Fecha del informe	**15-12-2025**
Tipo de informe	**Preliminar ( ) Final (X)**
Auditoría Interna	**Programada (X) Especial ( )**

1. NOMBRE DE LA AUDITORÍA

Auditoría al Modelo de Seguridad y Privacidad de la Información (MSPI) al Sistema de Medios Públicos RTVC.

2. OBJETIVO

Evaluar el grado de cumplimiento de los requisitos establecidos en la Resolución 2277 de 2025 de MINTIC y su anexo técnico, verificando la existencia, pertinencia y efectividad de los componentes, políticas, procedimientos y controles definidos por RTVC.

Analizar el avance en la adopción de las cinco fases del MSPI (Diagnóstico, Planificación, Operación, Evaluación del Desempeño y Mejoramiento Continuo) y su integración con los procesos institucionales y de tecnología de la información.

Confirmar la coherencia entre la implementación del modelo y los lineamientos de la Política de Gobierno Digital, el Decreto 620 de 2020, la Ley 1581 de 2012 (protección de datos personales) y demás disposiciones aplicables en materia de seguridad y privacidad de la información.

Determinar la capacidad del Modelo de Gestión de Seguridad y Privacidad en RTVC, para cumplir los requisitos legales, reglamentarios, normativos, contractuales y establecidos por la entidad.

Determinar la eficacia del Modelo de Gestión de Seguridad y Privacidad en RTVC frente al cumplimiento de los objetivos establecidos.

Identificar áreas de mejora potencial del Modelo de Gestión de Seguridad y Privacidad en RTVC.

3. ALCANCE DE LA AUDITORÍA

Proceso de Gestión de Tecnología de la Información y procesos relacionados al Modelo de Gestión de Seguridad y Privacidad en RTVC.

4. CRÍTERIOS DE AUDITORÍA

- Constitución Política de Colombia, artículos 15, 209 y 269.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.

- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las entidades del Estado.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por el que se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 1083 de 2015 establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- • Decreto 620 de 2020. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- • 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 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 338 de 2022 Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- 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 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Decreto 767 de 2022. "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"
- Decreto 1083 de 2015 y sus modificaciones y actualizaciones.

- Decreto 767 de 2022. “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- Decreto 1263 de 2022. “Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con e fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública”.
- CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad digital.
- CONPES 4144 de 2025. Política Nacional de Inteligencia Artificial
- CONPES 3975 del 2019 política nacional para la transformación digital e inteligencia artificial
- Norma ISO/IEC 27001:2022, Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.

Otras normas internacionales para tener en cuenta:

GDPR (Reglamento General de Protección de Datos): Se recomienda adoptar prácticas inspiradas en este reglamento, especialmente en lo relacionado con derechos del titular, principios de minimización, portabilidad, notificación de brechas de seguridad y consentimiento explícito, como complemento a la Ley 1581 de 2012.

NIST SP 800-53: Puede ser utilizado como guía técnica para complementar los controles de seguridad del MSPI, especialmente en sistemas críticos o servicios de procesamiento masivo de datos. Su adopción es flexible, gradual y adaptada al contexto local.

Guía de Implementación del MSPI (MinTIC) – Documentos de apoyo y lineamientos metodológicos oficiales.

Mapa de procesos.

Documentación de los procesos

5. LÍDER(ES) DEL PROCESO / ÁREA / PROYECTO/ AUDITADO

Coordinador de Gestión de TI - Nohora Mora

6. DESCRIPCIÓN GENERAL DEL PROCESO / ÁREA / PROYECTO /

Proceso de Gestión de Tecnología de la Información

7. EQUIPO AUDITOR

El equipo auditor que desarrolló la presente auditoría está conformado por:

Líder Auditor: Germán Andrés Sánchez Ortegón
Grupo Auditor: Miguel Ángel Suárez Benítez (Auditor)
Luis Carlos Sanmartin Santamaría (Auditor)

8. DESARROLLO DE LA AUDITORÍA

Para el desarrollo del ejercicio auditoría se consideraron los lineamientos establecidos en MANUAL DE AUDITORÍA INTERNA BASADA EN RIESGOS de la Oficina de Control Interno.

La auditoría se desarrolló mediante entrevistas in situ, muestreo documental, observación directa del trabajo, listas de verificación basadas en los requisitos del MSPI, trazabilidad normativa de hallazgos, análisis de evidencias objetivas y auditoría cruzada entre procesos, siguiendo las metodologías del Manual de Auditoría Interna Basada en Riesgos de RTVC y la Guía del DAFP. Estas técnicas permitieron validar la implementación de controles, identificar brechas funcionales y emitir recomendaciones alineadas con los estándares de seguridad de la información.

El informe preliminar fue remitido con radicado No. 202501200023603 del 25 de noviembre de 2025, a la Coordinación de Tecnologías de la Información T.I. para que, de acuerdo con el Procedimiento de Auditoría Interna, los auditados pudieran hacer sus observaciones debidamente soportadas, dentro de los cinco (5) días hábiles siguientes, iniciando desde el primer día hábil posterior a la presente comunicación. El día 28 de noviembre de 2025, la Coordinación de T.I., a través de correo electrónico, solicitó la ampliación de cinco (5) días adicionales al plazo inicialmente establecido para la entrega de la respuesta, esto es hasta el día 10 de diciembre de 2025, con el fin de contar con el tiempo necesario para realizar el análisis completo y emitir las observaciones correspondientes, incluyendo las otras áreas que participaron en la auditoria; fue así como cumplido el plazo anteriormente indicado se recibieron las siguientes observaciones:

“Observaciones desde la Coordinación de Tecnologías de la Información

NC1 y NC2 – Contexto organizacional y partes interesadas: Actualmente se encuentra en proceso de actualización el PESI 2026, el cual se incorporará el análisis de contexto y la identificación de partes interesadas del MSPI. Estos ajustes se encuentran en fase de validación.

NC3 – Rol de Seguridad de la Información: Actualmente la entidad no cuenta con un “Oficial de Seguridad de la Información” designado formalmente. Sin embargo, las actividades de seguridad digital y el soporte al MSPI están siendo apoyadas operativamente por la Especialista de Seguridad Digital adscrita a la Coordinación de Tecnologías de la Información.

NC4 – Declaración de Aplicabilidad (SoA): La Declaración de Aplicabilidad (SoA), alineada a los controles del Anexo A de ISO/IEC 27001:2022 y al Modelo de Seguridad y Privacidad de la Información – MSPI, se encuentra actualmente en proceso de construcción y validación técnica. Este documento será incorporado dentro del marco documental de seguridad de la información para la vigencia 2026.

NC5, NC6 y OM4 – Planificación y Gestión de Riesgos: Se encuentra en formulación el procedimiento institucional de Gestión de Riesgos de Seguridad Digital, así como la matriz de riesgos, construida con base en el inventario de activos actualmente en levantamiento.

NC7 y NC8 – Auditoría Interna y Revisión por la Dirección: La presente auditoría constituye el primer ejercicio formal específico al MSPI, a partir del cual se estructurará el ciclo de mejora continua y las futuras revisiones por la alta dirección.

NC9 – Clasificación de Activos de Información: El inventario de activos de información se encuentra en levantamiento, proceso que permitirá aplicar formalmente el esquema de clasificación conforme a confidencialidad, integridad y disponibilidad.

NC10 y NC11 – Gestión de Incidentes: Se cuenta con un procedimiento institucional de gestión de incidentes en proceso de actualización y alineación con ISO 27035, junto con el fortalecimiento del modelo de reporte, clasificación y cierre.

NC12 – Continuidad del Negocio: Si bien actualmente no existe un BCP ni un DRP formalmente aprobados como instrumentos del MSPI, la entidad sí dispone de capacidades técnicas de continuidad parcial, entre ellas una estrategia de respaldo y recuperación en AWS mediante AWS Backup, que protege bases de datos RDS e instancias EC2 con políticas de respaldo diario, semanal y mensual (RPO de 24 horas y RTO estimado de 2 horas), así como una cuenta separada destinada a DRP inicialmente configurada con AWS Elastic Disaster Recovery.

NC14 y NC15 – Propiedad Intelectual y Activos Intangibles: Se reconoce la brecha en la gestión de estos activos, la cual será incorporada dentro del inventario institucional y la matriz de riesgos del MSPI.

NC17 – Gestión de Capacidad: Aunque existe infraestructura redundante, no se cuenta aún con un modelo formal documentado de gestión de capacidad.

NC18 – Prevención de Fuga de Información (DLP): Existen controles parciales; no obstante, no se dispone de una solución formal de DLP, lo cual se proyecta como iniciativa de fortalecimiento.

NC19 – Desarrollo Seguro y Gestión de Cambios: El procedimiento de Gestión de Cambios se encuentra en proceso de actualización, y el componente de Desarrollo Seguro será fortalecido para la vigencia 2026.

Observaciones de la Oficina Asesora Jurídica

En cuanto a las observaciones asociadas a funciones de la Oficina Asesora Jurídica y de la Coordinación de Procesos de Selección, se adjunta el correo remitido por la Jefe de la Oficina Asesora Jurídica, en el cual se aclaran aspectos relevantes respecto a la asignación de responsabilidades dentro del informe preliminar.

Las observaciones jurídicas están relacionadas principalmente con las siguientes no conformidades del informe:

NC13 – Matriz normativa / requisitos legales: Jurídica aclara que la construcción de una matriz normativa consolidada no recae exclusivamente en su dependencia, dado que la responsabilidad es compartida entre varias áreas (Tecnología, Planeación, Jurídica y Soporte Corporativo).

Hallazgos relacionados con ausencia de cláusulas contractuales de seguridad, privacidad y continuidad: La Oficina Jurídica aclara que no tiene competencia técnica para definir requisitos de seguridad digital, cifrado, continuidad o incidentes, sino únicamente para incorporarlos jurídicamente cuando las áreas técnicas los determinan.

Hallazgos sobre gestión de riesgos en proveedores: Jurídica precisa que la identificación y tratamiento de riesgos tecnológicos en proveedores corresponde a las áreas técnicas, no a su dependencia.

Hallazgos sobre integración del MSPI en procesos de contratación: Jurídica y Procesos de Selección ejecutan los procedimientos, pero no definen estándares técnicos ni criterios de criticidad. Por ello, no es procedente atribuirles responsabilidad por la ausencia de estos requisitos.

Finalmente, se deja constancia de que el informe preliminar de la Auditoría al Modelo de Seguridad y Privacidad de la Información (MSPI) al Sistema de Medios Públicos RTVC fue socializado con las diferentes áreas que participaron en el ejercicio. No obstante, la única respuesta formal recibida dentro del plazo establecido fue la emitida por la Oficina Asesora Jurídica, la cual se incorpora a esta respuesta."

Tras la revisión de las observaciones enviadas por la Coordinación de T.I., el equipo auditor concluyó que no constituyen soporte suficiente para modificar o eliminar las no conformidades detalladas en el correo mencionado. Por consiguiente, dichas no conformidades se mantienen en el informe final.

9. PERÍODO DE EJECUCIÓN DE LA AUDITORÍA

La presente auditoría se realizó desde el 23/10/2025 hasta el 03/12/2025, iniciando con la reunión de apertura y terminando con la reunión de cierre y entrega del informe final de auditoría.

10. RIESGOS

No aplica.

11. VERIFICACIÓN EFICACIA DE PLANES DE MEJORAMIENTO

No aplica.

12. HALLAZGOS

Los hallazgos son observaciones o hechos significativos que el equipo auditor identificó durante el ejercicio y que considera importante comunicar a la entidad, con el fin de fortalecer el proceso de mejora continua.

Igualmente, se debe realizar el análisis de las causas de las no conformidades, para generar las acciones correctivas y/o preventivas necesarias, para elaborar los correspondientes planes de mejoramiento.

12.1. FORTALEZAS

F1. Se tiene Plan de Seguridad y Privacidad de la Información 2025, publicado en enero 2025 lo cual garantiza el cumplimiento de lineamientos normativos y de Gobierno Digital.

F2. La política operacional de seguridad digital establece explícitamente que la Alta Dirección

es responsable de facilitar los recursos humanos, técnicos y financieros necesarios para la implementación, mantenimiento y promoción del cumplimiento de la política, alineado con el numeral 7.2.1 Liderazgo y compromiso del modelo.

F3. La política operacional de seguridad digital contempla directrices específicas para el uso aceptable de correo electrónico, acceso a Internet, redes sociales corporativas y dispositivos móviles. Incluye medidas como bloqueo de contenidos no permitidos, autenticación multifactor (2FA), restricciones de uso en redes públicas y protección ante pérdida o hurto de dispositivos, lo que contribuye a la protección de la información y los activos relacionados.

F4. Todos los servicios digitales expuestos al ciudadano incorporan mecanismos criptográficos para proteger la información, como certificados digitales, firmas electrónicas, protocolos seguros y funciones hash. Esta práctica está alineada con los controles A.5.14 (transferencia de información) y A.8.24 (uso de criptografía).

F5. La política operacional de seguridad digital remite a la Política de Protección de Datos Personales de RTVC, exige cláusulas de confidencialidad en los contratos y prohíbe la exposición de información personal o reservada en enlaces públicos sin mecanismos de autenticación. Esto refuerza el cumplimiento de los principios de privacidad y confidencialidad.

12.2. OPORTUNIDADES DE MEJORA

OM1. Se evidencia la necesidad de incluir explícitamente al MSPI dentro del modelo de gestión integrada, incorporar la seguridad y privacidad al análisis de contexto, y mejorar la especificidad del análisis de partes interesadas, incluyendo nuevos actores y separando adecuadamente los roles. Actualmente, estos elementos están dispersos o en construcción, lo que limita la articulación del MSPI con la estrategia institucional. Esta integración facilitará la coherencia entre sistemas de gestión y fortalecerá la gobernanza.

OM2. Se evidencia la necesidad de integrar la planificación operativa del MSPI con el sistema institucional de seguimiento y control, a través de la formalización de un plan operacional alineado a los objetivos y requisitos del MSPI, incorporar la matriz de controles de gestión al Plan Institucional y consolidar el uso de SuiteVision como herramienta oficial de monitoreo. Esta integración permitirá fortalecer la trazabilidad de las actividades operativas, automatizar la gestión del sistema, generar alertas de incumplimiento y estandarizar la forma en que se realiza el seguimiento. Además, permitirá incorporar indicadores específicos del MSPI que midan aspectos críticos como incidentes, vulnerabilidades o cumplimiento de controles, actualmente ausentes en el conjunto institucional.

OM3. Se evidencia la necesidad de actualizar las políticas organizacionales para que identifiquen de forma clara a los roles clave involucrados en la gestión de seguridad y privacidad de la información, así como sus responsabilidades y autoridades específicas. Actualmente, las políticas sólo hacen referencia al contexto general sin este nivel de detalle. Esta mejora permitirá alinear mejor las directrices institucionales con los requisitos del MSPI y facilitar su aplicación práctica.

OM4. Se evidencia la necesidad de estructurar un enfoque integral de gestión del riesgo conforme a la metodología de análisis y evaluación de riesgos que exige el MSPI, y alineada con la ISO/IEC 27005:2022, estableciendo criterios claros de aceptación, asignación formal de roles a los dueños del riesgo, definición de una periodicidad

adecuada de reevaluación y documentación de las relaciones entre riesgos, activos y controles. Actualmente, la guía para la administración de riesgos aprobada por el Comité Institucional de Gestión y Desempeño no contempla riesgos de seguridad y privacidad, no se relacionan adecuadamente los riesgos con los activos críticos, y no existen criterios uniformes para la aceptación o tratamiento. Estos vacíos generan subjetividad, dificultan la trazabilidad y debilitan la asignación estratégica de recursos. Al integrar el análisis de riesgos al ciclo institucional de planeación y seguimiento, se garantiza una visión estratégica de las amenazas, se prioriza la protección con base en el valor del activo y se facilita la toma de decisiones del liderazgo con criterios técnicos y normativos.

Se evidencia la necesidad de complementar la guía de administración de riesgos ya aprobada por el Comité Institucional de Gestión y Desempeño, incluyendo criterios, categorías y metodologías de análisis alineadas con la valoración de riesgos de seguridad y privacidad de la información. Esta mejora aumentará la precisión, cobertura y aplicabilidad del análisis de riesgos en el marco del MSPI.

OM5. Se evidencia la necesidad de integrar la privacidad al análisis de riesgos, realizar evaluaciones de impacto, establecer controles específicos para proveedores, definir procedimientos para incidentes con IIP e implementar formación periódica para todos los funcionarios. Actualmente, los riesgos de privacidad no están considerados en la gestión de riesgos de RTVC, ni se tienen cláusulas técnicas para terceros, y la gestión de incidentes no contempla notificación a titulares o autoridades. Incorporar estos elementos permitirá cumplir con el MSPI y responder proactivamente ante requerimientos regulatorios, protegiendo los derechos de los titulares y fortaleciendo la confianza institucional.

OM6. Se evidencia la necesidad de robustecer el proceso de gestión de incidentes de seguridad de la información, actualizar y complementar el Plan de Respuesta a Incidentes conforme a ISO/IEC 27035, definiendo roles y responsabilidades claras y estableciendo flujos de escalamiento jerárquico y funcional, implementando simulacros y ejercicios de entrenamiento, y consolidando un catálogo de incidentes y eventos conocidos. En la actualidad, el plan de 2022 está desactualizado, no existen mecanismos formales de escalamiento ni criterios estandarizados de evaluación. La carencia de un SOC o SIEM operativo, sumado a la falta de integración con los procesos de continuidad y gestión de riesgos, limita la capacidad de detección y respuesta. Esta oportunidad permitirá incrementar significativamente la capacidad institucional de reacción, mejorar la coordinación inter-áreas y establecer mecanismos eficaces de contención y recuperación ante eventos disruptivos.

OM7. Se evidencia la necesidad de implementar un proceso sistemático de aprendizaje posterior a incidentes mediante la creación de un proceso formal de lecciones aprendidas, generar plantillas estandarizadas de informes post-incidente e integrar este ciclo con los procesos de gestión de cambios, continuidad y riesgos. Actualmente, no existen mecanismos formales de análisis posterior, plantillas o repositorios de aprendizaje. Tampoco se realiza formación en técnicas como análisis de causa raíz (Ishikawa, 5 Porqués), lo cual limita la capacidad investigativa y la prevención de recurrencias. Establecer esta práctica permitirá institucionalizar el aprendizaje y evitar la repetición de errores.

OM8. Se evidencia la necesidad de consolidar un sistema de monitoreo, seguimiento y control del MSPI y formalizar procedimientos integrales de seguimiento y medición del sistema, asegurar la correcta aplicación de métodos de cálculo, mejorar el análisis de tendencias de indicadores y ampliar su cobertura conforme a las normas ISO/NIST. Actualmente los análisis carecen de profundidad y no existe un tablero de control unificado. Esto genera

decisiones poco informadas, desalineación con el modelo de control y poca visibilidad para la dirección. La consolidación de este sistema permitirá aumentar la precisión de la medición, facilitar la toma de decisiones y asegurar el cumplimiento de los requisitos del MSPI.

Se evidencia la necesidad de establecer un sistema de seguimiento formal que permita evaluar los avances anuales de los planes estratégicos del MSPI (2022, 2023, 2024, 2025), consolidar los resultados de auditorías y documentar los logros y desvíos. Actualmente se realizan auditorías, pero no se consolida ni evalúa su impacto de forma planificada. Esta mejora facilitará la rendición de cuentas, permitirá ajustar las estrategias y asegurará el cierre efectivo del ciclo de mejora continua.

OM9. Se evidencia la necesidad de formalizar el proceso de revisión por la Alta Dirección. La oportunidad radica en establecer un proceso anual formal de revisión del MSPI, consolidar la información en un solo informe, incluir la evaluación del estado de riesgos, revisar recursos y roles asignados, e integrar los resultados en un tablero de control estratégico. Actualmente, la revisión se encuentra fragmentada, sin un informe único ni documentación oficial de decisiones. Esta situación debilita la gobernanza del sistema y limita su alineación con los objetivos organizacionales. Formalizar esta revisión permitirá cumplir con la cláusula 9.3 del MSPI, facilitar la toma de decisiones informadas y fortalecer el compromiso de la alta dirección con la seguridad de la información y la privacidad.

OM10. Se evidencia la necesidad de alinear el MSPI con los requisitos legales, reglamentarios y contractuales. Consolidar una matriz única de requisitos legales, mapear obligaciones hacia controles del MSPI, generar indicadores normativos, establecer un procedimiento para gestionar cambios regulatorios y centralizar la documentación legal en un repositorio del sistema. Actualmente, la normativa se encuentra distribuida por áreas, sin integración unificada y con responsabilidades que dependen de cada líder de proceso. Esta dispersión dificulta auditorías, incrementa el riesgo de incumplimiento y reduce la trazabilidad. Alinear estos elementos permitirá mejorar la visibilidad normativa, apoyar decisiones del liderazgo y fortalecer el cumplimiento conforme al control 5.31 del MSPI.

OM11. Se evidencia la necesidad de proteger de forma estructurada los registros y activos críticos de información. Es importante alinear la clasificación de documentos con la de seguridad de la información, actualizar instrumentos de archivo, integrar los riesgos documentales al análisis del MSPI, definir estándares de protección digital y asegurar la continuidad operativa documental. En la actualidad, existen brechas entre las TRD y el MSPI, los riesgos archivísticos no están formalmente evaluados, y los mecanismos de respaldo, cifrado y retención electrónica no están estandarizados. Esta protección estructurada mejorará la disponibilidad, integridad y confidencialidad de la información durante todo su ciclo de vida, alineándose con el control 5.33 del MSPI.

OM12. Se evidencia la necesidad de fortalecer la gestión de riesgos asociados a proveedores e identificar a los proveedores como activos de información, establecer riesgos específicos asociados a servicios contratados que involucren seguridad y privacidad, y definir obligaciones contractuales vinculadas al cumplimiento normativo. Actualmente, los proveedores no están reconocidos como activos, sólo hay dos riesgos identificados y no se consideran aspectos regulatorios en los contratos. Asimismo, no existe un responsable único de esta gestión, lo que genera fragmentación en el tratamiento. Fortalecer esta área permitirá reducir vulnerabilidades externas, asegurar compromisos contractuales alineados con la seguridad de la información y mejorar la trazabilidad en la gestión de terceros.

OM13. Se evidencia la necesidad de actualizar los resultados del FURAG conforme a la realidad actual del sistema, y estructurar un plan de mejoramiento que consolide las acciones derivadas del diagnóstico institucional de acuerdo con el Manual Planes de Mejoramiento K-M-4. Actualmente, existe un plan de cierre de brechas que no es reconocido como plan de mejoramiento, y se identifican evidencias sueltas sin una referencia clara al marco MINTIC. Abordar esta necesidad permitirá asegurar la memoria institucional y la mejora continua del sistema de forma estructurada.

OM14. Se evidencia la necesidad de actualizar el Manual del Sistema Integrado de Gestión para incluir explícitamente los lineamientos del MSPI, su aplicabilidad y su relación con los procesos institucionales. Aunque se mencionan procesos formalizados, no se establece dicha integración. Incluir estos lineamientos permitirá consolidar la implementación del modelo y garantizar coherencia normativa y operativa.

OM15. Se evidencia la necesidad de fortalecer la gestión de identidades y trazabilidad de accesos en el entorno operativo. Aunque RTVC cuenta con una infraestructura técnica robusta y controles implementados para autenticación y autorización, se identifican brechas relevantes en los procesos de asignación de permisos, separación de funciones, y monitoreo de accesos, conforme a los controles de accesos. La oportunidad consiste en consolidar procedimientos que aseguren una correcta administración de identidades, establezcan trazabilidad clara sobre accesos, y refuercen la revisión periódica de permisos. Esto permitirá mejorar el control operativo y reducir riesgos asociados a accesos indebidos.

OM16. Se evidencia la necesidad de asegurar una cobertura contractual integral en materia de seguridad de la información. Aunque RTVC incluye cláusulas de confidencialidad en los contratos laborales estas no están presentes en todos los tipos de vinculación, especialmente en los regímenes de nombramiento público. La oportunidad consiste en revisar y actualizar los instrumentos contractuales y administrativos para incluir compromisos específicos sobre confidencialidad, integridad y disponibilidad. Esto reforzará el marco de responsabilidad individual y contribuirá al cumplimiento normativo.

OM17. Se evidencia la necesidad de ejecutar de manera efectiva el plan de formación en seguridad de la información. RTVC ha diseñado un plan para el año 2026, sin embargo, no se cuenta con evidencias de su implementación en el año actual. La falta de ejecución práctica, así como la ausencia de campañas, talleres o mecanismos de evaluación, limita el impacto del programa. Se recomienda activar el plan institucional, definir contenidos por perfil de riesgo y aplicar mediciones que aseguren su eficacia, lo que fortalecerá la cultura de seguridad organizacional.

OM18. Se evidencia la necesidad de garantizar que las obligaciones contractuales de los empleados incluyan explícitamente el reporte de eventos de seguridad de la información. Aunque RTVC cuenta con una mesa de servicio, no se ha documentado en los perfiles, contratos o funciones la responsabilidad de los usuarios de informar incidentes. La formalización de este compromiso en los instrumentos laborales es clave para una detección temprana, una respuesta oportuna y una cultura de corresponsabilidad frente a eventos críticos.

12.3. NO CONFORMIDADES

NC1. No se evidencia una definición de la comprensión del contexto organizacional que incorpore el modelo de seguridad y privacidad de la información. Esto limita la alineación del MSPI con el entorno y sus actores clave, incumpliendo la cláusula 7.1.1 del MSPI.

NC2. No se evidencia la identificación formal de las partes interesadas y necesidades y expectativas relacionadas a la seguridad y privacidad de la información, incluyendo al MINTIC como ente regulador. Esta falta impide una planificación coherente del MSPI, en incumplimiento de la cláusula 7.1.2 del MSPI.

NC3. No se evidencia la designación formal de un Oficial de Seguridad de la Información, ni se describen sus funciones en la estructura organizacional. Esta ausencia afecta la gobernanza y control del sistema, incumpliendo la cláusula 7.2.3 y el control A.5.2 del Anexo del MSPI.

NC4. No se evidencia un documento formal de Declaración de Aplicabilidad que refleje los controles seleccionados, justificaciones de exclusiones, y su correspondencia con el plan de tratamiento. Esta omisión incumple la cláusula 7.3.3 del MSPI.

NC5. No se evidencia una planificación operacional alineada al MSPI ni la integración de sus actividades en una matriz de controles que garantice trazabilidad, control y mejora continua. Esta omisión incumple la cláusula 8.1 del MSPI, afectando la eficacia operativa del sistema.

NC6. No se evidencia la aplicación de una metodología formal para la identificación, evaluación y aceptación de riesgos de seguridad de la información. La ausencia de criterios definidos, matrices aplicadas y un plan de tratamiento estructurado impide la trazabilidad de los riesgos y la gestión del riesgo residual, incumpliendo la cláusula 8.2 del MSPI.

NC7. No se evidencia la realización de auditorías internas al MSPI. Esta situación representa un incumplimiento de la cláusula 9.2 del MSPI.

NC8. No se evidencia la realización de revisiones por la dirección del MSPI, lo cual impide una evaluación periódica y estructurada de la eficacia del sistema. Esta situación representa un incumplimiento de la cláusula 9.3 del MSPI.

NC9. No se evidencia un procedimiento formal, actualizado y aplicado para la clasificación de los activos de información conforme a los principios de confidencialidad, integridad y disponibilidad. Tampoco existe un mecanismo de actualización periódica ni participación formal de propietarios y custodios. Esta situación incumple el control A.5.9 del Anexo del MSPI.

NC10. No se evidencia la inclusión de los aspectos de privacidad en la gestión de incidentes de seguridad de la información. Esta omisión limita la capacidad de respuesta integral ante eventos que comprometan datos personales, incumpliendo el control A.5.24 del Anexo del MSPI.

NC11. No se evidencia un proceso documentado, integral y formal de gestión de incidentes de seguridad de la información. Se carece de criterios de clasificación, procedimientos de respuesta, actividades de aprendizaje organizacional y directrices para la recolección de evidencias. Esta carencia representa un incumplimiento de los controles A.5.24 a A.5.28 del Anexo del MSPI, y limita la capacidad de respuesta efectiva frente a eventos de seguridad.

NC12. No se evidencia la existencia de planes, procedimientos, mecanismos o pruebas que preparen la infraestructura TIC para soportar la continuidad operativa. Esta ausencia representa un incumplimiento de los controles A.5.29 y A.5.30 del Anexo del MSPI, y deja a la entidad expuesta a la pérdida de disponibilidad de servicios críticos durante interrupciones.

NC13. No se evidencia una matriz actualizada de requisitos legales, regulatorios y

contractuales aplicables al MSPI. Última fecha de actualización 23 de julio de 2024. No se evidencia la inclusión de la Resolución 2277 ni del modelo MSPI en el normograma institucional. Esto genera un riesgo de incumplimiento normativo y afecta la trazabilidad legal del sistema, lo cual representa un incumplimiento del control A.5.31 del Anexo del MSPI.

NC14. No se evidencia un riesgo documentado específico asociado a la protección de activos de propiedad intelectual. Esta ausencia representa una brecha en la gestión del riesgo y el cumplimiento del control A.5.32 del Anexo del MSPI.

NC15. No se evidencia la identificación y protección de activos intangibles claves como los derechos de propiedad intelectual, ni su gestión documental asociada. Esta omisión, junto con la falta de integración del componente de privacidad y protección de la información personal al MSPI, vulnera los controles A.5.32, A.5.33 y A.5.34 del Anexo del MSPI, exponiendo a la organización a sanciones regulatorias y pérdidas de activos críticos.

NC16. No se evidencia la aplicación de revisiones independientes al sistema de seguridad de la información, ni mecanismos que garanticen el cumplimiento sistemático de políticas ni procedimientos operativos documentados y actualizados para todos los controles relevantes del MSPI. Esta deficiencia representa un incumplimiento de los controles A.5.35, A.5.36 y A.5.37 del Anexo del MSPI, y afecta directamente la gobernanza, estandarización y control de las operaciones del sistema.

NC17. No se evidencia la implementación de un modelo formal de gestión de la capacidad tecnológica. Aunque RTVC cuenta con infraestructura redundante y recursos críticos disponibles, no existe documentación que evalúe la capacidad actual, ni se han definido criterios o umbrales para anticipar sobrecargas, degradaciones del servicio o necesidades futuras. Esta situación compromete la disponibilidad y rendimiento de los sistemas, en incumplimiento del control A.8.6 del Anexo del MSPI.

NC18. No se evidencia la implementación de herramientas tecnológicas para prevenir la fuga de información confidencial. RTVC no cuenta con controles DLP ni medidas activas en endpoints que permitan monitorear o restringir la exfiltración de datos, lo que representa un riesgo elevado especialmente en contextos de trabajo remoto o acceso móvil. Esta ausencia compromete la confidencialidad de la información, en incumplimiento del control A.8.12 del Anexo del MSPI.

NC19. No se evidencia la aplicación de buenas prácticas de seguridad en el ciclo de desarrollo de software ni en la gestión de cambios. Actualmente, los controles A.8.25 a A.8.34 presentan una madurez inicial, sin documentación de directrices de desarrollo seguro, arquitectura del sistema seguro y principio de ingeniería, desarrollo subcontratado y gestión de cambios. Esta falta incrementa la exposición a vulnerabilidades durante el desarrollo y despliegue de sistemas, incumpliendo los controles A.8.25 a A.8.34 del Anexo del MSPI.

13. CONCLUSIONES

Con base en los resultados de auditoría y en los criterios normativos aplicables, se presentan las siguientes conclusiones estructuradas por cada uno de los objetivos de auditoría definidos para el MSPI en RTVC:

1. Evaluar el grado de cumplimiento de los requisitos establecidos en la Resolución 2277 de 2025 y su anexo técnico, verificando la existencia,

pertinencia y efectividad de los componentes, políticas, procedimientos y controles definidos por RTVC.

Conclusión:
RTVC ha avanzado en la implementación de los componentes exigidos por la Resolución 2277 de 2025, incluyendo políticas, procedimientos y controles de seguridad. Sin embargo, se identificaron brechas en la documentación y trazabilidad de ciertos controles, especialmente en la articulación con los requisitos específicos del anexo técnico de la Resolución. Esto sugiere un cumplimiento medio que requiere ajustes y fortalecimiento en áreas críticas.

2. Analizar el avance en la adopción de las cinco fases del MSPI (Diagnóstico, Planificación, Operación, Evaluación del Desempeño y Mejoramiento Continuo) y su integración con los procesos institucionales y de tecnología de la información.

Conclusión:
La entidad ha evidenciado avances importantes en las fases de Planificación y Operación del MSPI. No obstante, las fases de Diagnóstico, Evaluación del Desempeño y Mejoramiento Continuo presentan debilidades.

3. Confirmar la coherencia entre la implementación del modelo y los lineamientos de la Política de Gobierno Digital, el Decreto 620 de 2020, la Ley 1581 de 2012 (protección de datos personales) y demás disposiciones aplicables en materia de seguridad y privacidad de la información.

Conclusión:
La implementación del MSPI en RTVC se alinea en gran medida con los lineamientos del Decreto 620 de 2020 y la Política de Gobierno Digital, incluyendo aspectos clave como seguridad digital, privacidad de la información y protección de datos personales conforme a la Ley 1581 de 2012. No obstante, persiste la necesidad de ajustar y fortalecer los mecanismos de control en áreas críticas como lo relacionado con la transferencia de datos personales y la trazabilidad del consentimiento.

4. Determinar la capacidad del Modelo de Gestión de Seguridad y Privacidad en RTVC, para cumplir los requisitos legales, reglamentarios, normativos, contractuales y establecidos por la entidad.

Conclusión:
El MSPI de RTVC incorpora controles que permiten atender adecuadamente los requisitos legales, normativos y contractuales aplicables, especialmente mediante la implementación de un marco normativo. Sin embargo, se identificó la necesidad de actualizar y completar la identificación de requisitos legales y normativos, se deben fortalecer los controles asociados a los derechos de propiedad intelectual y a la protección de los registros, para asegurar una trazabilidad completa en cumplimiento normativo.

5. Determinar la eficacia del Modelo de Gestión de Seguridad y Privacidad en RTVC frente al cumplimiento de los objetivos establecidos.

Conclusión:
No se puede establecer una conclusión frente a la demostración de la eficacia en el cumplimiento de los objetivos, debido a que no se han establecido objetivos estratégicos de seguridad y privacidad, de igual manera no existen planes de acción para alcanzar estos objetivos ni mediciones asociadas.

6. Identificar áreas de mejora potencial del Modelo de Gestión de Seguridad y Privacidad en RTVC.

Conclusión:
Se identifican las siguientes áreas de mejora para fortalecer el MSPI en RTVC:

- Ampliar la capacitación y actividades de toma de conciencia en seguridad de la información.
- Fortalecer los procesos de evaluación y tratamiento de riesgos.
- Mejorar la recolección y análisis de incidentes de seguridad.
- Consolidar la revisión independiente del modelo y las auditorías internas y la revisión por la dirección.
- Integrar métricas de desempeño y acciones correctivas como parte del ciclo de mejora continua.

Con base en los hallazgos de auditoría y los criterios normativos aplicables, se concluye lo siguiente respecto al Modelo de Seguridad y Privacidad de la Información (MSPI) implementado por RTVC:

El Modelo de Seguridad y Privacidad de la Información (MSPI) implementado por RTVC presenta un nivel de eficacia medio, logrando establecer controles fundamentales que permiten gestionar riesgos y proteger los activos de información, aunque con deficiencias en el monitoreo continuo, la gestión de incidentes y la retroalimentación del sistema. En cuanto a su adecuación, el modelo se encuentra alineado con marcos normativos como la Resolución 2277 de 2025, la Ley 1581 de 2012 y la Política de Gobierno Digital, pero requiere ajustes puntuales en la documentación, trazabilidad de datos personales y control de terceros. Desde la perspectiva de conveniencia, el modelo se articula con los procesos institucionales y de tecnología de la información, reflejando un enfoque pertinente al contexto operativo de RTVC; no obstante, es necesario fortalecer los procesos de mejora continua, sensibilización del personal y evaluación independiente, conforme con los lineamientos del MSPI. Se recomienda cerrar las brechas identificadas para asegurar un SGSI maduro, resiliente y conforme con los lineamientos del MSPI.

Nombre: Germán Andrés Sánchez Ortegón Firma:  **Auditor Líder**	Nombre: José Ricardo Tobo González Firma:  **Asesor Oficina de Control Interno**