación del MSPI.

Tabla 3 Resultados por Fases del MSPI

FASE DEL MSPI	RESULTADO (%)	ESTADO ACTUAL
Diagnóstico	20%	Inventarios y evidencias insuficientes.
Fase 1 – Planificación	40%	Políticas y roles definidos parcialmente.
Fase 2 – Operación	30%	Controles implementados de forma básica.
Fase 3 – Evaluación	26,7%	Auditorías internas limitadas y sin revisión por la Dirección.
Fase 4 – Mejoramiento	20%	Ausencia de acciones correctivas y preventivas formales.

Fuente: Oficina de Control Interno – Informe de Auditoría MSPI 2025.

- **Fortaleza principal:** Controles de personas (70%).
- **Nivel intermedio:** Controles organizacionales y tecnológicos (entre 52% y 57%).
- **Brechas críticas:** Cláusulas del sistema y seguridad física (por debajo de 40%).

Estos resultados muestran la necesidad de fortalecer la gobernanza, los procesos de evaluación y los mecanismos de mejora continua del modelo.

CONTEXTO ESTRATEGICO

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) constituye un instrumento obligatorio de planeación para las entidades públicas, en cumplimiento del Decreto 612 de 2018. Su formulación anual permite articular la gestión de seguridad digital con el Plan de Acción institucional y con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).

El PESI se encuentra alineado con la Plataforma Estratégica 2023–2026 de RTVC, integrándose de manera transversal a la gestión institucional, la transformación digital y la protección del servicio público de comunicación. Asimismo, fortalece la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), asegurando que los procesos, servicios y activos de información sean gestionados bajo principios de confidencialidad, integridad, disponibilidad y privacidad.

En coherencia con la misión y visión institucional, el PESI contribuye a salvaguardar el patrimonio audiovisual del país, garantizar la continuidad operativa y promover la confianza digital en las plataformas y contenidos administrados por RTVC. Adicionalmente, soporta el cumplimiento de los objetivos estratégicos del PEI al mejorar la resiliencia tecnológica, incorporar controles de seguridad en proyectos y servicios digitales, fortalecer las capacidades institucionales y promover una cultura de seguridad digital.

El PESI contribuye directamente al cumplimiento de los objetivos estratégicos institucionales, así:

- **Objetivo 1:** Al proteger los sistemas y plataformas que soportan la producción y difusión de contenidos, el PESI asegura la integridad y la disponibilidad de los servicios de transmisión y los contenidos digitales relevantes, convergentes e incluyentes.

- **Objetivo 2:** Asegura la continuidad del servicio de la red pública mediante estrategias de gestión de incidentes, respaldo y recuperación, fortaleciendo la resiliencia tecnológica de la entidad, generando de esta manera valor público a los consumidores de nuestros servicios, que es la ciudadanía en general.

- **Objetivo 3:** Apoya la cultura de innovación y la gestión del conocimiento mediante el resguardo de la información crítica, los activos digitales y los sistemas de análisis de audiencias.

- **Objetivo 4:** Se articula con la transformación digital institucional al implementar controles de seguridad en los procesos automatizados, velando por el cumplimiento normativo en protección de datos y seguridad digital.

- **Objetivo 5:** A través del desarrollo y actualización de políticas, procedimientos y controles, el PESI impulsa buenas prácticas de seguridad digital, fortalece las capacidades del talento humano y promueve una cultura institucional orientada a la gestión del riesgo y la protección de la información.

RIESGOS Y CONTROLES

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) se encuentra expuesto a diversos riesgos de proceso que pueden afectar el cumplimiento de sus objetivos, especialmente aquellos relacionados con la gestión de activos de información, la implementación gradual del MSPI, la continuidad del servicio y la adopción de controles técnicos y administrativos de seguridad digital.

Los riesgos descritos a continuación impactan directamente la ejecución del PESI y, en general, pueden generar retrasos en el fortalecimiento del MSPI, la disminución del nivel de madurez institucional y la limitación en la capacidad de mejora continua. Para cada riesgo se identifican sus causas y los controles orientados a su mitigación.

Tabla 4 Riesgos Asociados al PESI y Controles Definidos

Riesgo	Control	Consecuencia
R1. Identificación y valoración insuficiente de los riesgos de seguridad digital en los procesos institucionales, lo que puede impedir la implementación de controles adecuados y aumentar la exposición a incidentes que comprometan la información y los servicios	• Aplicación de la metodología de gestión del riesgo de seguridad digital. • Actualización periódica de inventarios de activos y riesgos asociados. • Definición, seguimiento y actualización del Plan de Tratamiento de Riesgos.	• Implementación inadecuada de controles. • Incremento de la probabilidad y el impacto de incidentes. • Retraso en el fortalecimiento del MSPI y estancamiento del nivel de madurez institucional.
R2. Dificultades para implementar controles de seguridad digital debido a limitaciones de recursos, capacidades técnicas o nivel de madurez institucional, lo cual puede aumentar la vulnerabilidad de la entidad frente a incidentes que comprometan la información y los servicios	• Priorización de controles de acuerdo con criticidad, madurez y recursos disponibles. • Planeación gradual en el marco del PESI y del Plan de Acción. • Fortalecimiento de la gobernanza del MSPI y de los roles de seguridad digital. Fortalecimiento de la gobernanza de seguridad digital.	• Controles aplicados parcialmente o de manera tardía. • Persistencia de brechas de seguridad en procesos críticos. • Incumplimiento de metas estratégicas del PESI
R3. Exposición a vulnerabilidades y amenazas de seguridad digital afecten la disponibilidad, integridad o confidencialidad de la información institucional.	• Implementación progresiva de medidas de seguridad física, administrativa y tecnológica. • Prácticas institucionales de monitoreo, revisión y mantenimiento preventivo. • Aplicación del ciclo PHVA para el mejoramiento continuo del MSPI.	• Aumento de probabilidad de incidentes de ciberseguridad. • Interrupciones operativas o fuga de información. * Impacto reputacional y operativo para RTVC.
R4. Incidentes de seguridad digital que afecten la operación institucional, la protección de datos personales o la disponibilidad, integridad y confidencialidad de los servicios y la información	• Adopción del procedimiento institucional de gestión de incidentes de seguridad. • Definición de roles y mecanismos de coordinación y comunicación. • Definición de roles y mecanismos de coordinación y comunicación.	• Interrupción de servicios y plataformas críticas. • Riesgos legales por afectación a datos personales. • Pérdida de confianza institucional.
R5. Riesgos derivados de terceros y proveedores que no cumplen los requisitos mínimos	• Inclusión de requisitos de seguridad digital en procesos de contratación.	• Brechas de seguridad introducidas por servicios tercerizados

Riesgo	Control	Consecuencia
de seguridad digital establecidos por la entidad, lo que puede comprometer la protección de la información y la continuidad de los servicios	• Evaluación periódica del cumplimiento por parte de proveedores. • Supervisión continua de obligaciones contractuales relacionadas con seguridad digital.	• Afectación de continuidad y cumplimiento normativo por fallas de proveedores.
R6 Insuficiencia de controles físicos para la protección de la infraestructura tecnológica crítica, lo que puede aumentar la exposición a accesos no autorizados, daños, fallas operativas o interrupciones en los servicios institucionales	• Fortalecimiento del control de acceso físico y supervisión de áreas críticas. • Actualización y formalización de lineamientos de seguridad física. • Revisión de prácticas de protección de infraestructura crítica.	• Accesos no autorizados. • Riesgos de daño, pérdida o interrupción de servicios. • Vulnerabilidad de la infraestructura tecnológica.
R7. Limitada cultura de seguridad digital en servidores públicos y contratistas, lo que puede aumentar la probabilidad de incidentes que comprometan la información institucional y la continuidad de los servicios.	• Ejecución del programa institucional de sensibilización y formación en seguridad digital. • Campañas de apropiación y divulgación de buenas prácticas. • Inclusión de lineamientos de seguridad en inducciones	• Incremento de errores humanos e incidentes. • Baja adopción de controles. • Dificultad para elevar la madurez del MSPI y consolidar una cultura de seguridad digital.
R8. Falta de mecanismos de seguimiento, indicadores y procesos de evaluación del MSPI, impidiendo la identificación oportuna de desviaciones, limitando así la mejora continua y afectando la eficacia de la gestión de seguridad y privacidad de la información.	• Definición e implementación de indicadores estratégicos del PESI/MSPI. • Ejecución de auditorías internas y externas de seguridad digital. • Revisión por la Dirección y definición de planes de mejora.	• Limitaciones para identificar desviaciones. • Ausencia de mejora continua. • Dificultad para demostrar avances en auditorías y compromisos institucionales.

Fuente: Elaboración propia – PESI RTVC 2026

PROCESO DE FORMULACIÓN

1. Situación Actual

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) se formula en un momento en el que RTVC avanza en la estructuración y fortalecimiento de su Sistema de Gestión de Seguridad de la Información (SGSI) y en la implementación progresiva del Modelo de Seguridad y Privacidad de la Información (MSPI).

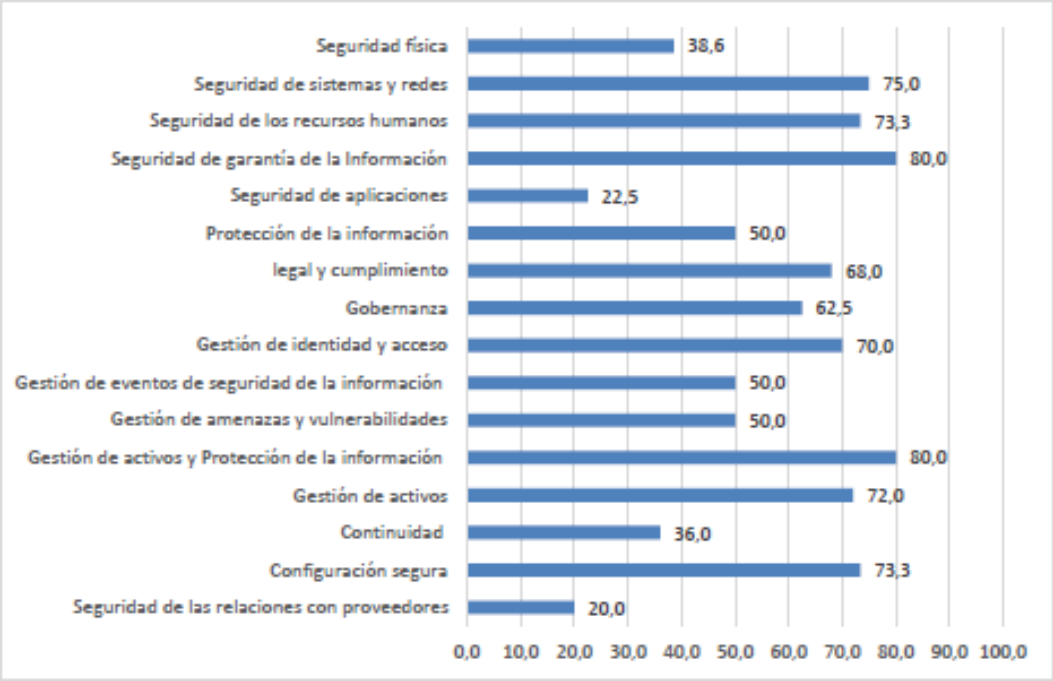
Si bien la entidad cuenta con lineamientos base como la Política General de Seguridad de la Información, actividades de sensibilización y ciertos procedimientos operativos, aún requiere robustecer aspectos esenciales como la gestión integral del riesgo, la formalización de la gobernanza del modelo, la estandarización de controles y el fortalecimiento de los mecanismos de evaluación y mejora continua.

Como insumo clave para este PESI, **la Oficina de Control Interno de RTVC**, en cumplimiento del Programa Anual de Auditoría Basado en Riesgos 2025, realizó la auditoría al Modelo de Seguridad y Privacidad de la Información (MSPI). Este ejercicio permitió identificar el nivel de madurez institucional del modelo y las brechas asociadas a su implementación dentro de la entidad.

Los resultados evidenciaron un nivel **intermedio de madurez**, con avances importantes en capacidades relacionadas con seguridad de redes, seguridad de recursos humanos y gestión de accesos, pero con brechas significativas en componentes como seguridad física, continuidad del negocio, gestión del riesgo y gobernanza del modelo.

A continuación, se presenta el resultado general del diagnóstico consolidado por capacidades operativas del MSPI:

Tabla 5 Resultados detallados por capacidades operativas del MSPI



Fuente: Oficina de Control Interno – Informe de Auditoría MSPI 2025.

Estos resultados reflejan la necesidad de fortalecer de manera prioritaria las capacidades de gobernanza, seguridad física, valoración del riesgo, continuidad del negocio y protección de activos críticos. Dichas brechas orientan las acciones estratégicas del PESI 2026 para avanzar hacia un modelo más robusto, coherente y alineado con los lineamientos del Ministerio TIC.

En este escenario, el PESI se encuentra en una fase de fortalecimiento estructural, cuyo propósito es organizar, formalizar y priorizar las iniciativas necesarias para que RTVC incremente de forma gradual y sostenible su nivel de madurez en seguridad digital durante la vigencia 2026.

2. Situación Deseada

RTVC proyecta consolidar para la vigencia 2026 un Modelo de Seguridad y Privacidad de la Información (MSPI) fortalecido, articulado con la planeación institucional y con un mayor nivel de madurez en sus capacidades operativas. La situación deseada contempla que la entidad cuente con una estructura de seguridad digital más robusta, documentada, estandarizada y orientada a la gestión preventiva del riesgo y a la protección de los activos de información.

En este escenario, RTVC busca avanzar hacia un modelo de seguridad digital que asegure la continuidad del servicio público de comunicación, el cumplimiento normativo, la mejora continua y la consolidación de una cultura organizacional comprometida con la protección de la información.

A continuación, se presentan las estrategias institucionales y sus objetivos estratégicos proyectados:

Tabla 6 Estrategias Institucionales y Objetivos Estratégicos del MSPI

Estrategia Institucional	Objetivo Estratégico
1. Fortalecimiento de la Gobernanza del MSPI	Consolidar la estructura de gobierno del Modelo de Seguridad y Privacidad de la Información mediante la actualización de políticas, roles, funciones, responsabilidades y mecanismos de decisión, asegurando su articulación con la planeación institucional.
2. Gestión Integral del Riesgo de Seguridad Digital	Socializar la metodología institucional para la identificación, valoración y tratamiento de riesgos en todos los procesos, permitiendo priorizar controles y proteger los activos críticos de información.
3. Protección y Gestión de Activos de Información	Garantizar la actualización, clasificación y protección de los activos de información, asegurando su trazabilidad y la aplicación de controles acordes a su criticidad y sensibilidad.
4. Fortalecimiento de Controles Administrativos, Físicos y Tecnológicos	Implementar y mejorar los controles definidos en el MSPI y en la ISO/IEC 27002, priorizando la seguridad física, la protección de infraestructura, la gestión de vulnerabilidades, el monitoreo y la continuidad del servicio.
5. Integración de la Seguridad Digital en Procesos, Proyectos y Adquisiciones	Incorporar criterios de seguridad digital en adquisiciones, contratación, desarrollo de software, arquitectura tecnológica y proyectos de transformación digital, garantizando que los proveedores cumplan requisitos mínimos de seguridad.
6. Cultura Organizacional y Sensibilización en Seguridad Digital	Fortalecer la apropiación institucional mediante programas de formación, sensibilización, simulaciones y campañas que promuevan el uso seguro de la información y la corresponsabilidad del personal.
7. Evaluación, Monitoreo y Mejora Continua del MSPI	Establecer mecanismos de revisión por la Dirección, medición de indicadores y acciones de mejora que aseguren la evolución del nivel de madurez del MSPI.

Fuente: Elaboración propia – PESI 2026, con base en diagnóstico MSPI 2025 y lineamientos MinTIC (Resolución 02277 de 2025).

Portafolio de Proyectos y Productos Esperados

El siguiente portafolio consolida los proyectos y actividades estratégicas que RTVC desarrollará durante la vigencia 2026 para fortalecer la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y avanzar en el nivel de madurez del Sistema de Gestión de Seguridad de la Información (SGSI).

Cada proyecto se organiza según las Estrategias Institucionales de Seguridad Digital y presenta los productos esperados, asegurando coherencia con las recomendaciones del diagnóstico MSPI 2025 y los lineamientos de MinTIC – Resolución 02277 de 2025.

Tabla 7 . Portafolio de Proyectos y Productos Esperados – Vigencia 2026

Estrategia Institucional	Proyectos / Actividades Clave	Productos Esperados
1. Gobernanza del MSPI	• Actualización de políticas, roles y alcance del MSPI. • Actualización del SoA. • Revisión y actualización del marco documental del SGSI.	• Políticas y roles actualizados. • SoA versión 2026. • Documentación formalizada.
2. Gestión del Riesgo de Seguridad Digital	• Identificación, valoración y actualización de riesgos por proceso. • Actualización del Plan de Tratamiento de Riesgos (PTR).	• Matrices de riesgo actualizadas. • PTR institucional consolidado.
3. Gestión de Activos de Información	• Actualización del inventario de activos. • Clasificación de la información.	• Inventario consolidado. • Matriz de clasificación y etiquetado.
4. Controles Administrativos, Físicos y Tecnológicos	• Fortalecimiento de seguridad física. • Gestión de vulnerabilidades y remediación. • Implementación/mejora de controles tecnológicos priorizados.	• Informes de vulnerabilidades. • Controles fortalecidos. • Evidencias de seguridad física.
5. Seguridad en Proyectos, Contratación y Adquisiciones	• Inclusión de requisitos de seguridad en proyectos TI y servicios en la nube. • Revisión de seguridad en desarrollos y adquisiciones.	• Proyectos con requisitos de seguridad aplicados. • Informes de revisión y cumplimiento.
6. Cultura de Seguridad Digital	• Ejecución del Plan de Sensibilización. • Campañas y simulaciones de phishing/ingeniería social.	• Funcionarios sensibilizados. • Reportes de campañas y simulacros.
7. Monitoreo, Evaluación y Mejora del MSPI	• Auditoría interna. • Revisión por la Dirección. • Implementación de indicadores del SGSI/MSPI.	• Informe de auditoría. • Acta de revisión.

Fuente: Elaboración propia – Plan Estratégico de Seguridad y Privacidad de la Información PESI 2026, con base en los resultados del Diagnóstico MSPI 2025 y lineamientos MinTIC (Resolución 02277 de 2025).

CRONOGRAMA

El presente cronograma organiza las actividades estratégicas del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) para la vigencia 2026 a través de tres momentos de ejecución: Inicial, Intermedio y Final.

Este enfoque permite estructurar la implementación sin definir fechas exactas dentro del plan estratégico, dado que la programación detallada será especificada en el Plan de Trabajo Técnico para la Implementación y Mejora del MSPI, el cual se anexa como documento complementario conforme a las recomendaciones de la auditoría interna 2025.

Momentos de ejecución

Las actividades se agrupan en tres momentos que orientan su realización dentro de la vigencia:

- **Inicial:** Actividades de preparación, ajuste documental y definición de lineamientos del MSPI.
- **Intermedio:** Actividades operativas de implementación de controles, gestión de riesgos y ejecución de programas de seguridad digital.
- **Final:** Actividades de evaluación, verificación, revisión por la dirección y mejora continua.

Tabla 8 Cronograma Estratégico del PESI 2026

No.	Componente / Línea Estratégica	Actividad Estratégica	Inicial	Intermedio	Final
1	Gobernanza del MSPI	Revisión y actualización de políticas, roles, responsabilidades y alcance del MSPI	X		
2	Gobernanza del MSPI	Actualización del marco documental (políticas, lineamientos y procedimientos)	X	X	
3	Gestión de Activos de Información	Actualización del inventario y clasificación de activos	X	X	
4	Gestión del Riesgo	Aplicación de la metodología de riesgos en procesos institucionales		X	
5	Gestión del Riesgo	Actualización del Plan de Tratamiento de Riesgos		X	

No.	Componente / Línea Estratégica	Actividad Estratégica	Inicial	Intermedio	Final
6	Cultura de Seguridad Digital	Definición del Plan de Sensibilización y Cultura	X		
7	Cultura de Seguridad Digital	Ejecución de actividades de sensibilización y simulaciones		X	
8	Controles Tecnológicos	Implementación y fortalecimiento de controles tecnológicos.		X	
9	Seguridad Física	Fortalecimiento de controles físicos en áreas críticas		X	
10	Gestión de Vulnerabilidades	Análisis de vulnerabilidades y verificación de remediaciones		X	X
11	Gestión de Incidentes	Actualización del procedimiento de gestión de incidentes	X		
12	Gestión de Incidentes	Ejecución de simulacros de respuesta a incidentes		X	X
13	Evaluación del MSPI	Ejecución de auditoría interna del MSPI			X
14	Revisión por la Dirección	Consolidación de resultados del MSPI			X
15	Mejora Continua	Implementación de acciones de mejora del MSPI			X

Nota:

Las actividades aquí descritas representan una planificación estratégica orientada al cumplimiento del PESI 2026.

La definición de fechas, responsables, recursos, hitos y entregables detallados se realizará en el Plan de Trabajo Técnico del MSPI, el cual se anexa a este documento y será la guía oficial para la ejecución operativa durante la vigencia.

El cronograma podrá ser ajustado conforme a:

- Disponibilidad presupuestal,
- Lineamientos institucionales,
- Actualizaciones normativas,
- Priorizaciones estratégicas definidas por la Gerencia y la Coordinación de TI.

SEGUIMIENTO Y CONTROL

El seguimiento y control del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) se realizará mediante la medición periódica del avance de las actividades estratégicas definidas para la vigencia 2026.
Este proceso permitirá verificar el cumplimiento de los objetivos, identificar oportunidades de mejora y garantizar la actualización continua del Modelo de Seguridad y Privacidad de la Información (MSPI), conforme a los lineamientos del MinTIC y las prácticas de gestión institucional.

Tabla 9 Ficha del Indicador del PESI

Nombre del indicador	Fórmula de medición	Frecuencia	Meta anual	Tipología
Nivel de avance del PESI	(Número de actividades ejecutadas ÷ Total de actividades definidas) × 100	Semestral y Anual	**≥ 70 % anual** (umbral mínimo satisfactorio alineado al MSPI)	Eficacia / Resultado

Tabla 10 Escala de medición del indicador

Estado de avance	Rango (%)	Descripción
Satisfactorio / Alto	70–100 %	Cumplimiento adecuado del PESI, el avance permite fortalecer el MSPI según lo planificado.
Medio	40–69 %	Cumplimiento parcial. Se requiere seguimiento para evitar retrasos en el fortalecimiento del MSPI.
Bajo / Crítico	0–39 %	Cumplimiento insuficiente que compromete la mejora continua del MSPI y los objetivos del PESI.

Mecanismos de seguimiento

El seguimiento se efectuará mediante los siguientes mecanismos institucionales:

1. Revisión periódica de avances del PESI por parte de la Coordinación de Tecnologías de la Información.
2. Presentación de informes semestrales y anuales al Comité Institucional de Gestión y Desempeño (CIGD).
3. Evaluación de indicadores y verificación de cumplimiento de actividades estratégicas.
4. Auditorías internas y externas relacionadas con el MSPI, conforme al Programa Anual de Auditoría Basado en Riesgos.

5. Actualización de acciones y ajustes al PESI conforme al desempeño observado y a los lineamientos del MinTIC.

ROLES Y RESPONSABILIDAD

Los roles y responsabilidades definidos para la ejecución del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) se encuentran alineados con la Política Operacional de Administración de Riesgos (Código I-A-3, Versión 8, 19-12-2022), la cual establece el esquema institucional de Líneas de Defensa para la gestión del riesgo. En coherencia con este marco, el PESI articula las funciones de cada actor involucrado en la operación, seguimiento y evaluación del MSPI, asegurando una distribución clara de responsabilidades y una adecuada gobernanza del modelo.

Tabla 11 Roles y Responsabilidades del PESI

Roles	Responsabilidades
Primera Línea de Defensa – Procesos y Dependencias de RTVC	• Ejecutar las actividades del PESI relacionadas con sus procesos. • Identificar y reportar riesgos, incidentes y brechas de seguridad digital. • Implementar los controles definidos en el MSPI aplicables a su operación. • Mantener actualizada la información requerida para activos, riesgos y evidencias del modelo. • Garantizar el cumplimiento de políticas y lineamientos institucionales de seguridad digital.
Segunda Línea de Defensa – Coordinación de Tecnología	• Liderar la implementación operativa del PESI y del MSPI. • Brindar acompañamiento técnico a las áreas para la gestión de riesgos, activos y controles. • Administrar y actualizar el marco documental de seguridad digital (políticas, lineamientos, procedimientos). • Monitorear vulnerabilidades, incidentes y cumplimiento de controles. • Realizar seguimiento a proveedores y asegurar el cumplimiento de requisitos de seguridad digital. • Consolidar indicadores, avances y reportes de seguimiento del PESI.
Tercera Línea de Defensa – Oficina de Control Interno	• Evaluar la eficacia del PESI y del MSPI mediante auditorías internas. • Verificar el cumplimiento de políticas, controles y responsabilidades asignadas. • Formular recomendaciones de mejora para la gestión del riesgo y la seguridad digital. • Hacer seguimiento a planes de mejoramiento derivados de auditorías.
Alta Dirección (Gerencia, Subgerencias, Comité Institucional	• Aprobar el PESI y sus actualizaciones. • Proveer los recursos necesarios para la gestión de seguridad digital. • Orientar la toma de decisiones estratégicas en materia de seguridad de la información. • Participar en la Revisión por la Dirección del MSPI.

Roles	Responsabilidades
de Gestión y Desempeño – CIGD)	• Garantizar el cumplimiento de los lineamientos de la Política de Gobierno Digital y del MSPI.
Administradores de Plataformas TI	• Implementar controles técnicos, parches, configuraciones seguras y remediación de vulnerabilidades. • Gestionar credenciales privilegiadas bajo los lineamientos institucionales. • Apoyar la ejecución del procedimiento de incidentes de seguridad digital. • Registrar evidencias operativas que soporten el cumplimiento del MSPI.
Servidores Públicos y Contratistas de RTVC	• Cumplir las políticas y lineamientos de seguridad digital. • Participar en las actividades de sensibilización y formación. • Manejar adecuadamente la información institucional y reportar incidentes o anomalías. • Utilizar de manera segura los sistemas y activos tecnológicos asignados.

COMUNICACIÓN Y DIVULGACIÓN

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) será comunicado a los diferentes grupos de valor mediante los canales institucionales definidos por RTVC, garantizando su adecuada socialización, comprensión y adopción.

Las acciones de comunicación se desarrollarán de la siguiente manera: Canales y acciones de

divulgación

- Presentación del PESI al Comité Institucional de Gestión y Desempeño (CIGD) para su revisión, retroalimentación y aprobación formal.
- Publicación del documento en la página web institucional, conforme al Decreto 612 de 2018 y las directrices de Gobierno Digital.
- Incorporación del PESI en los procesos de inducción, para fortalecer la apropiación en servidores públicos y contratistas.

Estas acciones aseguran que los actores institucionales conozcan el alcance, responsabilidades y líneas estratégicas definidas en el plan.

GESTION DEL CONOCIMIENTO

La gestión del conocimiento en el marco del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) de RTVC se orienta a garantizar que la información, las buenas prácticas, las experiencias operativas y los aprendizajes generados durante la

implementación, seguimiento y mejora del MSPI sean registrados, organizados, transferidos y reutilizados de manera sistemática.

Este enfoque se alinea con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y con los principios del Modelo Integrado de Planeación y Gestión (MIPG), promoviendo la continuidad operativa, la gestión del riesgo y la mejora continua en materia de seguridad digital.

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.

ANEXOS

Los siguientes documentos constituyen el soporte técnico y metodológico del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) 2026 y permiten evidenciar los insumos utilizados para su formulación:

1. Diagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) – Vigencia 2025.
2. Plan de Trabajo Técnico del MSPI.

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	Actualización integral del PESI para la vigencia 2026. Se incorporan: diagnóstico MSPI 2025, actualización de objetivos, análisis de contexto, estrategias institucionales, portafolio de proyectos, cronograma estratégico y mecanismo de seguimiento y control.	Coordinación de Gestión de Tecnologías de la Información	27/01/2026

	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