Contadores públicos y
consultores gerenciales

INSTITUTO DE FOMENTO DE HIPOTECAS ASEGURADAS –FHA

AUDITORÍA DE ESTADOS FINANCIEROS
AL 31 DE DICIEMBRE DE 2016

VERIFICACIÓN DE LA SEGURIDAD Y CONFIABILIDAD DE LOS PROCESOS ELECTRÓNICOS DE INFORMACIÓN

Arévalo Pérez, Iralda y Asociados, S.C.

Arévalo Pérez, Iralda y Asociados, S.C.

PKF

Contadores públicos y
consultores gerenciales

13 de enero de 2017

Señores
Junta Directiva
Instituto de Fomento de Hipotecas Aseguradas –FHA
Ciudad

Estimados señores:

Como parte de la auditoría a los estados financieros del Instituto de Fomento de Hipotecas Aseguradas –FHA al 31 de diciembre de 2016 y por el año terminado en esa fecha, efectuamos una revisión en las áreas de los principales procesos electrónicos de información definidos por la Administración.

Tanto las operaciones realizadas en el Instituto relacionadas con las áreas mencionadas en el primer párrafo, como la correspondiente documentación de respaldo son responsabilidad de la Administración de la referida Entidad.

Nuestra responsabilidad se limita a expresar nuestras conclusiones sobre la eficacia de los procedimientos y controles que el Instituto tiene en operación para el manejo de cada área, y en general de la forma como opera el Instituto.

Derivado de dicha revisión, les informamos que no observamos hallazgos importantes que deban ser reportados a su Administración; así mismo efectuamos el seguimiento a los hallazgos observados en la revisión de sistemas automatizados de información en auditorías anteriores, los cuales se describen en el memorándum adjunto.

Atentamente,

Licda. Olga Siomara Arévalo Iralda
Socia de Auditoría

Copia: Arquitecto Daniel López
Gerente General

Tel (502) 2332-8831 | (502) 2332-8832 | (502) 2363-1068 | (502) 2363-1078 | (502) 2363-1088
Fax (502) 2363-0568 | (502) 2363-0328 | Email: arevalo@pkfguatemala.com
PKF | 13 calle 2-60 Zona 10, Edificio Topacio Azul, Oficina 1202 | Guatemala 01010 | Guatemala, C.A

INSTITUTO DE FOMENTO DE HIPOTECAS ASEGURADAS –FHA

Auditoría de estados financieros al 31 de diciembre de 2016

SEGUIMIENTO A LAS OBSERVACIONES RELACIONADAS CON LOS PROCESOS ELECTRÓNICOS DE INFORMACIÓN DERIVADAS DE AUDITORIAS ANTERIORES

Como parte de los procedimientos de auditorías aplicados al 31 de diciembre de 2016, efectuamos el seguimiento a las observaciones de sistemas automatizados de información de auditorías anteriores, y excepto por los asuntos mencionados a continuación, los demás ya fueron implementados:

1. *Falta de estandarización para la asignación de permisos, usuarios y perfiles.*

Dada la variedad del conjunto de sistemas (auxiliares y principales) que componen la infraestructura informática del FHA, existen diferentes elementos que involucran al mismo usuario. De la evaluación de los aplicativos la asignación de permisos (con excepción del módulo de recurso humano) no está basada en perfiles, sino se asignan directamente al usuario, lo que complica la administración de permisos a todo el core de la institución. En algunos casos (como el seguro de desgravamen o primas por cobrar) ni siquiera tienen usuario asignado sino se trata de un ejecutable instalado en la computadora del usuario.

Recomendación:

Evaluar la posibilidad a nivel de proyecto informático de consolidar la asignación de permisos de los diferentes usuarios de los aplicativos que permita:

a) Un usuario único para todas las aplicaciones.

b) Una estructura basadas en rol (perfil)/permiso y niveles de roles que simplifique la asignación a los diferentes usuarios.

c) Que todas las aplicaciones tengan un usuario y un rol sin excepción (mitigar problemas de seguridad).

Comentario de Administración al 30 de junio de 2016

Como parte del proceso de modernización de los sistemas ya se cuenta con el documento denominado DERCAS (Documento de especificación de requerimientos y criterios de aceptación del software) para el Módulo de Seguridad, por lo que formará parte de los aplicativos que serán reemplazados próximamente y formará parte de los aplicativos que se incluirán en el primer evento de licitación pública.

Cabe indicar que este aspecto fue del conocimiento de Junta Directiva quien estuvo de acuerdo con el cronograma y el plan de inversión.

Comentario de Administración al 31 de diciembre de 2016:

Durante el mes de Enero del año 2017, se iniciará el proceso de licitación para los primeros diez módulos de los nuevos aplicativos que conforman el núcleo (Core) del negocio del Instituto, dentro de los cuales está incluido el Módulo de Seguridad, modulo que ya considera el manejo de perfiles de usuario para los accesos a las aplicaciones.

2. *Falta de un Plan de Contingencias – Recuperación de Desastres debidamente documentado*

El Instituto no cuenta con un Plan de Contingencias para la recuperación de desastres debidamente documentado.

Recomendación:

Recomendamos se analice la posibilidad de elaborar un Plan de Contingencias para la *Recuperación de Desastres debidamente documentado.*

Por lo que es necesario desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la institución. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias.

El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.

En base al marco de trabajo se debe desarrollar el plan de continuidad de TI, el cual debe ser diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio.

Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI.

También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas al plan.

Comentario de Administración al 30 de junio de 2016

Dentro del Plan Estratégico del Departamento de Informática, se tiene programada la ejecución de las acciones para atender esta recomendación, a la fecha se cuenta con algunas alternativas para la implementación del Sitio Alterno, las cuales fueron presentadas a Junta Directiva; y está pendiente de determinarse cuál de las alternativas podría ser la más conveniente a los intereses de la Institución.

Comentario de Administración al 31 de diciembre de 2016

El 22 de noviembre de 2016 se adjudicó a la empresa Servicios de TI, S.A. (Kio Networks) la contratación de un sitio alterno para los servidores críticos y de criticidad media del Instituto por un año, en el mes de diciembre se iniciaron los trabajos de configuración de la replicación de la información los que se espera queden finalizados durante el mes de enero del año 2017.