Auditoría Interna

Informe Definitivo

Gestión de cambios a infraestructura crítica

AIRI-16-2020

Julio, 2020

Tabla de Contenido

I. Resumen Ejecutivo

Objetivo General	Evaluar los cambios que se realizan a la infraestructura crítica de TI, con el fin de determinar si se cumple la normativa establecida y si se mitigan los riesgos que impactan la disponibilidad e integridad del entorno productivo del Banco.
Objetivos Específicos	✓ Evaluar la gestión de los componentes en los cambios de infraestructura crítica de TI, con el fin de determinar si se ejecutan en línea con lo planificado en la solicitud de cambio y si se mitigan los riesgos de afectación en el entorno productivo. ✓ Evaluar el proceso de planificación, priorización, categorización y autorización de cambios en infraestructuras críticas, con la finalidad de verificar si se ejecutan en línea con lo normado y si se gestionan los riesgos identificados sobre el impacto del cambio.
Alcance	Considera el seguimiento a la gestión de cambios de las infraestructuras críticas: Core de Comunicaciones (Nexus y Netscaler), Switch Transaccional, Web Transaccional y Active ID para el periodo de enero del 2019 al primer trimestre del 2020, ampliándose cuando fue requerido.
Comunicación verbal de los resultados	El pasado 6 de julio del 2020, se efectuó la reunión de discusión de los resultados del estudio con la participación de los siguientes funcionarios de la Administración: Pablo Navarro Cerdas, Asistente de la Dirección de Tecnología de Información, Jorge Mayorga Castillo, Jefe de la División de Control Operativo y Rene Quesada Oronó, Jefe del Área de Aseguramiento de la Calidad. Por su parte, la Auditoría Interna estuvo representada por: Edgar Bolaños Jara, Director de la Auditoría de Tecnología de Información, Gerardo Zúñiga Hernández, Supervisor de la Auditoría de Tecnología de Información y Noelia Machado Rodríguez, Auditora de TI asignada. Los puntos y recomendaciones que requirieron ajustes fueron realizados y se incorporaron.
Conclusión	Los controles implementados en la gestión de cambios a la infraestructura crítica del Banco no aseguran una efectiva mitigación de los riesgos asociados a la ejecución de cambios no autorizados o la ejecución de reimplementaciones que puedan afectar la disponibilidad e integridad de los sistemas, servicios o canales del Banco.

Se determina que los Gestores de Cambios del Área de Aseguramiento de la Calidad, actualmente ejecutan un rol pasivo en la planificación y ejecución de los cambios a componentes de infraestructura, lo que, aunado a la falta de una solución integral de gestión de la configuración, no asegura una adecuada trazabilidad de las actividades de un cambio, especialmente cuando se requiere activar planes de retorno, realizar varios pases a producción y atender incidentes relacionados con el cambio.

Por otra parte, un uso incorrecto de modalidades para la gestión de cambios que no están normadas impide una adecuada cobertura de riesgos asociados a la priorización y clasificación de cambios a componentes de infraestructura.

Finalmente, se determinó la necesidad de una coordinación más integral entre proveedores que gestionan infraestructura, fiscalizadores, personal de operaciones y gestores de cambio, con la finalidad de mitigar la ocurrencia de incidentes como los identificados en esta evaluación.

Calificación de riesgo y control

Muy bueno	Satisfactorio	Necesita Mejorar	Necesita mejorar significativamente	Insatisfactorio
		✓		

II. Resumen de hallazgos

Calificación de riesgo:	Alto	Medio	Bajo

Núm.	Hallazgo	Riesgo
1	Ausencia de controles para la gestión de cambios por terceros.	Medio
2	Falta de administración en el flujo de cambios.	Medio
3	Débil control integral de cambios de infraestructura crítica.	Medio
4	Falta de una línea base en la gestión de la infraestructura crítica.	Medio

III. Observaciones y Recomendaciones

1. Ausencia de controles para la Gestión de Cambios por Terceros.

No se determinó la existencia de controles sobre los cambios gestionados por terceros (proveedores) en infraestructura crítica del Banco, que permita minimizar cambios no autorizados. Al respecto, se identificaron las siguientes situaciones:

- **Cambios no registrados a nivel interno.** En la revisión efectuada a cambios realizados a componentes del core de comunicaciones, tales como el Netscaler y Nexus[1], no se evidenció una atención adecuada y controlada por parte del personal del Área de Aseguramiento de la Calidad, tampoco se lleva el registro en el Service Manager, según se muestra a continuación:

Consecutivo de RACSA	Nombre RFC-RACSA	Fechas propuestas	Elemento asociado
RFC473	Revisión de puertos en Nexus 7K-2 de Monte Popular	07-02-2019	NEXUS
RFC910	Cambio fuente de poder Nexus	19-10-2019	NEXUS
RFC1027	Integración del NODO 2 en Monte Piedad	25-01-2020	Balanceador/Netscaler
RFC1079	Migración Balanceadores	21-02-2020	Balanceador/Netscaler

Fuente: Herramienta ARANDA, reporteo del proveedor RACSA

[1] Nexus (switch core) corresponde a un dispositivo que permite la conexión de equipos y periféricos a la red para que puedan comunicarse entre las redes. Netscaler corresponde alBalanceo de cargas para gestionar la distribución del tráfico de internet o aplicaciones entre varios servidores.

- **Eventos no considerados cambios:** Se evidenciaron casos de mantenimiento y mejoras de componentes de la infraestructura crítica del Banco que no fueron tramitados como cambios ni registrados por los técnicos ni proveedores en los sistemas de control del Banco, incluso el personal con el rol de gestores de cambio no fue involucrado ni notificado. A continuación, se mencionan 2 casos:

  - ✓ El 05 de mayo 2020, se realizó un balanceo manual en el Netscaler para lograr una sincronización al activar nuevamente la opción de *Alta Disponibilidad* del ActivID[2], lo cual requirió una ventana de tiempo aproximada de 5 minutos. El único registro que se realizó fue la solicitud MA239471 del Área de Seguridad Operativa para que lo ejecutara el personal de Redes y Telecomunicaciones, sin la intervención de los gestores de cambios.

  - ✓ Entre febrero y marzo de 2019, el proveedor Grupo Babel realizó la migración de la Base de Datos de la web comercial a una granja de servidores para contar con alta disponibilidad, no obstante, el cambio se consideró como mejora y no se documentó como cambio.

Las situaciones señaladas anteriormente, se presentan debido a lo siguiente:

- Ausencia de normativa interna para fiscalizar la gestión del cambio de los componentes tecnológicos gestionados por proveedores.
- Poco involucramiento de los gestores de cambios del Área de Aseguramiento de la Calidad para ejercer acciones de: análisis, revisión y validación de cambios de terceros, más bien ha sido una responsabilidad que se ha delegado a la contraparte técnica interna del contrato.
- Los técnicos internos poseen un rol tanto de solicitante como ejecutor del cambio, es decir, no solo indican la necesidad del cambio son ellos mismos responsables de ejecutarlo a nivel de infraestructura.

Para mejorar la gestión de cambios, el **Marco de Trabajo de Referencia para el Gobierno y Administración de la Tecnología de Información Empresarial COBIT 5,** recomienda la siguiente práctica:

> **BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio**
> *Evaluar todas las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI, y analizar si el cambio afectará negativamente al entorno operativo e introducirá un riesgo inaceptable. Asegurar que los cambios son registrados, priorizados, categorizados, analizados, autorizados, planificados y programados.*

[2] Dispositivo de autenticación empleado para el control de acceso a la web transaccional y al App de Banca Móvil

Específicamente, la actividad No. 7:

> *Considerar el impacto en los proveedores de servicios contratados (ej. Procesamiento de negocio externalizado, infraestructuras, desarrollo de aplicaciones y servicios compartidos) en el proceso de gestión del cambio, incluyendo la integración de la gestión de cambios organizativos con los procesos de gestión de cambios de los proveedores de servicios y el impacto en términos contractuales y ANS's.*

La falta de controles efectivos sobre la gestión de cambios de infraestructura ha ocasionado la pérdida del control de versionamiento de los componentes tecnológicos y; por tanto, de la línea base para gestionar futuros cambios. Así mismo, esta situación genera un riesgo de aumento en la cantidad de reimplementaciones y dificulta la identificación de la causa raíz de incidentes.

Recomendación

Para: Dirección de Tecnología de Información

1. Realizar las acciones que corresponda para que los fiscalizadores que gestionan contratos que incluyen mantenimiento a componentes de infraestructura, coordinen con los gestores de cambio todas las actividades de mantenimiento preventivo y correctivo que impactan los servicios críticos del Banco, según los cronogramas de trabajo para tales actividades que presentan los proveedores, con el fin de que los gestores de cambio puedan realizar una planificación de los cambios y generar un accionar proactivo, verificando su registro en línea con la normativa de gestión de cambios.

Fecha cumplimiento: 31/10/2020 Nivel de Riesgo: Medio TR: CI

2. Falta de administración en el flujo de cambios.

En la evaluación al proceso de clasificación, priorización y documentación de los cambios a infraestructura, se determinaron las siguientes debilidades de control:

- **Falta de formalización de cambios por excepción:** La creación y registro de requerimientos de Alta Prioridad no forma parte de los tipos de cambio normados en el proceso de gestión de cambios, no obstante, según se determinó se está utilizando este mecanismo como una vía rápida para el Negocio y TI para realizar pases a producción.

  Se evidenció, además, que normalmente se abren requerimientos de Alta Prioridad para dar como resueltos incidentes, que según la normativa deben atenderse en un corto periodo de tiempo, a diferencia de los requerimientos (solicitudes de cambio), situación que causa una distorsión sobre los resultados de tiempos de atención de incidentes.

Por ejemplo, se identificó que para el Switch Transaccional, en el período de enero del 2019 a marzo del 2020, se han gestionado cambios para 8 requerimientos de alta prioridad, como medida para cumplir tiempos de resolución de incidentes y obtener un mayor de tiempo para encontrar una solución al evento. Como es el caso del SR2178819, que fue creado el 9 de agosto de 2019 asociado al incidente IR2178736 de la misma fecha. Sin embargo, el IR pasó a estado "resuelto" el 14 de agosto de 2019, y el cambio CR2194334 se pasó a producción hasta el 28 de agosto de 2019.

Por otra parte, se evidenció que se carece de un detalle de las aplicaciones cuyos cambios deben calificarse como pre-aprobados, lo que genera una vía para gestionar un cambio con menor cantidad de aprobaciones y por ende más expedito.

Por ejemplo, en el control de plataformas de seguridad informática que califican como pre-aprobados, se evidenció que no se detallan las plataformas específicas que serán sujetas a este tipo de cambios, tampoco se especifica si corresponde a una actualización, incremento o disminución de licencias, mantenimiento de componentes, activación de alta disponibilidad y cuál sería su nivel de afectación a los servicios en operación del Banco, solamente se hace mención de manera general a "Mantenimiento a plataformas administradas por Seguridad Informática". Esto incrementaría el riesgo que cambios con un mayor impacto pasen desapercibidos y no se gestionen adecuadamente los riesgos asociados.

- **Falta de revisión de Planes de Retorno (Rollback):** No se evidenció la realización de revisiones por parte de los gestores de calidad de los planes de retorno, que permita validar su usabilidad y si el nivel de detalle requerido de previo a la ejecución de un cambio en el ambiente productivo es suficiente.

  Los planes de retorno forman parte del proceso de gestión del cambio, para lograr un regreso al estado anterior y así evitar afectaciones en el ambiente productivo.

  Se identificó el caso de un cambio a la plataforma ActivID, donde el plan de retorno para el cambio CR2257149 en noviembre del 2019 se limitó a indicar "Contactar a soporte técnico del proveedor", sin desglosar los pasos, los responsables ni los tiempos requeridos para el retorno a la situación original. El cambio provocó un incidente de sincronización entre los servidores y hubo una baja de disponibilidad de los servicios de canales. Al respecto, el personal técnico del Área de Seguridad Operativa Informática indica que no fue necesario aplicar el plan de retorno al no darse una interrupción total del servicio.

  Otro caso identificado corresponde al cambio CR2219779 asociado al Netscaler, donde el pase a producción no fue exitoso y se requirió utilizar el Plan de Retorno, que consistía según la documentación en "Volver a instalar el equipo actual"; en este caso tampoco se enlistaron los pasos y componentes requeridos para el retorno y el responsable de ejecutarlo. En la aplicación del del rollback se originó

el incidente IR2239949 del 29-10-2019 que tuvo una afectación en distintos servicios y canales de aproximadamente de 17 minutos, de acuerdo con el reporte del proveedor RACSA.

- **Falta de gestión del periodo post-implementación:** No se evidenció acciones que permitan confirmar el cumplimiento de los resultados esperados del cambio ni las evaluaciones durante el periodo de garantía. El periodo de garantía se toma como un requisito como parte de la documentación de la gestión de cambios y no como un período para estabilizar la solución.

  Así, por ejemplo, al cambio en el ActivID CR2257149, se le asocia el incidente IR2259045 que fue ingresado el 22 de noviembre de 2019, un día siguiente al cambio. En este caso el incidente fue resuelto hasta el 11 de febrero de 2020; es decir, casi tres meses después, de su respectivo reporte; o sea, el periodo de garantía ya estaba vencido (abarcaba desde el 21/11/2019 hasta el 21/12/2019). Este incidente generó una degradación del servicio y eventos recurrentes en los cambios de contraseña de usuarios. La resolución fue atendida como parte del soporte y mantenimiento contractual con SISAP (No. 238-2016) y no se gestionó con un costo adicional.

Las situaciones anteriores, se derivan de un accionar limitado y reactivo por parte de los gestores de cambio, que se circunscriben al control de la documentación, sin tener una participación más activa en el proceso de cambio; aunado a la falta de recursos en el Área de Aseguramiento de la Calidad.

Al respecto, el **Marco de Trabajo de Referencia para el Gobierno y Administración de la Tecnología de Información Empresarial COBIT 5**, recomienda, la implementación de la siguiente práctica:

> ***BAI07.06 Pasar a producción y gestionar los lanzamientos***
> *Pasar la solución aceptada al negocio y las operaciones. Donde sea apropiado, ejecutar la solución como un proyecto piloto o en paralelo con la solución antigua durante un período de tiempo definido y comparar su comportamiento y resultados. Si se dieran problemas significativos, reinstaurar el entorno original de acuerdo al plan de marcha atrás o alternativo. Gestionar los lanzamientos de los componentes de la solución.*

También se asocia la siguiente práctica:

> ***BAI07.08. Ejecutar una revisión post-implementación***
> *Llevar a cabo una revisión post-implantación para confirmar salidas y resultados, identificar lecciones aprendidas y desarrollar un plan de acción. Evaluar y verificar el rendimiento actual y las salidas del servicio nuevo o modificado respecto al rendimiento y salidas previstas (es decir, el servicio esperado por el usuario o el cliente).*

Estas situaciones no permiten tener una visibilidad proactiva del impacto de la implementación del cambio y su posible afectación a la estabilidad del ambiente productivo. Esta gestión poco controlada no brinda garantía de que lo registrado en el cambio sea consecuente a la solución implementada y cumpla con las expectativas de las partes.

Recomendaciones

Para: Área de Aseguramiento de la Calidad

2. Definir e implementar dentro de los procedimientos de TI los lineamientos para la creación y atención de los requerimientos de Alta prioridad y su alineación con la gestión de incidentes y cambios.

Fecha cumplimiento: 31/10/2020	**Nivel de Riesgo: Medio**	**TR: CI**

3. Definir e incorporar controles para garantizar que, durante el periodo de post-implementación (garantía), se asegure la trazabilidad con incidentes o reimplementaciones relacionados al cambio.

Fecha cumplimiento: 31/10/2020	**Nivel de Riesgo: Medio**	**TR: CI**

4. Establecer un plan de mejora del catálogo de cambios pre-aprobados, donde se pueda identificar las plataformas y los tipos de cambio que les aplican.

Fecha cumplimiento: 31/10/2020	**Nivel de Riesgo: Medio**	**TR: CI**

5. Incorporar en los reportes trimestrales de la gestión de cambios, el detalle de los cambios no exitosos o reimplementaciones sobre la infraestructura crítica del Banco y el análisis de la causa raíz de posibles incidentes asociados.

Fecha cumplimiento: 31/10/2020	**Nivel de Riesgo: Medio**	**TR: CI**

6. Definir e incorporar en el proceso de cambios, las acciones de revisión y control de los Planes de Retorno, que permita evidenciar los pasos a seguir, tiempos, responsables y puntos de decisión de su aplicación; con el fin de asegurar su usabilidad con el personal técnico.

Fecha cumplimiento: 31/10/2020	**Nivel de Riesgo: Medio**	**TR: CI**

3. Débil control integral de cambios de infraestructura crítica.

Se determinó que el Área de Aseguramiento de la Calidad no posee controles integrales y automatizados que permitan llevar de manera completa el ciclo de vida del cambio. Al respecto, se identificaron las siguientes situaciones:

- **Débil control documental:** A falta de documentación, existe una dependencia del personal técnico para conocer en detalle el cambio y su respectiva implementación, de lo contrario, no es posible detallar las fechas en las cuales se ha reprogramado y planificado la puesta en producción. Se evidenciaron gestiones que no son adjuntadas en la aplicación Service Manager. Tal es el caso Netscaler-CR2219779; que el cambio continúa abierto después de más de 7 meses y no tiene asociado el incidente IR223921 producto del primer intento de implementación del cambio.

- **Incongruencia de registros de cambios:** La documentación del cambio se debe realizar por medio de la aplicación Service Manager, no obstante, se determinó que no todos los gestores de cambio utilizan esa herramienta, sino que llevan controles manuales en Excel, puesto que consideran que el Service Manager no les permite llevar un control adecuado; no obstante, tampoco se evidenció la existencia de gestiones por parte del Área de Aseguramiento de la Calidad para solicitar mejoras al Service Manager, o bien, la revisión de otras soluciones disponibles en el mercado.

  Por consiguiente, al comparar ambos controles, se evidenciaron incongruencias, en especial en cambios de infraestructura, ya que la plantilla en Excel está orientada a cambios de software aplicativo. La siguiente tabla muestra los cambios que solamente se registraron en el Service Manager, pero que no cuentan con trazabilidad por parte de los gestores de cambio:

RFC	SISTEMA O MODULO	Desc, Cambio o Sistema
CR2307004	Autoriza7	DCAL-0501-2018 implementar el cobro de comisiones "Surcharge" a clientes internacionales a través del switch transaccional de Autoriza 7
CR2219779	NETSCALER	Sustitución por renovación del Balanceador de Cargas Netscaler
CR2145600	Switch Transaccional	RQ de Alta Prioridad corrección en TRIAL BALANCE de ATMs por error en pgr y variables donde se ubican transacciones negadas con montos muy elevados
CR2321404	Switch Transaccional	instalación en Autorizador e inicio de aplicativo en Switch Transaccional
CR2154299	Switch Transaccional	DCNT-07799-2017- Convertir caracteres especiales que aparecen en los campos alfanuméricos DCNT-1138-2017 Proyecto CIC Registrar moneda de Origen

- **Falta de alineación de los riesgos del cambio**: En el registro de cambios de Infraestructura existe un apartado dedicado a los riesgos; sin embargo, estos no consideran factores relacionados con la criticidad del cambio, que permitan al gestor realizar una priorización y categorización adecuada del mismo.

Tal es el caso del cambio CR2049032 registrado para el Netscaler, donde en el apartado de Análisis de Impacto se documenta como riesgo "Personal Indispuesto" y no se hace referencia a otros riesgos asociados directamente con el cambio como el atraso del proyecto de actualización de T24 a la versión R17 en caso de no realizarse el cambio.

Las situaciones anteriores, se producen debido a la falta de una cultura documental, la poca explotación sobre herramientas o búsqueda de soluciones internas alternativas para el aprovechamiento de recursos. Además, de una visión limitada a la automatización de las actividades, y así mismo a un rol de gestor de cambios pasivo.

Como complemento de lo anterior, el Área de Aseguramiento de Calidad se ha visto afectada por la disminución del personal con el rol de gestor de cambios, ya que un recurso se acogió a su pensión en mayo 2020, y otro fue asignado a tiempo completo en el proyecto de migración a R17. Actualmente, se mantienen 2 recursos con el rol de gestor de cambios.

Sobre la definición e implementación de un control unificado de la gestión de cambios COBIT5 en el proceso

> ***BAI06.03 Hacer seguimiento e informar de cambios de estado***
> *Mantener un sistema de seguimiento e informe que documente los cambios rechazados, comunique el estado de cambios aprobados y en proceso y de cambios completados. Asegurar que los cambios aprobados son implementados como esté previsto.*

La ausencia de un control unificado y automatizado de la gestión de cambios ha generado dependencia al personal técnico interno, perdida de la trazabilidad del ciclo de vida del cambio y la materialización de eventos de interrupción o degradación de servicios y canales del Banco, al no contar con una visión completa del ámbito del cambio y su respectivo análisis.

Recomendaciones

Para: Área de Aseguramiento de la Calidad

7. Implementar un control integral de la gestión del cambio, que permita generar el histórico de un cambio desde su registro hasta su cierre, incluyendo reimplementaciones e incidentes asociados.

Fecha cumplimiento: 31/10/2020	**Nivel de Riesgo: Medio**	**TR: CI**

8. Realizar una revisión y actualización del apartado de riesgos de la solicitud de cambios a infraestructura, de manera tal que permita a los gestores de cambio realizar un análisis más efectivo sobre el impacto de un cambio y de esta manera priorizarlo y establecer medidas efectivas para la mitigación de un evento.

Fecha cumplimiento: 31/10/2020 Nivel de Riesgo: Medio TR: CI

4. Falta de una línea base en la gestión de la infraestructura crítica.

El Banco ha dedicado una inversión importante en equipos tecnológicos de última generación y ha invertido en contratos con terceros, sin embargo, no es posible asegurar el versionamiento de sus componentes ni el adecuado control de la configuración, tal y como se evidencia a continuación:

- **Inadecuado control para la gestión del versionamiento:** Actualmente, el intercambio de componentes o ejecutables se realiza por medio de carpetas compartidas entre el personal técnico y los gestores de cambio, sin que exista alguna validación de los componentes brindados contra lo establecido en el registro del cambio por parte de estos gestores.

- **Falta de soluciones integrales para la gestión de la configuración:** Cada área técnica, por medio de hojas de EXCEL, gestiona su propio control manual de la configuración sobre sus componentes tecnológicos, tales como aplicativos y base de datos. Por ello, no es posible visualizar de manera integral la relación entre componentes y sus interacciones o dependencias.

  El Área de Aseguramiento de la Calidad ha realizado esfuerzos desde el 2018 para adquirir e implementar una solución integral para la gestión de la configuración (CMDB[3]); sin embargo, no se ha concretado ni se han explorado herramientas internas del Banco como medida temporal.

Las situaciones señaladas anteriormente se presentan debido a lo siguiente:

- Falta de una visión estratégica y orientada a la Gestión del Ciclo de Vida de los Servicios Tecnológicos por parte de la Dirección de Tecnología de Información, ya que el accionar se ha enfocado en mantener el nivel operativo de los servicios.
- Por un rol pasivo del Área de Aseguramiento de la Calidad, que ha ocasionado que a la fecha no se cuenta con una justificación de la necesidad de adquirir una solución integral de gestión de la configuración; y por tanto, no ha sido una inversión que se visualice como estratégica para una correcta operación de TI, lo que ha impedido que se le asigne contenido presupuestario para su ejecución.

[3] CMDB Base de Datos de la Gestión de la Configuración y sus siglas en ingles CMDB. Es una base de datos que contiene detalles relevantes de componentes de configuración y la relación entre ellos ya sea incidentes, cambios, problemas y otros datos del servicio de tecnológico.

Sobre un adecuado control de la línea base y versionamiento, el **Marco de Trabajo de Referencia para el Gobierno y Administración de la Tecnología de Información Empresarial COBIT** 5, recomienda, la implementación de la siguiente práctica:

> ***BAI10.02 Establecer y mantener un repositorio de configuración y una base de referencia.***
> *Establecer y mantener un repositorio de gestión de la configuración y crear unas bases de referencia de configuración controladas.*
>
> ***BAI10.03 Mantener y controlar los elementos de configuración.***
> *Mantener un repositorio actualizado de elementos de configuración rellenado con los cambios.*

Específicamente, las siguientes actividades:

- *Identificar regularmente todos los cambios en los elementos de configuración.*
- *Revisar los cambios propuestos a los elementos de configuración respecto a la base de referencia para garantizar su integridad y precisión.*
- *Actualizar los detalles de configuración con los cambios aprobados a los elementos de configuración.*

Las situaciones señaladas anteriormente aumentan la dependencia sobre el personal técnico, limitan la capacidad de control sobre los efectos de un cambio en el ambiente productivo, lo que aumenta el riesgo de que se produzcan cambios no exitosos y con ello reimplementaciones que afectan la disponibilidad de servicios en el Banco y la oportunidad en la implementación de mejoras.

Recomendación

Para: División de Control Operativo

9. Realizar un caso de negocio para una solución de gestión de la configuración (CMDB), con el fin de determinar la factibilidad de su adquisición e implementación.

Fecha cumplimiento: 30/11/2020	**Nivel de Riesgo: Medio**	**TR: CI**

IV. Equipo de Auditoria

EDGAR BOLAÑOS JARA (FIRMA)
Firmado digitalmente por EDGAR BOLAÑOS JARA (FIRMA)
Fecha: 2020.07.10 14:14:26 -06'00'

Director

GERARDO ENRIQUE ZUÑIGA HERNANDEZ (FIRMA)
Firmado digitalmente por GERARDO ENRIQUE ZUÑIGA HERNANDEZ (FIRMA)
Fecha: 2020.07.10 09:38:52 -06'00'

Auditor Supervisor

NOELIA PATRICIA MACHADO RODRIGUEZ (FIRMA)
Firmado digitalmente por NOELIA PATRICIA MACHADO RODRIGUEZ (FIRMA)
Fecha: 2020.07.10 09:08:45 -06'00'

Auditora Encargada

Anexo:

AIRI-16-2020 Minuta discusión.pc