Banco Hipotecario de la Vivienda

Informe Final TI-OP-001-2018

AUDITORÍA SOBRE LA ADMINISTRACIÓN DEL ÁREA DE DESARROLLO DE TI

08/03/2019

RESUMEN EJECUTIVO

En esta auditoria se evaluaron algunos de los controles relacionados con la administración y el seguimiento que se ejecuta sobre los requerimientos de los sistemas de información efectuados por los usuarios finales, como parte del mantenimiento de sistemas que realiza el Departamento de Tecnologías de Información.

Dentro de los hallazgos se localizó una limitada administración y control sobre los requerimientos que se realizan como parte del mantenimiento de las aplicaciones vigentes; esto debido a que las herramientas tecnológicas institucionales no lo permiten.

También se encontró una debilidad relacionada con los lapsos estipulados por los analistas encargados de los mantenimientos de sistemas, al no estar establecido alguna contraparte técnica que valore dichos tiempos.

Otro de los hallazgos está vinculado con la limitación que tienen los dueños o encargados de los sistemas informáticos del Banco, al no contar con los insumos que les permitan llevar un control sobre todos los requerimientos de sus sistemas que están siendo ejecutados por el área de Mantenimiento.

Adicionalmente, se encontró una debilidad relacionada con la trazabilidad del tiempo que se le pueda dar a cada estado en que se encuentre un requerimiento, tales como asignados, detenidos, en atención, entre otros.

Los detalles de cada aspecto indicado en los párrafos anteriores, son ampliados a lo largo de este documento.

INDICE

AUDITORÍA SOBRE LA ADMINISTRACIÓN DEL ÁREA DE DESARROLLO DE TI

1. INTRODUCCIÓN

1.1 Justificación de la auditoría

Este estudio forma parte del Plan Anual de Trabajo de esta Auditoría Interna para el año 2018 y está fundamentado en el Artículo 31 de la Ley 7052 del Sistema Financiero Nacional para la Vivienda, en el Artículo 22 de la Ley 8292, Ley General de Control Interno, en los cuales se establece que la Auditoría Interna deberá velar y fiscalizar el uso adecuado de los recursos del BANHVI.

1.2 Objetivo

Evaluar la gestión realizada por el área de Desarrollo y Mantenimiento de Sistemas sobre los requerimientos a las aplicaciones Institucionales.

1.3 Alcance

El estudio abarcó la documentación, información y procesos operativos vigentes al 31 de Diciembre del 2018 relacionados con la administración y el uso del sistema indicado.

1.4 Metodología de Trabajo

Se aplicó la metodología establecida en el Manual para el ejercicio de la práctica de la Auditoría Interna. Además, se aplicó el Manual de Normas Generales de Auditoría para el Sector Público emitido por la División de Fiscalización Operativa y Evaluativa. Otras normas y estándares utilizados fueron:

- ✓ Reglamento SUGEF 14-17 – COBIT 5
- ✓ Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).
- ✓ Ley General de Control Interno.
- ✓ Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE).
- ✓ Normas Generales de Auditoria para el Sector Publico

- ✓ Normativa Interna vigente (Metodología – Manuales- Políticas – Procedimientos)
- ✓ Norma 308 Comunicación de resultados.
- ✓ ISO/IEC 27002:2016 Tecnologías de la información – Código de buenas prácticas para controles de seguridad de la información

Además, se aplicaron técnicas de auditoría comúnmente aceptadas como entrevistas, revisión documental de la gestión administrativa y visitas de campo para la verificación del control interno.

Específicamente se ejecutaron entrevistas con los funcionarios que tienen relación directa con la administración y control del área de Desarrollo y Mantenimiento de Sistemas de Información. Adicional se evaluó la existencia y razonabilidad de la documentación formal y procesos establecidos sobre dicho proceso.

Los resultados de las pruebas ejecutadas y demás documentos que respaldan el trabajo realizado, se mantienen como papeles de trabajo en el expediente electrónico de la Auditoria Interna. Las deficiencias detectadas, tanto en aspectos de control interno como operativas, de la presente revisión, se detallan en la siguiente sección de Resultados de la Evaluación.

2. RESULTADOS DE LA EVALUACIÓN

2.1 Administración sobre los requerimientos de sistemas de información

La mayoría de sistemas de información con los que cuenta la Institución, deben llevar un proceso de mantenimiento, el cual consiste ya sea en solucionar algún problema que se presente en las aplicaciones o en desarrollar un nuevo requerimiento que surja por la operativa diaria de cada área. Para esto y de acuerdo al procedimiento P-DTI-AI2-002 "*Mantenimiento de Sistemas*", se utiliza en el Banco la herramienta de la Mesa de Servicio, donde se detallan las necesidades correspondientes de los usuarios y una vez que es tomada por el área de Desarrollo y Mantenimiento, es delegada al funcionario de TI que le brinda mantenimiento a dicha aplicación. En este punto, cada necesidad es puesta en una cola de requerimientos previos que administra cada desarrollador (en el software llamado Project Manager) y seguidamente ellos mismos establecen el tiempo probable que podrían tardar en su ejecución, así como las fechas de finalización correspondientes.

De acuerdo a lo detallado en el párrafo anterior y a la información evaluada, se encontró que el sistema de la Mesa de Servicio no es lo suficientemente robusto para centralizar y administrar completamente todos los requerimientos efectuados a los sistemas institucionales, sino que básicamente se utiliza como un repositorio para que el usuario incluya sus necesidades; siendo necesario utilizar otras herramientas para tratar de llevar al menos un orden en prioridades, tiempo y ejecución de cada requerimiento que llegue al área de Desarrollo y Mantenimiento.

Adicionalmente, no se encontró evidencia donde se valore o discuta si los lapsos establecidos por cada analista para el desarrollo de los diferentes requerimientos, son los adecuados y se ajustan al trabajo real requerido.

En el COBIT 5, la práctica de gestión BAI02.01 que trata sobre la definición y mantenimiento de los requerimientos técnicos y funcionales de negocio, indica:

> "*Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información de negocio, funcionales, técnicos y de control que cubra el alcance/entendimiento de todas las iniciativas necesarias para alcanzar los resultados esperados de la solución de negocio de TI propuesta*."

También el artículo 14.2.2 "*Procedimientos de control de cambios del sistema*", de la sección 14.2 sobre seguridad en los procesos de desarrollo y soporte, del ISO 27002:2016, detalla:

"Los cambios en los sistemas dentro del ciclo de vida de desarrollo deberían ser contralados mediante el uso de procedimientos formales de control de cambios…

Para garantizar la integridad del sistema, aplicaciones y productos, deberían documentarse y hacerse cumplir los procedimientos formales de control de cambios, desde las etapas tempranas de diseño a través de todas las tareas de mantenimiento posteriores. La introducción de nuevos sistemas y cambios importantes a sistemas existentes debería seguir un proceso formal de documentación, especificación, pruebas, control de calidad, y gestión de implementación.

Este proceso debería incluir una evaluación de riesgo, el análisis de los impactos de los cambios, y la especificación de los controles de seguridad necesarios. Este proceso también debería asegurar que los procedimientos existentes de seguridad y control no sean comprometidos, que a los programadores de apoyo se les da el acceso sólo a aquellas partes del sistema necesario para su trabajo y que se tenga un acuerdo formal y aprobación para cualquier cambio."

De acuerdo a lo investigado, una posible razón de que se administren de esta forma los requerimientos a los sistemas de información, se debe a que se considera que con el uso de la Mesa de Servicios y el Microsoft Project, es suficiente para llevar el listado de los requerimientos, así como las fechas y tiempos correspondientes.

No contar con algún insumo automatizado para controlar totalmente los requerimientos realizados a los sistemas, puede incidir negativamente en la administración de los tiempos de asignación, ejecución, seguimiento, cumplimiento y entrega final; viéndose afectado tanto el área de Desarrollo y Mantenimiento como las necesidades del usuario final.

2.2 Seguimiento por parte de los usuarios finales

En la auditoría al revisar el proceso efectuado por los usuarios para solicitar y administrar las necesidades que les surjan referentes a los sistemas de información, se determinó que no cuentan con la posibilidad de monitorear el estado y avance de cada una de las solicitudes de servicio efectuadas al área de Desarrollo. Esto es que no tienen el insumo para extraer la totalidad de requerimientos que ha solicitado para determinar aquellos que estén pendientes, detenidos, rechazados, cumplidos, etc.

En la práctica de gestión BAI06.01 del COBIT 5 "*Evaluar, priorizar y autorizar peticiones de cambio*" y que es un subproceso del BAI02, referente a gestionar la definición de requisitos, se indica lo siguiente:

> "*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***." El destacado es propio.

Por último, en la actividad de control número 1 de la práctica de gestión DSS02.02 "*Registrar, clasificar y priorizar peticiones e incidentes*", se menciona:

> *"Registrar todos los incidentes y peticiones de servicio, registrando toda la información relevante de forma que pueda ser manejada de manera efectiva y se mantenga un registro histórico completo*"

La limitación del seguimiento que tienen las diferentes áreas o departamentos sobre el estado de sus requerimiento en sistemas, se debe a que la herramienta sistematizada que se utiliza (en este caso la Mesa de Servicio), no cuenta con las características técnicas que permitan ejecutar dicho control.

Esta limitación repercute directamente en la administración de las actividades que cada unidad debe controlar sobre los sistemas de información asignados bajo su responsabilidad. Así mismo y en vista de que pueden existir requerimientos de importancia que afecten la operativa del área, se podría ver disminuido el control interno

2.3 Estado de requerimientos de sistemas

Como parte del estudio se evaluaron los diferentes estados que tienen los requerimientos (de Sistemas de Información) en las bases de datos contenidas en la Mesa de Servicio. Dichos estados van variando de acuerdo a las labores ejecutadas tanto por el desarrollador como por el usuario final y podrían estar variando entre Asignados, Detenidos, Rechazados, Resueltos, entre otros. En la auditoría se determinó que no se ha implementado algún control enfocado a brindarle seguimiento a tales estados, así como a las fechas de entrega y a los tiempos de ejecución. Se detallan seguidamente algunos de los estados localizados y su situación vigente al 30 de Noviembre del 2018:

- ✓ El número de caso 3635 tiene estado "Detenido" esperando la verificación por parte del usuario y cuenta con 418 días desde su registro.

- ✓ Existen 34 registros con estado “Detenido” por el analista utilizando como razón las cargas de trabajo. Estos requerimientos van desde los 311 hasta los 685 días desde que fueron registrados.

- ✓ Se localizaron 41 requerimientos con estado de “Asignado” y que de acuerdo al sistema están asignados al especialista. Al evaluar las fechas de registro, al menos 6 de estos requerimientos tenían más de 320 días desde su registro.

- ✓ Los números de caso 3315, 3322 cuentan con 546 días y el caso 3911 tiene 314 días, desde que fueron ingresados al sistema. Los tres casos se encuentran en espera por requerimientos por el usuario.

- ✓ Se encontraron 6 registros que están siendo atendidos y que contaban con más de 200 días.

De acuerdo a los diferentes estados mencionados anteriormente, se logra determinar la carencia de un mecanismo que lleve la trazabilidad del tiempo en que estuvo cada requerimiento en los diferentes estados. Adicionalmente, al no controlarse los tiempos reales invertidos por cada analista, no existe forma de comprobar si estos se ajustan a los lapsos previstos por dichos funcionarios una vez que les fueron asignados e incluidos en sus pertinentes colas de trabajo.

En el COBIT 5, se encuentra en el proceso DSS06 relacionado a gestionar los controles de proceso de negocio, la siguiente práctica de gestión:

> *“**DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades y de información.***
> *Asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan. Esto permite trazabilidad de la información a lo largo de su ciclo de vida y procesos relacionados. Proporciona garantía de que la información que conduce el negocio es de confianza y ha sido procesada acorde a los objetivos definidos.”*

Una de las principales razones de las situaciones indicadas, se debe a la carencia de normativa interna que regule y controle más a detalle, todo el proceso relacionado con los tiempos y estados de los requerimientos a los sistemas de información. Esto ya que el procedimiento P-DTI-AI2-002 no cuenta con el detalle suficiente para controlar las debilidades indicadas.

Como parte de las posibles consecuencias de la carencia de estos controles, se tiene que se podrían ampliar los tiempos de respuesta al usuario final con respecto a sus necesidades en las aplicaciones que utilicen; viéndose de esta manera afectada directa o indirectamente la eficiencia de las operaciones en las áreas que dependen de los sistemas informáticos para su función.

3. CONCLUSIÓN

En el transcurso de la auditoría sobre la administración del área de Desarrollo de TI, se logró determinar que se carecen de controles básicos para una correcta administración de los requerimientos sobre los sistemas de información actuales.

De igual forma como parte de los resultados del estudio, se logra determinar que los usuarios dueños de sistemas, tienen limitaciones técnicas para administrar de forma completa el seguimiento a las necesidades remitidas al área de Desarrollo.

La ejecución del trabajo fue realizado aplicando las técnicas de auditoria correspondiente, evaluando la normativa vigente referente al mantenimiento de sistemas de información, así como los controles existentes sobre este tema.

En general las deficiencias encontradas y detalladas en la sección dos de este informe, generan ciertas limitaciones considerables sobre el control interno que debe ejercer tanto el área de TI como los encargados oficialmente de administrar las aplicaciones informáticas del Banco.

En la sección siguiente se explica con más detalle las recomendaciones que según la Auditoría Interna deben implementarse para mejorar el proceso de administración y control de los requerimientos de sistemas de información de todas las aplicaciones vigentes.

4. RECOMENDACIONES

En relación con los informes de la Auditoria Interna dirigidos a los titulares subordinados, la Ley General de Control Interno No. 8292 en su artículo 36 establece:

*"Artículo 36. —**Informes dirigidos a los titulares subordinados**. Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*

a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.

b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.

c) *El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda."*

A continuación se presentan las recomendaciones de acuerdo al orden en que fueron expuestas en la sección de resultados.

4.1 Administración sobre los requerimientos de sistemas de información

Al Departamento de TI

4.1.1 Debe evaluarse la factibilidad técnica de contar con alguna herramienta para mantenimiento de sistemas, con la que se pueda centralizar y administrar completamente todos los requerimientos o necesidades sobre las aplicaciones que son solicitadas constantemente por los usuarios finales.

Nivel de Riesgo: **Alto**

4.1.2 Es necesario incorporar al proceso de mantenimiento de sistemas, una etapa normada donde se valore ya sea por el Coordinador del área de Soporte o Mantenimiento o por otro funcionario del Departamento de TI, si los tiempos definidos por cada analista para cumplir con los requerimientos asignados, se adecúan a la realidad de cada necesidad.

Nivel de Riesgo: **Alto**

4.2 Seguimiento por parte de los usuarios finales

Al Departamento de TI

4.2.1 Se debe valorar alguna opción técnica para que los dueños de sistemas de información puedan darle un seguimiento detallado a cada una de las recomendaciones relacionadas con sus aplicaciones. Como parte de las características deseables que debería tener el nuevo control, están que las jefaturas puedan administrar sus prioridades de requerimientos de acuerdo a sus necesidades, también que puedan verificar en qué etapa se encuentra cada requerimiento, tiempos de ejecución, avisos o alertas en atrasos por etapa o entrega finales, aprobación en las etapas que les correspondan, entre otros.

Nivel de Riesgo: **Alto**

A la Gerencia General

4.2.2 Como parte de la normativa institucional, debe instaurarse asociado a los controles que debe ejercer cada Dirección o Jefatura encargada de algún Sistema de Información, la ejecución de revisiones periódicas sobre el avance y cumplimiento de los requerimientos efectuados a sus aplicaciones. La actividad debe quedar documentada para futuras revisiones ya sea de la Auditoría Interna o de algún otro ente contralor.

Nivel de Riesgo: **Alto**

4.3 Estado de requerimiento de sistemas

Al Departamento de TI

4.3.1 Se debe establecer para el área de Desarrollo y Mantenimiento de Sistemas un control que brinde un seguimiento sobre cada uno de los estados (Asignado, Detenido, En Atención, Rechazado, Resuelto, etc) en que pueda estar un requerimiento de sistemas; esto con la finalidad de evaluar posibles cuellos de botella o atrasos importantes que afecten la entrega final del producto.

Nivel de Riesgo: **Alto**

4.3.2 Debe implementarse un control dirigido a llevar un pulso más detallado a las fechas finales en que se resuelve la necesidad de mantenimiento de sistemas definidas por el usuario final; esto con el fin de determinar si los tiempos totales se ajustaron a los previstos inicialmente. Esta actividad debe estar normada y documentada.

Nivel de Riesgo: **Alto**

4.3.3 Se debe elaborar o ampliar la normativa referente al mantenimiento de sistemas de información, con la cual se pueda controlar los tiempos de ejecución tanto de los diferentes estados que puede tener un requerimiento, como de los tiempos totales utilizados para el cumplimiento del mismo.

Nivel de Riesgo: **Medio**

4.3.4 Debe efectuarse una revisión de los diferentes tiempos y estados detallados en el hallazgo 2.3 de este informe, con el objetivo de evaluar si los lapsos utilizados (hasta la fecha de corte del informe) para el cumplimiento de tales requerimientos son correctos según las demás actividades realizadas por los analistas respectivos.

Nivel de Riesgo: **Bajo**

MBA. Gustavo Flores Oviedo.
Auditor Interno.