POLÍTICA DE GESTIÓN DEL CAMBIO

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Gabriel Cayupan	Nombre: Roberto Maldonado	Nombre: Directorio CDB
Cargo: Jefe de Infraestructura Redes y Soporte	Cargo: CTO Vantrust	

I. Control de revisión

Nº Rev.	Descripción	Fecha
01	Versión inicial	28/04/2022
02	Cambios en Alcance, Desarrollo, Responsabilidades. Cambios Menores.	12/04/2024

II. Tabla de Contenido

1 OBJETIVO

El objetivo de la Política de Gestión del Cambio es establecer lineamientos para permitir que las modificaciones realizadas a la Infraestructura de Tecnologías de la Información (TI) sean efectuadas de manera segura y controlada.

2 ALCANCE

Las disposiciones descritas en el presente documento aplican a todos los colaboradores, proveedores y terceros de: Vantrust Capital Administrador General de Fondos S.A. y Vantrust Capital Corredora de Bolsas S.A., en adelante Vantrust Capital, empresa o compañía, cada colaborador involucrado en la gestión de vulnerabilidades y parches debe leer, entender e implementar los lineamientos descritos en el documento.

Variaciones a este documento no están permitidas sin la aprobación del Directorio de la respectiva Compañía y de su CTO, debiendo documentarse los motivos de las excepciones implementadas.

3 DESARROLLO

- Se deberá priorizar los cambios siguiendo un plan de trabajo autorizado.
- El plan de trabajo deberá especificar las actividades por realizar, la ventana de trabajo, se puede utilizar una lista de verificación para usuarios que apoyen con las pruebas, etc.
- Los cambios deberán ser realizado por personal calificado autorizado por Vantrust Capital, dicho personal deberá contar con el perfil (rol) necesario para las actividades aprobadas en el plan de trabajo, de requerirse, Vantrust Capital brindará los accesos (usuario y contraseña) para dicha actividad.
- Todo cambio critico debe ser aprobado por el Comité de TI (Tecnologías de la Información), mientras que todo cambio no crítico (cambios menores) debe ser aprobado por el área del respectivo CTO de Vantrust Capital.
- Todo cambio critico deberá ser aprobado con una anticipación mínima de quince (15) días hábiles, mientras todo cambio no crítico (cambios menores) deberá ser aprobado con una anticipación mínima de cinco (05) días hábiles.
- El área de TI (Tecnologías de la Información) deberá informar del trabajo antes y después del cambio, se podrá informar a los usuarios afectados y/o a las gerencias y/o jefaturas de áreas antes y después de los cambios.
- El área de Seguridad de la Información gestionara el cumplimiento desde su planificación hasta su finalización según política y procedimiento.
- Antes de realizar el cambio en el ambiente de producción, los cambios de software o hardware o configuración deben de ser probados en el ambiente de prueba.
- Antes del inicio del cambio se deberá contar con un respaldo total del software y de su configuración en caso se necesite hacer un rollback mediante una versión guardada de snapshot, Backup de BD o lo que corresponda a las aplicaciones.

- Todo respaldo será alojado en un repositorio corporativo autorizado por la compañía.
- Todo respaldo previo deberá ser versionado y salvado en un repositorio corporativo autorizado por Vantrust Capital.
- En caso se trate de un pase de un desarrollo de software, el proveedor deberá considerar (además del plan de trabajo) un instructivo de pase (librerías, compiladores, scripts, imágenes, formularios, etc.) para el pase al ambiente de pruebas y/o de producción.
- Los equipos intervenidos deben ser reiniciados una vez finalizado el cambio.
- Las pautas de pruebas de todo aplicativo deben ser generados de acuerdo a las especificaciones funcionales y técnicas, descritas en la documentación del sistema y ejecutadas y aprobadas por el usuario de dicha solución (líder funcional)

4 RESPONSABILIDADES

4.1 El CTO Vantrust Capital se encargará de la revisión y mantenimiento de la Política para la Gestión del Cambio. La política se revisará siempre que haya un cambio organizacional, se requiera alinear con el estándar nuevo existente, y, mínimo una vez al año.

4.2 El soporte de TI también velará por el desarrollo y comunicación de las políticas de gobernanza de seguridad de la información.

4.3 Usuario / Líder Funcional, debe certificar, la completitud y calidad de los desarrollos entregados a operación sistémica.

5 EJECUCIONES

Todo colaborador de la organización, incluidos proveedores de servicio, contratistas, terceros, consultores, personal temporal y otros trabajadores deberán cumplir con la "Política de Gestión del Cambio" de Vantrust Capital.

El incumplimiento o la violación de la política podría estar sujeto a acciones disciplinarias. La acción disciplinaria será de acuerdo con la gravedad del incidente, según lo determinado por una investigación.

6 EXCEPCIONES

Cualquier excepción para adherirse a esta política y sus cláusulas debe ser aprobada por el Comité de TI (Tecnología de la Información).

7 REFERENCIAS

Esta política está dictada conforme a la normativa vigente y a la NCG 510 y a la Circular 2054.

Aprobación Directorio:

Fecha de sesión: 23 de diciembre de 2024.