ESCUELA
POLITÉCNICA
NACIONAL

Política de Gestión de Cambios

Código	Política de Gestión de Cambios
Versión:	1.0.0
Fecha de la versión:	23-02-2023
Creado por:	Grupo
Aprobado por:	Líder
Nivel de confidencialidad:	Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
23/02/2023	1.0.0	Grupo	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS 4

2. POLÍTICA DE GESTIÓN DE CAMBIOS 4

2.1. PROCESO FORMAL DOCUMENTADO 4
2.2. ESPECIFICACIÓN TÉCNICA O GUÍA 4
2.3. PRUEBAS Y CONTROL DE CALIDAD 4
2.4. GESTIÓN DE IMPLEMENTACIÓN 4
2.5. EVALUACIÓN DE RIESGOS 5
2.6. REQUISITOS DE SEGURIDAD 5
2.7. PROCESOS DE APROBACIÓN FORMAL 5
2.8. RESTRICCIÓN DE ACCESOS 5
2.9. CONTROL DE PERSONAL Y DE TIEMPOS 5
2.10. CONTROL DE VERSIONES DE SOFTWARE 6
2.11. CONTROL DE IMPACTO EN APLICACIONES EN SERVICIO 6
2.12. LIMITACIÓN DE ACTUALIZACIONES AUTOMÁTICAS EN APLICACIONES CRÍTICAS 6
2.13. UTILIZACIÓN DE BIZAGI COMO HERRAMIENTA 6

3. VALIDEZ Y GESTIÓN DE DOCUMENTOS 7

1. Objetivo, alcance y usuarios

El objetivo de esta política es garantizar que todos los cambios realizados en los sistemas de información sean planificados, evaluados, autorizados, implementados y evaluados de manera segura y efectiva.

2. Política de Gestión de Cambios

2.1. Proceso Formal Documentado

Se establecerá un proceso formal documentado para llevar a cabo los cambios en los sistemas de información. Este proceso incluirá:

- Identificación y registro de los cambios a realizar
- Evaluación del impacto y riesgos asociados a los cambios
- Planificación y programación de los cambios
- Realización de pruebas y control de calidad antes de la implementación de los cambios
- Autorización formal de los cambios
- Implementación y verificación de los cambios realizados
- Evaluación post-implementación

2.2. Especificación Técnica o Guía

Se documentará una especificación técnica o guía sobre la actuación para realizar los cambios. Esta especificación incluirá:

- Descripción detallada del proceso de cambio
- Procedimientos de evaluación de riesgos
- Procedimientos de control de calidad y pruebas
- Procedimientos de autorización y planificación de cambios
- Procedimientos de implementación y verificación de cambios
- Procedimientos de evaluación post-implementación

2.3. Pruebas y Control de Calidad.

Todos los cambios realizados serán sometidos a pruebas y control de calidad antes de su implementación. Esto incluirá:

- Pruebas de funcionalidad
- Pruebas de integración
- Pruebas de aceptación
- Verificación de la calidad del código

2.4. Gestión de Implementación

La implementación de los cambios será gestionada mediante procesos de autorización, control de permisos y planificación de los cambios. Esto incluirá:

- Autorización formal de los cambios
- Control de permisos para acceder a los sistemas afectados
- Planificación detallada de los cambios a realizar
- Comunicación clara y efectiva a los usuarios afectados por los cambios

2.5. Evaluación de Riesgos

Se realizará una evaluación de riesgos antes de realizar y planificar los cambios. Esta evaluación incluirá:

- Identificación de posibles impactos y riesgos asociados a los cambios
- Evaluación del riesgo de interrupción del servicio
- Evaluación del riesgo de comprometer la seguridad de los sistemas afectados

2.6. Requisitos de Seguridad

Se controlará que los requisitos de seguridad de los sistemas afectados no se vean comprometidos en la fase de implementación de los cambios. Esto incluirá:

- Verificación de que los sistemas afectados cumplan con los requisitos de seguridad necesarios
- Control de los permisos de acceso a los sistemas afectados
- Control de los permisos de los usuarios

2.7. Procesos de Aprobación Formal

Todos los cambios realizados deberán ser aprobados formalmente antes de su implementación. Esto incluirá:

- Identificación de los responsables de la aprobación de los cambios
- Procedimientos de autorización formal de los cambios
- Comunicación clara y efectiva de los cambios a los usuarios afectados

2.8. Restricción de Accesos

Se restringirá el acceso a los sistemas afectados durante la implementación de los cambios. Esto incluirá:

- Restricción del acceso a los sistemas afectados durante el proceso de cambio
- Control de los permisos de acceso a los sistemas afectados
- Comunicación clara y efectiva a los usuarios afectados sobre la restricción de acceso durante el acceso al sistema

2.9. Control de Personal y de Tiempos

Se controlará el personal y los tiempos dedicados a la implementación de los cambios. Esto incluirá:

- Identificación de los responsables de la implementación de los cambios
- Control de los tiempos dedicados a la implementación de los cambios
- Asignación de responsabilidades claras y definidas

2.10. Control de Versiones de Software

Se controlará la versión de software utilizada en los sistemas afectados. Esto incluirá:

- Control de las versiones de software utilizadas en los sistemas afectados
- Verificación de que la versión de software utilizada es compatible con los cambios a realizar
- Comunicación clara y efectiva a los usuarios afectados sobre la versión de software utilizada

2.11. Control de Impacto en Aplicaciones en Servicio

Se controlará el impacto en las aplicaciones en servicio durante la implementación de los cambios. Esto incluirá:

- Identificación de las aplicaciones en servicio que puedan verse afectadas por los cambios
- Evaluación del impacto de los cambios en las aplicaciones en servicio
- Comunicación clara y efectiva a los usuarios afectados sobre el impacto en las aplicaciones en servicio

2.12. Limitación de Actualizaciones Automáticas en Aplicaciones Críticas

Se limitarán las actualizaciones automáticas en las aplicaciones críticas. Esto incluirá:

- Identificación de las aplicaciones críticas
- Evaluación del impacto de las actualizaciones automáticas en las aplicaciones críticas
- Restricción de las actualizaciones automáticas en las aplicaciones críticas

2.13. Utilización de Bizagi como herramienta

Para utilizar Bizagi en la automatización de procesos relacionados con esta política, se pueden seguir los siguientes pasos:

- Definir los procesos y los flujos de trabajo relacionados con el establecimiento de un proceso formal documentado para llevar a cabo los cambios, la realización de pruebas y control de calidad sobre los cambios introducidos, gestionar la implementación mediante procesos de autorización, control de permisos y de planificación de los cambios, la realización de una evaluación de riesgos antes de realizar y planificar los cambios, controlar que los requisitos de seguridad de los sistemas afectados no se vean comprometidos en la fase de implementación de los cambios, procesos de aprobación formal, restricción de accesos, control de personal y de tiempos, control de versiones de software, control de impacto en aplicaciones en servicio y limitación de actualizaciones automáticas en aplicaciones críticas.

- Documentar las especificaciones técnicas o guía sobre la actuación para realizar los cambios, así como los requisitos de seguridad de los sistemas afectados.
- Utilizar Bizagi para automatizar el flujo de trabajo para la implementación de cambios. Por ejemplo, se puede diseñar un formulario de solicitud de cambio que incluya los requisitos y la evaluación de riesgos. El formulario puede ser enviado a los responsables de la aprobación formal y, una vez aprobado, se puede utilizar Bizagi para asignar tareas a los responsables de la implementación de los cambios.
- Utilizar Bizagi para controlar las versiones de software utilizadas en los sistemas afectados. Por ejemplo, se puede configurar un sistema de control de versiones en Bizagi para asegurarse de que la versión correcta de software se utiliza durante la implementación de los cambios.
- Utilizar Bizagi para limitar las actualizaciones automáticas en las aplicaciones críticas. Por ejemplo, se puede configurar un sistema de alertas en Bizagi que notifique al equipo de IT si una actualización automática en una aplicación crítica está programada.
- Utilizar Bizagi para monitorizar y auditar la implementación de cambios. Por ejemplo, se puede configurar un sistema de reportes en Bizagi para que el equipo de IT pueda ver la actividad en tiempo real y hacer un seguimiento de los tiempos dedicados a la implementación de los cambios.
- La automatización de estos procesos con Bizagi permitiría una mayor eficiencia y eficacia en la implementación de cambios y una mejor gestión de riesgos en la organización.

Esta política será revisada y actualizada periódicamente para garantizar su eficacia y adaptación a las necesidades cambiantes de la organización.

3. Validez y gestión de documentos

Este documento es válido hasta el año 2026.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de obligaciones de la organización que ya existían pero que no fueron identificadas.
- Cantidad o monto de multas pagadas por el no cumplimiento de obligaciones.
- Cantidad de días de atraso en el cumplimiento de la obligación.

Líder
[firma]