
Banco Hipotecario de la Vivienda

Informe Final TI-SIS-001-2016

AUDITORÍA SOBRE EL SISTEMA DE INVENTARIOS

26/09/2016

INDICE

A. RESUMEN EJECUTIVO	3
1. INTRODUCCIÓN	4
1.1 JUSTIFICACIÓN DE LA AUDITORÍA.....	4
1.2 OBJETIVO.....	4
1.3 ALCANCE.....	4
1.4 METODOLOGÍA DE TRABAJO.....	4
2. RESULTADOS DE LA EVALUACIÓN.....	6
2.1 BITÁCORA DEL SISTEMA Y CONTROLES EN LÍNEA.....	6
2.2 EVALUACIONES SOBRE LA INFORMACIÓN CONTENIDA EN EL SISTEMA	7
2.3 PRUEBAS EN LAS BASES DE DATOS	8
2.4 USUARIOS CON PRIVILEGIOS ACTIVOS.....	9
2.5 AUDITORÍA SOBRE LAS TABLAS DEL SISTEMA	11
2.6 ROLES Y PERFILES DEL SISTEMA	13
2.7 CONCENTRACIÓN DE FUNCIONES	13
3. CONCLUSIÓN.....	15
4. RECOMENDACIONES	16
4.1 BITÁCORA DEL SISTEMA Y CONTROLES EN LÍNEA	17
4.2 EVALUACIONES SOBRE LA INFORMACIÓN CONTENIDA EN EL SISTEMA	17
4.3 PRUEBAS EN LAS BASES DE DATOS	18
4.4 USUARIOS CON PRIVILEGIOS ACTIVOS.....	18
4.5 AUDITORÍA SOBRE LAS TABLAS DEL SISTEMA	18
4.6 ROLES Y PERFILES DEL SISTEMA	19
4.7 CONCENTRACIÓN DE FUNCIONES.....	19

A. RESUMEN EJECUTIVO

En esta auditoria se evaluaron los principales controles existentes en el sistema de Inventarios institucional, revisando tanto el proceso de administración de la herramienta como las áreas lógicas básicas para una adecuada utilización y control.

Como parte de las debilidades localizadas se encuentra la inexistencia de una bitácora de auditoría lógica que resguarde transacciones poco comunes o que no deberían de existir por naturaleza. Estas bitácoras normalmente van ligados con controles automáticos que informen en línea (inmediatamente de que acontecen) a los dueños del sistema, tales situaciones anormales (entiéndase como modificación o eliminación de información); dichos controles tampoco se han definido.

Todos los sistemas de información institucionales tienen definido un responsable o “dueño” encargado de velar por el uso adecuado que se le dé al mismo y por la información que contengan. Al respecto el área responsable del sistema de Inventarios es la Proveeduría del Banco, la cual según se investigó no tiene normado estar valorando lo correcto y completo de los datos incluidos en la aplicación.

Al realizar ciertas pruebas en la base de datos del sistema, específicamente en las diferentes tablas y campos correspondientes, se localizaron una serie de inconsistencias y falta de integridad entre la información que las componen. Lo anterior tomando en cuenta que los dueños del proceso deberían contar con muchos más criterios para el desarrollo de este tipo de pruebas y por ende, la posibilidad de hallar aún más deficiencias.

Se investigó sobre los privilegios que tenían asignados todos los usuarios habilitados para utilizar la aplicación y se determinó la existencia de personal ajeno al proceso de inventarios con accesos y privilegios habilitados, más amplios de los que deberían. En mucho esto se debe a la inexistencia de normativa para la evaluación periódica de los roles y perfiles correspondientes.

A nivel de control y seguimiento, puede ser relevante o necesario poder determinar cuál funcionario fue el que ejecutó una acción específica en el sistema, ya sea una inclusión, modificación o borrado. Esta situación no se podría ejecutar actualmente en la aplicación de Inventarios porque carece de los campos necesarios para su evaluación.

Por último, se mantiene una concentración de funciones sobre el personal del área de Proveeduría, situación que ya ha sido informada por la Auditoría Interna en otras ocasiones.

Los detalles de cada aspecto indicado, son ampliados a lo largo del informe.

BANCO HIPOTECARIO DE LA VIVIENDA

AUDITORÍA INTERNA

Informe Final N° TI-SIS-001-2016

26 de Setiembre del 2016

AUDITORÍA SOBRE EL SISTEMA DE INVENTARIOS

1. INTRODUCCIÓN

1.1 Justificación de la auditoría

Este estudio forma parte del Plan Anual de Trabajo de esta Auditoría Interna para el año 2016 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 suficiencia de controles implementados en el Sistema de Inventarios administrado por el área de Proveeduría del Banco Hipotecario de la Vivienda.

1.3 Alcance

El estudio abarcó la normativa, información y procesos operativos vigentes al 31 de Julio del 2016 relacionados con el uso y la administración del Centro de Procesamiento Alterno.

1.4 Metodología de Trabajo

Se aplicó la metodología establecida en el Manual para el ejercicio de la práctica de la Auditoría Interna, y el Procedimiento de Auditoría, emitido y aprobado en el 2012, por el Auditor Interno. 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:

- ✓ Las normas ISO 27002:2005 Tecnologías de Información – Código de buenas prácticas para la gestión de la seguridad de la información
- ✓ Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información N-2-2007-CO-DFOE
- ✓ El reglamento SUGEF 14-09
- ✓ El Manual de Normas de control interno para el Sector Público N-2-2009-CO-DFOE
- ✓ La versión 4.0 del estándar COBIT

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 el funcionario responsable de la administración del inventario institucional. Adicional se evaluó la existencia y razonabilidad de la documentación formal y procesos establecidos para controlar la información.

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 Auditoría Interna. Las deficiencias detectadas, tanto en aspectos de control interno como operativas, de la presente revisión, se detallan en la sección de Resultados.

2. RESULTADOS DE LA EVALUACIÓN

2.1 Bitácora del Sistema y Controles en Línea.

Al investigar sobre la existencia de una bitácora del módulo de Inventarios, se determinó que desde que se puso en producción el sistema, el área de Proveeduría no ha solicitado la creación de la misma, en la cual se registren únicamente aquellas transacciones que no son normales o correctas desde el punto de vista operativo del área. Sobre este tema y según se investigó, como resultado de una recomendación de la Auditoría Interna sobre otra evaluación, de acuerdo al número de caso N° 2556 del 30-06-2016, el área de Proveeduría solicitó al Departamento de TI la creación de una bitácora sobre el sistema de Activos y de forma muy general amplió el requerimiento a las demás aplicaciones que están bajo su responsabilidad. No obstante se comprobó que la solicitud no es lo suficientemente clara y específica sobre la información que debería incluirse en tales bitácoras, así como los controles de seguimiento respectivos.

Adicionalmente se encontró que para el sistema de Inventarios tampoco se han establecido controles en línea que monitoreen y avisen sobre cambios en la base de datos que sean de relevancia a nivel de la administración del inventario institucional.

En el en el proceso DS13 del COBIT, Administración de Operaciones, se declara en el punto 13.6 lo siguiente:

“13.6 Bitácora de Operación

Los controles de la Gerencia deberán garantizar que se almacene en bitácoras suficiente información cronológica de las operaciones para permitir la reconstrucción, la revisión y el examen oportunos de las secuencias de tiempo de procesamiento y otras actividades que rodean y soportan el procesamiento.”

De igual forma el proceso AI3 del COBIT, detalla los siguientes controles con respecto a este tipo de actividades:

“AI3.2 Protección y disponibilidad del recurso de infraestructura

Implantar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensibles por todos aquellos que desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso.”

La razón fundamental por la que no existe una bitácora de la aplicación de Inventarios así como un monitoreo en línea, se debe a que no se ha normado en el área de Proveduría la implementación y revisión de este tipo de controles automatizados.

En los casos en que no existen bitácoras de sistemas, no se podría determinar si las modificaciones o borrados de información para los datos más importantes del sistema, fueron correctas y debidamente procesadas. De igual forma, al no tener controles que informen automáticamente sobre cambios no autorizados, es más factible modificar o borrar datos o parámetros que afecten la consistencia e integridad de la información.

2.2 Evaluaciones sobre la información contenida en el Sistema

No se realizan pruebas periódicas por parte del área de Proveduría para determinar si la principal información que procesa y resguarda el sistema de Inventarios es correcta, completa y adecuada.

En el dominio de Entrega y Soporte, en el proceso DS11 el punto 11.7, “Chequeos de Exactitud, Suficiencia y Autorización”, dicta lo siguiente:

“Los datos de transacciones, ingresados para su procesamiento (generados por personas, por sistemas o entradas de interface) deberán estar sujetos a una variedad de controles para verificar su exactitud, suficiencia y validez. Asimismo, deberán establecerse procedimientos para asegurar que los datos de entrada sean validados y editados tan cerca del punto de origen como sea posible.”

El Manual de Control Interno de la Contraloría, en el artículo 1.4 denominado “Responsabilidad por el control interno”, detalla lo siguiente:

“La responsabilidad principal por el diseño, la implantación, la operación, la evaluación, el mejoramiento y el perfeccionamiento del control interno es inherente al jerarca y a los titulares subordinados de cada organización. Por su parte, las jefaturas en cada área de la institución deben velar porque las medidas de control específicas relativas a su ámbito de acción sean suficientes y válidas, y porque los funcionarios sujetos a su autoridad jerárquica las apliquen cumplidamente.”

La valoración de la base de datos del sistema de Inventarios no se ejecuta debido a que no se han establecidos los procedimientos relacionados con dicho fin.

Como consecuencia de no desarrollar evaluaciones periódicas de los datos del sistema, se puede presentar información incorrecta, inconsistente, incompleta o nula y que por estar de esa forma afecte la confiabilidad sobre la información de los inventarios del Banco.

2.3 Pruebas en las bases de datos

Como parte de la auditoría se ejecutaron ciertas pruebas sustantivas sobre la consistencia e integridad de las bases de datos del sistema de Inventarios del Banco, encontrando de acuerdo a los criterios utilizados por la Auditoría, ciertas anomalías con respecto a la información que se resguarda en cada tabla y que seguidamente se detallan:

- a) En la tabla ARINHA que almacena el histórico de artículos, al recalcularse el monto del saldo total de los artículos de acuerdo a las unidades disponibles y al monto por unidad, se encontraron 2006 registros que presentan diferencias con el campo del SALDO_MO.
- b) Realizando un recálculo del costo unitario de los artículos inventariados, ubicados también en la tabla ARINHA, se localizaron 4.511 registros que presentan diferencias entre el campo COSTO_UNI.
- c) También en la tabla ARINHA se ubicaron 108 artículos que tenían un saldo igual o mayor a 1 pero sin ningún monto en el campo SALDO_MO. Sobre este mismo punto se encontraron 559 registros que tenían cero cantidades de artículos pero su saldo era mayor que cero.
- d) En la tabla ARINMN que resguarda los movimientos mensuales de inventarios, se localizaron 1.191 registros donde el usuario que registró el movimiento y el que lo aprobó fueron los mismos, específicamente 90 registros fueron de Karla Porras y 1.101 de Jorge Moreno.
- e) En la tabla ARINMA que contiene la información del maestro de artículos, al efectuar un recálculo se ubicaron 49 registros donde el costo unitario del artículo es distinto al presentado en el campo que guarda esa misma información (COSTO_UNI). En esa misma tabla se localizaron 58 artículos que presentaban un saldo de unidades mayor o igual a 1, pero con sus fechas de ingreso y vencimiento Nulas (NULL).

El proceso DS11 de COBIT denominado “Administración de Datos”, brinda la siguiente declaración.

“11.7 Chequeos de Exactitud, Suficiencia y Autorización

Los datos de transacciones, ingresados para su procesamiento (generados por personas, por sistemas o entradas de interfase) deberán estar sujetos a una variedad de controles para verificar su exactitud, suficiencia y validez. Asimismo, deberán establecerse procedimientos para asegurar que los datos de entrada sean validados y editados tan cerca del punto de origen como sea posible.”

Uno de los motivos que se determinó como básico para los resultados indicados, se debe a para el diseño de las tablas no se implementaron controles de

consistencia entre los campos que deben tener relación entre ellos mismos. Lo anterior aunado a que desde que se empezó a operar la aplicación (2010 según los primeros registros), nunca se han realizado revisiones de consistencia e integridad de la información ahí contenida.

Como motivo principal por el que se encuentren inconsistencias en la base de datos del sistema de Inventarios, se debe a que no existe normativa enfocada a realizar validaciones periódicas de la información que contiene dicho sistema.

Uno de los efectos principales de tener inconsistencias en las bases de datos, es que se tengan datos de los Inventarios que no sean correctos, adecuados o exactos, situación que podría permitir la pérdida o daño de cualquier activo.

2.4 Usuarios con privilegios activos

Al evaluar los usuarios que tienen permisos activos para ingresar al sistema de Inventarios, se localizó que al momento de la auditoría la funcionaria Karla Porras Coto contaba con el rol que habilita todos los privilegios para utilizar esa aplicación, esto a pesar de que no es funcionaria del área de Proveeduría. Al respecto se determinó que tiempo atrás la señora Porras estuvo colaborando con el área de Proveeduría, de ahí que en ese momento se le habilitaran todos los permisos, pero los mismos nunca fueron eliminados una vez que la funcionaria volvió a su puesto original.

Sobre usuarios con privilegios en el sistema de Inventarios, también se localizaron otros funcionarios que ya no trabajan en el Banco y contaban con los permisos activos en la aplicación, específicamente el señor Juan de Dios Rojas Castante, Alejandro Bejarano Castillo y Carlos Cortés Ortiz. Con estos últimos exfuncionarios se corroboró que a pesar de que estaban activos en el sistema, a nivel de base de datos habían sido eliminados.

En el siguiente cuadro se muestra agrupado por permisos, cada uno de los usuarios indicados:



Reporte de Accesos
BANCO HIPOTECARIO DE LA VIVIENDA
 Reporte de Accesos por Sistema
 MÓDULO DE INVENTARIOS
Instancia: BANHVI

SG01RE03
 08/17/2016
 11:12:46 AM
 JORRAMIREZ

Rol: INVR01	Descripción OFICIAL INVENTARIO
Login	Nombre Usuario
INVENT	DUEÑO ESQUEMA INVENTARIO
JORMORENO	MORENO MONTES JORGE
KARPORRAS	<u>PORRAS COTO KARLA VANESSA</u>
MARCONEJO	CONEJO CARMONA MARGIE
Rol: INVR02	Descripción APROBADOR INVENTARIO
Login	Nombre Usuario
ALEBEJARANO	<u>BEJARANO CASTILLO ALEJANDRO</u>
ALESANDOVAL	ALEXANDER SANDOVAL LORÍA
ANAFERNANDEZ	FERNÁNDEZ CHAVARRÍA ANA
ASM	SOLANO MONTERO ALEXIS
CARCASTRO	CASTRO MIRANDA CARLOS
CARCORTES	<u>CORTÉS ORTIEZ CARLOS LUIS</u>
DAVLOPEZ	LÓPEZ PACHECO DAVID
EDULEON	LEÓN CHENG EDUARDO
EQG	QUESADA GONZÁLEZ EDUARDO
ERIMASIS	MASÍS CALDERÓN ERICKA
GUSFLORES	FLORES OVIEDO GUSTAVO
HUGMATA	MATA NAVARRO HUGO
INVENT	DUEÑO ESQUEMA INVENTARIO
JLQ	LEÓN QUIROS JENNY
JORMORENO	MORENO MONTES JORGE
JOSDURAN	DURÁN RODRÍGUEZ JOSÉ
JUAROJAS	<u>ROJAS CASCANTE JUAN</u>
MAGLONGAN	LONGHAN MOYA MAGALY
MARCAMACHO	CAMACHO MURILLO MARTHA
MARCAMPOS	CAMPOS BARRANTES MARGOTH
MARCONEJO	CONEJO CARMONA MARGIE
MARMENDEZ	MÉNDEZ CONTRERAS MARCO TULIO
MARMORALES	MORALES RAMÍREZ MARIANELA

El proceso DS5 de COBIT orientado a garantizar la seguridad de los sistemas, detalla en el proceso 5.4 el siguiente criterio:

“DS5.4 Administración de cuentas del usuario

Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema como otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.”

Como principal razón por la que existen personas ajenas al proceso de inventarios con privilegios activos en ese sistema, se debe a que el área de Proveeduría no ha normado la revisión periódica de los permisos de los usuarios que han sido habilitados en el sistema de Inventarios.

Una posible consecuencia de esta situación, es que se registren procesos en la aplicación de Inventarios por personas ajenas su administración y control, dando como resultado problemas de inconsistencias en esas bases de datos o hasta inconvenientes con la razonabilidad de los activos institucionales.

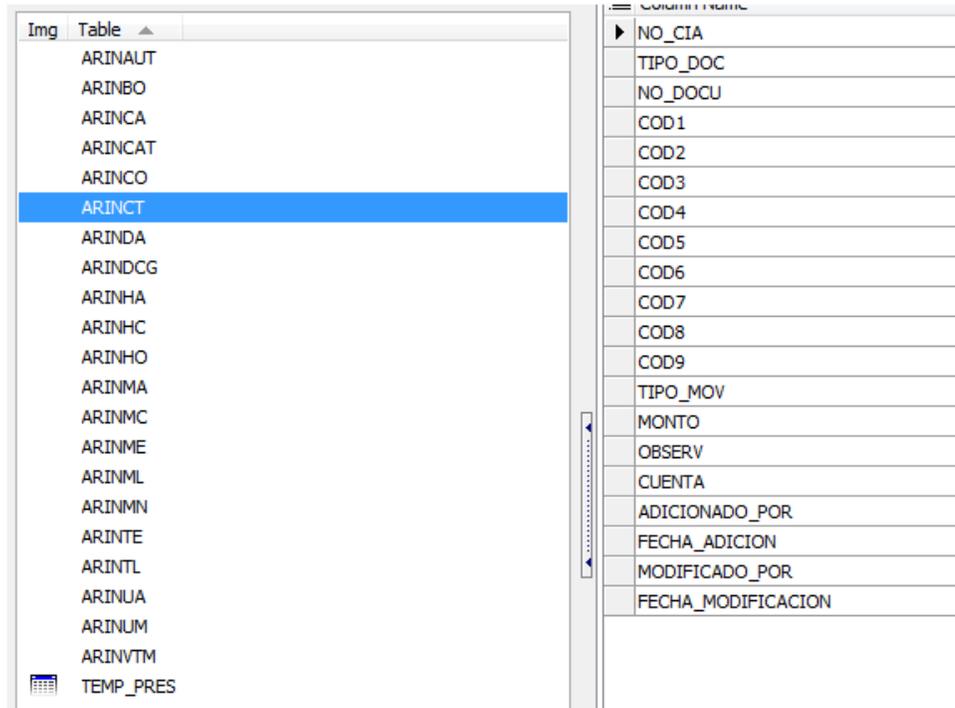
2.5 Auditoría sobre las tablas del sistema

Al evaluar la estructura de las tablas utilizadas para administrar y resguardar la información del sistema de Inventarios, se determinó que casi en su totalidad (20 de 21) no se han implementado controles mínimos de auditoría sobre todos los registros que se crean, donde al menos se pueda identificar el usuario que adicionó el movimiento, la fecha de adición, el usuario que modificó el dato y la fecha de modificación. Este control solo se localizó únicamente en la tabla "ARINCT", la cual según el detalle que presenta registrar las transacciones contables pero de forma temporal ya que después de procesar la información la envía a otra tabla de históricos de movimientos, quedando "ARINCT" sin ningún registro.

Seguidamente se presenta un cuadro con el detalle de todas las tablas del sistema de Inventarios y donde se marca la única tabla que contiene los campos de control indicados:

Detalle de tablas del sistema de Inventarios

•	ADICIONADO_POR	4		N	VARCHAR2 (30 Byte)
•	FECHA_ADICION	5		N	DATE
•	MODIFICADO_POR	6		Y	VARCHAR2 (30 Byte)
▶	FECHA_MODIFICACION	7		Y	DATE



El manual de Normas técnicas para la gestión y el control de las Tecnologías de Información de la Contraloría General de la República, detalla en el capítulo de prestación de servicios y mantenimiento lo siguiente:

“4.3 Administración de los datos

La organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura.”

Se determina como causa principal de la carencia de controles mínimos de auditoría en las tablas del sistema de Inventarios, a que los mismos no fueron identificados como necesarios por el dueño de la aplicación al momento de definir los controles de la misma y hasta la fecha de la auditoría, nunca se ha valorado su necesidad.

El efecto principal de la carencia de campos de auditoría sobre la mayoría de las tablas de ese sistema, es que resultaría imposible determinar en caso de

requerirse, la persona que ingreso, modificó o eliminó cualquier tipo de información de los inventarios del Banco.

2.6 Roles y perfiles del sistema

En la auditoría se comprobó que el área de Proveeduría no realiza evaluaciones periódicas de los privilegios definidos en los roles y perfiles del sistema de Inventarios. De igual forma no se ha solicitado ningún control en línea que avise de automáticamente al personal correspondiente, sobre cualquier cambio en los privilegios lógicos establecidos en los roles vigentes (INVR01, INVR02, INVR03, INVR04, INVR20 y INVR21) o sobre la otorgación de esos roles a algún funcionario del Banco sin su debida autorización.

El COBIT, en su proceso de Administración de cambios, define en los objetivos 6.1 y 6.4 lo siguiente:

“A16.1 Estándares y procedimientos para cambios

Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y patches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.”

“A16.4 Seguimiento y reporte del estatus de cambio

Establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio y las plataformas fundamentales.”

Estas situaciones se presentan ya que el área de Proveeduría no tiene incluido dentro de su normativa la revisión de los permisos establecidos en los roles vigentes. Además, a la fecha no se ha solicitado la implementación de un requerimiento que controle los cambios en los roles o sus asignaciones.

Al no contar con una correcta administración y control de los roles y perfiles definidos en el sistema, se podrían brindar más privilegios de los requeridos a un grupo de usuarios que tengan establecido un rol específico, habilitando la posibilidad de que se ejecutan alteraciones incorrectas en la información de inventarios.

2.7 Concentración de funciones

Como parte del examen, se logró determinar una completa concentración de funciones de la persona encargada de la administración y control de todo el inventario de la institución, la cual debe solicitar, recibir, registrar, plaquear, inventariar, administrar, pagar y en ocasiones hasta solicitar y comprar nuevos

activos. Adicional, el mismo funcionario que utiliza en su totalidad el Sistema de Inventarios, también cuenta con todos los privilegios en los sistemas de Compras, Activos y Cuentas por Pagar; además de tener que ingresar al sistema de Control de Bancos para generar el pago a los proveedores correspondientes.

Esta situación ya ha sido indicada por la Auditoría Interna según consta en el informe **FO-OP-001-2012** del 03 de setiembre del 2012 y en el informe **TI-SW-001-2015** del 17 de julio del 2015; de los cuales la Dirección Administrativa ha realizado varias gestiones para su cumplimiento; sin embargo, a la fecha de la revisión aún se mantenía dicha debilidad.

Las Normas de Control Interno para el Sector Publico (N-2-2009-CO-DFOE) de la Contraloría General de la República, en el punto 2.5.3 relacionado con la separación de funciones incompatibles y del procesamiento de transacciones, dictan lo siguiente:

“El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que las funciones incompatibles, se separen y distribuyan entre los diferentes puestos; así también, que las fases de autorización, aprobación, ejecución y registro de una transacción, y la custodia de Inventarios, estén distribuidas entre las unidades de la institución, de modo tal que una sola persona o unidad no tenga el control por la totalidad de ese conjunto de labores. Cuando por situaciones excepcionales, por disponibilidad de recursos, la separación y distribución de funciones no sea posible debe fundamentarse la causa del impedimento. En todo caso, deben implantarse los controles alternativos que aseguren razonablemente el adecuado desempeño de los responsables.”

Esa misma norma define las “*funciones incompatibles*” de la siguiente forma:

*“Tareas cuya concentración en las competencias de una sola persona, **podría permitir la realización o el ocultamiento de fraudes, errores, omisiones o cualquier tipo de irregularidades**, y en consecuencia debilitar el SCI y el logro de los objetivos institucionales. Incluyen, por ejemplo, las funciones de autorización, ejecución, aprobación y registro de transacciones, así como las de custodia de recursos.”* El destacado es nuestro.

Tal concentración de funciones (y por ende dependencia de la persona encargada), se presenta debido a la limitación de personal que tiene el área de Proveeduría, contando únicamente con dos funcionarios (de los cuales uno es jefatura) para ejecutar todas las tareas que están bajo su responsabilidad.

Una de los principales efectos de que la gran mayoría de actividades necesarias para administrar los Inventarios del Banco estén bajo una misma persona, es que se puedan dar pérdidas por omisión, error o dolo en los activos del Banco y no exista forma de determinarlo.

3. CONCLUSIÓN

Al efectuar la auditoría del sistema de Inventarios y de algunos de los procesos con los que se relaciona, se logró determinar que se carecen de controles esenciales para una correcta administración tanto de la aplicación como de la información que la compone.

La ejecución del trabajo fue realizado aplicando las técnicas de auditoria correspondiente, evaluando la normativa vigente aplicable a los sistemas de información así como los controles definidos en el sistema hasta el momento de la revisión; incluyendo la ejecución de pruebas sustantivas sobre las bases de datos correspondientes y la evaluación de sus estructuras, consistencia e integridad de la información.

Referente al control para la utilización del sistema, se localizaron debilidades sobre el uso de los roles y perfiles existentes, así como privilegios asignados a usuarios que no pertenecen al área de Proveeduría.

Estos aspectos dan como contraste deficiencias en el sistema de control interno relacionado con la aplicación y su utilización, limitando un adecuado seguimiento y administración sobre las áreas relacionadas con el inventario total de la institución.

En la sección siguiente se explica con mucho más detalla las recomendaciones que según la Auditoría Interna deben implementarse para mejorar el proceso de continuidad del negocio, en una posible contingencia que afecte los recursos tecnológicos.

4. RECOMENDACIONES

En relación con los informes de la Auditoría 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 Bitácora del Sistema y Controles en Línea

A la Dirección Administrativa

4.1.1 Definir con la colaboración del Departamento de TI, una bitácora del sistema de Inventarios que registre para la información más relevante según el criterio de los dueños de los datos, todas las transacciones inusuales o incorrectas de acuerdo a la operatividad del área. Para una adecuada trazabilidad del movimiento los campos mínimos que debe contener la bitácora son el valor antes y después del cambio, el usuario del sistema operativo, el usuario del sistema de información, la fecha y hora, el nombre de la PC que generó el cambio, la herramienta con la que se hizo el cambio (TOAD, SQL, ODBC, Forms, etc.), así como aquellos que los dueños del sistema consideren relevantes.

Nivel de Riesgo: **Alto**

4.1.2 Implementar en el sistema de Inventarios controles en línea destinados a monitorear y valorar accesos, modificaciones o borrados de información que sean ejecutados de forma inusual o por personal externo al proceso, sobre los principales datos del sistema. Como parte de tales controles debe crear avisos en línea que comuniquen de forma inmediata a los dueños de los datos, cada vez que se ejecute alguna de las actividades descritas.

Nivel de Riesgo: **Alto**

4.1.3 Una vez implementada la bitácora, se debe incluir en la normativa de la Dirección Administrativa, una revisión periódica sobre la información contenida en ella, incluyendo la necesidad de dejar documentada tal revisión.

Nivel de Riesgo: **Medio**

4.2 Evaluaciones sobre la información contenida en el Sistema

A la Dirección Administrativa

Crear los procedimientos respectivos enfocados a valorar de forma periódica la consistencia e integridad de los datos más relevantes del sistema de Inventarios. La actividad de control debe quedar documentada.

Nivel de Riesgo: **Alto**

4.3 Pruebas en las bases de datos

A la Dirección Administrativa

La Dirección Administrativa debe realizar un estudio detallado de la base de datos del Sistema de Inventarios y evaluar las inconsistencias o irregularidades que se detallan en el punto 2.3 de este informe, esto con la finalidad de depurar las que sean posibles y solucionar los problemas de consistencia entre los campos y tablas para que no se presenten más errores de este tipo en el futuro. Para esta actividad deben solicitar la colaboración del Departamento de TI, puesto que tal depuración normalmente se realiza directamente en la base de datos previo las solicitudes correspondientes.

Nivel de Riesgo: **Medio**

4.4 Usuarios con Privilegios Activos

A la Dirección Administrativa

4.4.1 Deben eliminarse los permisos en el sistema de Inventarios de la funcionara Karla Porras Coto, que actualmente labora en el Banco; así como desactivar el resto de exmpleados que en su momento tuvieron ciertos privilegios en la aplicación, pero que ya no laboran en la institución.

Nivel de Riesgo: **Medio**

4.4.2 Elaborar la normativa necesaria para determinar lo adecuado de los privilegios de los distintos funcionarios del Banco que tengan habilitado el acceso al sistema de Inventarios.

Nivel de Riesgo: **Medio**

4.5 Auditoría sobre las tablas del sistema

A la Dirección Administrativa

Solicitar la implementación de los campos de auditoría de "ADICIONADO_POR, FECHA_ADICCION, MODIFICADO_POR, FECHA_MODIFICACIÓN, para todas las tablas del sistema de Inventarios que lo ameriten. Es importante recalcar que este control es distinto a la creación de una bitácora de auditoría, puesto que a diferencia de crear una nueva tabla con movimientos inusuales o incorrectos (la bitácora), los

campos a adicionar según esta recomendación se incluirían en las tablas ya existentes y se aplicarían para todas las transacciones que ingresen, modifiquen o eliminen información.

Nivel de Riesgo: **Alto**

4.6 Roles y perfiles del sistema

A la Dirección Administrativa

4.4.1 Incluir dentro de la normativa de la Dirección Administrativa a nivel de política y procedimiento la revisión periódica de los privilegios establecidos en los roles y perfiles del sistema de Inventarios.

Nivel de Riesgo: **Alto**

4.4.2 Gestionar con el Departamento de TI un control en línea que le indique a la Dirección de forma automática (un correo electrónico por ejemplo) cada vez que se aplique un cambio o modificación sobre cualquiera de los privilegios aplicados en los roles o perfiles del sistema de Inventarios. Así mismo debe informarse automáticamente cuando sea otorgado alguno de los roles de ese sistema a funcionarios que antes no los tenían o contaban con alguno distinto.

Nivel de Riesgo: **Alto**

4.7 Concentración de Funciones

A la Gerencia General

Deben efectuarse las gestiones necesarias y suficientes para solucionar de una vez el problema de concentración de funciones y dependencia de personal, existente en el área de Proveeduría del Banco; mismo que ha reiterado la Auditoría Interna en varias ocasiones.

Nivel de Riesgo: **Alto**

MBA. Gustavo Flores Oviedo.
Auditor Interno.