Banco Hipotecario de la Vivienda

Informe Final TI-SI-001-2018

AUDITORÍA SOBRE EL SISTEMA DE EXPEDIENTES DE PROYECTOS Y ART. 59

19/06/2018

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 BITÁCORA DEL SISTEMA Y CONTROLES EN LÍNEA. 6
2.2 ROLES Y USUARIOS DEL SISTEMA 6
2.3 CONCENTRACIÓN DE FUNCIONES 8
2.4 CONSISTENCIA E INTEGRIDAD DE BASE DE DATOS 9
2.5 CASOS DE BONO PENDIENTES DE PAGO 11

3. CONCLUSIÓN 13

4. RECOMENDACIONES 14

4.1 BITÁCORA DEL SISTEMA Y CONTROLES EN LÍNEA 15
4.2 ROLES Y USUARIOS DEL SISTEMA 15
4.3 CONCENTRACIÓN DE FUNCIONES 16
4.4 CONSISTENCIA E INTEGRIDAD DE BASE DE DATOS 16
4.5 CASOS DE BONO PENDIENTES DE PAGO 17

A. RESUMEN EJECUTIVO

En esta auditoria se evaluaron los principales controles existentes en el sistema de Expedientes de Proyectos y Art. 59, revisando tanto el proceso de administración de la herramienta como las áreas lógicas básicas para una adecuada utilización y control.

Dentro de los hallazgos se localizó la carencia de una bitácora de movimientos que vaya registrando los movimientos que de acuerdo al área dueña del sistema, no sean comunes o correctos. Tampoco se ha establecido avisos automáticos que informen inmediatamente se registre alguna transacción sospechosa.

En la evaluación de la seguridad de la aplicación a nivel de roles y accesos, se localizaron usuarios habilitados en el sistema que por distintas razones ya no laboran en esa área y aún se mantienen con permisos vigentes. Además se carece de un control automático que avise sobre algún cambio en los roles existentes.

Otro de los hallazgos está vinculado con una concentración de funciones a nivel de permisos lógicos y acciones ejecutadas en el sistema a lo largo de varios años, por dos funcionarias del FOSUVI.

Valorando la consistencia e integridad de los datos, de acuerdo a la visión de la Auditoría Interna, se localizaron campos con falta de información o con inconsistencia entre otros campos similares.

Por último, también a nivel evaluación de la información del sistema, se ubicaron casos de bonos de vivienda que no han sido finalizados a pesar de tener (al menos a nivel de base de datos) a satisfacción los procesos anteriores.

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 Nº TI-SI-001-2018
19 de Junio del 2018

AUDITORÍA SOBRE EL SISTEMA DE EXPEDIENTES DE PROYECTOS Y ART.59

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 los controles existentes y la administración realizada por el dueño del Sistema de Expedientes de Proyectos y Artículo 59.

1.3 Alcance

El estudio abarcó la documentación, información y procesos operativos vigentes al 31 de Diciembre del 2017 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
- ✓ Manual para el ejercicio de la práctica de la Auditoria Interna.
- ✓ Norma 308 Comunicación de resultados
- ✓ ISO 27002:2005 Tecnologías de Información – Código de buenas prácticas para la gestión de la 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 utilizan el sistema de Expedientes de Proyectos y Artículo 59 y con el personal técnico interno que colabora con el soporte del mismo. Adicional se evaluó la existencia y razonabilidad de la documentación formal y procesos establecidos para controlar la aplicación.

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 sección de Resultados de la Evaluación.

2. RESULTADOS DE LA EVALUACIÓN

2.1 Bitácora del Sistema y Controles en Línea.

En el proceso de auditoría se tenía previsto evaluar los registros existentes en la bitácora de movimientos del sistema de Expedientes de Proyectos y Art. 59. Al respecto se determinó que no se ha implementado una bitácora de base de datos que se genere a partir de transacciones que de acuerdo al criterio de esa área, no sean normales o correctas desde el punto de vista operativo o de control.

De igual forma no se localizaron controles en línea que informen en el momento sobre cambios en ciertos datos que la unidad haya establecido de mayor relevancia y que se realicen sin autorización previa por la Dirección.

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."*

La razón fundamental por la que no existe una bitácora del sistema así como un monitoreo en línea a sus bases de datos, se debe a que no se ha normado en la Dirección FOSUVI la implementación y revisión de este tipo de controles automatizados.

La inexistencia de bitácoras sobre la información relevante, impide determinar si las modificaciones o borrados de los datos fueron correctas y debidamente procesadas. De igual forma, al no contar con controles lógicos que informen automáticamente y en el momento preciso de la acción sobre cambios no autorizados, limita el pronto accionar de los dueños de la información, pudiendo darse por aceptados procesos o actividades incorrectas.

2.2 Roles y usuarios del sistema

En la evaluación de los roles y perfiles lógicos asignados en el sistema de Expedientes de Proyectos y Art. 59., se determinó que no se ejecutan revisiones periódicas sobre la correcta asignación y vigencia de los mismos. Sobre este

particular, se localizaron en la aplicación funcionarios activos que por distintas razones ya no pertenecen a esa la Dirección FOSUVI. Seguidamente se muestra un cuadro resumen este hecho:

EXFUNCIONARIOS ACTIVOS Y VIGENTES EN EL SISTEMA EXPEDIENTES DE PROYECTOS Y ARTÍTUCLO 59

NOMBRE DE USUARIO	ID_USUARIUO	ROL	ESTADO
ARCE BOLAÑOS CARLOS	CARARCE	SEPR02	A
ARTAVIA HUERTAS MARCO	MARARTAVIA	SEPR02	A
MATA NUÑEZ ESTRELLA	ESTMATA	SEPR02, SEPR03	A
CHINCHILLA CAMPOS FRANKLIN	FRACHINCHILLA	SEPR04	A
CASTRO MORALES GERALDINNE	GERCASTRO	SEPR02, SEPR03	A
CASTRO MARIN KAROLINA	KARCASTRO	SEPR02, SEPR03	A
ALVAREZ SANCHEZ LUIS	LUIALVAREZ	SEPR03	B
ARTAVIA HUERTAS MARCO	MARARTAVIA	SEPR03	A
MONGE QUIROS MARIANELA	MARMONGE	SEPR03	C

A= Exfuncionario del Banco
B= Funcionario trasladado a otro departamento
C= Funcionaria licencia sin goce de salario

Además con el tema de control sobre los roles se halló la inexistencia de avisos en línea que notifiquen de forma automática a los funcionarios responsables sobre cualquier cambio o asignación de privilegios lógicos a otros funcionarios, sin la previa autorización del dueño del sistema.

En el BAI10.05 del COBIT 5, subproceso del BAI10 relacionado con la gestión de la configuración, se indica lo siguiente:

> "***Verificar y revisar la integridad del repositorio de configuración***.
> *Revisar periódicamente el repositorio de configuración y verificar la integridad y exactitud con respecto al objetivo deseado."* El subrayado es nuestro.

También en el COBIT 5, en el subproceso DSS05.04 del dominio de Construir, Adquirir e Implantar (BAI), con respecto a los derechos de acceso se dicta lo siguiente:

> *"**DSS05.04 Gestionar la identidad del usuario y el acceso lógico***
> *Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio."*

Estas situaciones se presentan debido a que no existe ninguna normativa interna enfocada a verificar de forma periódica los privilegios lógicos establecidos en el Sistema Expedientes de Proyectos y Art. 59 a nivel de roles y perfiles.

No tener implementado un control que brinde seguimiento a las modificaciones o permisos sobre los roles y perfiles del sistema, incrementa la posibilidad de modificaciones o accesos no autorizados en los datos referentes a Expedientes de Proyectos y Art. 59, pudiendo verse afecta la integridad y seguridad de la información, sin que pueda ser detectado por el encargado de la aplicación.

2.3 Concentración de Funciones

Al evaluar los roles existentes en el sistema de Expedientes de Proyectos y Art. 59, se logró determinar que las funcionarias Hannia Martínez Cordero, Lisseth Araya Quiros y Pamela Quiros Espinoza, poseen un control total por tener asignados todos los roles vigentes (SEPR01, SEPR02 y SEPR03); situación que por defecto genera una concentración lógica sobre las funciones de la aplicación.

Al respecto de este tema y evaluando los movimientos en bases de datos, se localizaron 1.900 registros en los que fueron adicionados y modificados por la señorita Martínez Cordero y 4 registros con la misma situación por parte de Lisseth Araya.

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."* El subrayado es propio.

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.

En la práctica de gestión DSS06.03 del COBIT 5, relacionada con gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización; se encuentra el siguiente criterio:

"Gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Autorizar el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia del negocio, de TI y de terceras partes. Esto asegura que el negocio sabe donde están los datos y quien los está manejando en su nombre."

Una de las principales causas de esta concentración lógica, se debe a la carencia de alguna normativa interna que limite darle todas las potestades lógicas a un mismo usuario en determinado sistema.

Dentro de las consecuencias de esta concentración, se encuentra la posibilidad de que existan errores o modificaciones no autorizadas en la información de los bonos o proyectos, que no logren ser detectados.

2.4 Consistencia e Integridad de base de datos

En el proceso de revisión de la base de datos, se logró comprobar que no se realizan pruebas periódicas por parte de los dueños del sistema, enfocadas a determinar si la principal información que procesa y resguarda el sistema de Expedientes de Proyectos y Art. 59 es consistente e íntegra.

Como parte de la auditoría se ejecutaron algunas pruebas sustantivas sobre la totalidad de la información contenida en la base de datos del sistema, encontrando ciertas inconsistencias de acuerdo a los criterios utilizados por la Auditoría Interna, mismas que seguidamente se detallan:

a) Se encontraron 12 registros de diferentes tipos de bonos (proyectos, artículo 59, individuales llave en mano, individuales indígenas, etc), en los que el caso fue aprobado para ser desembolsado por Junta Directiva (APDJ), pero sin embargo no cuentan con ningún número de oficio (NUM_OFICIO_REC) que los respalde.

b) Evaluando la integridad del campo del monto aprobado (MTO_APROBADO) para los tipos de bono de expediente técnico del proyecto (EXPP), proyectos de casos individuales de 5 a 20 casos (PRCI)

y proyectos del Triángulo de Solidaridad (PRTS), se ubicaron 259 registros que tienen esa información en cero o nula a pesar de estar como aprobados por Junta Directiva (APDJ). Además sobre este mismo campo, se localizaron 7 transacciones donde el monto aprobado tiene un valor de 1 y también en estado APDJ. De acuerdo a lo evaluado en la revisión, cuando un caso ya tiene el estado de APDJ, se debe a que ya cumplió con las revisiones correspondientes y está listo para ser desembolsado.

c) El sistema cuenta con dos campos enfocados a determinar el estado de los casos, específicamente el de RESULTADO y el de ID_ESTADO_PROY. En la revisión se localizaron inconsistencias con relación a estos dos campos, donde existen 30 movimientos en los que el registro tiene un RESULTADO de Aprobado (A), pero con estado Devuelto (DEVE) en el campo ID_ESTADO_PROY.

d) De los mismos dos campos citados en el punto c), se ubicaron 10 registros con el estado del RESULTADO devuelvo (D), pero aprobados por Junta Directiva (APJD). Así mismo, existen 515 registros con el RESULTADO pendiente (P) y también con en estado APJD.

e) La base de datos cuenta con dos campos básicos de seguimiento, uno para determinar cuál fue el usuario que creo el registro (ADICIONADO_POR) así como su respectiva fecha (FECHA_ADICION); y otro campo que indica el último usuario que modificó el mismo registro (MODIFICADO_POR) así como su respectiva fecha (FECHA_MODIFICACION). Al respecto se encontró que el 08/06/15 se registraron 2.737 movimientos donde el usuario que modificó la información es el utilizado por el Administrador de la base de datos (SYSTEM). Por los límites que tiene la base de datos a nivel de trazabilidad (indicado en este informe en el hallazgo 2.1), es imposible determinar cuál fue la información que fue modificada.

f) Evaluando los diferentes tipos de bonos individuales que se administran en el sistema, se localizaron varios tipos a los que ya se les había aprobado se pago (APDJ), pero sin ningún detalle del monto aprobado (MTO_APROBADO). Específicamente las siguientes cantidades:

- ✓ 5 registros de casos individuales de segundo bono (CI50)
- ✓ 283 registros de casos de artículo 59 (CI59)
- ✓ 1707 registros de casos individuales de llave en mano (CILM)
- ✓ 415 registros de casos individuales de indígenas (CIRI)
- ✓ 46 registros de casos individuales del Triángulo de Solidaridad (CITS)

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."*

En el manual de Control Interno de la Contraloría N-2-2009-CO-DFOE, en su artículo 4.4 denominado "Exigencia de confiabilidad y oportunidad de la información", se detalla:

> *''El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente que se recopile, procese, mantenga y custodie información de calidad sobre el funcionamiento del SCI y sobre el desempeño institucional, así como que esa información se comunique con la prontitud requerida a las instancias internas y externas respectivas...''*

Como parte de los motivos por los que se presentan algunas de las debilidades indicadas, se debe a la carencia de controles de consistencia entre los campos que deben tener relación entre ellos. Lo anterior aunado a que desde que empezó a operar la aplicación (2010 según los primeros registros), no se han realizado revisiones de consistencia e integridad de la base de datos por la falta de alguna norma que lo obligue.

Las inconsistencias y faltas de integridad en las bases de datos tienden a limitar la toma de decisiones cuando no se está seguro si la información brindada por la aplicación es veraz o correcta. En este caso por el tipo de datos, podrían presentarse problemas al momento de gestionar o entregar alguno de los bonos administrados en el sistema de Expedientes de Proyectos y Art. 59.

2.5 Casos de bono pendientes de pago

La revisión de la base de datos por el alcance de la auditoría, se realizó en su gran mayoría sobre la información del sistema de Expedientes de Proyectos y Art. 59. Sin embargo y debido a la forma en que esta aplicación se liga con el Sistema de Vivienda, se efectuaron algunas consultas sobre dicha relación.

Como resultado de este trabajo, al verificar el flujo de pago de algunos bonos, se localizaron 36 casos que fueron aprobados por Junta Directiva (APJD) desde los años 2012 al 2016 y que tan siquiera han sido emitidos por el área del FOSUVI,

esto significa que están solamente como digitados por la Entidad Autorizada (y se mantienen en esa base de datos). Adicionalmente, se localizaron para los años del 2013 al 2016, 183 registros que ya habían sido emitidos por el Banco y aprobados para ser desembolsados, pero aún no se han girado los recursos correspondientes.

En el artículo 4.5 de las Normas de Control Interno para el Sector Publico (N-2-2009-CO-DFOE), se dicta lo siguiente:

> *"**4.5 Garantía de eficiencia y eficacia de las operaciones***
> *El jerarca y los titulares subordinados, según sus competencias, deben establecer actividades de control que orienten la ejecución eficiente y eficaz de la gestión institucional. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de sus operaciones y los riesgos relevantes a los cuales puedan verse expuestas, así como los requisitos indicados en la norma 4.2*

Además, en el proceso DSS06 del COBIT 5, en la práctica de gestión DSS06.02, se menciona con relación al procesamiento de la información:

> *"**DSS06.02 Controlar el procesamiento de la información***
> *Operar la ejecución de las actividades de proceso de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de la información es válido, completo, preciso, oportuno y seguro (es decir, refleja el uso de negocio autorizado y legitimado.)"*

Dentro de las posibles causas para que se presenten los atrasos en los desembolsos indicados, se encuentra la carencia de ayudas o avisos en línea en el sistema que vayan informando periódicamente a la Dirección sobre estos atrasos u otros temas que deban ser valorados con mayor prontitud.

El efecto directo de esta situación lo tienen los posibles beneficiarios del bono de vivienda, al no contar con una solución para sus problemas con la diligencia que corresponda de acuerdo a la normativa vigente.

3. CONCLUSIÓN

En el transcurso de la auditoría del sistema de Expedientes de Proyectos y Artículo 59, se logró determinar que se carecen de controles básicos para una correcta administración tanto de la aplicación como de la información que la compone. Así mismo, en los resultados del estudio se resalta el exceso de permisos lógicos sobre algunos funcionarios y la falta de valoraciones periódicas sobre los datos contenidos en la aplicación.

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.

En general las deficiencias encontradas y detalladas en la sección dos de este documento, traen un detrimento de control sobre muchas de las actividades relacionadas con Expedientes de Proyectos y Art. 59 y que son administradas utilizando las tecnologías de información.

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

4.1 Bitácora del Sistema y Controles en Línea

4.1.1 Definir con la colaboración del Departamento de TI, una bitácora del sistema de Expedientes de Proyectos y Art. 59 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.

Nivel de Riesgo: **Alto**

4.1.2 Implementar en el Sistema de Expedientes de Proyectos y Art. 59, controles en línea (correo electrónico por ejemplo) que informen inmediatamente se genere alguna acción indebida sobre ciertos datos y que haya sido previamente identificada por el dueño de la aplicación.

Nivel de Riesgo: **Alto**

4.1.3 Una vez implementada la bitácora, debe elaborarse la normativa correspondiente enfocada a una revisión periódica (al menos una vez al año) sobre la información contenida en ella. La actividad debe quedar documentada.

Nivel de Riesgo: **Medio**

4.2 Roles y usuarios del sistema

4.2.1 Se deben eliminar los permisos en el sistema de Expedientes de Proyectos y Art. 59 a cada uno de los funcionarios indicados en este informe y que por diversas razones ya no laboran en esa Dirección o no deberían estar habilitados como usuarios de la aplicación por estar ubicados operativamente en otros departamentos del Banco.

Nivel de Riesgo: **Medio**

4.2.2 Coordinar con el Departamento de TI la implementación de un control automático que avise de forma inmediata a los funcionarios que esa Dirección considere convenientes, sobre cualquier alteración o asignación de privilegios del sistema a nuevos usuarios.

Nivel de Riesgo: **Alto**

4.3 Concentración de Funciones

4.3.1 Deben ser revocados los controles totales al sistema de Expedientes de Proyectos y Art. 59 a las funcionarias Hannia Martínez Cordero, Lisseth Araya Quiros y Pamela Quiros Espinoza; con el objetivo de evitar la concentración de funciones lógicas vigentes sobre la aplicación

Nivel de Riesgo: **Alto**

4.3.2 Es necesario instituir alguna norma en la que se regule y limite la asignación de permisos lógicos totalmente a cualquiera de los usuarios que utilicen los sistemas de la Dirección FOSUVI.

Nivel de Riesgo: **Medio**

4.4 Consistencia e Integridad de base de datos

4.4.1 Se debe realizar un estudio detallado de la base de datos del sistema de Expedientes de Proyectos y Art. 59 y evaluar las inconsistencias o irregularidades que se detallan en el punto 2.4 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.

Nivel de Riesgo: **Medio**

4.4.2 Coordinar con el Departamento de TI la implementación de controles a nivel de base de datos (no de la forma), destinados a validar la consistencia entre los campos que lo ameriten, impidiendo así que se utilicen valores que no correspondan de acuerdo al avance que lleve el estado del caso o a los valores mínimos (no nulos por ejemplo) que debería contener cada campo.

Nivel de Riesgo: **Medio**

4.4.3 Crear la normativa suficiente enfocada a valorar de forma periódica la consistencia e integridad de la principal información contenida en el sistema de Expedientes de Proyectos y Art. 59. Esta actividad debe quedar documentada y debe ser revisada por la Dirección Administrativa
Nivel de Riesgo: **Medio**

4.5 Casos de Bono Pendientes de Pago

4.5.1 Se debe hacer un estudio detallado sobre los registros indicados en el hallazgo 2.5 de este informe, específicamente sobre los 36 casos emitidos y los 183 casos que están listos para ser girados desde hace más de dos años (en algunos casos hasta 6 años), y que a la fecha de la auditoría aún se encontraban pendientes de ser girados. El resultado del estudio debe ser remitido a la Auditoría Interna como respaldo de la labor ejecutada.

Nivel de Riesgo: **Medio**

4.5.2 Coordinar con el Departamento de TI la implementación de avisos periódicos que informen después de cierto tiempo (a definir por el dueño del sistema), la demora o detención del proceso de pagos y desembolsos para los diferentes tipos de bonos que se administran en el sistema de Expedientes de Proyectos y Art. 59 y en el sistema de Vivienda.

Nivel de Riesgo: **Medio**

MBA. Gustavo Flores Oviedo.
Auditor Interno.