TABLA DE CONTENIDO

Contenido

1. INTRODUCCIÓN

El presente Manual de Lineamientos de Gestión de Control de Cambios de Tecnologías de la Información (TI) establece el marco normativo, las directrices y los controles estratégicos necesarios para asegurar que toda modificación, actualización, eliminación o incorporación de componentes tecnológicos en Inravisión- Radio Televisión Nacional de Colombia se realice de manera planificada, controlada, trazable y segura. La gestión institucional de los cambios constituye un pilar fundamental de la gobernanza de TI para garantizar la continuidad, estabilidad y calidad de los servicios tecnológicos que soportan los procesos misionales, estratégicos y de apoyo de la entidad, estableciendo los criterios para minimizar los riesgos asociados a la indisponibilidad de servicios, afectación a la operación institucional, pérdida de información o materialización de incidentes de seguridad digital.

Este documento se fundamenta en los principios de Gestión de Servicios de TI definidos por ITIL v4, específicamente en la práctica de Change Enablement, así como en los lineamientos de política establecidos por el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, y las normas internacionales aplicables en materia de seguridad de la información. En concordancia con lo anterior, el lineamiento integra de manera transversal los principios de confidencialidad, integridad y disponibilidad, dictaminando que cada cambio sea evaluado bajo una visión integral desde los componentes técnico, operativo, funcional y de seguridad digital, asegurando el cumplimiento de los niveles de autoridad y validación institucional antes de su ejecución.

El marco aquí definido es de obligatorio cumplimiento tanto para cambios planificados como para cambios de carácter urgente o emergente, y vincula a las diferentes áreas técnicas, funcionales y de seguridad, así como a proveedores o terceros tecnológicos, promoviendo una cultura de coordinación institucional y toma de decisiones informada. Asimismo, este manual define el estándar uniforme para la gobernanza del ciclo de vida de los cambios tecnológicos, estableciendo las responsabilidades, evidencias y puntos de control requeridos para fortalecer la transparencia, facilitar los procesos de auditoría y control interno, y contribuir a la excelencia y mejora continua de la gestión tecnológica en Inravisión.

2. OBJETIVOS

2.1 General:

Definir los lineamientos para la ejecución controlada de cambios tecnológicos en los ambientes de TI, orientados a maximizar la estabilidad de los sistemas y reducir el riesgo operativo asociado a los despliegues de infraestructura y software.

2.2 Específicos:

- Garantizar la trazabilidad absoluta de las modificaciones mediante el registro, clasificación, evaluación y documentación de cada solicitud, asegurando que el despliegue solo ocurra tras una fase rigurosa de pruebas y validación técnica

- Validar que cada solicitud de cambio responda a una necesidad institucional justificada, fundamentándose en un análisis integral de impacto, riesgos y dependencias técnicas.
- Establecer protocolos de retroceso (rollback) y planes de contingencia para cada implementación, asegurando que ante cualquier falla durante el despliegue se pueda restaurar la operatividad en el menor tiempo posible.

3. GLOSARIO

Cambio: Cualquier modificación, adición, eliminación o actualización que afecte directa o indirectamente los componentes de infraestructura tecnológica, software, configuraciones o servicios institucionales.

RFC (Request for Change / Solicitud de Cambio): Formato o registro oficial mediante el cual se documenta la solicitud de cambio. Contiene la descripción técnica, justificación, impacto, riesgos, responsables, plan de ejecución, plan de reversión y evidencias de validaciones previas.

Despliegue (Release / Deployment): Proceso mediante el cual se instala, configura o publica una nueva versión, componente o servicio tecnológico en un entorno determinado (desarrollo, pruebas, producción), bajo condiciones controladas y seguras.

Gestión de Cambios: Conjunto de actividades planificadas para garantizar que todas las modificaciones a los sistemas o infraestructuras sean evaluadas, aprobadas, implementadas y verificadas adecuadamente, minimizando riesgos y manteniendo la continuidad operativa.

Comité de Cambios (CAB – Change Advisory Board): Instancia técnica de evaluación conformada por representantes de Tecnología, Seguridad Digital, Desarrollo y otras áreas clave. Su función es analizar, aprobar o rechazar los cambios según su nivel de impacto o criticidad.

Cambio Estándar: Cambio rutinario, predefinido y de bajo riesgo, cuya ejecución está documentada y aprobada de manera automática por seguir un procedimiento previamente validado.

Cambio Normal: Cambio planificado que requiere revisión técnica y aprobación formal del Comité de Cambios (CAB) antes de su ejecución.

Cambio Emergente o Urgente: Cambio no planificado que debe ejecutarse de manera inmediata para restaurar un servicio crítico o mitigar un incidente grave. Debe ser informado al CAB posterior a su ejecución, junto con el análisis del evento.

Ambiente de Pruebas (QA / Staging): Entorno controlado e independiente donde se realizan pruebas técnicas, funcionales y de seguridad antes de desplegar una actualización o cambio en producción.

Rollback (Plan de Reversión): Conjunto de pasos y procedimientos documentados para revertir un cambio o restaurar el estado previo del sistema ante fallas o resultados no esperados durante el despliegue.

Concepto de Seguridad: Evaluación emitida por el especialista de Seguridad Digital o su delegado, en la que se analiza el nivel de riesgo, cumplimiento de controles y estado de seguridad del cambio antes de su aprobación.

Validación Post-Implementación: Conjunto de pruebas y verificaciones realizadas una vez completado el cambio o despliegue, con el objetivo de asegurar que el servicio funciona correctamente y que no se han generado vulnerabilidades o errores operativos.

CMDB (Configuration Management DataBase): Base de datos que contiene los elementos de configuración de los sistemas tecnológicos y sus relaciones, actualizada con la información de los cambios aprobados y ejecutados.

4. NORMATIVIDAD

El proceso de Gestión de Cambios y Despliegues se fundamenta en el cumplimiento de los siguientes marcos normativos y estándares técnicos:

Estándares Internacionales

- ISO/IEC 27001:2022: Requisitos para el SGSI. Se enfoca en la protección de la confidencialidad, integridad y disponibilidad mediante los controles de Gestión de Cambios (8.32) y Ciclo de Vida de Desarrollo (8.25).
- ISO/IEC 27002:2022: Guía detallada de controles de seguridad, proporcionando directrices para la gestión de vulnerabilidades y la aplicación segura de configuraciones.
- ISO/IEC 20000-1:2018: Estándar de Gestión de Servicios de TI que exige la planificación y control de despliegues para minimizar fallos operativos.
- ITIL 4: Marco de mejores prácticas que define las prácticas de Change Enablement y Deployment Management, priorizando la agilidad con trazabilidad.
- NIST SP 800-128: Guía para la gestión de configuraciones enfocada en seguridad, asegurando que los cambios no degraden la postura de seguridad del sistema.

Marco Legal y Sectorial (Colombia)

- Modelo de Seguridad y Privacidad de la Información (MSPI - MinTIC): Lineamientos obligatorios para entidades públicas en Colombia, específicamente en los dominios de Gestión de Operaciones y Seguridad en el Ciclo de Vida de los Sistemas.
- Ley 1581 de 2012: Ley General de Protección de Datos Personales (Colombia), aplicable cuando los cambios tecnológicos afecten bases de datos con información sensible.

Normativa Interna Institucional

- Política de Seguridad de la Información y Seguridad Digital: Marco rector que establece la obligatoriedad de los controles técnicos y administrativos sobre la infraestructura de la entidad.
- Lineamientos de la Coordinación de Tecnología y Seguridad Digital: Instrucciones operativas específicas que regulan la ejecución técnica en ambientes de producción.

4. ALCANCE

El presente manual establece las directrices, responsabilidades y controles para la gestión integral del ciclo de vida de los cambios tecnológicos en la Entidad. Su aplicación es de carácter obligatorio y comprende los siguientes ámbitos:

Ámbito Tecnológico
Las disposiciones de este manual rigen sobre cualquier modificación, actualización o retiro de componentes en los siguientes entornos:

Infraestructura y Conectividad: Servidores (físicos, virtuales y en la nube), redes de datos, sistemas de almacenamiento, seguridad perimetral (firewalls, IDS/IPS) y servicios de respaldo.

Sistemas de Información y Aplicaciones: Software de misión crítica, desarrollos propios, aplicativos de terceros, bases de datos, APIs e integraciones institucionales.

Configuraciones Lógicas: Ajustes en parámetros de sistemas operativos, scripts de automatización, políticas de grupo (GPO), reglas de acceso y despliegue de parches de seguridad.

Ámbito del Ciclo de Vida
Este manual regula todas las etapas del proceso de cambio, incluyendo la identificación de la necesidad, el análisis de impacto y riesgos, la etapa de pruebas en ambientes controlados, la autorización formal, el despliegue en producción y la evaluación post-implementación.

Ámbito de Aplicación
Este marco normativo es vinculante para:
Personal Interno: Servidores públicos y trabajadores oficiales de todas las dependencias que intervengan en procesos tecnológicos.
Terceros Interesados: Contratistas, consultores, proveedores externos de servicios gestionados y aliados estratégicos que ejecuten acciones sobre los activos tecnológicos de la Entidad.

5. CONTEXTO

Las presentes políticas establecen los lineamientos, criterios y condiciones que regulan la gestión de control de los cambios tecnológicos dentro de Inravisión - Sistema de Medios Públicos, garantizando su adecuada planeación, evaluación, aprobación, implementación, seguimiento y cierre.
Estas disposiciones buscan fortalecer la gobernanza, el control y la trazabilidad de los cambios que afecten los servicios tecnológicos, la infraestructura y los sistemas de información institucionales, asegurando su alineación con los objetivos estratégicos, las buenas prácticas internacionales (ITIL 4, COBIT 2019, ISO 20000-1 e ISO 27001) y las políticas del Modelo Integrado de Planeación y Gestión – MIPG.
Su aplicación es de carácter obligatorio para todas las dependencias, funcionarios, contratistas y proveedores que intervengan en la gestión, soporte o administración de los activos y servicios tecnológicos de RTVC.

6. DESARROLLO DEL MANUAL

6.1 Registro y Documentación Obligatoria

Universalidad del RFC: Todo cambio sin excepción (Estándar, Normal o Emergente) debe ser registrado mediante una solicitud de cambio (RFC) en la herramienta de mesa de servicio. El sistema asignará un consecutivo único para su trazabilidad.

Soporte Documental: El solicitante es responsable de registrar y adjuntar toda la documentación de soporte o trazabilidad de correo del cambio en la herramienta de mesa de servicio.

Integridad de la Clasificación: La clasificación final del cambio debe quedar consignada en el RFC y será validada por el delegado líder de soporte para asegurar que corresponde a la naturaleza de la intervención.

Actualización del Inventario: Tras cada cambio, es obligatorio actualizar el Registro Central de Activos Tecnológicos. Cualquier movimiento (servidores, software, redes) debe reportarse para mantener el inventario al día.

6.2. Evaluación y Aprobación por Tipo de Cambio

Sesiones del Comité (CAB): El CAB se reunirá de forma ordinaria una vez por semana y de forma extraordinaria cuando sea requerido. La convocatoria la realizará el delegado líder de soporte, con al menos 24 horas de antelación. Las sesiones podrán realizarse de forma virtual o presencial, dejando evidencia de la convocatoria, participantes y decisiones.

Conformación del CAB:
Coordinador de Tecnologías de la Información (quien lo preside).
Líder de Sistemas de Información.
Líder de Infraestructura Tecnológica.
Especialista de Seguridad de la Información.
Delegado líder de soporte
Otros profesionales invitados según la naturaleza del cambio.

Validación de Cambios Normales: Además de la revisión del CAB, los cambios normales deben contar obligatoriamente con un concepto técnico y de seguridad previo a su aprobación.

Prioridad de Emergencia: El solicitante debe priorizar la gestión de cambios de emergencia frente a cualquier otra solicitud asignada.

6.3. Garantía de Calidad y Continuidad

Todo cambio será evaluado con base en:
Riesgos técnicos y operativos.
Impacto en los servicios institucionales.
Resultados de pruebas y plan de rollback.
Concepto de seguridad de la información.

Los cambios se considerarán aprobados una vez cuenten con el visto bueno de la Coordinación de Tecnología e Información.

El delegado líder de soporte comunicará el resultado (aprobado, no aprobado o aplazado) a los responsables y usuarios afectados, mediante correo institucional o herramienta de gestión.

Los cambios aprobados deberán ejecutarse conforme a las ventanas de mantenimiento autorizadas y con las evidencias documentadas en el FORMATO SOLICITUD DE CAMBIOS INFORMÁTICOS -RFC registro formal de una solicitud de cambio tecnológico.

6.4. Comunicación y Cierre

Notificación a Interesados: Todos los cambios aprobados deben comunicarse al personal impactado a través del apoyo del diseñador del área mediante la creación de una pieza informativa, la cual posteriormente se enviará al correo comunicaciones@rtvc.gov.co para su divulgación.

Registro de Resultados: Los resultados, lecciones aprendidas y conclusiones del análisis post-implementación deben registrarse en la herramienta de mesa de servicio para el cierre formal del ciclo.

7. ROLES Y RESPONSABILIDADES

La gestión segura de cambios y despliegues requiere la participación coordinada de varios roles institucionales.
A continuación, se describen sus funciones y responsabilidades principales dentro del proceso:

Rol / Cargo	Responsabilidades Principales
Coordinador(a) de Tecnología e Información	**-** Liderar y autorizar la ejecución de todos los tipos de cambios. - Aprobar o rechazar los cambios, incluyendo los de emergencia.
Delegado líder de Soporte	- Garantizar que toda la documentación quede registrada en el Formato RFC.

Rol / Cargo	Responsabilidades Principales
	- Convocar y presidir las sesiones del Comité de Control de Cambios (CAB). -Programar y comunicar la ventana de mantenimiento.
Comité de Cambios (CAB)	- Revisar y analizar el FORMATO SOLICITUD DE CAMBIOS INFORMÁTICOS -RFC registro formal de una solicitud de cambio tecnológico, según su tipo y nivel de riesgo. - Evaluar el impacto, riesgos y viabilidad técnica de los cambios. - Realizar seguimiento a la implementación y registro del cambio. - Consolidar reportes. - Aprobar, aplazar o rechazar cambios con base en los conceptos técnicos y de seguridad.
Solicitante del Cambio	- Identificar la necesidad del cambio. - Diligenciar el Formato RFC Gestión de Cambios, incluyendo riesgos, plan de rollback y pruebas. - Sustentar técnicamente la solicitud ante el CAB o la Coordinación
Ejecutor del Cambio	- Implementar las actividades aprobadas según el plan definido. - Documentar las evidencias y resultados de las pruebas. - Aplicar el plan de Rollback cuando sea necesario.
Especialista de Seguridad de la Información	- Revisar los riesgos de seguridad asociados al cambio. - Emitir concepto técnico de validación previo a la aprobación. - Registrar observaciones en el FORMATO SOLICITUD DE CAMBIOS INFORMÁTICOS -RFC registro formal de una solicitud de cambio tecnológico.
Líder de Sistemas / Infraestructura / Servicios	- Supervisar la correcta ejecución del cambio dentro de su ámbito. - Validar la documentación técnica y funcional. - Coordinar pruebas funcionales con los usuarios.
Responsable del Servicio / Dueño de Aplicación	Es el funcionario o área líder que utiliza el sistema. Su función es avalar que el cambio propuesto es necesario para la operación y autorizar las pruebas de aceptación de usuario (UAT)
Mesa de Servicio	- Registrar las solicitudes de cambio y asignar número de seguimiento. - Actualizar los estados en la herramienta de gestión o registro.
Usuarios Funcionales o Áreas Afectadas	- Validar la efectividad del cambio en la etapa de revisión post-implementación (PIR). - Reportar incidentes o fallas posteriores.

8. CLASIFICACIÓN DE LOS CAMBIOS TECNOLÓGICOS

La clasificación de los cambios permite definir su nivel de riesgo, la formalidad requerida para su aprobación y los controles de seguridad que deben aplicarse antes de la ejecución.

Cada cambio debe clasificarse en una de las siguientes categorías, de acuerdo con su impacto, urgencia y alcance.

Tipo de Cambio	Nivel de Aprobación	Descripción
Cambio Normal	**Comité de Control de Cambios (CAB)**	Cambio planificado que requiere evaluación técnica, funcional, de impacto y de riesgos. Incluye modificaciones mayores o menores que puedan afectar los servicios, sistemas o infraestructura tecnológica. Debe ser presentado ante el CAB con la documentación completa en el FORMATO SOLICITUD DE CAMBIOS INFORMÁTICOS -RFC registro formal de una solicitud de cambio tecnológico, para su análisis y aprobación formal.
Cambio Estándar	**Aprobación previa del CAB (cambio original o padre)**	Cambio documentado y previamente aprobado por el CAB como actividad recurrente, de bajo riesgo e impacto. Sus ejecuciones rutinarias derivadas no requieren nueva aprobación, siempre que se mantengan dentro del alcance y condiciones definidas en el cambio padre. Ejemplo: actualizaciones periódicas o mantenimientos automáticos previamente validados.
Cambio de Emergencia	**Coordinador(a) de Tecnologías de la Información**	Cambio que debe realizarse de manera inmediata para resolver incidentes críticos, vulnerabilidades o fallas que afecten la disponibilidad, integridad o seguridad de los servicios. Puede aprobarse por correo institucional, dejando evidencia en el FORMATO SOLICITUD DE CAMBIOS INFORMÁTICOS -RFC registro formal de una solicitud de cambio tecnológico dentro de las 24 horas siguientes a su ejecución.

9. CONTROL DE CAMBIOS

Versión	Descripción del cambio	Área productora	Fecha de Publicación
1	Creación del Documento	Coordinación Gestión de tecnologías de la Información	13/05/2026

10. ELABORÓ, REVISÓ, APROBÓ

	ELABORÓ	REVISÓ	APROBÓ

Nombres y Apellidos	Brenda Lizeth Carranza Molina	Javier Orlando Amezquita -Julieth Andrea Gutierrez pineda - Cesar Orlando Parra Sanabria	Nohora Piedad Mora Parada
Cargo/Rol	Contratista de TI (Procesos)	Contratistas (Aseguramiento a la calidad y Arquitectura - Especialista en seguridad - Líder Infraestructura)	Coordinadora Tecnologías de la Información