1. POLÍTICA

Política de Copias de Seguridad y Recuperación de la Información.

2. ALCANCE

La presente política aplica a los activos de información de RTVC – Sistema de Medios Públicos que requieran mecanismos de respaldo para garantizar su disponibilidad, integridad y recuperabilidad, incluyendo servidores físicos, máquinas virtuales, bases de datos, sistemas de información, plataformas tecnológicas y demás componentes que soporten los procesos misionales, estratégicos, de apoyo y administrativos de la entidad, tanto en ambientes on-premise como en servicios en la nube.

Así mismo, aplica a funcionarios, contratistas, terceros y proveedores autorizados que administren, operen, gestionen o tengan custodia sobre activos de información, servicios o infraestructura tecnológica bajo responsabilidad de RTVC – Sistema de Medios Públicos, independientemente del ambiente tecnológico en el que operen.

El incumplimiento de los lineamientos establecidos en la presente política podrá dar lugar a las medidas disciplinarias, contractuales o legales a que haya lugar, conforme a la normatividad vigente aplicable y a los lineamientos internos de RTVC – Sistema de Medios Públicos.

3. MARCO NORMATIVO

Norma	Descripción
Ley 1273 de 2009	Establece disposiciones relacionadas con la protección de la información y los delitos informáticos, incluyendo sanciones frente a conductas que afecten la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, justificando la implementación de mecanismos de respaldo y recuperación de la información institucional.
Ley 1581 de 2012	Establece la obligación de implementar medidas técnicas, administrativas y organizacionales para garantizar la seguridad, integridad, disponibilidad y recuperación de los datos personales tratados por la entidad.
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector Tecnologías de la Información y las Comunicaciones, que establece lineamientos asociados a Gobierno Digital, continuidad de servicios tecnológicos y seguridad de la información en entidades públicas.

Decreto 338 de 2022	Establece lineamientos para fortalecer la gobernanza de la seguridad digital, la gestión de riesgos y la respuesta a incidentes cibernéticos, incluyendo capacidades de recuperación y continuidad ante afectaciones sobre la infraestructura tecnológica y la información institucional.
Resolución MinTIC 500 de 2021	Define los lineamientos para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), incluyendo controles asociados a disponibilidad, recuperabilidad y protección de la información institucional.

Norma	Descripción
Resolución MinTIC 02277 de 2025	Actualiza el Anexo 1 de la Resolución 500 de 2021, incorporando lineamientos alineados con la norma ISO/IEC 27001:2022, incluyendo controles relacionados con copias de seguridad y recuperación de información.
ISO/IEC 27001:2022	Norma internacional para la implementación y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo controles asociados a respaldo y recuperación de información.
ISO/IEC 27002:2022	Código de buenas prácticas para controles de seguridad de la información, incluyendo lineamientos relacionados con copias de seguridad, monitoreo, protección y recuperación de información.

4. GLOSARIO

Término	Definición
Activo de Información	Elemento que contiene, procesa, almacena o transmite información y que posee valor para RTVC – Sistema de Medios Públicos, incluyendo información, aplicaciones, servicios, infraestructura tecnológica y recursos asociados.
Backup / Copia de Seguridad	Copia de la información o configuración de un activo tecnológico que permite su recuperación ante pérdida, corrupción, incidente o indisponibilidad.
Respaldo Full	Copia completa de la información seleccionada para respaldo.
Respaldo Incremental	Copia de la información modificada desde el último respaldo realizado.
Recuperación	Proceso mediante el cual se restablece información, servicios o componentes tecnológicos a partir de una copia de seguridad.
Restauración	Ejecución técnica del proceso de recuperación de información respaldada hacia un ambiente autorizado.
Retención	Periodo de tiempo durante el cual las copias de seguridad deben conservarse antes de su eliminación controlada.
RPO (Recovery Point Objective)	Punto máximo de pérdida de información tolerable medido en tiempo entre el último respaldo válido y el momento del incidente.
RTO (Recovery Time Objective)	Tiempo máximo definido para restablecer un servicio o activo tecnológico después de una interrupción.
Disponibilidad	Propiedad de la información que garantiza que los datos y servicios puedan ser accedidos y utilizados cuando sean requeridos.

Integridad	Propiedad de la información que garantiza que esta se mantiene completa, exacta y sin modificaciones no autorizadas.
Confidencialidad	Propiedad de la información que garantiza que esta solo sea accesible por personas, procesos o sistemas autorizados.
Recuperabilidad	Capacidad de restaurar información, servicios o componentes tecnológicos dentro de los tiempos definidos por la entidad.
Infraestructura On-Premise	Infraestructura tecnológica alojada y administrada directamente por RTVC – Sistema de Medios Públicos dentro de sus instalaciones o centros de datos institucionales.
Servicios en la Nube	Servicios tecnológicos suministrados mediante modelos cloud autorizados por RTVC – Sistema de Medios Públicos para el almacenamiento, procesamiento o

Término	Definición
	recuperación de información institucional.
Repositorio de Backup	Ubicación física o lógica destinada al almacenamiento de copias de seguridad institucionales.
Prueba de Restauración	Actividad controlada mediante la cual se verifica la capacidad de recuperación e integridad de la información respaldada.
Incidente de Seguridad de la Información	Evento que puede comprometer la confidencialidad, integridad, disponibilidad o recuperabilidad de la información institucional.
MSPI	Modelo de Seguridad y Privacidad de la Información definido por MinTIC para fortalecer la seguridad digital y la protección de la información en entidades públicas.

5. DESARROLLO DE LA POLÍTICA

5.1 LINEAMIENTOS GENERALES PARA LA GESTIÓN DE COPIAS DE SEGURIDAD

RTVC – Sistema de Medios Públicos deberá implementar, mantener y controlar mecanismos formales de copias de seguridad que permitan proteger la información institucional frente a pérdida, alteración, corrupción, eliminación no autorizada, fallas tecnológicas, errores operativos, incidentes de seguridad digital o eventos que puedan afectar la continuidad de la operación misional.

Las copias de seguridad constituyen un control de seguridad digital orientado a garantizar la disponibilidad, integridad, confidencialidad y recuperabilidad de la información institucional, en cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, la Política de Gobierno Digital y los lineamientos institucionales de continuidad operativa.

La gestión de copias de seguridad deberá aplicarse sobre todos los ambientes tecnológicos de RTVC – Sistema de Medios Públicos, incluyendo infraestructura on-premise y servicios en la nube, conforme a las necesidades operativas, capacidades tecnológicas y lineamientos institucionales de seguridad de la información. Las actividades operativas asociadas a la gestión de copias de seguridad se encuentran definidas en el procedimiento institucional correspondiente.

RTVC – Sistema de Medios Públicos deberá definir y mantener esquemas de respaldo, recuperación y retención alineados con los requerimientos operativos, regulatorios, tecnológicos y de seguridad de la información aplicables a la entidad, garantizando la recuperación de la información institucional dentro de los tiempos definidos para la continuidad de la operación.

5.2 CLASIFICACIÓN, FRECUENCIA Y RETENCIÓN DE RESPALDOS

La definición de los esquemas de respaldo deberá realizarse conforme al nivel de criticidad de los activos de información, el impacto de su indisponibilidad sobre la operación institucional, los requerimientos de continuidad del negocio, el análisis de riesgos y las disposiciones regulatorias aplicables a RTVC – Sistema de Medios Públicos.
Los esquemas definidos aplican tanto para ambientes on-premise como para servicios en la nube administrados por la entidad.

Nivel de Criticidad	Descripción del Activo	Esquema de Respaldo	Frecuencia	Retención	Tipo de Ejecución
Alto	Activos cuya indisponibilidad genera afectación alta o interrupción inmediata de servicios institucionales, misionales o tecnológicos esenciales. Incluye aplicaciones core, bases de datos productivas, servicios de autenticación e infraestructura crítica.	Full + Incremental	Full semanal / Incremental diario	Diario: 7 días / Semanal: 8 semanas	Automática
Medio	Activos de soporte operativo, administrativo o tecnológico cuya indisponibilidad genera impacto moderado sobre la operación institucional.	Full + Incremental	Full quincenal / Incremental cada dos (2) días	Semanal: 4 semanas /: 3 meses	Automática
Bajo	Activos con bajo impacto operativo, información temporal, histórica o componentes cuya recuperación puede realizarse con menor nivel de prioridad.	Full	Full mensual / Incremental semanal o bajo demanda	Mensual: 3 meses o conforme a necesidades institucionales	Automática o manual

Los tiempos de retención podrán ajustarse conforme a requerimientos regulatorios, necesidades de continuidad del negocio, lineamientos de gestión documental, obligaciones contractuales, crecimiento de la infraestructura tecnológica o análisis de riesgos institucionales, debiendo quedar documentados y aprobados por la Coordinación de Gestión de Tecnologías de la Información.

5.3 SEGURIDAD DE LAS COPIAS DE SEGURIDAD

Las copias de seguridad institucionales deberán protegerse mediante controles de seguridad que garanticen la confidencialidad, integridad, disponibilidad y recuperabilidad de la información respaldada, incluyendo:

- Controles de autenticación y acceso restringido a los repositorios y herramientas de backup, aplicando el principio de mínimo privilegio y segregación de funciones.
- Mecanismos de cifrado para las copias que contengan información sensible, datos personales, credenciales, información clasificada o cualquier otra información con requerimientos especiales de protección, tanto en tránsito como en reposo, conforme a la Ley 1581 de 2012 y los lineamientos del MSPI del MinTIC.
- Controles de trazabilidad y registro de accesos, modificaciones y operaciones sobre los repositorios de backup, garantizando la disponibilidad de evidencias para procesos de auditoría interna y externa.

- Protección frente a accesos no autorizados, alteraciones, pérdida de información, corrupción de datos o eventos de ciberseguridad que afecten los respaldos institucionales.

Para activos de criticidad crítica, RTVC – Sistema de Medios Públicos podrá implementar mecanismos de almacenamiento inmutable, offline o tecnologías equivalentes que fortalezcan la protección y recuperabilidad de la información respaldada.

Los terceros autorizados que administren infraestructura tecnológica o servicios en la nube para RTVC – Sistema de Medios Públicos deberán cumplir los lineamientos y controles de seguridad definidos en la presente política, lo cual deberá quedar estipulado en los acuerdos contractuales correspondientes.

5.4 RECUPERACIÓN Y PRUEBAS DE RESTAURACIÓN

RTVC – Sistema de Medios Públicos deberá garantizar mecanismos que permitan la recuperación de información, servicios o componentes tecnológicos respaldados conforme a la criticidad de los activos y las necesidades de continuidad de la operación.

Las pruebas de restauración deberán ejecutarse periódicamente con la siguiente frecuencia mínima:

- Semestral para activos de criticidad alta.
- Semestral para activos de criticidad media y baja.

Las pruebas deberán realizarse en ambientes controlados y autorizados, previa autorización formal de la Coordinación de Gestión TI, sin afectar los ambientes productivos.

Los resultados de las pruebas de restauración deberán documentarse y conservarse como evidencia de cumplimiento conforme a los lineamientos institucionales definidos por RTVC – Sistema de Medios Públicos.

Los incidentes asociados a pérdida, corrupción, indisponibilidad o imposibilidad de recuperación de respaldos deberán gestionarse conforme al Procedimiento de Gestión de Incidentes de Seguridad de la Información y al

procedimiento institucional de Copias de Seguridad, registrándose en la mesa de servicio institucional definida por la entidad.

5.5 MONITOREO, GESTIÓN DE CAMBIOS Y MEJORA CONTINUA

RTVC – Sistema de Medios Públicos deberá implementar mecanismos de monitoreo y seguimiento sobre la ejecución de los respaldos institucionales, tanto en ambientes on-premise como en la nube, identificando fallos, alertas o eventos que afecten su correcta operación.

El monitoreo deberá permitir identificar fallos, alertas o eventos que afecten la correcta operación de los respaldos institucionales.

Toda modificación relacionada con configuraciones, periodicidad, alcance, repositorios, herramientas o mecanismos de respaldo deberá gestionarse conforme al proceso institucional de Gestión de Cambios, garantizando la trazabilidad de los ajustes realizados y su impacto sobre los esquemas de backup vigentes.

Los registros, logs, reportes y evidencias asociados a la ejecución, monitoreo y recuperación de respaldos deberán conservarse conforme a los lineamientos institucionales de trazabilidad y deberán estar disponibles para los procesos de auditoría interna y externa de RTVC – Sistema de Medios Públicos.

La presente política deberá revisarse y actualizarse anualmente o ante cambios normativos, tecnológicos, operativos o de seguridad de la información aplicables a RTVC – Sistema de Medios Públicos, o ante la ocurrencia de incidentes relevantes que evidencien la necesidad de ajuste.

5.6 ELIMINACIÓN SEGURA Y CONSERVACIÓN DE EVIDENCIAS

Las copias de seguridad deberán conservarse durante los tiempos de retención definidos en la Sección 5.2 y eliminarse de forma controlada cuando hayan cumplido su periodo de conservación, evitando la recuperación, exposición o uso no autorizado de la información.

La eliminación de respaldos deberá realizarse mediante mecanismos de borrado seguro que garanticen la trazabilidad, seguridad e irrecuperabilidad de la información institucional eliminada, dejando evidencia formal de la operación ejecutada conforme a lo establecido en el procedimiento institucional de Copias de Seguridad.

Los registros y evidencias asociados a la ejecución, restauración, monitoreo y eliminación de respaldos deberán mantenerse disponibles conforme a los lineamientos institucionales de gestión documental y auditoría, facilitando la verificación del cumplimiento de la presente política por parte de los entes de control competentes.

5.7 EXCEPCIONES

Cualquier excepción a los lineamientos definidos en la presente política deberá estar debidamente justificada, documentada y aprobada por la Coordinación de Gestión TI y el área o responsable de Seguridad de la Información de RTVC – Sistema de Medios Públicos, considerando el análisis de riesgos, el impacto sobre la

operación institucional y las medidas compensatorias requeridas. Las excepciones aprobadas deberán revisarse periódicamente con el fin de evaluar su vigencia y necesidad de continuidad.

6. ROLES Y RESPONSABILIDADES

Rol / Area	Responsabilidades
Coordinación de Gestión TI	Aprobar los lineamientos, esquemas y controles generales asociados a la gestión de copias de seguridad institucionales. Supervisar el cumplimiento de la presente política y gestionar el escalamiento de incidentes críticos asociados a pérdida o indisponibilidad de información institucional.

Rol / Area	Responsabilidades
Líder de Infraestructura Tecnológica	Administrar y garantizar la disponibilidad de la infraestructura tecnológica requerida para la ejecución y almacenamiento de respaldos institucionales en ambientes on-premise y nube. Validar técnicamente cambios de infraestructura que puedan afectar los esquemas de backup.
Administrador de Backups	Ejecutar, monitorear y verificar las copias de seguridad institucionales. Gestionar fallos de ejecución, realizar pruebas de restauración y mantener los registros y evidencias asociados a la operación de respaldos.
Responsable de Seguridad de la Información	Verificar el cumplimiento de los controles de seguridad definidos en la presente política y participar en la gestión de incidentes que afecten la seguridad de la información relacionada con respaldos institucionales.
Dueño Funcional del Activo de Información	Definir la criticidad funcional del activo de información y validar los requerimientos de recuperación necesarios para garantizar la continuidad del proceso o servicio asociado.
Administrador de Base de Datos (DBA)	Gestionar técnicamente las actividades de respaldo y restauración asociadas a motores de bases de datos institucionales que requieran administración especializada.
Mesa de Servicio	Recibir, registrar y escalar solicitudes, incidentes o fallos asociados a la ejecución de respaldos institucionales mediante los canales oficialmente definidos por RTVC – Sistema de Medios Públicos.
Terceros y Proveedores Autorizados	Cumplir los lineamientos y controles definidos por RTVC – Sistema de Medios Públicos para la gestión de respaldos sobre infraestructura o servicios administrados bajo su responsabilidad contractual.
Auditoría Interna	Verificar periódicamente el cumplimiento de la presente política, la conservación de evidencias y la ejecución de controles asociados a la gestión de copias de seguridad institucionales.

7. MEDICIÓN

Con el fin de evaluar el cumplimiento y efectividad de la presente política, RTVC – Sistema de Medios Públicos podrá realizar seguimiento a los siguientes indicadores:

INDICADOR	OBJETIVO	FÓRMULA / MÉTODO DE MEDICIÓN	FRECUENCIA DE SEGUIMIENTO
Cumplimiento de ejecución de respaldos	Verificar la correcta ejecución de las copias de seguridad institucionales.	(Número de backups ejecutados exitosamente / Número total de backups programados) x 100	Mensual
Cumplimiento de pruebas de restauración	Verificar la ejecución periódica de pruebas de recuperación de información.	(Número de pruebas de restauración ejecutadas / Número de pruebas programadas) x 100	Semestral

Los resultados de los indicadores podrán utilizarse como insumo para el seguimiento de controles del Modelo de Seguridad y Privacidad de la Información (MSPI), procesos de mejora continua, auditorías internas y evaluación de riesgos asociados a la continuidad y recuperabilidad de la información institucional.

8. SEGUIMIENTO Y SOCIALIZACIÓN

La presente política deberá revisarse como mínimo una vez al año o cuando se presenten cambios normativos, tecnológicos, operativos o de seguridad de la información que impacten la gestión de copias de seguridad de RTVC – Sistema de Medios Públicos.

El seguimiento al cumplimiento de la política estará a cargo de la Coordinación de Gestión TI, con apoyo del responsable o área de Seguridad de la Información, cuando aplique, mediante la revisión de indicadores, registros de ejecución de respaldos, resultados de pruebas de restauración, incidentes asociados y evidencias de cumplimiento definidas en la presente política.

La socialización de la política se realizará a través de los mecanismos institucionales definidos por RTVC – Sistema de Medios Públicos, incluyendo correo electrónico institucional, intranet, actividades de sensibilización, capacitaciones, lineamientos internos o demás medios oficiales de divulgación que la entidad considere pertinentes.

9. VIGENCIA

La presente Política fue aprobada en el Comité Institucional de Gestión y Desempeño del día 25 de junio de 2026 y entrará en vigencia a partir de su aprobación y publicación en el Sistema Integrado de Gestión (SIG) de RTVC – Sistema de Medios Públicos.

10. CONTROL DE CAMBIOS

Versión	Descripción del cambio	Área productora	Fecha de Publicación
1	Creación del documento	Coordinación de tecnologías de la información	25/06/2026
1	Se realiza nuevamente el cargue del documento en el cual se incluye el logo de RTVC, se ajusta el código de acuerdo con la parametrización de SUITE VISIÓN, se incluye control de cambios, así mismo dando cumplimiento a los lineamientos del manual de marca. V2 y a la Guía de Administración de Información Documentada SIG.	Coordinación de Planeación	05/10/2026

11. ELABORÓ, REVISÓ, APROBÓ

	ELABORÓ	REVISÓ	APROBÓ
Nombres y Apellidos	Julieth Andrea Gutierrez Pineda	Javier Orlando Amezquita Rodríguez	Nohora Piedad Mora Parada
Cargo/Rol	Contratista	Contratista	Coordinadora Gestión de Tecnologías de la Información