Proceso de control de cambios

1. Introducción

El objetivo del proceso es describir los pasos a seguir al momento de realizar un cambio en la infraestructura TI en los ambientes definidos por el Gobierno de San Juan. De ahora en adelante cuando hablemos de activo de infraestructura TI (ATI) nos referimos a:

- Aplicaciones, sistemas y sus integraciones y componentes
- Servidores, almacenamiento, routers, switches, firewalls y equipos de ciberseguridad (IPS, IDS, VPN Concentrators, etc.)
- Softwares del sistema operativo
- Softwares de base de datos

2. Objetivo

Tener control y trazabilidad de cada cambio el cual debe estar documentado y autorizado en post de haber realizado el procedimiento de testing pertinente, con el fin de garantizar:

- Realizar solo cambios autorizados;
- Gestionar el riesgo de manera activa;
- Estén debidamente probados;
- Hacerlos solo en horario aprobado;
- Disponibilidad de la evidencia sobre controles y documentación suficientes para que el proceso de control de cambios exista y sea efectivo.

3. Contenido

La Dirección de Ciberseguridad define las medidas necesarias para el control de cambios en los ambientes de Producción (PRD), estableciendo las condiciones que deben cumplirse para efectuar dichos cambios.

4. Solicitud de Cambio

Las solicitudes de cambio (Adjunto I) se utilizan para ejecutar y documentar los cambios que se cubren en esta norma. Toda la documentación relacionada con la solicitud de cambio (formularios de solicitud de cambio aprobado, desarrollo y modificación, prueba y aceptación, y la documentación de implementación) debe conservarse y almacenarse o referenciarse dentro de la solicitud de cambio para fines de auditoría.

5. Categorización de los cambios

Se establecen las siguientes categorías de cambio:

a) Cambio Menor

Corresponde a un cambio que no tiene impacto de riesgo potencial en el ambiente en el cual se implementa.

Un cambio se categoriza como menor cuando cumple con las siguientes condiciones:

- No afecta a los datos.
- No afecta el esquema de seguridad.
- No requiere cambios en la infraestructura.
- No afecta la arquitectura del ATI.
- No afecta la funcionalidad del ATI.
- No afecta a otros ATI.
- En caso de implementaciones no satisfactorias, los riesgos y su resolución son de menor impacto.

Como ejemplos de cambios menores se pueden señalar: cambio de logos, de labels (etiquetas), de información estática, entre otros.

b) Cambio Regular

Por exclusión, serán todos los cambios que no sean catalogados como menores. Si el cambio a realizar no cumple con alguna de las condiciones indicadas en el punto anterior, será tratado como Cambio Regular.

6. ROLES Y RESPONSABILIDADES

Propietario: Funcionario que tiene la responsabilidad de la gestión y es responsable de la información. Autoridad de cada Organismo perteneciente al Gobierno de San Juan. También llamado Solicitante.

Coordinador de Cambio (PM): es el responsable de gestionar las actividades de comunicación y seguimiento entre el solicitante (Propietario o Referente) y el Equipo de Modernización. Completa y presenta la Solicitud del Cambio.

Líder Técnico: tiene la responsabilidad de coordinar las tareas operativas que permitan llevar adelante internamente el cambio. El rol del Líder Técnico puede ser cubierto por personal del Equipo de Modernización.

Implementador: es el técnico responsable de la ejecución del cambio. Este rol puede ser cubierto por personal del Equipo de Modernización, o por personal contratado.

Oficial de Ciberseguridad y Responsable del activo TI: Aprueba el cambio validando los datos descritos en la Solicitud presentada y realiza una evaluación del impacto.

Funcionales: Una vez hecho el cambio realizan pruebas pertinentes, tanto en testing como en producción.

6.1 Para metodología SCRUM

En el procedimiento de SCRUM los responsables de los equipos pueden abarcar uno o más roles:

Facilitador: Solicitante/Propietario

Facilitador TIC: coordinador del Cambio (PM).

Referente técnico: Líder Técnico, Implementador/Desarrollador.

Facilitador de Operaciones: Oficial Ciberseguridad, Responsable Activo TI.

SCRUM Master: tiene la responsabilidad de velar por que el cumplimiento del proceso se ajuste a las políticas y procedimientos definidos.

Para mejoras continuas en donde el cierre del proyecto está dividido en sprint, cada sprint se comporta y tiene las mismas características que un proyecto.

7. DESCRIPCIÓN DEL PROCESO

a) Solicitud de un cambio menor

El Líder Técnico evaluará dicha solicitud y determinará si es correcta la categorización de el/los cambios.

De comprobarse que se trata de un cambio menor, se deberá entregar la siguiente documentación mínima y obligatoria:

- Formulario de Implementación del Cambio (Adjunto I)
- Registro del cambio en la herramienta de seguimiento de proyectos REDMINE. Los cambios a realizarse deben estar identificados con un nivel de granularidad tal, que permitan entender, verificar y generar la trazabilidad del/los cambios efectuados.

La Dirección de Ciberseguridad se reserva el derecho de rechazar la documentación presentada, en caso de que el contenido de los entregables no cumpliese con la completitud y nivel de detalle necesario para llevar adelante las tareas relacionadas con la implementación del cambio. De considerarlo necesario, la Dirección de Ciberseguridad podrá solicitar al Propietario la replanificación de las fechas comprometidas.

El Coordinador de Cambio y el Líder Técnico son los responsables de liderar el cambio, a nivel organizativo y operativo respectivamente.

El solicitante deberá actualizar el repositorio generado previamente por el Líder Técnico como canal de presentación de entregables y con toda documentación mínima y obligatoria, deberá dar aviso al Líder Técnico y al Coordinador del Cambio, de que existe un cambio.

b) Solicitud de un cambio regular

Caso 1 - Implementación de una aplicación o producto

De tratarse de una nueva aplicación, el Propietario o quien éste designe formalmente en su reemplazo (Referente), deberá realizar una comunicación oficial dirigida al Director de Ciberseguridad, con la siguiente documentación mínima y obligatoria:

- Manual de Instalación, de usuario y de seguridad (permisos, perfilería, infraestructura, etc)
- Documento de Alcance Funcional
- Definición de los Requerimientos Funcionales y no Funcionales
- Instructivo con desglose de tareas y su diagrama de gantt correspondiente, cargado previamente en REDMINE

La Dirección de Ciberseguridad se reserva el derecho de rechazar la documentación presentada, en caso de que el contenido de los entregables no cumpliese con la completitud y nivel de detalle necesario para llevar adelante las tareas relacionadas con la implementación de la aplicación. De considerarlo necesario, la Dirección de Ciberseguridad podrá solicitar al Propietario la replanificación de las fechas comprometidas.

El Líder Técnico solicitará la creación de un repositorio con el fin de generar un canal de presentación de entregables a través de este medio. Esto no reemplaza bajo ningún concepto la presentación formal de los entregables requeridos en una contratación.

El solicitante deberá actualizar el repositorio con toda documentación mínima y obligatoria y dar aviso al Líder Técnico y al Coordinador del Cambio asignados como responsables del cambio.

El Líder Técnico deberá gestionar la creación y los accesos del Ambiente Desarrollo con el fin de que el Implementador lleve adelante sus actividades y pueda verificar -previo a la entrega- el funcionamiento correcto.

Por otro lado, el Líder Técnico tiene la responsabilidad de verificar la completitud de la información, validar y velar por la calidad de los entregables.

El Líder Técnico o quién éste designe, es el responsable de verificar la correcta implementación, parametrizar el ambiente de producción y dar aviso a las Área correspondientes de la consecución exitosa de estas tareas. Si el manual de instalación es claro y consistente con las tareas a realizar y la implementación resulta correctamente ejecutada, configurada y parametrizada, informará al Área correspondiente, la disponibilidad del ambiente para que dicha área pueda ejecutar sus estrategias de pruebas.

En caso de que la implementación resulte fallida, el Coordinador dará aviso al Líder Técnico para efectuar las correcciones que sean necesarias.

El Solicitante es el responsable de las pruebas de aceptación, deben considerar el análisis detallado y aprobación del contenido, y la forma en cómo se presentará la información. El Coordinador del Cambio es el responsable de solicitar al Propietario los resultados de las pruebas de aceptación. Con el resultado favorable, el Líder Técnico o quién éste designe, coordinará la puesta en producción de la versión homologada y verificada.

El Líder Técnico o quién éste designe, es el responsable de ejecutar el plan de puesta en marcha contemplando la solicitud de puesta en producción, posterior verificación y comunicación de que la nueva implementación fue correctamente ejecutada en el Ambiente PRD. El Propietario en este ambiente, verificará funcionalmente y aprobará

el contenido del nuevo ATI, y el Líder Técnico o quién éste designe, solicitará la habilitación del cambio en el Ambiente PRD.

Caso 2 - Implementación de una versión nueva o cambio evolutivo

El Líder Técnico hará la primera evaluación del impacto de el/los cambios y a partir de una comunicación oficial dirigida al Director de la Dirección de Ciberseguridad, entregará la siguiente documentación mínima y obligatoria:

- Instructivo con desglose de tareas y su diagrama de gantt correspondiente, cargado previamente en REDMINE
- Formulario de control de cambio (Adjunto I)
- Registro de los requerimientos que generaron el/los cambios efectuados en la nueva versión.

Dicho registro debe ser efectuado en la herramienta de seguimiento de proyectos, REDMINE. Los cambios a realizarse deben estar identificados con un nivel de granularidad tal, que permitan entender, verificar y generar la trazabilidad del/los cambios efectuados.

La Dirección de Ciberseguridad se reserva el derecho de rechazar la documentación presentada, en caso de que el contenido de los entregables no cumpliese con la completitud y nivel de detalle necesario para llevar adelante las tareas relacionadas con la implementación de la nueva versión. De considerarlo necesario, la Dirección de Ciberseguridad podrá solicitar al Propietario la replanificación de las fechas comprometidas.

El Coordinador de Cambio y el Líder Técnico del aplicativo son los responsables de liderar el cambio, a nivel organizativo y operativo respectivamente.

El Implementador previo a la entrega, debe realizar en el Ambiente de desarrollo las tareas que le permitan verificar en la infraestructura de Producción el funcionamiento correcto de los cambios efectuados.

Por otro lado, el Líder Técnico tiene la responsabilidad de verificar la completitud de la información actualizada, validar y velar por la calidad de los entregables.

El Líder Técnico o quién éste designe, es el responsable de verificar la correcta implementación, parametrizar en el Ambiente de Producción y dar aviso a la Dirección de Ciberseguridad de la consecución exitosa de estas tareas. En caso de que la instalación de la aplicación resulte fallida, el Coordinador de la Instalación dará aviso al Líder Técnico para efectuar las correcciones que sean necesarias.

El Propietario es el responsable de la información que se publicará en la nueva implementación; en consecuencia las pruebas de aceptación que éste realice, deben considerar el análisis detallado y aprobación del contenido, y la forma en cómo se presentará la información. El Coordinador del Cambio es el responsable de solicitar al Propietario los resultados de las pruebas de aceptación. Con el resultado favorable, el Líder Técnico o quién éste designe, coordinará la puesta en producción de la versión homologada y verificada.

El lanzamiento de una nueva versión es responsabilidad del Propietario, y éste deberá generar el plan de implementación y el plan de puesta en marcha -si el impacto de los

cambios así lo requieren-; contemplando los aspectos técnicos, de capacitación a usuarios, el aviso a Mesa de Ayuda

8. CAMBIO DE EMERGENCIA

Se requieren cambios de emergencia en caso de que haya un problema grave que deba corregirse inmediatamente y no se pueda aplicar el proceso estándar de control de cambios debido a la criticidad temporal del problema. Debido al requisito de corrección inmediata del problema, las aprobaciones vía mails son aceptables. Para ello se requiere:

- Pruebas de cambios de emergencia
- Formulario de control de cambio

Esta información debe entregarse dentro de dos días hábiles, como máximo, posteriores a la implementación del cambio.

9. CUMPLIMIENTO

Todos los empleados y contratistas del Gobierno de San Juan están sujetos a esta norma y son responsables de su cumplimiento. El mismo está sujeto a control, monitoreo y auditoría. El incumplimiento de este puede resultar en una acción disciplinaria contra el empleado.

10. DOCUMENTACIÓN, ALMACENAMIENTO Y RETENCIÓN

Los cambios deberán ser documentados utilizando el formulario adjunto I, una vez aprobados deberán almacenarse en la carpeta de Control de Cambios disponible en la instancia de producción que la Dirección de Ciberseguridad provea.

Anexo I - DESPLIEGUE EN PRODUCCIÓN (escenarios y procedimientos)

Al momento de un nuevo despliegue o un cambio de algún servicio ya implementado se contemplan 3 escenarios.

1) Responsable del Servidor: Informático/tecnológico que administre el servidor. El mismo tiene privilegios de Administrador Local (siempre con un usuario de dominio) y acceso RDP o SSH al mismo (por ningún motivo SMB, si es necesario SFTP).
2) Responsable de la Aplicación: Tiene accesos a configuración específicas de la aplicación. Incluye acceso SFTP a carpetas específicas y/o administración remota mediante algún cliente de la aplicación.
3) Sin Acceso: No tiene ningún tipo de acceso y el despliegue de algún cambio o implementación se realizará mediante un equipo de técnicos que definirá el Comité de Cambios.

Aclaraciones para todos los escenarios

a. Es importante aclarar que mientras más privilegios de accesos tenga el solicitante mayor será la responsabilidad y el compromiso sobre el servidor, aplicación y servicio.
b. El servidor deberá cumplir con las condiciones impuestas por el Comité de Cambios (unido al dominio ejecutivo.sanjuan.gob, instalado vmtools, symantec, agente fusioninventory, agente wazuh, etc). Si por circunstancias particulares, incluyendo soporte, licenciamiento, conocimiento, tiempo de desarrollo o despliegue, lo anterior no puede cumplirse, se debe obtener aprobación del Comité de Cambios.
c. Para despliegue de un nuevo servicio se completará el formulario 130 (creación de servidor) en donde se definen los requerimientos del servidor.
d. Existe un área de Base de Datos, el solicitante puede llegado el caso pedir la responsabilidad del Servidor donde está la aplicación y dejarle la responsabilidad de la base de datos al área correspondiente.
e. Todos los SO deben estar licenciados o ser opensource. En el caso de Windows solo podrán ser Windows Servers soportados por Microsoft.
f. Todos los Servidores Web, estarán detrás del Nginx administrado por Gobierno Abierto.
g. Los Servidores estarán solamente en la 10.2.132.X.
h. El acceso a los Servidores será vía Vmware y vía rdp (usando SFTP si es necesario compartir archivos) solo desde las PCs de los miembros de los equipos (con todo lo del punto “b” instalado).
i. El usuario administrador local se deshabilita y se crea uno nuevo con pasw fuerte y lo almacena Ciberseguridad.
j. Si es necesario compartir el pasw se hará mediante https://passbolt.sanjuan.gov.ar/ y https://qlink.it/.

1) Responsable del Servidor

El procedimiento para nuevo despliegue o cambio será:

1. Completar formulario de cambio F013.
2. Envía formulario al comité vía correo electrónico a lista.cambios@sanjuan.gob.ar como mínimo 48hs antes del cambio.

Al momento de recibir el formulario se habilitará una ventana de tiempo (especificada en el formulario) donde el usuario tendrá privilegios de administrador local y acceso remoto para la despliegue/cambio.

El comité evaluará el despliegue/cambio y en caso que detecte algún riesgo informará al solicitante para redefinir el cambio.

Responsabilidades:

En este escenario el solicitante es responsable del correcto funcionamiento de los servicios, software, aplicación, base de datos y sistema operativo, tienen la labor de revisar periódicamente que las actualizaciones del SO estén al día y que el antivirus esté activo (luz verde). Bajo ninguna circunstancia deberá bajar los servicios que vienen predefinidos en el template del servidor (agente fusion, agente wazuh, etc) .

2) Responsable de la Aplicación

El procedimiento para nuevo despliegue o cambio será:

1. Completar formulario de cambio F013.
2. Envía formulario al comité vía correo electrónico a lista.cambios@sanjuan.gob.ar como mínimo 48hs antes del cambio.

Al momento de recibir el formulario se habilitará una ventana de tiempo (especificada en el formulario) donde el usuario tendrá SFTP a la carpeta definida, para la despliegue/cambio.

El comité evaluará el despliegue/cambio y en caso que detecte algún riesgo informará al solicitante para redefinir el cambio.

Responsabilidades:

En este escenario el solicitante es responsable del correcto funcionamiento de los servicios, software, aplicación y base de datos.

El equipo de Ciberseguridad tiene que revisar periódicamente que las actualizaciones del SO estén al día y que el antivirus esté activo (luz verde). Al igual que el correcto funcionamiento de los servicios que vienen predefinidos en el template del servidor (agente fusion, agente wazuh, etc) .

3) Sin Acceso

Supuestos de los equipos de despliegue (metodología SCRUM):

a. Conformado por: 1 Ciberseguridad, 1 desarrollo, 1 base de datos, 1 Gobierno Abierto y 1 Scrum Master (DevOps).
b. Solo estos equipos tendrán acceso a la plataforma de producción (acceso a vmware y SO siempre por active directory). El permiso será de “operadores avanzados” tanto en los SO como en vmware.
c. Para compartir la documentación requerida se hará con nextcloud
d. Todos los servicios deben tener el modelo SW->BD

El procedimiento para nuevo despliegue o cambio será:

1. Se entregará al equipo de despliegue documentación sobre la aplicación/cambio, tecnología necesaria, recursos necesarios, archivos necesarios y el procedimiento explicado detalladamente para su despliegue. Esta documentación será entregada por el líder técnico de desarrolladores al SCRUM Master del equipo de despliegue.
2. El equipo de despliegue completará el formulario de cambio F013.
3. Envía formulario al comité vía correo electrónico a lista.cambios@sanjuan.gob.ar como mínimo 48hs antes del cambio.

Adjunto I - Formulario de Control de Cambios

GOBIERNO DE SAN JUAN | MINISTERIO DE HACIENDA Y FINANZAS | DIRECCIÓN DE CIBERSEGURIDAD

CONTROL DE CAMBIO

F 013

INFORMACIÓN DE CONTACTO

Nombre y Apellido _____ Fecha _____
Cargo _____ Área _____ Teléfono _____

DESCRIPCIÓN Y TIPO DE CAMBIO

Menor _____
Regular ☐ Implementación de una aplicación o producto ☐ Implementación de una versión nueva o cambio evolutivo
Sistema afectados _____ Fecha estimada del cambio _____

Descripción del cambio propuesto

Riesgos identificados _____
Impacto en las personas, los procesos o tecnológicos _____
Áreas o personas involucradas o afectadas por el cambio _____

PLAN DE IMPLEMENTACIÓN

Actividad _____
Responsable _____
Intervención o corte Fecha _____ Hora inicio ___:___ Hora final ___:___

PLAN DE PRUEBAS Y RECUPERACIÓN

Actividad _____
Responsable _____ Fecha _____

APROBACIÓN DEL CAMBIO

Quien lo aprueba _____ **Cargo y área** _____
Responsable del seguimiento _____ **Cargo y área** _____
Validación el cambio _____ **Cargo Ciberseguridad** _____

RESULTADO DEL CAMBIO

☐ **Positivo** ☐ **Negativo** **Fecha:** _____

Adjunto II – Diagrama Aprobación de Cambios