GESTIÓN DE CONTROL DE CAMBIOS

CONTROL DE EMISIÓN

Elaboró	Revisó	Aprobó
I.S.C. Mario Valdez Velázquez	Mtra. Gabriela Gutiérrez García	Dr. Juan Humberto Sossa Azuela
Firma:	Firma:	Firma:

CONTROL DE CAMBIOS

Número de versión	Fecha de actualización	Descripción del cambio
01	23-Jul-25	Elaboración de primera vez

I. PROPÓSITO DEL PROCEDIMIENTO

Gestionar los cambios en plataformas tecnológicas antes, durante y posterior a su realización.

II. ALCANCE

El Centro de Investigación en Computación (en adelante CIC) en su estructura tiene a la Subdirección de Desarrollo Tecnológico, siendo uno de sus propósitos apoyar al desarrollo tecnológico, motivo por el cual este procedimiento es aplicable para las plataformas tecnológicas administradas y operadas por la Subdirección de Desarrollo Tecnológico, incluyendo los convenios y servicios realizados cuando estos así lo permitan.

III. DOCUMENTOS DE REFERENCIA Y NORMAS DE OPERACIÓN

Manual de Organización del Centro de Investigación en Computación. - 4 de julio de 2025.

Norma ISO 9001:2015 - Sistema de Gestión de la Calidad- Requisitos NMX-CC-9001-IMNC-2015.

Norma ISO 9000:2015 - Fundamentos y vocabulario NMX-CC-9000-IMNC-2008.

Norma ISO/IEC 27001:2022 – Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información.

ISO/IEC 27002:2022 Seguridad de la Información, Ciberseguridad y Protección de la Privacidad – Controles de Seguridad de la Información.

ISO/IEC 27005:2022 Tecnología de la Información – Técnicas de Seguridad – Gestión del riesgo en la Seguridad de la Información.

DOF: 06/09/2021. ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.

Objetivos alineados a la Política General de SI. https://www.ipn.mx/assets/files/cenac/docs/normatividad/objetivos-alineados.pdf

POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN. (29/10/2021). https://www.ipn.mx/assets/files/cenac/docs/normatividad/politica-seguridad.pdf

IV. POLÍTICAS DE OPERACIÓN

1. El control de cambios será obligatorio para cambios mayores, ejemplo, actualización de versiones de software que impacten a la operación, continuidad y disponibilidad; así también, cuando se habilite, baje o reemplace una plataforma.

2. El responsable del control de cambios será el administrador y responsable de la plataforma, con rol de funcionario.

3. Siempre deberá haber un aprobador del control de cambios, mismo que será el superior inmediato, en caso de no haberlo, podrá ser un homologo.

4. Cuando el control de cambios sea generado por la Subdirección de Desarrollo Tecnológico, la aprobación será por la Coordinación de Enlace y Gestión Técnica.

5. Siempre deberá haber evidencia de los controles de cambios, incluyendo el propio documento de solicitud.

ACTIVIDAD	RESPONSABLE	REGISTROS
1. Solicitante documenta la solicitud de cambio en la plataforma correspondiente, incluyendo: • Descripción del cambio propuesto • Justificación técnica • Impacto esperado • Recursos requeridos • Plan de ejecución y recuperación	DSTO, DIT, DDA, SDT	Control de Cambios
2. La solicitud se remite al responsable de aprobación (Comité de Cambios o autoridad designada) para su evaluación.	DSTO, DIT, DDA, SDT	
3. Se determina si el cambio es aprobado. No: 4, Si: 7	DSTO, DIT, DDA, SDT	Control de Cambios
4. Analiza si la solicitud requiere modificaciones para ser reconsiderada 5. No: 5, Si: 6		
6. Responsable de aprobación elabora un reporte de cierre, justificando el rechazo del cambio y notificando al solicitante.	DSTO, DIT, DDA, SDT	
7. Solicitante ajusta la solicitud conforme a las observaciones recibidas y la vuelve a presentar para aprobación Pasa a 2	DSTO, DIT, DDA, SDT	
8. Realiza las tareas técnicas descritas en la solicitud aprobada.	DSTO, DIT, DDA, SDT	Evidencia
9. Recopila evidencias del proceso (capturas, logs, reportes de ejecución).		
10. Determina si el cambio fue exitoso No: 9, Si: 11	DSTO, DIT, DDA, SDT	
11. Ejecuta el plan de recuperación del servicio definido en la solicitud, con el objetivo de revertir el cambio y restaurar la operación normal.	DSTO, DIT, DDA, SDT	Evidencia
12. Verifica si las acciones de recuperación fueron exitosas Si: 11, No: 12	DSTO, DIT, DDA, SDT	

ACTIVIDAD	RESPONSABLE	REGISTROS
13. Solicitante elabora un informe técnico que incluye: • Resultado del cambio • Evidencias • Impacto observado • Recomendaciones	DSTO, DIT, DDA, SDT	Reporte
14. Se convoca a una reunión de incidente mayor con las áreas técnicas involucradas para analizar la falla crítica.	SDT	
15. Solicitante elabora un reporte técnico detallado sobre la falla que impidió la recuperación del servicio.	DSTO, DIT, DDA, SDT	Reporte
16. Documenta el cierre del servicio como incidente mayor.		
FIN DE PROCEDIMIENTO		