# ANÁLISIS DE PROYECTO DE IMPLANTACIÓN DE SOFTWARE FRENTE A LOS DOMINIOS DEL MARCO DE TRABAJO COBIT

Sánchez, David.
davids911@gmail.com
Universidad Piloto de Colombia

***Abstract***: This document aims to build an approachment of an application of control for the risk management, provided by the COBIT framework, applicable for management of consulting projects, software development, set up, and releasement, in a financial related company.

***Key words***: Risk management, IT governance, software implantation, framework.

***Resumen***: El presente documento busca hacer un acercamiento a la aplicación de los controles para la gestión del riesgo provistos por el marco de trabajo COBIT 4.1 y que sean aplicables para la administración de proyectos de consultoría, desarrollo e implantación de software en una compañía perteneciente al sector financiero.

***Índice de términos***: Gestión del riesgo, gobierno de TI, Implantación de software, marco de trabajo.

## I. INTRODUCCIÓN

COBIT es una guía de mejores prácticas o marco de trabajo que cuenta con aceptación internacional y está enfocado hacia la investigación y desarrollo de un marco de control del gobierno de tecnologías de la información o TI.

El presente análisis pretende identificar los posibles fallos cometidos al interior de la compañía durante la ejecución de un proyecto de implantación de software y migración de datos, usando para ello el marco de trabajo COBIT en su versión 4.1, el cual encaminará a la compañía y al proyecto a una planeación que garantice el logro de los objetivos, siendo esto posible por la naturaleza misma del marco de trabajo mencionado, el cual está orientado al negocio, a procesos, basado en controles e impulsado por mediciones. Dichas mediciones ayudarían a detectar cambios en las necesidades del negocio, las cuales podrían ser atendidas de manera oportuna sin afectar el desarrollo efectivo del proyecto.

## II. ANTECEDENTES

La compañía a la cual se le efectúa el presente análisis pertenece al sector financiero y es una de las más importantes del país. En años anteriores gestionaba su portafolio de inversiones mediante el uso de hojas de cálculo y un par de sistemas de origen nacional y el otro internacional.

Recientemente las empresas del sector comenzaron a actualizar gradualmente sus sistemas a plataformas más robustas de origen internacional que les permiten entrar a competir más fuertemente en otros mercados con los productos estandarizados que allí se tranzan y que en Colombia son bastante particulares. El mismo caso se presentó en la compañía, la cual decidió después de un estudio de las opciones disponibles en el mercado, actualizar su sistema adquirido años atrás y hacía tiempo había dejado de recibir soporte por parte del proveedor. Las razones principales para la selección de esta herramienta y este proveedor son las siguientes: familiaridad del banco con herramienta, experiencia en el uso de la misma, el prestigio del proveedor y la presencia en la ciudad de socios estratégicos con conocimiento de su producto, lo que facilitaría en gran medida la adaptación del sistema a la normatividad

del mercado colombiano.

El proyecto se planteó para ser ejecutado en varias fases. La primera de ellas consistía en la implantación del nuevo sistema adquirido por la compañía, seguido de labores de pruebas y adaptación del sistema a los procesos de la compañía, la migración de los productos desde hojas de cálculo y versión anterior del sistema, la salida a producción y finalmente la etapa de acompañamiento y soporte de producción. Esta primera fase se planeó para poco menos de un año, pero por varias complicaciones y sucesivos cambios en el alcance y sobre la marcha, terminó por extenderse por más de tres años, aumentando el costo del proyecto y llegando incluso a forzar la salida de uno de los proveedores de consultoría, encargado del levantamiento de requerimientos funcionales, el cual no obtuvo la rentabilidad esperada por el tipo de contrato realizado inicialmente con la compañía para la ejecución de dicho proyecto.

Actualmente el proyecto se encuentra en la etapa planeación de la segunda fase, la cual consistirá en un *upgrade* o actualización del sistema, la migración de datos de nuevos productos administrados desde hojas de cálculo y desde un sistema conocido de origen colombiano.

Hasta el momento se han empezado a definir los requerimientos de infraestructura y las principales tareas del proyecto. Se han realizado algunas pruebas de conceptos y se han evaluado herramientas para la transformación y migración de datos.

Con la experiencia obtenida en la fase anterior, la compañía busca generar un cronograma y un presupuesto más acertado y por consiguiente lograr desarrollar el resto del proyecto más eficientemente. Es por esto que se ha decidido realizar el presente estudio de la metodología del proyecto respecto al marco de trabajo COBIT para identificar de forma clara los errores que se han venido cometiendo y generar así recomendaciones que ayuden a mejorar la gestión y su desarrollo, evitando que se vuelvan a cometer los mismos errores del pasado.

## III. ANÁLISIS DEL PROYECTO FRENTE A LOS DOMINIOS DE COBIT

### *A. Planear y Organizar*

Este dominio propone realizar la alineación estratégica de TI y el negocio, así como también lograr la correcta administración y óptimo uso de los recursos para prestar servicios con la calidad apropiada de acuerdo con las necesidades del negocio.

1) *Definir un plan estratégico de TI:* Se dio inicio a la planeación del proyecto a partir de una decisión de la gerencia y no se conocen planes ni prioridades de TI. De igual forma, no se cuenta con resultados de alguna evaluación de desempeño y capacidades actuales del sistema. Lo anterior hace inferir que no existe alineación estratégica de TI con el negocio y por lo tanto sería recomendable definir un plan estratégico para éste.

2) *Definir la arquitectura de la información:* Se cuenta actualmente con una rigurosa clasificación y control de acceso a la información, así como un sistema documental que garantiza la uniformidad de la información recibida y generada desde las diferentes áreas involucradas en el proyecto. Lo anterior indica que se definió acertadamente la arquitectura de la información.

3) *Determinar la dirección tecnológica:* Existe actualmente un plan para fortalecer la arquitectura tecnológica existente como respuesta a requerimientos de la compañía que se encaminan hacia el aumento del número de servicios a prestar por el sistema y al proceso de migración que está

por adelantarse. El sistema de información adquirido, adopta estándares internacionales, lo cual brinda la seguridad de que con la ayuda de modificaciones *in-house* cumplirá también con los estándares tecnológicos locales y se podrá adaptar en un tiempo aceptable a los nuevos requerimientos y regulaciones futuras debido a un marco de trabajo propio del sistema que permite su adaptación a las necesidades de la compañía.

4) *Definir los procesos, organización y relaciones de TI:* Aunque el proyecto se encuentra en una fase incipiente, se cuenta con los recursos y la definición de los roles a ser desempeñados por los miembros del equipo de proyecto. No se definen roles para administrar riesgos de TI y se presenta una dependencia del personal técnico, por lo que sería recomendable asignar recursos adicionales para la debida segregación de funciones.

5) *Administrar la inversión en TI:* Existe un marco de trabajo para la administración financiera que evalúa los costos de acuerdo con el cronograma del proyecto y gestiona las contrataciones y asignación del personal al proyecto. Sin embargo, no hay actividades de monitoreo que apoyen la administración de costos de TI, lo cual lo expone a problemas de sobrecostos al no realizarse a tiempo las actividades del proceso presupuestal.

6) *Comunicar las aspiraciones y la dirección de la gerencia:* Aunque dentro del proyecto se hace énfasis en el cumplimiento de las políticas y reglamentos, se falla al momento de comunicar las nuevas aspiraciones y direcciones de la gerencia luego de haberlas definido o modificado en reuniones en las cuales no se encuentra todo el personal relevante y omitiendo el uso de medios de comunicación para informarlos y dejando el proceso de divulgación en manos de los asistentes.

7) *Administrar los recursos humanos de TI:* Aunque este proceso se encuentra bien definido respecto al reclutamiento de personal competente, la correcta asignación de roles y un adecuado entrenamiento al personal de TI. Se presentan problemas respecto a la rotación del personal de TI y demoras en la eliminación de privilegios de acceso aún cuando se reporta de manera oportuna la desvinculación de algún miembro del equipo de proyecto.

8) *Administrar la calidad:* Aparte de un procedimiento definido para la gestión de requerimientos, no se sigue un estándar de desarrollo, no existe monitoreo de la calidad ni un plan de mejora continua. Se deja a criterio del líder de cada proceso la selección de las prácticas a seguir para el aseguramiento de la calidad.

9) *Evaluar y administrar riesgos de TI:* No hay en el proyecto un marco de trabajo de administración de riesgos de TI que se alinee a la gestión de riesgos de la organización. No existen planes de acción de riesgos ni de evaluación de estos. Lo anterior supone que el proyecto puede estar expuesto a riesgos desconocidos a los cuales no se les podría dar respuesta oportuna y causarían tropiezos en la ejecución y gastos importantes a la organización.

10) *Administrar proyectos:* Si bien este proceso se encuentra bien definido, presenta fallas a nivel de la declaración del alcance del proyecto, la cual no es bien controlada y no está en completa sintonía con el proceso de control de cambios, afectando finalmente variables como costos, cronograma y calidad. Lo anterior dificulta el cierre del proyecto y lo llevaría a prolongarse por largo tiempo antes de darlo por finalizado.

*B. Adquirir e Implementar*

Este dominio busca controlar la integración de nuevas soluciones de TI, modificarlas y dar soporte a las existentes.

Pretende lograr que dichas soluciones satisfagan las necesidades del negocio dentro del tiempo y dentro del presupuesto del proyecto, con la calidad esperada y sin afectar la operación actual del negocio.

1) *Identificar soluciones automatizadas:* Dado que se trata de un sistema ya adquirido, se realizan pruebas de concepto de los procesos de negocio que serán soportados por la aplicación y los que deben convertirse en requerimientos a ser desarrollados para llegar a ser soportados por la plataforma.

Se definen requerimientos técnicos y funcionales del negocio, pero no se realizan análisis de riesgos asociados a los mismos.

2) *Adquirir y mantener software aplicativo:* No existe de momento un plan para aseguramiento de la calidad del software, así como tampoco auditoría de las aplicaciones.

El proceso de desarrollo consiste en el levantamiento de la información, la especificación, la estimación (diseño de alto nivel), la aprobación, el análisis y diseño detallado, la codificación, las pruebas unitarias, la certificación y paso a producción. Aunque en ocasiones se involucra al usuario final en la etapa de certificación, existe el riesgo de que el resultado final no sea el deseado, esto implica un reprocesamiento importante al tener que volver a las etapas iniciales de la cadena de desarrollo. También existe el riesgo de que llegue a producción un requerimiento que cause insatisfacción por parte de los usuarios.

3) *Adquirir e implementar infraestructura tecnológica:* Existe actualmente el plan para adquisición y mantenimiento de infraestructura tecnológica. También se siguen estrategias de mantenimiento y existen ambientes de pruebas y de desarrollo en los cuales se realizan pruebas de desempeño ante cambios importantes en la infraestructura.

4) *Facilitar la operación y el uso:* Se realizan capacitaciones al personal de TI cada vez que se presentan cambios importantes a nivel de servicios e infraestructura, sin embargo, no es común que se presenten capacitaciones o entrenamiento a los usuarios finales como medida de transferencia de conocimiento, salvo si se incluyen cambios de índole normativo que afectan a la totalidad de los usuarios y las gerencias correspondientes son conscientes de la necesidad de capacitar al personal.

5) *Adquirir recursos de TI:* Hay satisfacción con los proveedores actuales y con los procesos seguidos por estos para la adquisición de hardware y software requeridos. Los procesos de adquisición de TI cubren las necesidades actuales del proyecto, pero en ocasiones presentan demoras debido a la rigurosidad de los mismos.

6) *Administrar cambios:* Se siguen procedimientos claros para la administración de cambios, apoyados con herramientas para el control de estados de los requerimientos e incidentes. Los requerimientos son categorizados y priorizados de acuerdo con su naturaleza. Se realiza auditoría sobre la documentación entregada en cada caso, pero se carece de un repositorio o manual general en donde se incluyan todos los cambios y los ajustes sobre la funcionalidad del sistema.

En ocasiones pasan a producción cambios de emergencia sin seguir estrictamente los procedimientos establecidos, pero se cumple posteriormente con la documentación requerida. Para estos casos se solicita siempre aprobación de nivel superior.

7) *Instalar y acreditar soluciones y cambios:* Quienes reciben los requerimientos del usuario y elaboran las especificaciones correspondientes son personas que comprenden los procesos

del negocio, pero que carecen de experiencia en metodologías de pruebas.

Se cuenta con ambientes y planes de prueba, pero no siempre se cuenta con planes de "vuelta atrás" luego de implantaciones fallidas.

Se presentan en ocasiones pruebas de aceptación por parte de los usuarios finales y se deja bajo la responsabilidad de los desarrolladores la seguridad y el desempeño de los cambios. Normalmente no se realizan revisiones posteriores a la implantación de los cambios en producción.

*C. Entregar y dar soporte*

Este dominio tiene por objetivo garantizar la entrega real de de los servicios requeridos de acuerdo con la prioridad del negocio, así como la administración de la seguridad y el apoyo a los usuarios de dichos servicios.

1) *Definir y administrar niveles de servicio:* Existe definición de niveles de servicios en el grupo de soporte con el fin de priorizar y optimizar los tiempos de respuesta a los usuarios, pero aunque se definen acuerdos de niveles de servicios para los proveedores internos y externos que participan en el proceso de desarrollo; estos no son monitoreados constantemente y son sólo evaluados cuando se presentan inconformidades con algún proveedor. La priorización de requerimientos e incidencias se realiza de acuerdo con los niveles definidos de "severidad", pero no hay un proceso definido para la asignación de esta calificación y la mayoría de los requerimientos son creados con calificación 4/5 "urgente". Solo se tiene claro la asignación del nivel 5/5 "crítico" para eventos que afectan la disponibilidad de producción.

2) *Administrar servicios de terceros:* Existe una definición clara de los roles y responsabilidades de los proveedores incluidos en el proyecto. La compañía se involucra en los procesos de contratación y de asignación de nuevos recursos de los proveedores dentro de él y se realizan acuerdos de confidencialidad con el proveedor, aunque no con cada miembro del sus respectivos equipos de trabajo. Por tratarse de proveedores que cuentan con confianza y larga relación con la compañía, no se monitorea muy a menudo el desempeño de los mismos respecto a los acuerdos de niveles de servicios.

3) *Garantizar la continuidad del servicio:* Tecnológicamente se siguen ciertos controles de seguridad para garantizar la continuidad del servicio tales como copias de respaldo periódicas, ambientes de contingencia, instalaciones alternas en caso de necesidad de re-localización, etc. Dichos controles podrían ser adecuados para ciertos eventos de seguridad, pero en algunas ocasiones actividades como la instalación de parches de sistema operativo o de bases de datos han terminado por dejar el sistema fuera de funcionamiento por largo tiempo, ocasionando pérdidas importantes para la compañía y malestar general entre los usuarios.

No se conoce dentro del proyecto planes de continuidad de TI y no se ha participado en pruebas o entrenamientos de planes de continuidad.

4) *Garantizar la seguridad de los sistemas:* El proceso de administración de la identidad está presente para usuarios internos, externos y temporales, la administración de cuentas de usuario siguen el procedimiento definido por la gerencia de cuentas de usuario, el monitoreo de las cuentas de usuario y la información que entra y sale de sus respectivas cuentas de correo es monitoreada por un sistema automatizado que impide la comunicación con cuentas externas y la transmisión de datos sensibles. Se realiza el bloqueo de medios de almacenamiento externo y filtrado web por reglas de firewall, impidiendo también

el acceso a servicios de almacenamiento en línea, email en la web, etc.

5) *Identificar y asignar costos:* La distribución de los costos de mantenimiento e inversión de TI se distribuyen entre diferentes centros de costos de acuerdo con la política existente en la compañía, la cual determina cómo distribuir los costos fijos de los servicios. Aparte de lo anterior, se desconocen los procesos de contabilización de TI y si existe modelado de costos y cargos.

6) *Educar y entrenar a los usuarios:* No se sigue un programa de entrenamiento formal para los miembros entrantes del proyecto sino que se opta por un periodo de autoaprendizaje mediante la lectura de manuales, seguido de trabajo guiado o coaching. No sucede igual con los usuarios finales, los cuales sí son capacitados para el uso de las herramientas y sobre los procesos que deberán seguir.

7) *Administración de la mesa de servicio y los incidentes:* Está presente dentro del proyecto la función de mesa de servicio, la cual atiende las consultas o llamadas de los usuarios y presta atención inmediata a sus necesidades. La mesa de servicio cuenta con niveles de servicio y procedimientos para el escalamiento a través del reporte de casos o incidencias, los cuales serán recibidos inicialmente por el grupo de TI. En la actualidad se realizan análisis del volumen semanal de consultas recibidas y resueltas por la mesa, pero no se miden los niveles de satisfacción del usuario ni los índices de abandono de llamadas.

8) *Administración de la configuración:* No se cuenta con un repositorio que contenga una línea base de configuración, sino que cada entrega de requerimiento que contenga configuración se hace con un manual específico para el componente desarrollado. De igual manera, no hay un procedimiento para la identificación de elementos de configuración y ésta se controla únicamente mediante los formatos de registro y solicitud de configuración. No se revisa periódicamente la integridad de la configuración, salvo en las ocasiones en las que se reporta un fallo en producción y se solicita formalmente detalles de la configuración para ser verificada.

9) *Administración de problemas:* Desde la mesa de soporte se realiza la clasificación e identificación de problemas. Actualmente se cuenta con flujos de trabajo definidos para el análisis y solución de incidentes que llevan a los equipos de trabajo a identificar las causas de los problemas para seguir con su solución definitiva. Se acuerda realizar los cierres de los incidentes reportados luego de certificar la validez de las soluciones definitivas o alternativas.

En la actualidad no se hacen de manera formal seguimientos de tendencias de las incidencias.

10) *Administración de datos:* Siguiendo la política de seguridad de la compañía, se cuenta con planes de respaldo y restauración, así como acuerdos respecto a los tiempos de retención y eliminación de copias de respaldo.

No se siguen procedimientos de prueba de copias de respaldo, pero hasta el momento han sido exitosos cada vez que se han solicitado restauraciones como parte de planes de pruebas.

11) *Administración del ambiente físico:* Las instalaciones están equipadas con sensores de humo, cámaras de seguridad, dispositivos de control de acceso y brigadistas capacitados. Los niveles y áreas de acceso son asignados a cada funcionario al momento de su ingreso a la organización. Se cuenta con centros de datos dentro y fuera de la ciudad, así como plantas alternas asignadas para cada área en las que podrían retomar sus actividades en caso de factores ambientales que impidan el uso de las instalaciones.

12) *Administración de operaciones:* Se siguen procedimientos para el mantenimiento de los equipos e instalaciones periódicas y realizadas durante fines de semana para evitar la afectación de los niveles de servicio, sin embargo en ocasiones se presentan incidentes relacionados con fallos que ponen fuera de línea a algunos sistemas y están relacionados con fallos en equipos de red.

*D. Monitorear y Evaluar*

Este dominio tiene como objetivo monitorear los controles existentes en busca de evaluar su efectividad respecto al cumplimiento regulatorio, las directivas y las políticas de la organización.

1) *Monitorear y evaluar el desempeño de TI:* No se realizan procedimientos de monitoreo y evaluación del desempeño de TI al interior del proyecto, sin embargo se reciben reportes ocasionales desde otras áreas respecto a temas de seguridad de la información y éstos son evaluados en reuniones dentro del proyecto para determinar el manejo que debe ser dado a las diferentes situaciones reportadas.

2) *Monitorear y evaluar el control interno:* No se emplea al interior del proyecto ningún marco de trabajo de control interno relacionado con TI, auditorías ni auto evaluaciones, aunque sí se controlan las obligaciones contractuales de terceros, así como sus obligaciones legales y regulatorias.

3) *Garantizar el cumplimiento con requerimientos externos:* La organización recibe y distribuye a la totalidad de las áreas interesadas, las notificaciones recibidas por parte de los entes regulatorios y gubernamentales para que sean evaluados por todos y definan la responsabilidad y las necesidades de cada una, frente a los ajustes a las políticas, estándares, procedimientos y metodologías necesarios para garantizar el cumplimiento de los requerimientos legales, regulatorios y o contractuales adquiridos. Es de aclarar que en la compañía y en el proyecto, la prioridad es tramitar con la máxima prioridad y a la mayor brevedad, todos los requerimientos legales y normativos exigidos por los entes reguladores.

4) *Proporcionar gobierno de TI:* Desde la óptica del proyecto, no es completamente visible la figura del gobierno de TI de la organización. Su soporte en las actividades del proyecto y en la asignación de los recursos es evidente, su entrega de valor es innegable y su nivel de cumplimiento respecto al proyecto es satisfactorio, sin embargo no se pueden apreciar los resultados del proceso de administración de riesgos.

## IV. CONCLUSIONES

Partiendo del conocimiento que se tiene de la constitución del proyecto y su etapa de planeación, se pueden apreciar fallas en la declaración de los alcances y en la falta de aprobación expresa de las partes interesadas. Lo anterior en conjunto con una adecuada gestión de control de cambios a los alcances del proyecto, habría sido suficiente para acortar los tiempos requeridos en su fase inicial y darle el cierre tempranamente para continuar con la siguiente fase.

Luego de analizar la metodología del proyecto frente a cada uno de los dominios de aportados por COBIT, se llega a varias recomendaciones, las cuales seguramente resultarían en caso de ser adoptadas en mejoras como la planeación más acertada del proyecto, reducción de costos y disminución en los tiempos de ejecución.

Es recomendable definir un plan estratégico de TI que encamine hacia la alineación estratégica del mismo con el proyecto y con el negocio. La exclusión de TI desde la definición del proyecto, la

selección del producto a ser adquirido y la especificación de requerimientos y servicios incluidos hasta ahora y entregados a TI, no permitieron que los procesos administrativos de TI dimensionaran los recursos requeridos por la aplicación, la arquitectura adecuada para su óptimo funcionamiento. Tampoco se integraron adecuadamente los nuevos procesos para administrar la nueva plataforma independientemente de otros productos y ésto seguramente ocasionaba eventos que atentaban contra la disponibilidad del sistema luego de su salida a producción.

Se recomienda definir al menos un miembro del proyecto que asuma el rol de la administración de riesgos de TI, dado que aunque existe el área de seguridad de la información en la compañía, se requiere de un enlace directo al interior del proyecto para canalización adecuada de sus directivas y recomendaciones.

Es necesario que desde los altos mandos del proyecto hasta los líderes y funcionarios se hagan conscientes de los riesgos presentes en el proyecto y aporten su empeño a la mitigación de los mismos y a la identificación y reporte de nuevos riesgos a la gerencia de gestión de riesgos, la cual debería participar activamente en el proyecto realizando evaluaciones de riesgos sobre los activos del proyecto y diseñando para ello planes de evaluación y de acción ante riesgos identificados.

Es recomendable implementar un plan de gestión de las comunicaciones y de los interesados para transmitir las nuevas aspiraciones y direcciones de la gerencia respecto al proyecto a todas las personas consideradas relevantes para recibir dicha información.

Se debe realizar análisis de riesgos a los requerimientos desde su etapa de análisis para evitar que eventos inesperados ocurran más adelante y se obliguen a realizar re-procesamientos costosos, así como pasos a producción con fallos que pudieran haber sido detectados con antelación. Para esto también se recomienda capacitar al personal encargado de las pruebas, en metodologías de pruebas para lograr enviar a producción desarrollos sin problemas que afecten la operativa, generen molestia entre los usuarios y por el contrario, aumenten su confianza y su satisfacción con el servicio a la vez que se logre disminuir los posibles niveles de resistencia al cambio presentes en este tipo de proyectos.

Es necesario incluir al usuario final en el proceso de certificación y aceptación de los desarrollos con el fin de evitar hasta el último momento que sean enviadas a producción soluciones inesperadas o inadecuadas, puesto que es muy costoso y delicado tener que hacer desmonte de desarrollos y configuraciones del ambiente de producción. Además de esto, se tendrían soportes de la aceptación de todos los desarrollos realizados y se podría hacer cierre de las fases del proyecto en el momento adecuado, una vez se completen todos los objetivos acordados dentro del alcance.

Dentro del plan de comunicación se debería informar a todas las áreas usuarias de la aplicación acerca de las funcionales que serán enviadas en cada periodo a producción, con el fin de que puedan detectar cualquier conflicto entre sus procesos y los de otras áreas. De igual manera, se deberán citar periódicamente a los usuarios que serán afectados por alguna nueva funcionalidad, para que sean debidamente capacitados y evitar picos en el reporte de consultas que afecten el desempeño de la mesa de servicio.

Con cada desarrollo o configuración enviada a producción, debería enviarse un plan de desmonte o marcha atrás que asegure que el ambiente de producción pueda ser regresado rápidamente a su

estado original en caso de fallos. Adicionalmente se deberían realizar planes de revisión funcional posteriores a la implantación de requerimientos, para garantizar que el sistema estará disponible para los usuarios.

Es importante realizar el monitoreo constante de los niveles de cumplimiento de los acuerdos de niveles de servicios de los terceros para asegurarse de que están teniendo el desempeño adecuado y de que se esté cumpliendo con el cronograma del proyecto.

TI no debe operar independientemente del proyecto y debería seguir un plan de continuidad que evite las interrupciones a los servicios. Para ésto es necesario que TI sea informada de todos los componentes de la arquitectura que tienen relación con el proyecto y sobre los cuales deberían reportar oportunamente cuando se planee hacer mantenimientos e instalación de parches. Sabiendo ésto se podrían programar primero dichas actividades en los ambientes de pruebas de la aplicación para detectar oportunamente fallos que de otra forma podrían golpear inesperadamente al sistema en producción.

Es importante que se incluyan las configuraciones del sistema en la línea base para que ésta pueda ser controlada adecuadamente.

Se deben seguir planes de pruebas de copias de respaldo por parte de TI para evitar que estos puedan fallar en el evento en el que se necesiten.

Para una compañía del sector financiero, su portafolio de inversiones debería estar disponible en todo momento, es por ésto que es absolutamente necesario realizar evaluaciones periódicas de los riesgos sobre los activos de red requeridos para la operación del sistema, puesto que las caídas del servicio aunque sean ocasionales, tienen un impacto económico negativo para la organización.

## REFERENCIAS

[1] IT Governance Institute, “The COBIT 4.1 framework specification”, 3701 Algonquin Road, Suite 1010, 2007.

[2] Villamizar Carlos, *Fundamentos de CobiT Presentation*, cvillamizar@globalsuite.es, Bogotá, 2015.