Banco Hipotecario de la Vivienda

Informe Final TI-SIS-002-2018

**AUDITORÍA SOBRE LA ADMINISTRACIÓN DEL SISTEMA DE
VIVIENDA EN LAS ENTIDADES AUTORIZADAS**

24/07/2018

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 MANUAL DE USUARIO DEL SISTEMA PARA LAS EAS.....	6
2.2 CAPACITACIÓN EN EL USO DEL SISTEMA.....	7
2.3 REQUERIMIENTOS DEL SISTEMA DE VIVIENDA ACTUAL.....	7
2.4 ADMINISTRACIÓN Y CONTROL SOBRE USUARIOS DE LAS EAS.....	9
2.5 CASOS DE USOS DE LAS EAS.....	12
3. CONCLUSIÓN.....	14
4. RECOMENDACIONES	15
4.1 MANUAL DE USUARIO DEL SISTEMA PARA LAS EAS	16
4.2 CAPACITACIÓN EN EL USO DEL SISTEMA.....	16
4.3 REQUERIMIENTOS DEL SISTEMA DE VIVIENDA ACTUAL	16
4.4 ADMINISTRACIÓN Y CONTROL SOBRE USUARIOS DE LAS EAS	17
4.5 CASOS DE USO DE LAS EAS	18

A. RESUMEN EJECUTIVO

En esta auditoria se evaluó administración, el uso y el control que se le da al Sistema de Vivienda con un enfoque hacia las Entidades Autorizadas (EAS).

Dentro de los primeros aspectos evaluados, se encontró la documentación existente sobre la aplicación, específicamente los manuales de usuario que deberían ser utilizados por los usuarios de las EAs. El resultado es un atraso en más de diez años desde la última actualización del documento, según la información a la que se tuvo acceso.

El Departamento de Análisis y Control se encarga de dar las capacitaciones sobre el uso del Sistema a los nuevos usuarios de las Entidades Autorizadas. Localizamos una carencia de instrucciones formales y escritas que deben existir para este tipo de actividades.

Como parte del ciclo de vida de cualquier sistema, es necesario estar efectuando actualizaciones al Sistema de Vivienda de acuerdo a los requerimientos que tengan los usuarios. Se encontró que no se deja una trazabilidad sobre las necesidades efectuadas por los funcionarios de las EAs y que las mismas quedan a criterio de la jefatura de Análisis y Control si son desarrolladas o se omiten por completo.

Desde el punto de vista de los controles lógicos sobre los usuarios de las Entidades que ingresan al sistema, se ubicaron debilidades en la administración del Active Directory; existencia de super usuarios para administrar bases de datos que nunca se han utilizado; falta de seguimiento en la creación, bloqueos y desbloques de funcionarios de EAs; usuarios activos en base de datos que ya no laboran para las Entidades y falta de comunicación por parte de las Entidades para la suspensión temporal de sus empleados a nivel del Sistema.

Por último al evaluar el avance sobre el diseño del nuevo Sistema de Vivienda, se logró determinar una ausencia total en la participación de las EAs en el proceso de definición de requerimientos (casos de uso).

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

BANCO HIPOTECARIO DE LA VIVIENDA

AUDITORÍA INTERNA

Informe Final N° TI-SIS-002-2018

24 de Julio del 2018

AUDITORÍA SOBRE LA ADMINISTRACIÓN DEL SISTEMA DE VIVIENDA EN LAS ENTIDADES AUTORIZADAS

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 importancia institucional brindada a las Entidades Autorizadas (EAs) en el uso del Sistema de Vivienda.

1.3 Alcance

El estudio abarcó la documentación, información y procesos operativos vigentes al 31 de Mayo del 2018 relacionados con la administración y utilización del Sistema de Vivienda por las Entidades Autorizadas (EAs).

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 Auditoría para el Sector Público
- ✓ Manual para el ejercicio de la práctica de la Auditoría Interna.
- ✓ Normativa Interna vigente (Metodología – Manuales- Políticas – Procedimientos)
- ✓ Norma 308 Comunicación de resultados

- ✓ ISO-IEC-27002:2016 Tecnología 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 de las políticas y procedimientos vigentes.

Adicionalmente se ejecutaron entrevistas con funcionarios claves, encargados de velar por la administración y la implementación de controles del Sistema de Vivienda utilizado por las Entidades Autorizadas.

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 de la Evaluación.

2. RESULTADOS DE LA EVALUACIÓN

2.1 Manual de Usuario del Sistema para las EAs

Al evaluar el manual de usuario vigente que es facilitado como herramienta de ayuda en el uso del Sistema de Vivienda para las Entidades Autorizadas (EAs), se logró concluir que el mismo se encuentra desactualizado por más de 10 años, ya que el último documento oficial tiene como fecha de modificación febrero del 2008.

En el inciso d) de la sección 12.5 relacionado con el control de software en producción, del ISO-IEC-27002:2016, se detalla lo siguiente:

“12.5.1 Instalación de software en los sistemas en producción
... Deberían considerarse las siguientes directrices para controlar cambios de software en los sistemas en producción:

(...)

- d) debería utilizarse un sistema de control de configuraciones para mantener el control de todo el software implementado así como de la documentación de sistema.... El subrayado es propio.

También en los puntos h) y k) del artículo 14.2 “Seguridad en los procesos de desarrollo y soporte” del ISO-IEC-27002:2016, se dicta lo siguiente:

“14.2.2 Procedimiento de control de cambios del sistema
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.

(...)

- h) asegurarse de que al terminar cada cambio la documentación de sistema sea actualizada y que la documentación antigua sea archivada o eliminada...

- k) asegurarse de que la documentación de operaciones (ver apartado 12.1.1) y los procedimientos de usuario sean cambiados según sea necesario para que permanezcan actualizados... Es subrayado es nuestro.

El motivo por el que se encuentra el Manual de Usuario del Sistema de Vivienda de las EAs desactualizado, se debe a la falta de seguimiento que sobre este tema le ha dado la Dirección FOSUVI (como dueños de la aplicación), incluyendo la designación de algún funcionario de esa área como responsable de tal actividad.

Uno de los efectos principales de esta situación es que el sistema no se utilice de forma correcta o que deban estar haciéndose consultas constantes sobre su uso tanto a las áreas del FOSUVI como al área de Soporte Técnico del

Departamento de TI, pudiendo verse afectado la celeridad del proceso inicial del trámite del bono ejecutado en las Entidades Autorizadas.

2.2 Capacitación en el uso del Sistema

De acuerdo a reuniones efectuadas con personal del área de Análisis y Control del FOSUVI, se determinó que dicha área es la encargada de dar capacitaciones en el uso del Sistema de Vivienda a funcionarios de las Entidades Autorizadas que así lo requieran, tal inducción es dada específicamente por los funcionarios Justin Rivera y Karina Coto. Sin embargo, no se sigue alguna guía documental donde se abarquen los tópicos mínimos que siempre deberían contemplarse para los diferentes enfoques que tienen el Sistema.

En el artículo 1.4.1 de la sección 1.4 “*Gestión de la seguridad de la información*”, de las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), se indica lo siguiente:

“1.4.1 Implementación de un marco de seguridad de la información

La organización debe implementar un marco de seguridad de la información, para lo cual debe:

a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.” El destacado es propio.

La causa por la que no se cuenta con una guía formal para dar las capacitaciones a los funcionarios de las Entidades Autorizadas, se debe a que no existe normativa interna que lo solicite, haciendo que la actividad se haya vuelto una práctica sistematizada.

Esta situación además de generar dependencia de los usuarios que conocen más la aplicación, incrementa la posibilidad de que se omitan temas de control del Sistema que sean importante al momento de ponerlos en práctica.

2.3 Requerimientos del Sistema de Vivienda actual

Al evaluar la definición y administración de necesidades de usuario (requerimientos) del Sistema de Vivienda de las EAs, se logró comprobar que las mismas son canalizadas a través de la jefatura del área de Análisis y Control (por estar definido como el dueño del Sistema) de FOSUVI. Dicho funcionario se encarga de revisar el requerimiento y determinar si lo considera adecuado para

que sea implementado en la aplicación, desarrollando en este último escenario las Mesas de Servicio para el área de Desarrollo de Sistemas con los detalles correspondientes. Sobre este particular se encontró que no se deja evidencia de las necesidades de los usuarios de las EAs que fueron rechazadas por la jefatura de Análisis y Control, así como tampoco una trazabilidad para determinar la totalidad de requerimientos que sí han sido aceptados y ya fueron implementados según un orden de prioridades preestablecido o aún se encuentran en espera de ser desarrollados.

La práctica de gestión BAI03.09 del proceso BAI03 referente a gestionar la identificación y construcción de soluciones, de COBIT 5, indica:

“BAI03.09 Gestionar cambios a los requerimientos

Hacer seguimiento del estado de los requerimientos individuales (incluyendo todos los requerimientos rechazados) a través de todo el ciclo de vida del proyecto y gestionar la aprobación de los cambios a los requerimientos.” El subrayado es propio.

En la actividad 4 de la práctica de gestión APO05.03 del proceso del COBIT 5 APO05 referente a la gestión de portafolios, se detalla lo siguiente:

“APO05.03 Evaluar y seleccionar los programas a financiar.

Basado en los requisitos de la mezcla general del portafolio de inversión, evaluar y priorizar casos de negocios de programas y decidir sobre las propuestas de inversión. Dedicar fondos e iniciar los programas (...)

4. Decidir qué programas candidatos deberían ser trasladados al portafolio de inversiones activas. Determinar si los programas rechazados deberían ser conservados para ser considerados en el futuro, o provistos con algún tipo de inversión para determinar si el caso de negocio puede ser mejorado o descartado.” El subrayado es propio.

El artículo 14.2.2 que trata sobre el control de cambios y que pertenece a la sección 14 de adquisición, desarrollo y mantenimiento de sistemas, del ISO-IEC-27002:2016, indica:

“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.”

El motivo principal de esta situación se debe a que el área de Análisis y Control nunca ha visto necesario darle un seguimiento más estricto a las necesidades lógicas de los usuarios de las EAs que utilizan diariamente la aplicación; generando que no se formalice internamente alguna norma para dicho fin.

Al no llevarse un control detallado sobre los requerimientos efectuados por las Entidades Autorizadas para el Sistema de Vivienda, se vuelve más difícil determinar si la totalidad de necesidades ya fueron resultas, si los tiempos de atención fueron adecuados, si existen controles lógicos importantes que no se han implementado, si se dejan requerimientos importantes y reiterativos sin ser atendidos, entre otros.

2.4 Administración y control sobre usuarios de las EAs

En el momento de revisar ciertos procesos relacionados con la administración y control de los usuarios de las Entidades Autorizadas, se localizaron algunas debilidades de control que seguidamente se detallan:

- a) Debido a la configuración de seguridad y conectividad que posee el Banco, los usuarios de las Entidades Autorizadas deben ser creados, activados o bloqueados (según corresponda) en la Base de Datos Oracle y en el Active Directory, para lo cual se elaboró en su momento el procedimiento P-DTI-SLA-018 denominado "*Bloqueo de cuentas de usuario no activas*". Según lo investigado, para la base de datos Oracle se tiene un control automatizado que bloquea a los usuarios después de 40 días de no haber ingresado al Sistema, sin embargo y de acuerdo al procedimiento indicado y los insumos recabados, en el Active Directory los usuarios se bloquean cada 6 meses (dos veces al año), pudiendo estar más de 140 días activos a pesar de que fueron bloqueados tiempo atrás en base de datos.
- b) En el área de Soporte Técnico se crearon por recomendación de la Auditoría Interna, dos super usuarios a nivel de base de datos ('SOPORTE_INF' y 'SOPORTE_SEG'), los cuales tenían como parte de sus funciones dar mantenimiento a los usuarios de las EAs, ya sea creando, activando, bloqueando o eliminando los usuarios que fueran necesarios. Todo lo anterior con el objetivo de poder identificar el personal de Soporte Técnico que realizó el trabajo a diferencia del DBA (Administrador de la Base de Datos). En la revisión se logró determinar que en la base de datos de Entidades, estos usuarios no se han utilizado una sola vez, sino que se han efectuado las modificaciones usando el usuario de SYSTEM que por defecto es el utilizado el DBA.
- c) Para la base de datos de Entidades, no existe ningún control lógico (Trigger) con el cual se pueda llevar un registro sobre la creación de usuarios de las Entidades Autorizadas, tampoco de las veces que han sido bloqueados o

desbloqueo, las fechas de esas acciones, ni cuál fue el usuario administrador que realizó la actividad. Este tipo de controles sí está implementado para la base de datos interna del Sistema de Vivienda.

- d) Al revisar los usuarios de las EAs vigentes en base de datos, se localizaron 9 usuarios que según lo indicado por el Administrador de la Base de Datos tuvieron que haber sido eliminados porque en su momento así fue solicitado por el área de Análisis y Control. Sin embargo aún están “activos” a pesar de que tengan un estatus de “Bloqueado” (Locked). Se muestra la lista correspondiente, donde además se puede detallar que no se guarda la fecha en que fueron bloqueados, según lo indicado en el punto c) anterior:

Usuarios de EAs Eliminados				
User	Status	User ID	Profile	Date Created
EA04	LOCKED	1022	PR_USUARIO_INTERNET	26/07/2012 07:09
EA04ESTUMANA	LOCKED	1773	PR_USUARIO_ESTANDAR	04/04/2016 09:54
EA04HENVARGAS	LOCKED	1695	PR_USUARIO_ESTANDAR	18/08/2014 08:29
EA04KARCOTO	LOCKED	1483	PR_USUARIO_ESTANDAR	14/02/2013 10:51
EA102GUAMORA	LOCKED	1770	PR_USUARIO_ESTANDAR	18/03/2016 10:42
EA26LUIGOMEZ	LOCKED	1142	PR_USUARIO_ESTANDAR	26/07/2012 07:17
EA27DANPEREZ	LOCKED	1161	PR_USUARIO_ESTANDAR	26/07/2012 07:19
EA88ROXFONSECA	LOCKED	1250	PR_USUARIO_ESTANDAR	26/07/2012 07:21
EA92EVEFALLAS	LOCKED	1715	PR_USUARIO_ESTANDAR	23/10/2014 08:23

- e) De acuerdo al procedimiento P-FOS-ANC-74 del departamento de Análisis y Control, esa jefatura es la encargada de informar al área de soporte cuando se debe suspender por un tiempo definido los accesos de alguno de los funcionarios de las Entidades Autorizadas ya sea por motivo de vacaciones, incapacidades, suspensiones, etc. Al respecto se determinó que esta actividad no se está realizando debido a que las EAs no comunican a ese departamento lo indicado, razón por la que esos usuarios son bloqueados solamente por falta de ingreso al Sistema.

Los incisos g), h) e i) del artículo 9.1.1 de la sección 9 relacionada con el Control de Accesos del ISO-IEC-27002:2016, detallan lo siguiente:

“9.1.1 Política de control de accesos

...Los propietarios de los activos deberían determinar las reglas de control de acceso apropiadas, los derechos de acceso y las restricciones para las funciones específicas de los usuarios, con respecto a sus activos con el nivel de detalle y el rigor de los controles que reflejan los riesgos asociados de seguridad de la información...

(...)

- g) *requisitos para autorizaciones formales de solicitudes de acceso (ver apartados 9.2.1 y 9.2.2);*
- h) *requisitos para revisión periódica de derechos de acceso (ver apartado 9.2.5);*
- i) *eliminación de derechos de acceso (ver apartado 9.2.6)”*

La actividad número 3 de la práctica de gestión BAI01.02 del proceso del COBIT 5 BAI01 relacionado con la gestión de programas y proyectos, indica lo siguiente:

*“3. Desarrollar un caso de negocio detallado para el programa, si se justifica. **Involucrar a todas las partes interesadas relevantes para desarrollar y documentar un entendimiento completo** de los resultados esperados por la empresa, cómo serán medidos estos resultados, el alcance total de las iniciativas requeridas, el riesgo involucrado y el impacto en todos los aspectos de la empresa. Identificar y evaluar los cursos de acción alternativos para lograr los resultados esperados por la empresa.”* El resaltado es nuestro.

En la práctica de gestión BAI03.10 del proceso BAI03 “*Gestionar la identificación y la construcción de soluciones*”, se muestra el siguiente enunciado:

“BAI03.10 Mantener soluciones

Desarrollar y ejecutar un plan para el mantenimiento de la solución y componentes de la infraestructura. Incluir revisiones periódicas respecto a las necesidades de negocio y requerimientos operacionales.”

De acuerdo a los temas indicados, se localizaron ciertas causas generales para tales situaciones, entre las que se indican las siguientes:

- Existe una falta de seguimiento interno sobre el cumplimiento de la normativa vigente y aplicable, incluyendo distintas actividades que de acuerdo al procedimiento debieron ser ejecutadas.
- Algunas de las debilidades detectadas no fueron previstas como controles necesarios a nivel operativo y lógico por las áreas involucradas.
- La existencia de ex funcionarios de las EAs aún vigentes (pero bloqueados) en la base de datos, se debe a una supervisión limitada sobre algunas de las actividades que deben ser ejecutadas por el DBA.
- Se carece de un mecanismo de comunicación más expedito entre las Entidades Autorizadas y el área de Análisis y Control, con el que se

facilite los avisos sobre suspensión de accesos al Sistema de forma temporal para funcionarios de las EAs que lo ameriten.

Como efectos de todas estas situaciones se pueden presentar modificaciones de permisos de usuarios de forma incorrecta, acceso a información por funcionarios de las EAs no autorizados o en tiempos no permitidos o acciones ejecutadas por personal de Soporte Técnico que no podrían ser trazables.

2.5 Casos de Usos de las EAs

Como parte de la evaluación se valoró la participación de las Entidades Autorizadas en el desarrollo del nuevo Sistema de Vivienda. Al respecto se nos indicó por la jefatura del Departamento de Análisis y Control y por la Administradora de Proyectos de TI, que los únicos requerimientos que hasta el momento se han tomado en cuenta para las EAs, son los que ha considerado y definido el señor Alexis Solano, esto a pesar de que no es una labor que le corresponda. Siendo así, no se han involucrado usuarios claves de las EAs para la definición de sus casos de usos.

Para la definición de requerimientos de las EAs también se localizó que no se contaba con los procesos definidos de las Entidades y sus distintas relaciones (entradas/salidas) a nivel del sistema. Sobre este tema se presentó a la Auditoría un borrador sobre el desarrollo de dichos procesos, pero aún en etapa de revisión.

Adicionalmente a la fecha de la auditoría tampoco se habían definido casos de uso por parte del Departamento Técnico del FOSUVI a nivel de los proyectos de vivienda, ya que se nos indicó que se está planteando por esa Dirección la adquisición de un sistema ya existente para la administración de dichos proyectos. Al respecto aún no se cuentan con los procesos finales aprobados por la Dirección FOSUVI.

En las actividades 1 y 2 de la práctica de gestión BAI03.02 del COBIT 5, encontramos el siguiente criterio relacionado con este tema:

“BAI03.02 Diseñar los componentes detallados de la solución.

Desarrollar, documentar y elaborar diseños detallados progresivamente usando técnicas de desarrollo ágiles o por fases acordadas previamente considerando todos los componentes (procesos de negocio y automatización relacionada y controles manuales, aplicaciones soporte de TI, servicios de infraestructura y productos tecnológicos y proveedores/fabricantes). Asegurar que el diseño detallado incluye ANSs y OLAs internos y externos.

1. *Diseñar progresivamente las actividades del proceso de negocio y los flujos de trabajo necesarios para llevar a cabo conjuntamente con el nuevo sistema de aplicación para alcanzar los objetivos de la empresa, incluyendo el diseño de actividades de control manuales.*
2. *Diseñar las etapas de procesamiento de la aplicación, incluyendo especificaciones de tipos de transiciones y reglas de negocio, controles automatizados, definiciones de datos/objetos de negocio, casos de uso, interfaces externos, limitaciones de diseño y otros requerimientos (por ejemplo, licencias, legales, estándares e internacionalización/localización).*

Una de las razones por las que no se hayan involucrado a la fecha funcionarios de las EAs en la definición de requerimientos se debe que a nivel administrativo se han enfocado solo hacia las necesidades internas del sistema.

Como parte de los efectos de estar desarrollando casos de uso sin involucrar a personal clave y sin contar aún con los procesos relacionados, es que una vez que se brinden los flujos de procesos definitivos, se tengan que efectuar reprocesos sobre los requerimientos previamente identificados, generando que el plazo final de conclusión del proyecto del nuevo Sistema de Vivienda se prolongue aún más.

3. CONCLUSIÓN

La auditoría sobre la administración efectuada del Sistema de Vivienda utilizado por las Entidades Autorizadas, se valoraron los insumos de relevancia a nivel de sistemas de información.

La ejecución del trabajo fue realizado aplicando las técnicas de auditoria correspondiente, evaluando la normativa vigente aplicable y los controles asociados identificados y definidos por la Administración Activa. También fueron realizadas entrevistas al personal clave involucrado directamente en su administración y control.

Se detectaron debilidades principalmente en la administración lógica de cuentas de usuarios y super usuarios, desactualización de documentación, carencia de normativa interna, falta de seguimiento a las necesidades del sistema para usuarios externos, limitada comunicación entre las Entidades Autorizadas y el área de Análisis y Control para una suspensión lógica temporal de sus empleados, entre otros.

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. Todas las recomendaciones están dirigidas para su seguimiento e implementación hacia la Dirección FOSUVI.

4.1 Manual de usuario del Sistema para las EAs

A la Dirección FOSUVI

4.1.1 Ejercer las gestiones suficientes para actualizar el Manual de Usuario del Sistema de Vivienda utilizado por las Entidades Autorizadas, de acuerdo a las actualizaciones que ha tenido la aplicación en los últimos 10 años.

Nivel de Riesgo: **Medio**

4.1.2 Designar el seguimiento y actualización del Manual de Usuario del Sistema de Vivienda (interno y externo) a alguno de los puestos existentes en la Dirección FOSUVI, actividad que debe ser ejecutada al menos una vez al año en vista de los cambios constantes que se dan en la aplicación.

Nivel de Riesgo: **Medio**

4.2 Capacitación en el uso del Sistema

A la Dirección FOSUVI

4.2.1 Elaborar una guía formal donde se contemplen todos los temas que deben ser incluidos al momento de capacitar a los funcionarios de las Entidades Autorizadas. Para esto debe implementarse la normativa interna correspondiente.

Nivel de Riesgo: **Bajo**

4.3 Requerimientos del Sistema de Vivienda Actual

A la Dirección FOSUVI

4.3.1 Debe evaluarse en conjunto con el Departamento de TI la posibilidad de implementar algún mecanismo sistematizado (que no sea el correo electrónico), con el cual las Entidades Autorizadas puedan dejar plasmados los distintos requerimientos que tenga sobre el Sistema de Vivienda de acuerdo a sus necesidades; abriendo la posibilidad de que tanto a nivel institucional como de los usuarios claves de las EAs, se pueda dar un seguimiento detallado al estado de dichas necesidades, así como para evidenciar los motivos por las que determinados requerimientos no fueron tomados en cuenta para ser desarrollados.

Nivel de Riesgo: **Medio**

4.4 Administración y control sobre usuarios de las EAs

Al Departamento de TI

4.4.1 Actualizar el procedimiento P-DTI-SLA-018 “Bloqueo de cuentas de usuario no activas”, de acuerdo a las herramientas tecnológicas que actualmente se están utilizando en el área de Soporte Técnico y donde se modifiquen los tiempos de ejecución de la tarea que bloquea a los usuarios en el Active Directory, para que no se realice cada 6 meses, sino una vez que fueron bloqueados en la base de datos Oracle.

Nivel de Riesgo: **Bajo**

4.4.2 Habilitar los usuarios de 'SOPORTE_INF' y 'SOPORTE_SEG' para que sean utilizados por el personal de Soporte Técnico del Departamento de TI según corresponda, dejando así el uso de SYSTEM exclusivamente para el Administrador de Base de Datos (DBA). Con esto en caso de ser necesario, se podría determinar el funcionario que ejecutó determinada acción en la base de datos interna o de Entidades.

Nivel de Riesgo: **Medio**

4.4.3 Implementar en la base de datos de Entidades un disparador (Trigger) que registre las fechas de los bloqueos, desbloqueos, eliminación o creación de usuarios de las Entidades Autorizadas; así como el funcionario de Soporte Técnico que ejecutó la actividad.

Nivel de Riesgo: **Bajo**

4.4.4 Deben eliminarse los 9 usuarios detallados en el punto d) del hallazgo 2.4 relacionado con la administración y control sobre los usuarios de las EAs.

Nivel de riesgo: **Medio**

A la Dirección FOSUVI

4.4.5 Se deben efectuar los ajustes necesarios al procedimiento P-FOS-ANC-74 del departamento de Análisis y Control, con el fin de coordinar de una mejor manera con las Entidades Autorizadas la comunicación sobre sus funcionarios que utilicen el Sistema de Vivienda y que deban suspender temporalmente los accesos a la aplicación ya sea por vacaciones, incapacidad, permisos, suspensiones, entre otros. De esta forma dichos usuarios podrían ser bloqueados por un tiempo definido por el área de Soporte Técnico del Banco.

Nivel de Riesgo: **Bajo**

4.5 Casos de Uso de las EAs

A la Dirección FOSUVI

4.5.1 Se deben identificar e involucrar usuarios claves de las Entidades Autorizadas para la definición de necesidades para el nuevo Sistema de Vivienda, teniendo así casos de uso específicos (requerimientos) de esos funcionarios, que se adapten a la operativa general de cada institución.

Nivel de Riesgo: **Alto**

4.5.2 Es necesario definir de manera formal, cuál será el rumbo a tomar para la administración y control de los proyectos de vivienda a nivel del nuevo Sistema de Vivienda, ya sea que se decida la compra de una aplicación a la medida o que se continúe con la definición de casos de uso para los proyectos.

Nivel de Riesgo: **Alto**

4.5.3 Deben gestionarse a la brevedad posible las aprobaciones correspondientes sobre los procesos (y sus flujos respectivos) del Sistema de Vivienda que están siendo desarrolladas por la Unidad de Planificación. Esto con la finalidad de tener los insumos finales adecuados para la elaboración de los casos de uso relacionados con las Entidades Autorizadas, evitando además reprocesos y por ende mayor ampliación en el lapso de conclusión del Sistema.

Nivel de Riesgo: **Medio**

MBA. Gustavo Flores Oviedo.
Auditor Interno.