

1. OBJETIVO

Establecer las directrices para controlar de manera adecuada los cambios requeridos en las instalaciones, sistemas de información, aplicaciones, servicios, y en general, la infraestructura tecnológica de RST ASOCIADOS PROJECT SAS.

2. ALCANCE

Este procedimiento define los lineamientos para controlar los cambios requeridos en las instalaciones, sistemas de información, aplicaciones, servicios e infraestructura tecnológica, a fin de lograr una mejor interacción con los clientes, usuarios y líderes de procesos.

Inicia con la solicitud de cambio a través de la mesa de ayuda, o por solicitud formal al Departamento de TI y finaliza con el cierre del cambio, siempre y cuando cumpla con los requisitos o funcionalidades esperados.

Aplica para los siguientes cambios:

- **SDLC:** Los cambios manejados en el ciclo de vida de desarrollo de software formal deben ser incluidos en el programa de gestión de cambios de la Empresa.
- **Hardware:** Instalación, modificación, retiro o reubicación de equipo de cómputo.
- **Software:** Instalación, aplicación de parches, actualización o eliminación de productos de software, incluyendo sistemas operativos y utilitarios.
- **Base de datos:** Cambios a la base de datos o archivos tales como adiciones, reorganización y mantenimientos estructurales.
- **Aplicación:** Cambios en las aplicaciones que se promueven a producción, así como la integración de nuevos sistemas de información y la eliminación de elementos obsoletos.
- **Movimientos, adiciones, cambios y eliminaciones:** Cambios en la configuración de los sistemas.
- **Cambios programados:** Requerimientos para creación, borrado o revisión de tareas (jobs), programación de backups y en general los cambios en la programación de las tareas (jobs).
- **Servicios de comunicaciones unificadas:** Instalación, modificación, desinstalación o reubicación de sistemas de telefonía, mensajería instantánea y buzón de voz.
- **Escritorio:** Cualquier modificación o reubicación de equipos o servicios de escritorio.

- **Cambios asociados:** Los que son requeridos para complementar los cambios descritos anteriormente.

Este procedimiento se encuentra alineado con las Políticas de Seguridad de la Información de RST ASOCIADOS.

3. RESPONSABLES

3.1 Solicitante del cambio:

- Responsable de formalizar el requerimiento de cambio, justificado y aprobado por el jefe de área o responsable del activo.

3.2 Aprobadores del cambio:

- Corresponde al Departamento de TI o las personas que cumplen el rol de aprobador, de la solicitud del cambio, estos pueden ser; dueños de proceso, jefes de área, líderes funcionales de aplicaciones y equipo de infraestructura tecnológica o física. Este rol debe considerar y aprovisionar los recursos que demanden el control de cambios, apoyándose para esta actividad, en el Ticket de mesa de ayuda.
- No está permitido adelantar cambios en la infraestructura tecnológica (servicios de TI, sistemas de información o aplicaciones, instalaciones) sin que se cuente con el aval del Departamento de TI, lo que se disminuye el riesgo de afectar la integridad, disponibilidad y confidencialidad de la información para RTS ASOCIADOS PROJECT.

3.3 Comité de Sistemas y Seguridad de Información:

Es el equipo de trabajo, quienes cuentan con la experiencia y conocimiento para validar técnicamente la conveniencia, impacto y forma de implementación de un cambio. Son a su vez los responsables por la ejecución exitosa del Procedimiento de Gestión de Cambios.

Sus integrantes tendrán las siguientes responsabilidades:

- Revisar, aceptar o rechazar las solicitudes de cambio realizadas formalmente, teniendo en cuenta:
 - ✓ Beneficios esperados del cambio propuesto.
 - ✓ Costos asociados al proceso de cambio.
 - ✓ Riesgos de seguridad de la información asociados.
 - ✓ Recursos necesarios para llevar a cabo el cambio con garantías de éxito.

- ✓ Tiempo estimado de ejecución del cambio.
- ✓ Impacto general sobre la infraestructura tecnológica.
- ✓ Participar en el análisis y diseño del cambio que se derive de la solicitud.
- ✓ Evaluar los resultados del cambio y proceder a su cierre.

3.4 Implementador del cambio:

Persona responsable de implementar el cambio de acuerdo a lo determinado por el Comité de Sistemas y Seguridad de la Información, el cual debe:

Elaborar un plan para ejecutar los cambios, teniendo en cuenta lo siguiente:

- Identificar los componentes tecnológicos que son afectados por el cambio.
- Validar que las actividades de implementación que se encuentran dentro del formato de solicitud de cambios sean las suficientes para implementar dicho cambio. En caso contrario, el Implementador del Cambio deberá definir los pasos que se requieren para poder lograr la implementación satisfactoria del cambio.
- Determinar y documentar el estado actual y funcionamiento del hardware, servicio, software o elemento donde se aplicará el cambio, con el fin de conocer el estado anterior y funcionamiento normal antes de la aplicación de dicho cambio.
- Determinar las acciones a ejecutar para retornar al estado anterior (Rollback).
- Realizar las copias de respaldo respectivas suficientes para poder ejecutar el procedimiento de retorno al estado anterior (Rollback), en caso que se requiera.
- Definir las pruebas respectivas antes de ejecutar el cambio.
- Comunicar a las partes interesadas.

Monitorear el Proceso de Cambio para asegurar que:

- Se ajusta a las especificaciones predeterminadas.
- Se cumplen los calendarios previstos y la asignación de recursos es la adecuada.
- El entorno de pruebas es realista y realiza una simulación adecuada.

4. DEFINICIONES Y ABREVIATURAS

- **Cambio:** Adición, modificación o eliminación de algún elemento que pueda tener un efecto directo o indirecto en los servicios (ITIL, 2019).
- **Disponibilidad:** Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada (ISO 27000).

- **Eventos:** Presencia o cambio de un conjunto particular de circunstancias, que puede ser una o varias ocurrencias con una o varias causas. Un evento puede consistir en algo que no está sucediendo (ISO 31000).
- **Gestión de cambios:** Proceso responsable del control del ciclo de vida de los cambios, permitiendo la ejecución de los cambios beneficiosos minimizando el impacto en los servicios de TI (ITIL, 2019).
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización) (ISO 31000).
- **Rollback:** Se define como el proceso de restaurar una base de datos o un programa a un estado anterior, generalmente se usa para recuperarse de un error o en caso de que realizado un cambio no resulte como fue planeado. (Propia de IPES).
- **RFC:** (Request for Change) Solicitud formal para la implementación de un Cambio (ITIL, 2019).
- **SDLC:** (Systems Development Life Cycle) Ciclo de Vida de Desarrollo de un Sistema.
- **TI:** Tecnologías de la Información.

5. CONDICIONES GENERALES

TICKET (Caso creado para solicitar el cambio): El Solicitante y el Comité de Seguridad de Información reúnen la información relevante sobre el cambio, la cual se registra en el Ticket de Control de Cambios. Éste deberá contar con la aprobación por parte del jefe del proceso o jefe del área, con este requisito, procede la creación del ticket en la herramienta MESA DE AYUDA.

Fuentes u origen del cambio: El siguiente listado corresponde a las fuentes u origen que generan la realización de este procedimiento:

- Acciones de mejora, correctivas o preventivas en la infraestructura tecnológica de RST ASOCIADOS PROJECT.
- Proyectos, mantenimientos previstos o ajustes requeridos en la infraestructura tecnológica del Instituto para RST ASOCIADOS PROJECT SAS.
- Retiro, ingreso o cambios de servicios de TI.

- Cambios en la infraestructura física.
- Cambios en la infraestructura tecnológica.
- Resolución de incidentes.
- Gestión de vulnerabilidades técnicas.
- Actualizaciones de software de terceros.
- La corrección de errores.
- La innovación y mejora de los servicios de TI de la entidad.
- El cumplimiento de una nueva legislación.

Prioridad del cambio: El Comité de Seguridad de Información establece la prioridad del cambio, considerando las necesidades establecidas por la misión de la Empresa de la siguiente manera:

- **Emergencia:** Un cambio que, de no ser aplicado inmediatamente, dejará a la Entidad expuesta a riesgos de seguridad de la información.
- **Alto:** Un cambio que es importante para la Entidad y debe ser implementado pronto para prevenir riesgos de seguridad de la información.
- **De rutina:** Un cambio que debe ser implementado para obtener beneficios del servicio producto de este cambio.
- **Bajo:** Un cambio preventivo, que no está condicionado en tiempo o disponibilidad.

Análisis del impacto técnico: Esta sección describe el criterio técnico que se debe aplicar para evaluar el impacto sobre la infraestructura tecnológica. El análisis del impacto técnico se debe documentar de tal forma que se pueda validar la viabilidad técnica y el riesgo que tendrá en el entorno de producción y la afectación al usuario final. Se deben considerar los siguientes criterios al revisar cualquier cambio:

- Evaluar los planes de cambio para medir el impacto y el efecto del cambio durante e inmediatamente después de la implementación del cambio.
- Revisar la integridad técnica del plan de cambio, incluyendo los activos e información asociada, impacto en el arranque o apagado de los sistemas, el impacto en los planes de recuperación de desastres, los requisitos para el respaldo de la información, para almacenamiento y para el sistema operativo.
- Evaluar la viabilidad técnica del cambio y todo el impacto en términos de: actuación, capacidad, seguridad y operatividad.
- Validar los aspectos técnicos y de factibilidad.

Nivel de clasificación según impacto técnico y emergencia: El Comité de Seguridad de Información debe asignar un nivel de clasificación con base en los siguientes criterios:

Bajo: Corresponde a las acciones de rutina y que normalmente reúnen las siguientes condiciones:

- Los recursos requeridos se encuentran dentro del proceso de Gestión de las Tecnologías de la Información.
- Baja complejidad, ya que no es requerida una coordinación técnica.
- Bajo riesgo para la disponibilidad del sistema.
- Fácil aplicación y no requiere un plan de contingencia.
- No hay impactos para los acuerdos de niveles de servicio.

Medio: Corresponde a las siguientes condiciones:

- Involucra recursos de más de un grupo de trabajo.
- Complejidad técnica significativa, es requerida la coordinación técnica para uno o más grupos funcionales.
- Riesgo moderado para la disponibilidad del sistema, requiere de un plan de contingencia.
- La implementación reviste de cierta complejidad.
- Posibles impactos para los acuerdos de niveles de servicio.

Alto: Corresponde a las acciones de mayor nivel de complejidad, urgencia y riesgo, comprende las siguientes condiciones:

- Involucra a diversos grupos de trabajo.
- Alta complejidad técnica, con una exigente coordinación entre los diversos grupos funcionales.
- Es posible la afectación de los datos y la seguridad de la infraestructura tecnológica.
- Es requerido el soporte externo especializado.
- Grado crítico de emergencia.

Operaciones que no requieren que se les aplique el presente procedimiento

- Recuperación de desastres.
- Todos aquellos que no fueron requeridos formalmente.
- Los cambios realizados en el proceso de soporte diario como son:
 - Gestión de contraseñas.
 - Gestión de cuentas usuarios.
 - Reinicio de sistemas, aplicaciones o equipos.
 - Cambios de permisos de archivos.

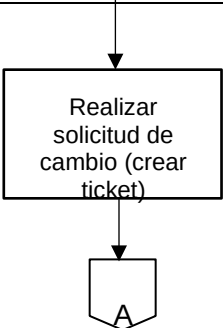
	Procedimiento Control de Cambios				Clasificación: 2
					Versión: 1.0
					Fecha de Actualización:
					Fecha: 16/01/2025

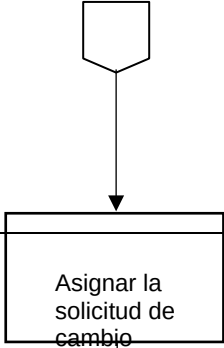
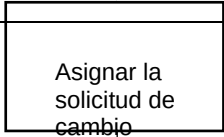
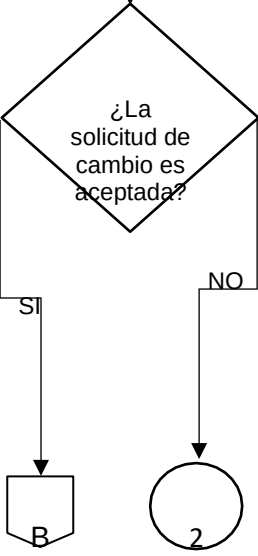
El Comité de Sistemas y Seguridad de Información puede modificar el alcance periódicamente para incluir elementos en el ámbito del proceso general de gestión del cambio de la Entidad.

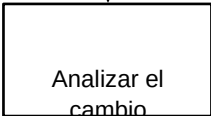
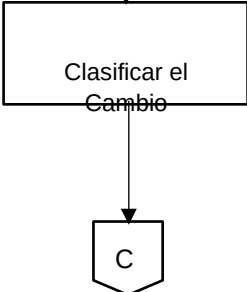
Tipo del cambio: categorías que especificarán el tipo de cambio

Categoría		Detalle
1	Hardware:	Accesorios, servidores, portátiles, computadores de escritorio, escritorios virtuales, dispositivos de red y de seguridad.
2	Migración producción:	Sistema de información, base de datos, red, sistema operativo.
3	Software:	Almacenamiento, aplicaciones de red, herramientas de seguridad y el Sistema Misional, en términos generales aplica para el inventario de aplicaciones y Sistemas de Información en producción RST ASOCIADOS PROJECT SAS.
4	Configuración:	Accesorios, sistemas de información, base de datos, red, servidores, equipos de comunicaciones y de seguridad.
5	Amplia cobertura:	Infraestructura, servicios, telecomunicaciones, entrenamiento en nuevos productos, seguridad física.
6	SDLC:	Cambios requeridos en las aplicaciones y sistemas de información de RST ASOCIADOS PROJECT SAS, durante su ciclo de vida.
7	Seguridad de la Información:	Cambios que afecten la gestión de seguridad de la información, activos, riesgos, controles.

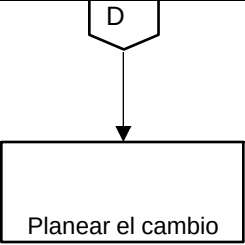
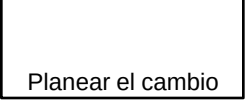
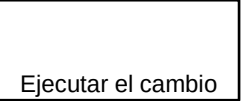
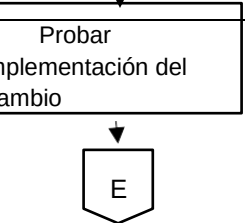
6. DESCRIPCIÓN DEL PROCEDIMIENTO

No.	Actividad (Diagrama de Flujo)	Descripción de la actividad	Responsable (s)	Punto de control	Registro
1		Inicio del Procedimiento			
2		<p>El solicitante del cambio deberá crear el ticket a la Mesa de Ayuda.</p> <p>La solicitud del cambio aplica para cambio en proyecto, para casos de mantenimiento y/o</p>	Solicitante del Cambio		Ticket Mesa deAyuda

No.	Actividad (Diagrama de Flujo)	Descripción de la actividad	Responsable (s)	Punto de control	Registro
		<p>soporte (se tiene en cuenta la prioridad del cambio).</p> <p>El cambio solo se activa en MESA DE AYUDA si se tiene:</p> <ul style="list-style-type: none"> La información completa requerida en el formato. Aprobación de la solicitud del cambio 			
3		La Mesa de Ayuda debe asignar al Oficial de Seguridad de la Información la solicitud de cambio.	Mesa de Ayuda		Avance en el ticket
4		<p>El Oficial de SI revisa el Ticket en GLPI y en el caso que no esté diligenciado correctamente se devolverá al solicitante informando la causal del rechazo.</p> <p>Revisar que infraestructura tecnológica afecta el cambio (aplicaciones, redes, sistemas operativos, sistemas de información, o hardware).</p> <p>Nota 1: Si el cambio solicitado es de infraestructura tecnológica y se afecta a uno o varios usuarios, deben ser anunciados a los líderes de proceso y se debe contar con las aprobaciones de</p>	Oficial de Seguridad de la Información o quien haga sus veces	Revisar el correcto diligenciamiento del Ticket y su contenido para determinar si procede o no el cambio	Avance del Ticket

No.	Actividad (Diagrama de Flujo)	Descripción de la actividad	Responsable (s)	Punto de control	Registro
		<p>las áreas que se vean involucradas en el cambio. Se escalará el cambio al Comité de Seguridad de Información para su respectiva gestión.</p> <p>¿La solicitud del cambio es aceptada por el Comité Técnico? SI: Pasa a la actividad No. 5. NO: Pasa a la actividad No. 2. La solicitud debe ser devuelta al solicitante para su revisión y ajuste. Nota 2: La aceptación de la solicitud del cambio no implica su posterior aprobación.</p>			
5		El Comité de Seguridad de Información, aprueba o rechaza las solicitudes de cambio, teniendo en cuenta las actividades descritas en el ítem de responsabilidades.	Comité de Seguridad de Información		Avance en el ticket
6		El Comité de Seguridad de Información realiza la clasificación del cambio teniendo en cuenta el tipo, prioridad e impacto técnico del mismo en el(los) proceso(s) y a nivel de seguridad de la información.	Comité de Seguridad de Información		Avance en el ticket

No.	Actividad (Diagrama de Flujo)	Descripción de la actividad	Responsable (s)	Punto de control	Registro
7	<pre> graph TD C{{C}} --> D{¿El cambio es aprobado?} D -- SI --> 9((9)) D -- NO --> 8[8] </pre>	<p>El Comité de Seguridad de Información toma la decisión con base en el resultado del análisis del cambio.</p> <p>¿El cambio es aprobado?</p> <p>Si: Pasa a la actividad No. 9</p> <p>No: Pasa a la actividad No. 8.</p> <p>Si el cambio es aprobado, entonces el Comité de Seguridad de Información asigna un Implementador del Cambio.</p>	Comité de Seguridad de Información		Avance en el ticket
8	<pre> graph TD A[Comunicar decisión de la solicitud de cambio] --> D{{D}} </pre>	<p>El Comité de Seguridad de Información por medio de correo electrónico informa a las partes interesadas la aprobación o no del cambio.</p> <p>Si el cambio NO es aprobado se documentan y comunican las razones por las cuales no se aprobó. Esto deberá notificarse tanto al Solicitante del Cambio, como a la Mesa de Ayuda, este último con el fin de</p>	Comité de Seguridad de Información		Avance Ticket Mesa de Ayuda

No.	Actividad (Diagrama de Flujo)	Descripción de la actividad	Responsable (s)	Punto de control	Registro
		actualizar el estado del ticket en la misma a "Cambio no Aprobado".			
9		El Implementador del Cambio realiza la planeación necesaria para garantizar el éxito del cambio, teniendo en cuenta las funciones descritas en el ítem de responsabilidades; y comunica a las partes interesadas.	Implementador del Cambio		Avance en el ticket Mesa de ayuda
10		El Implementador del Cambio ejecuta el cambio de acuerdo al plan elaborado. Además, monitorear el proceso de acuerdo a lo descrito en el ítem de responsabilidades. Debe tener en cuenta las sugerencias, se aclaran dudas y se da soporte a colaboradores, contratistas, proveedores y demás partes interesadas, según se requiera.	Implementador del Cambio		Avance en el ticket
11		El solicitante prueba el cambio y si cumple con los requerimientos, notifica al Implementador del Cambio por medio de correo electrónico la	Solicitante e Implementador del Cambio	Analizar los riesgos, controles o plan de tratamiento a realizar en caso de que se	Avance en el ticket

No.	Actividad (Diagrama de Flujo)	Descripción de la actividad	Responsable (s)	Punto de control	Registro
	<pre> graph TD E{{E}} --> D{¿El cambio es aprobado?} D -- SI --> C((14)) D -- NO --> F{{F}} C --> R[Ajustar Cambio] R --> F </pre>	<p>aprobación Post-Implementación</p> <p>Así mismo, el Implementador del Cambio analiza los resultados de las implementaciones de los cambios, evaluando si el análisis del riesgo e impacto previos a la implementación fue acorde con los requerimientos.</p> <p>Para los cambios de alto riesgo/impacto se realizará un seguimiento especial y se analizarán los resultados.</p>		materialice el mismo	
12		<p>¿El cambio cumple con lo solicitado?</p> <p>Si: Ir a la actividad No. 12.</p> <p>No: Ir a la actividad No. 11.</p>	Implementador del Cambio		Avance en el ticket
13		<p>Si el cambio realizado no fue exitoso, el Implementador del Cambio deberá diagnosticar la causa de la implementación fallida. Si se identifica una acción que permita corregir el resultado del cambio, se implementa de inmediato. Lo anterior con el fin de que sea</p>	Implementador del Cambio		Avance en el ticket

	Procedimiento Control de Cambios		Clasificación: 2
			Versión: 1.0
			Fecha de Actualización:
			Fecha: 16/01/2025

No.	Actividad (Diagrama de Flujo)	Descripción de la actividad	Responsable (s)	Punto de control	Registro
		exitoso. De lo contrario, el Implementador del Cambio deberá seguir las actividades de "Retorno al estado anterior (Rollback)".			
14	Cerrar Cambio	Si la evaluación final determina que el proceso y los resultados han sido satisfactorios, se procede al cierre del cambio por parte del responsable de éste. Adicionalmente, se debe comunicar a las partes interesadas la finalización del mismo. Así mismo, a la Mesa de Ayuda para el cierre del Ticket.	Implementador del Cambio	Verificar de acuerdo a la evaluación del cambio que haya sido satisfactorio	Ticket Mesa de Ayuda /
15	FIN	FIN DEL PROCEDIMIENTO			

7. MARCO NORMATIVO

- NTC-ISO/IEC 27001 Requisitos de Gestión de la Seguridad de la Información

8. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN DEL CAMBIO
V 1.0	25/06/2024	N/A	Elaboración del documento