PKF

Contadores públicos y
consultores gerenciales

INSTITUTO DE FOMENTO DE HIPOTECAS ASEGURADAS –FHA

AUDITORÍA DE ESTADOS FINANCIEROS
AL 31 DE DICIEMBRE DE 2018

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.

Contadores públicos y
consultores gerenciales

18 de enero de 2019

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

Estimados señores:

Como parte de la auditoría de los estados financieros del Instituto de Fomento de Hipotecas Aseguradas –FHA al 31 de diciembre de 2018 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 en el área de contabilidad.

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 al 31 de diciembre de 2018 observamos algunos hallazgos importantes que consideramos deben ser reportados a su Administración. En el memorándum adjunto se describen los procedimientos de revisión efectuados y los resultados de dicha revisión.

I. Hallazgos relacionados con los procesos electrónicos de información al 31 de diciembre de 2018.

II. Seguimiento a las observaciones relacionadas con los procesos electrónicos de información derivadas de auditorías anteriores.

III. Procedimientos de revisión efectuados al 31 de diciembre de 2018.

Atentamente,

Lic. Hugo Arévalo Pérez
Socio Director

Copia: Señora Carol Lucrecia del Carmen Garza Álvarez de Martínez
Gerente

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 2018

I. HALLAZGOS RELACIONADOS CON LOS PROCESOS ELECTRÓNICOS DE INFORMACIÓN AL 31 DE DICIEMBRE DE 2018.

1. Falta de integración de actividades de monitoreo de servicios, infraestructura, contingencia, y otros, en una administración de riesgos de TI.

El departamento de sistemas realiza actividades de gestión y monitoreo de aspectos relacionados con las tecnologías de información, como por ejemplo:

- Monitoreo de uso de recursos de infraestructura;
- Aseguramiento de los equipos;
- Gestión de incidentes;
- Revisión del software instalado en los equipos;
- Actividades de respaldo de información;
- Plan de recuperación ante desastres.

Sin embargo, consideramos que hace falta integrar todas estas actividades en una gestión efectiva de los riesgos de TI.

Riesgos:

- Una determinación inadecuada de las inversiones y acciones en materia de salvaguardar los activos de TI a nivel de infraestructura, hardware, software, entre otros.

Recomendación:

Es necesario contar con una administración de riesgos de TI efectiva. La administración de riesgos es el proceso de identificación de vulnerabilidades y amenazas a los recursos de información utilizados por una organización para lograr los objetivos del negocio y decidir qué contramedidas, salvaguardas o controles, tomar para reducir el riesgo a un nivel aceptable basado en el valor del recurso de información para la organización.

La administración de riesgos efectiva comienza con una comprensión clara del nivel de aceptación de riesgos de la organización. Esto impulsa todos los esfuerzos de gestión de riesgos y, en un contexto de TI, afecta las inversiones futuras en tecnología, la medida en que los activos de TI están protegidos y el nivel de seguridad requerido. La gestión de riesgos incluye identificar, analizar,

evaluar, tratar, monitorear y comunicar el impacto del riesgo en los procesos de TI. Una vez definido el nivel de aceptación de riesgos e identificado la exposición al riesgo, se pueden establecer estrategias para gestionar el riesgo.

Para poder administrar efectivamente los riesgos, se deben implementar herramientas, como por ejemplo, matrices, en las cuales se resuman los riesgos a los cuales se está expuesto, los controles implementados para mitigar los riesgos identificados, y así establecer el nivel de riesgo residual al que se queda expuesto. Adicionalmente, se deben utilizar las actividades que actualmente se tienen para establecer la cantidad de incidencias de los riesgos identificados, con la finalidad de asignar la probabilidad de ocurrencia de los mismos. Con esa información, se pueden tomar las decisiones para determinar las inversiones requeridas para salvaguardar los activos informáticos.

Comentarios de Administración:

De acuerdo a lo resuelto en el Plan Estratégico de FHA para el periodo 2019-2022, en la sección referente a Gobierno Corporativo, en el primer semestre del presente año se creará el Comité de Gestión de Riesgos y luego la Unidad de Administración de Riesgos.

Una vez conformada la Unidad de Administración de Riesgos, ésta procederá a implementar las herramientas para administrar los riesgos, identificarlos, establecer controles para mitigarlos y registrar los incidentes que puedan presentarse.

II. 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 2018, 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 Actualización al 31 de diciembre de 2018

Este hallazgo se encuentra en proceso de corrección. Observamos que se había contratado el servicio de la empresa SEGA, S. A. para el desarrollo que actualizaría los sistemas utilizados actualmente. Sin embargo, por convenir a ambas partes, el contrato con dicha empresa se modificó en el sentido de dejar sin efecto el desarrollo y aplicación de los módulos, quedando vigente el desarrollo y aplicación del módulo de seguridad.

Es necesario atender la necesidad de renovación de los sistemas, aprovechando las mejores prácticas de desarrollo y tendencias en cuanto a la automatización de procesos, el cual, como efecto, atenderá esta observación, y centralizará la administración de los usuarios.

Comentario de Administración al 31 de diciembre de 2018:

El departamento de Informática procederá a la definición de una estructura basada en roles para los aplicativos que actualmente utiliza la Institución.

III. PROCEDIMIENTOS DE REVISIÓN EFECTUADOS AL 31 DE DICIEMBRE DE 2018

Como parte de la auditoría realizada, efectuamos una revisión del ambiente de control interno implementado en los sistemas informáticos involucrados en los procesos incluidos en el alcance de nuestra revisión. Esto incluye, en términos generales, revisar el ambiente de control interno de los sistemas de información, incluyendo la evaluación del grado de implementación de las siguientes mejores prácticas generalmente aceptadas:

1. *Administración de la Seguridad de la Información*
2. *Administración de cambios en los Sistemas de Información*
3. *Administración de la implementación de nuevos sistemas*
4. *Administración de la Infraestructura de TI, sistemas de información, bases de datos y servicios de TI*
5. *Administración de las vulnerabilidades de TI*
6. *Administración de los controles de acceso lógicos*
7. *Administración de la continuidad de la operación*
8. *Administración de la seguridad física*

1. Administración de la Seguridad de la Información

Se evaluó la siguiente información:

- Organigrama de la entidad
- Organigrama del departamento de TI.
- Manual de misiones y funciones o documento similar que refleje las tareas desempeñadas por los integrantes del área mencionada.
- Plan estratégico de TI alineado con la estrategia de la institución.
- Matrices de riesgo utilizadas para la evaluación y monitoreo de las actividades de control relacionadas con los sistemas de información.
- Procedimientos de monitoreo de los riesgos identificados en las matrices mencionadas en el punto anterior.

- Política documentada de seguridad informática donde se indique: procedimiento de otorgamiento de claves a los usuario, estándares fijados para el acceso y autenticación de usuarios, cursos de acción a seguir en caso de inicio de sumarios a empleados o de
- Proceso de comunicación de la política de seguridad informática a todos los colaboradores, personal interno, personal externo, y/o a cualquier otra persona que utilice los servicios informáticos (hardware, software, comunicaciones, etc.) de la institución.
- Plan estratégico de TI alineado con la estrategia de la institución.
- Planificación o cronograma de tareas para el año 2018
- Informes de avances de las tareas planificadas enviados al Jefe de Tecnología Informática por parte de los responsables de cada sector y del Jefe de TI a la Gerencia.
- Listado y contratos de servicios tercerizados, y/o acuerdos con los proveedores donde se incluyan las cláusulas requeridas de confidencialidad y seguridad de la información. Así mismo, contratos de confidencialidad del personal del departamento de TI.

2. Administración de cambios en los Sistemas de Información

Se evaluaron los procesos que involucran la adquisición y/o desarrollo e implementación de las soluciones informáticas con las que cuenta el Banco, así como el mantenimiento de las mismas.

Para esto se revisó lo siguiente:

- Listado de proveedores de software así como copia de los contratos suscritos, si los hubiere.
- Evidencias del control y seguimiento realizado al proveedor de software con respecto a cambios en el aplicativo, actualizaciones, pedido de modificaciones, etc., donde aplique.
- Estándares de metodología para el diseño, desarrollo y mantenimiento de los sistemas aplicativos.
- Manual del usuario y documentación técnica de los aplicativos mencionados en el punto anterior.
- Esquema de separación entre los ambientes de desarrollo, prueba y producción.

- Procedimiento utilizado para el desarrollo de cambios en los aplicativos, y/o desarrollo de nuevos aplicativos, así como la evidencia documental de la ejecución de dicho procedimiento.
- Procedimientos de revisión, registro y aprobación de las nuevas versiones y las modificaciones de los aplicativos, incluyendo las pruebas de usuario y pruebas de control de calidad, antes de la implementación definitiva en el ambiente de producción.
- Procedimientos de actualización a los manuales de usuario y documentación técnica al momento de realizar modificaciones a los aplicativos.

3. Administración de la implementación de nuevos sistemas

Se evaluó la existencia de controles que reflejen una adecuada administración de la implementación de nuevos sistemas. Para esto se revisó lo siguiente:

- Procedimientos formalmente documentados y aprobados para la implementación de nuevos sistemas, ya sea desarrollados o adquiridos.
- Procedimientos formalmente documentados y aprobados que demuestren el plan de pruebas a los riesgos informáticos de los nuevos sistemas antes de su implementación.
- Procedimientos formalmente documentados y aprobados que aseguren la correcta migración de datos, en caso sea necesario un cambio de software a los procesos importantes de la institución.
- Procedimientos formalmente documentados y aprobados que aseguren la integridad de la información a lo largo de los nuevos sistemas.
- Procedimientos que aseguren el entrenamiento del personal técnico y usuarios de los nuevos sistemas.

4. Administración de la Infraestructura de TI, sistemas de información, bases de datos y servicios de TI

Se evaluó que se cuente con una administración adecuada de la infraestructura de TI, los sistemas de información, las bases de datos y los servicios de TI.

Para esto se revisó lo siguiente:

- Inventarios actualizados de su infraestructura de TI, de sus sistemas de información y de sus bases de datos.

- Personas / Puestos responsables de la administración de las bases de datos, así como la descripción de las funciones del personal mencionado.
- Evidencia del monitoreo de la infraestructura de TI, sistemas de información y bases de datos.
- Procesos de gestión de incidentes y de problemas, incluyendo los aspectos de infraestructura de TI, sistemas de información y bases de datos.

5. Administración de las vulnerabilidades de TI

Se evaluó la existencia de un programa de gestión de vulnerabilidades que se mantiene para la protección óptima de los sistemas, aplicaciones y datos. Para esto se revisó lo siguiente:

- Procedimiento para la implementación de parches de seguridad de software de terceros.
- Capturas de pantalla del software de antivirus utilizado
- Capturas de pantalla del software utilizado para la detección de malware en los correos electrónicos, antes de que éstos sean entregados a sus destinatarios, si aplica.
- Procedimiento de monitoreo de la configuración de la seguridad de los usuarios de los sistemas operativos y/o aplicativos.
- Controles utilizados para el monitoreo del software utilizado por el personal.

6. Administración de los controles de acceso lógicos

Se evaluó la existencia de medidas de control de acceso para garantizar la integridad y seguridad de los datos y la información utilizada para la presentación de informes financieros. Para esto se solicitó la siguiente información:

- Políticas de seguridad lógica, que incluyan los controles utilizados para la validación de usuarios, incluyendo controles biométricos, utilización de contraseñas, entre otros. Valores de configuración de las contraseñas tanto en sistemas operativos como en aplicativos.
- Procedimiento utilizado para la asignación de cuentas de usuario para sistemas operativos, aplicativos, correo electrónico, entre otros.
- Procedimiento utilizado para la revisión de la asignación de cuentas de usuario para sistemas operativos, aplicativos, correo electrónico y otros.

- Captura de pantalla de la política de contraseñas utilizada en los sistemas operativos, aplicativos, bases de datos y donde aplique.
- Captura de pantalla de la política de bloqueo de usuarios por intentos fallidos y/o inactividad.
- Captura de pantalla de la política implementada para la utilización de sesiones concurrentes para los usuarios.
- Diagrama topológico de red, incluyendo oficinas centrales, sitios principal y alterno (si aplica), entre otros.
- Telecomunicaciones: documentación que indique que los datos se transmiten encriptados a través de la red de Telecomunicaciones.
- Firewall o similar que detecte posibles intrusiones en las redes así como el procedimiento utilizado para el monitoreo de los logs emitidos por el mismo y evidencia relacionada con dicho monitoreo.
- Procedimiento utilizado para la revisión de las políticas implementadas en los equipos de firewall.
- Procedimiento utilizado para el monitoreo de las conexiones externas hacia los datos de la institución, incluyendo conexiones a través de Internet, VPN, aplicaciones móviles (si aplica), etc.
- Políticas de seguridad de acceso a aplicaciones móviles, si aplica.
- Procedimiento utilizado para el otorgamiento de permiso para acceder a las bases de datos por fuera de los aplicativos, si aplica.

7. *Administración* de la continuidad de la operación

Se verificó que el Banco aborde el respaldo y la recuperación para las necesidades de continuidad del negocio.

Para esto se evaluó la siguiente información:

- Documentación que indique la información de los backups: cantidad, frecuencia, medio, lugar donde se guarda, etc. En caso que se guarde una copia fuera de las instalaciones, documentación que evidencie la formalidad entre la institución y la empresa que realice el resguardo de los respaldos.
- Procedimiento de pruebas a la integridad de la información de los backups efectuados, así como evidencia de la realización de estas pruebas.

- Ubicación de las copias de respaldo y de la documentación de los procedimientos de restauración.
- Plan de contingencias/emergencias que asegure la continuidad del procesamiento ante una situación que afecte el normal desarrollo de las tareas de producción.
- Evaluación de los riesgos que determinen el impacto de distintos eventos, tanto en términos de magnitud de daño como del período de recuperación y la vuelta a la normalidad.
- Funcionario responsable del mantenimiento y actualización del mencionado plan.
- Cronograma formal de pruebas del Plan de Continuidad y evidencias de la realización de las mismas. Documentación formal de la satisfacción del usuario con el resultado de las pruebas.

8. Administración de la seguridad física

Se evaluó la existencia de controles de acceso físico alrededor de los sistemas de información críticos para el negocio. También se solicitó la información siguiente:

- Políticas de seguridad física que incluyan controles y medidas de prevención para resguardar adecuadamente la infraestructura de TI de acuerdo a la importancia definida por la institución conforme al riesgo a que esté expuesta.
- Controles de accesos al centro de procesamiento y registro de los mismos.
- Revisión de las medidas de seguridad física del sitio principal de operación.