Superintendencia de Notariado y Registro

MANUAL DE CONTROL DE CAMBIOS DE TI

Gestión de Tecnologías de la Información

SUPERINTENDENCIA
DE NOTARIADO Y REGISTRO

Código: GTI - MN - 004	Versión: 1	Fecha: 3/Oct/2025

JOSÉ RICARDO ACEVEDO SOLARTE
JEFE OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
JUAN CARLOS VALENZUELA BUITRAGO
PROFESIONAL OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
SANTIAGO CAMPO VICTORIA
JEFE OFICINA ASESORA DE PLANEACIÓN (E)
JUNIO 2025

República de Colombia

Ministerio de Justicia y del Derecho

Superintendencia de Notariado y Registro

TABLA DE CONTENIDO

1. INTRODUCCIÓN 5
2. OBJETIVO DEL MANUAL DE CONTROL DE CAMBIOS 5
3. ALCANCE DEL MANUAL 5
4. GLOSARIO DE TÉRMINOS 5
5. MARCO LEGAL 6
6. CONTROL DE CAMBIOS DE TI 7
6.1. ROLES Y RESPONSABLIDADES EN EL CONTROL DE CAMBIOS DE TI 7
6.2. LINEAMIENTOS GENERALES 7
6.3. SOLICITUD DE CAMBIOS 8
6.4. DOCUMENTACIÓN PARA LA SOLICITUD DE CAMBIOS 8
6.5. ANÁLISIS Y CATEGORIZACIÓN DEL CAMBIO 9
6.6. APROBACIÓN DE LA SOLICITUD DE CAMBIO 11
6.6.1. CAMBIOS PRE-APROBADOS 11
6.6.2. CAMBIOS NORMALES 11
6.6.2.1. MESA DE CONTROL DE CAMBIOS DE TI 12
6.6.3. CAMBIOS DE EMERGENCIA 13
6.7. EJECUCIÓN DE CAMBIOS Y PRUEBAS POSTERIORES 14
6.7.1. CAMBIOS NORMALES 14

6.7.2. CAMBIOS DE EMERGENCIA 14

6.8. COMUNICACIÓN DE LOS CAMBIOS 15

6.9. CIERRE DE LOS CAMBIOS 15

7. DOCUMENTOS ASOCIADOS. 15

8. BIBLIOGRAFÍA. 15

9. TABLA DE FIGURAS. 15

10. TABLA DE TABLAS. 15

1. INTRODUCCIÓN

En el marco del Sistema de Gestión de Seguridad de la Información (SGSI), la Superintendencia ha desarrollado este Manual de Gestión de Cambios de Seguridad de la Información. Este documento establece los lineamientos necesarios para gestionar adecuadamente los cambios en los sistemas de información, específicamente en sus ambientes productivos. A través de este documento se busca minimizar los riesgos asociados a las modificaciones en los sistemas de información y/o aplicaciones, garantizando la protección de la confidencialidad, integridad y disponibilidad de los activos de información. La implementación de estos controles es esencial para mantener un entorno seguro y confiable, permitiendo que la Superintendencia cumpla con sus responsabilidades de manera eficiente y segura.

El Manual de Control de Cambios es una herramienta fundamental que apoya la adecuada implementación de políticas y controles de seguridad. Este manual propende por asegurar que todos los cambios propuestos en los sistemas de información sean evaluados rigurosamente, aprobados de manera formal y documentados adecuadamente. Además, define roles y responsabilidades claras para todas las partes involucradas en el proceso de Control de Cambios, desde la identificación de la necesidad de un cambio hasta su implementación y revisión post-implementación.

2. OBJETIVO DEL MANUAL DE CONTROL DE CAMBIOS

Fomentar una cultura de seguridad en la información, promoviendo prácticas que prevengan incidentes de seguridad al momento de realizar modificaciones a los ambientes productivos y así asegurar la continuidad de la operación de la Entidad. De igual manera, este manual define los lineamientos necesarios para ejecutar adecuadamente el **PROCEDIMIENTO DE CONTROL DE CAMBIOS DE TI.**

3. ALCANCE DEL MANUAL

Los lineamientos establecidos en este manual aplican para todos los cambios en la infraestructura tecnológica productiva de la Superintendencia de Notariado y Registro. Así mismo, aplica para todas las partes que tengan acceso a la infraestructura tecnológica de la Organización y a la información de la Entidad.

4. GLOSARIO DE TÉRMINOS

Cambio: Cualquier adición, reemplazo, modificación o eliminación que afecte la infraestructura tecnológica productiva de la entidad.

CA Service Desk,: Plataforma a través de la cual se hacen las solicitudes y documentación de cambios y se gestiona la aprobación y documentación de los cambios.

Control: Es toda actividad o proceso relacionado a mitigar o evitar un riesgo en producción.

Control de Cambios: Proceso formal para gestionar, evaluar, y aprobar cambios en los sistemas de información.

Infraestructura tecnológica: Hardware y Software que soporta los sistemas de información utilizados por los clientes para funcionamiento normal de las operaciones de la Superintendencia.

Impacto: Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Parche: Actualización o corrección específica de software, diseñada para resolver problemas, mejorar la seguridad o añadir funcionalidades, y que se aplica a un programa o sistema operativo ya instalado.

Plan de Contingencia: Este plan identifica los riesgos potenciales, establece medidas preventivas y establece una estructura de respuesta para afrontar cualquier situación adversa de manera estructurada y organizada en caso de que algún cambio produzca resultados negativos.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Rollback" (o reversión): Revertir los cambios realizados a un sistema, base de datos o aplicación a un estado anterior, generalmente para solucionar problemas o errores causados por una actualización o modificación.

Solicitud de Cambio (Request For Change): Petición formal para modificar cualquier componente del entorno productivo de TI, asegurando que todos los cambios se gestionen de manera estructurada para minimizar riesgos y evaluar impactos.

5. MARCO LEGAL

- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

6. CONTROL DE CAMBIOS DE TI

6.1. ROLES Y RESPONSABLIDADES EN EL CONTROL DE CAMBIOS DE TI

Los roles que participan para llevar a cabo una adecuada gestión de cambios son los siguientes:

- Gestor de Cambios: Designado para consolidar, gestionar y hacer seguimiento a las solicitudes de cambios en las aplicaciones o sistemas de la Entidad.
- Mesa de Control de Cambios: Instancia encargada de la aprobación o rechazo de las solicitudes de cambio normales.
- Jefe de Oficina de Tecnologías de la Información
- Coordinadores de la Oficina de Tecnologías de la Información
- Oficial de Seguridad de la Información: Delegado responsable de liderar la formulación, ejecución y seguimiento de la Política de Seguridad de la Información en la Superintendencia de Notariado y Registro.
- Gestores de Aplicaciones: Funcionarios Oficina de Tecnologías de la Información encargados de aplicar, modificar o eliminar los controles Criptográficos.

Las responsabilidades se encuentran descritas en el desarrollo de este manual y el **PROCEDIMIENTO DE GESTIÓN DE CAMBIOS DE SISTEMAS DE INFORMACIÓN**.

6.2. LINEAMIENTOS GENERALES

Se definen los siguientes lineamientos generales, que buscan orientar una adecuada gestión de cambios en la Superintendencia de Notariado y Registro:

- La gestión de cambios aplica a toda la infraestructura tecnológica productiva que tenga la Superintendencia, incluyendo la desplegada en sus nubes privadas o públicas.
- Todo aquel que solicite autorización de efectuar cambios sobre algún sistema de información o dispositivo en ambiente de producción deberá plantear planes de reversión y tratamiento de riesgos enfocados a mitigación y planes de contingencia, los cuales tendrán que estar documentados dentro de la plataforma y/o formato establecido.
- Para el caso particular de los cambios sobre aplicaciones o sistemas de información, se deberá contar con el debido versionamiento de software, validado por el Gestor de Versiones, esto será requisito para poder aprobar los cambios por parte del gestor de cambios.

- Todo elemento que se adicione o se reemplace en la infraestructura tecnológica (equipo de red, de seguridad, servidores virtuales, bases de datos entre otros), deberá reportarse al Oficial de Seguridad, para adicionarse al inventario de activos del proceso.
- La única área autorizada para solicitar y ejecutar cambios sobre servicios productivos serán los integrantes de la Oficina de Tecnologías de la Información o sus terceros contratados y siempre deberá realizarse la gestión a través de la plataforma correspondiente.
- Durante la implementación de los cambios (cualquiera que sea su clasificación), es necesaria la permanente comunicación del éxito o la falla en el proceso entre los Gestores de Aplicación, el Gestor de Cambio, el Oficial de Seguridad, los coordinadores y el Jefe de la Oficina de Tecnologías de la Información.

6.3. SOLICITUD DE CAMBIOS

La solicitud de cambios (Request For Change) se debe realizar por parte de los colaboradores de la Oficina de Tecnología de la Información, a través del módulo disponible en la herramienta CA Service Desk. El gestor de cambios verificará si corresponde a una modificación que afecte la infraestructura tecnológica productiva contemplada en los siguientes casos (sin limitarse solo a estas situaciones):

- Modificación/reemplazo de dispositivos de hardware, incluyendo situaciones donde se ejecuten actividades urgentes para la gestión de incidentes de seguridad de la información.
- Modificación de servicios de producción en la nube de la entidad o en la infraestructura tecnológica en sus centros de datos propios.
- Programas nuevos que puedan afectar los procesos misionales de la organización.
- Desarrollo y/o mantenimiento de software productivo.

Otro aspecto fundamental, es que, como prerrequisito para poder solicitar un cambio hacia producción, todo deberá ser debidamente validado y documentado en los ambientes de prueba o calidad.

6.4. DOCUMENTACIÓN PARA LA SOLICITUD DE CAMBIOS

Los solicitantes de los cambios (tanto normales como de emergencia) deberán realizar la solicitud de cambio dentro de la plataforma establecida en momentos distintos dada su naturaleza conforme con el procedimiento **de Control de Cambios de TI**. En la solicitud de cambio, deberá adjuntarse como mínimo el siguiente documento para realizar la respectiva validación y aprobación:

- Formato de Solicitud de Cambios totalmente diligenciado, el cual incorpora análisis de riesgos, impactos, minuto grama y plan de pruebas.

Se podrá crear un cambio general para realizar varias liberaciones, siempre y cuando las mismas se encuentren dentro de un mismo alcance u objeto definido dentro de un proyecto particular, sin embargo, los avances deberán ser documentados periódicamente.

Nota: Solo en casos excepcionales, no se solicitará Plan de Pruebas, ya que pueden existir sistemas de información o infraestructura tecnológica que no cuentan con ambientes de prueba para validar las modificaciones y deberá realizarse el ajuste directo en ambiente productivo. Esto quedará bajo consideración del gestor de cambios y el comité de cambios.

6.5. ANÁLISIS Y CATEGORIZACIÓN DEL CAMBIO

Los solicitantes del cambio deben crear la solicitud en la plataforma para gestión de cambios adjuntando el Formato de Solicitud de Cambios correspondiente.

Dentro del diligenciamiento del Formato, se encuentran dos aspectos fundamentales que el solicitante debe tener en cuenta para categorizar el cambio adecuadamente: Tipo de cambio e impacto del cambio, los cuales se definen a continuación:

TIPO DE CAMBIO
CAMBIO NORMAL • Cambio en los servicios de TI que sigue el proceso estándar de gestión de cambios y no requiere una implementación inmediata. Estos cambios son planificados y evaluados con suficiente antelación para mitigar cualquier riesgo potencial y asegurar una implementación ordenada. • La documentación completa del cambio, incluyendo el análisis de impacto y riesgos, el plan de implementación, y los resultados de las pruebas, debe ser presentada para evaluación del respectivo comité de cambios y así surtir el proceso de aprobación correspondiente. Esto asegura que toda la información relevante esté disponible para futuras referencias y auditorías.

TIPO DE CAMBIO
CAMBIO DE EMERGENCIA • Cambios que están asociados a la corrección inmediata o contención de un incidente o evento imprevisto que está afectando la integridad, confidencialidad o disponibilidad de la información y que puede afectar la reputación o puede causar incumplimientos legales. • Dado que la prioridad de implementación de estos cambios es extremadamente alta, la documentación se realizará en paralelo a la ejecución del cambio o inmediatamente después de que se haya contenido el incidente. Esto garantiza que la respuesta rápida no comprometa el registro y la trazabilidad del cambio. • La solicitud del cambio de emergencia debe ser aprobada por el jefe de la Oficina de Tecnología o por el Oficial de Seguridad de la Información

TIPOS DE IMPACTO
IMPACTO CRÍTICO • Interrupción total de uno (1) o más servicios misionales de cara a la ciudadanía. • Interrupción total de los sistemas de información en horario hábil que afecten a más de un proceso. • La implementación es crítica, por lo cual, el cambio debe realizarse. • Comprende actividades como: Migraciones de centros de datos, reemplazo o migración de componentes centrales como Switches Core, Firewalls e Hipervisores. • Migración, implementación o actualizaciones significativas de sistemas de información que afecten a toda la organización o que involucre la disponibilidad del personal de más de dos (2) procesos de la entidad. • Actualizaciones significativas (nueva interfaz gráfica o nuevas páginas web) de sistemas de información que afecten trámites y/o servicios con la ciudadanía y que requieran un proceso de divulgación masivo.
IMPACTO ALTO • Interrupción parcial o degradación de los servicios tecnológicos involucrados por tiempo superior a 4 horas e inferior a 48 horas que no supongan interrupciones en horario hábil. • Degradación de Servicios de cara a la ciudadanía (lentitud o intermitencia). • **Interrupción total de los sistemas de información en horario hábil que afecten a un proceso.** • Comprende actividades como: Actividades de mantenimiento o actualización orientadas al fortalecimiento de las aplicaciones a nivel funcional, de infraestructura, de desempeño y/o seguridad. • Actualizaciones como nuevas funcionalidades, correcciones de errores o bugs, mejoras específicas de interfaz y/o mejoras de seguridad de sistemas de información que afecten trámites y/o servicios con la ciudadanía. • Liberación de nuevos sistemas de información (trámites y/o servicios con la ciudadanía) y que requieran un proceso de divulgación masivo. **Nota:** Podrán clasificarse como **IMPACTO ALTO** cambios que generen una interrupción total de uno (1) o más servicios misionales de cara a la ciudadanía solo si se cuenta con la autorización y aval de un tiempo específico por parte de los líderes funcionales de los aplicativos o tomando como base los ANS establecidos para los sistemas de información.

TIPOS DE IMPACTO
IMPACTO MEDIO • Interrupción de los servicios tecnológicos involucrados por tiempo interior a 4 horas. • **El cambio afecta solo un PROCESO de la entidad o a un grupo focal específico de la entidad.** • Comprende actividades como: Actividades de mantenimiento o actualización orientadas al fortalecimiento de las aplicaciones a nivel funcional, de infraestructura, de desempeño y/o seguridad. • Actualizaciones como nuevas funcionalidades, correcciones de errores o bugs, mejoras específicas de interfaz y/o mejoras de seguridad de sistemas de información que afecten trámites y/o servicios con la ciudadanía. • Creación de servidores para ambientes productivos de aplicaciones o solicitud de designación de recursos de forma masiva que puedan afectar la capacidad tecnológica de la superintendencia.
CAMBIOS DE IMPACTO BAJO O MUY BAJO • Realizar el cambio no requiere del cumplimiento de requisitos, prerrequisitos y dependencias. (Diseño, plan, pruebas, implementación, post-implementación, reprogramación). • Se consideran casos de soporte. • Afecta a un usuario o un grupo muy limitado, por ejemplo, Ej. Aprovisionar un servidor, implementar un nuevo backup, instalar parches en equipos y/o servidores, mantenimiento o reemplazo de equipos de usuario final etc.)

Para determinar el tipo de cambio y el tipo de impacto, deben cumplirse con todos los requisitos de cada tipo definido, de lo contrario, los cambios pueden ser devueltos si están mal categorizados.

Teniendo en cuenta la categorización del cambio, el gestor de cambios y el comité de cambios podrá tomar las decisiones más acertadas respecto al manejo de cada solicitud en particular.

6.6. APROBACIÓN DE LA SOLICITUD DE CAMBIO

6.6.1. CAMBIOS PRE-APROBADOS

Los cambios de IMPACTO BAJO estarán preaprobados, ya que en esencia son casos de soporte y deben solicitarse y gestionarse a través de la mesa de ayuda. La creación de servidores (para ambientes de desarrollo y pruebas) o creación de instancias de bases de datos (para ambientes de desarrollo y pruebas), serán cambios PREAPROBADOS. Sin embargo, deberá realizarse la evaluación del consumo de recursos disponibles y así actualizar los análisis de capacidad.

6.6.2. CAMBIOS NORMALES

Los cambios categorizados como normales tendrán las siguientes condiciones para ser aprobados:

1. Ser creados y documentados a través de la plataforma.

2. Luego tendrán una revisión previa por parte del gestor de cambios, para posteriormente ser postulados al comité de cambios para la respectiva revisión y aprobación.
3. Los cambios serán postulados al comité por orden de llegada, teniendo un límite máximo de 4 cambios.
   Nota: Si existen cambios previos abiertos sin la documentación y cierre correspondiente, se denegará la solicitud de nuevos cambios para el comité hasta que se haya completado la documentación pendiente de los cambios anteriores.
4. Se recibirán solicitudes de cambio hasta los martes a las **16:00** horas. Posterior a ese umbral límite los cambios entrarán encolados para la siguiente semana.

6.6.2.1. MESA DE CONTROL DE CAMBIOS DE TI

La Mesa de Control de Cambios de TI será la encargada de aprobar y aplazar o rechazar los cambios normales según su criterio; así mismo, será la encargada de brindar recomendaciones para las solicitudes de cambio expuestas en esta mesa. Los cambios deben ser aprobados por unanimidad.

Esta mesa estará compuesta por:

- Jefe de la Oficina de Tecnología (o quien delegue) – tiene voto
- Coordinadores de la Oficina de Tecnología – cada uno tiene voto
- Gestor de Cambios – tiene voto
- Oficial de Seguridad de la Información – tiene voto
- Invitados (funcionarios, Contratistas y/o Proveedores involucrados en el cambio) – tienen voz

La mesa será convocada por el Gestor de Cambios una vez a la semana, sesionará (virtual o presencialmente) los miércoles o jueves según disponibilidad y siempre que se cuente con solicites de cambios en trámite. En cada sesión, el funcionario o contratista que solicita el cambio deberá hacer la presentación del respectivo requerido ante los miembros de la mesa incluyendo todos los aspectos considerados en la solicitud.

Nota: Los cambios de IMPACTO CRÍTICO además de ser aprobados por la mesa de control de cambios de TI, deberán escalarse al comité institucional de gestión y desempeño (CIGD) para aprobación final, por lo tanto, deberán planificarse con al menos dos (2) meses de anticipación, para que exista un tiempo prudencial para poder escalar el cambio al CIGD más próximo.

Una vez concluida cada sesión, el Gestor de Cambios informará vía correo electrónico a los participantes sobre las conclusiones de la mesa, los cambios aprobados, los cambios rechazados y demás información complementaria.

6.6.3. CAMBIOS DE EMERGENCIA

La solicitud de cambios de emergencia podrá realizarse a través de un correo electrónico donde se indique como mínimo la siguiente información:

1. **DESCRIPCIÓN DEL CAMBIO** – En que consiste el cambio a realizar y los sistemas que se verán afectados.

2. **JUSTIFICACIÓN DEL CAMBIO** – Indicar el incidente o situación adversa que justifica la maniobra de emergencia.

3. **CONSECUENCIAS DE NO EFECTUAR EL CAMBIO DE EMERGENCIA** – Indicar que puede ocurrir si no se ejecuta el cambio de emergencia.

4. **EQUIPO RESPONSABLE DE EFECTUAR EL CAMBIO** – Indicar nombres de los involucrados en las actividades.

5. **TIEMPO ESTIMADO DE EJECUCIÓN** – Indicar el tiempo estimado del cambio y las pruebas de validación de la efectividad del cambio.

Con esta información mínima podrá evaluarse la pertinencia del cambio de emergencia.

Los únicos autorizados para solicitar cambios de emergencia son los COORDINADORES de la Oficina de Tecnologías de la Información, por lo tanto, los solicitantes directos deberán informar a los coordinadores para que se haga un primer filtro de las solicitudes.

Los cambios categorizados como de Emergencia tendrán las siguientes condiciones para ser aprobados.

1. Únicamente los coordinadores de la Oficina de Tecnologías de la Información podrán solicitar cambios de emergencia, dirigiendo su solicitud al jefe de la Oficina de Tecnologías de la Información, al gestor de cambios y al oficial de seguridad.
2. La solicitud de cambio de emergencia será evaluada por el jefe de la Oficina de Tecnologías de la Información, el gestor de cambios o el oficial de seguridad.
3. Posterior a la aprobación del cambio, los solicitantes podrán proceder con la ejecución de las actividades.

4. Una vez ejecutadas las actividades de contención y/o solución del incidente o evento adverso, el solicitante deberá crear el cambio inmediatamente en la plataforma y realizar la documentación correspondiente, para garantizar la trazabilidad de las acciones realizadas.

Una vez efectuados los cambios de emergencia, se deberá llevar a cabo la documentación en la plataforma de gestión de cambios, adjuntando el formato de solicitud de cambios diligenciado en su totalidad, para tener la trazabilidad de las actividades realizadas como de los resultados.

6.7. EJECUCIÓN DE CAMBIOS Y PRUEBAS POSTERIORES

Una vez se aprueba el cambio solicitado (sea normal o de emergencia), deberá ejecutarse en los tiempos establecidos y se deberán ejecutar las siguientes actividades según corresponda.

6.7.1. CAMBIOS NORMALES

- Si el cambio NO FUE EXITOSO se deberá ejecutar las actividades de ROLLBACK y diligenciarse por segunda vez el formato de solicitud de cambio, en la pestaña PLAN DE PRUEBAS y documentar que el sistema de información volvió satisfactoriamente a su estado original previo al cambio.
- Si el cambio FUE EXITOSO deberá diligenciarse por segunda vez el formato de solicitud de cambio, en la pestaña PLAN DE PRUEBAS y documentar las pruebas posteriores, donde se evidencie que el sistema de información funciona conforme a lo esperado después del cambio.
- Debe adjuntarse recibo a satisfacción del cambio (correo electrónico) por parte del área funcional del sistema de información, para garantizar que se suple la necesidad con el cambio realizado.

6.7.2. CAMBIOS DE EMERGENCIA

- Una vez efectuado el cambio de emergencia, el solicitante deberá validar la efectividad de este ante la situación adversa que se estaba buscando mitigar.
- Si el cambio de emergencia NO FUE EXITOSO, el solicitante deberá implementar nuevas medidas hasta que se logre mitigar el incidente generado.
- Si el cambio de emergencia FUE EXITOSO, solucionando el incidente y/o situación adversa, se deberá inmediatamente allegar la documentación del cambio a través de la plataforma, adjuntando el formato de gestión de cambios totalmente.
- Debe adjuntarse recibo a satisfacción del cambio (correo electrónico) por parte del área funcional del sistema de información, para garantizar que se cumple el objetivo con el cambio realizado.

6.8. COMUNICACIÓN DE LOS CAMBIOS

El solicitante del cambio coordinará las estrategias de comunicación de las ventanas de cambio según corresponda.

Los cambios de impacto Crítico y Alto serán informados por el jefe de la Oficina de Tecnología o uno de los coordinadores al Despacho del Superintendente para que la gerencia pueda tener conocimiento de estas actividades.

6.9. CIERRE DE LOS CAMBIOS

Únicamente el gestor de cambios podrá realizar el cierre de los cambios, una vez se hayan cumplido todos los requisitos descritos en este manual y pueda catalogarse como completado. Es importante indicar que los cambios podrán tener 3 posibles cierres:

- **EXITOSO:** El cambio cumplió con las salidas esperadas, sin presentar contratiempo o fallas en los sistemas involucrados.
- **EXITOSO CON ERRORES:** El cambio cumplió mayormente con las salidas esperadas, pueden producirse algunas desviaciones o contratiempos, pero la funcionalidad de los sistemas no se ve afectada en mayor medida.
- **NO EXITOSO:** El cambio presentó fallas graves en los sistemas involucrados y requirió la ejecución de las actividades de Rollback para traer el sistema al punto inicial, previo a la ejecución del cambio.

7. DOCUMENTOS ASOCIADOS.

No aplica.

8. BIBLIOGRAFÍA.

No aplica.

9. TABLA DE FIGURAS.

No aplica.

10. TABLA DE TABLAS.

No aplica.

VERSIÓN DE CAMBIOS			
Código:	**Versión:**	**Fecha:**	**Motivo de la actualización:**
GTI - MN - 004	1	3 de Octubre de 2025	Se hace necesario ajustar la documentación en el marco del fortalecimiento institucional con el fin de alinearlos al Sistema Integrado de Gestión y el nuevo modelo por procesos de la Entidad.

ELABORACIÓN Y APROBACIÓN			
ELABORÓ	**APROBÓ**	**REVISIÓN METODOLOGICA**	**Vo.Bo Oficina Asesora de Planeación**
Juan Carlos Valenzuela Buitrago	José Ricardo Acevedo Solarte	Alberto Higuita Goez Juan Sebastián Ávila	Santiago Campo Victoria
Oficina de tecnología de la Información y las Comunicaciones	Jefe Oficina de Tecnología de la Información	Oficina Asesora de Planeación	Oficina Asesora De Planeación
Fecha: 22 de septiembre 2025	Fecha: 25 de septiembre 2025	Fecha: 30 de septiembre 2025	Fecha de Aprobación: 3 de Octubre 2025