PKF

Contadores públicos y
consultores gerenciales

INSTITUTO DE FOMENTO DE HIPOTECAS ASEGURADAS –FHA

AUDITORÍA DE ESTADOS FINANCIEROS
AL 31 DE DICIEMBRE DE 2010

REVISIÓN 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

21 de enero de 2011

Licenciado
Guido Orlando Rodas
Gerente General
INSTITUTO DE FOMENTO DE HIPOTECAS ASEGURADAS –FHA
Ciudad

Estimado Licenciado Rodas:

Como parte de nuestra auditoria de los estados financieros del Instituto de Fomento de Hipotecas Aseguradas al 31 de diciembre de 2010 y por el año terminado en esa fecha, efectuamos una revisión de los principales procesos electrónicos de información, y derivado de la misma, observamos algunos hallazgos que se incluyen en el memorándum adjunto, que incluye las siguientes secciones:

A. Observaciones relacionadas con los sistemas automatizados de información derivadas de nuestra auditoría al 31 de diciembre de 2010

B. Observaciones relacionadas con los sistemas automatizados de información derivadas de auditorías anteriores

C. Procedimientos aplicados para la revisión de los principales procesos electrónicos de información

Atentamente,

Lic. Hugo Arévalo Pérez
Socio Director

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

MEMORANDUM DE OBSERVACIONES DERIVADAS DE NUESTRA REVISIÓN DE LOS PROCESOS ELECTRÓNICOS DE INFORMACIÓN

Auditoria de estados financieros al 31 de diciembre de 2010

Como resultado de los procedimientos aplicados durante nuestra revisión, y descritos en las páginas siguientes, establecimos lo siguiente:

A. OBSERVACIONES RELACIONADAS CON LOS SISTEMAS AUTOMATIZADOS DE INFORMACIÓN DERIVADAS DE NUESTRA AUDITORÍA AL 31 DE DICIEMBRE DE 2010

Estructura organizacional (recursos humanos)

No se encontró ningún hallazgo importante.

Tecnología (hardware y software)

No se encontró ningún hallazgo importante.

Servicios de tecnología internos y externos (proveedores)

No se encontró ningún hallazgo importante.

Seguridad física y lógica

1. Falta de actualizaciones de Microsoft .NET Framework 3.5 en el servidor DCFHAEX

El Service Pack 1 de .NET Framework 3.5 es una actualización acumulativa completa que incluye muchas características nuevas. Estas nuevas características de generación incremental en la versión 2.0 de .NET Framework, .NET Framework 3.0 y .NET Framework 3.5. También incluye actualizaciones acumulativas de servicios a los subcomponentes dependientes de .NET Framework 2.0 y .NET Framework 3.0.

Riesgos:

- Problemas en la ejecución de las aplicaciones desarrolladas internamente que utilicen .NET.

Recomendación:

Aplicar las actualizaciones necesarias en los servidores si se utilizan aplicativos desarrollados con estas versiones de .NET Framework.

2. *Falta de parches de seguridad en el sistema operativo del servidor DCFHAEX*

Durante nuestra revisión encontramos que el servidor DCFHAEX no cuenta con los últimos parches de seguridad. Esto se debe también a que el servidor está configurado a que reciba las actualizaciones, pero se necesita que un usuario las apruebe.

Riesgos:

- Que los servidores estén vulnerables a ataques internos y externos.

Recomendación:

Evaluar y aplicar los parches de seguridad pendientes de instalarse, y configurar el equipo para que no se necesite la intervención de un usuario para instalar las actualizaciones.

3. *El servidor DCFHAEX tiene habilitado el "AutoRun" para medios extraíbles.*

De acuerdo a la información obtenida durante la prueba de red, se encontró que el servidor DCFHAEX tiene habilitada la opción de ejecución automática al insertar un medio extraíble, como un CD, DVD o medios por USB.

Riesgos:

- Que se instalen programas no deseados, o virus, en los servidores centrales.

Recomendación:

Deshabilitar la opción mencionada en todos los servidores.

B. OBSERVACIONES RELACIONADAS CON LOS SISTEMAS AUTOMATIZADOS DE INFORMACIÓN DERIVADAS DE AUDITORÍAS ANTERIORES

1. Debilidad en el manejo de las copias de respaldo.

Actualmente se quedan las copias de respaldo dentro de la institución, sin haber una copia fuera de la misma.

Riesgos:

- Pérdida de la información en caso de algún siniestro ocurrido dentro de la institución.

Recomendación:

Es necesario establecer las medidas necesarias para mantener una copia de respaldo actualizada fuera de la institución para poder recuperar la misma en caso suceda un siniestro dentro de la institución que cause la pérdida de la información.

Comentario de Actualización:

Según la información obtenida, las copias de respaldo se almacenan dentro de la institución, *por lo que la situación continúa vigente.*

2. No se cuenta con una Política de Seguridad Informática debidamente documentada y autorizada por la gerencia.

Actualmente se cuenta con algunas políticas en documentos aislados, como la política general de uso de la red y correo electrónico.

Riesgos:

- Implementación empírica de las políticas de seguridad informática.

Recomendación:

A pesar que ya se han realizado acciones para definir una Política de Seguridad Informática, es necesario darle la debida importancia al tema, ya que con ésto se tendrán, entre otras cosas, políticas claras para la utilización de los recursos informáticos, acciones definidas en caso de detectar una posible intrusión y se podrá sensibilizar a los usuarios con los problemas ligados con la seguridad de los sistemas informáticos.

Comentario de Actualización:

Si bien se tienen implementadas algunas políticas relacionadas con la seguridad informática, aún no se ha confeccionado un documento que reúna todas estas políticas, p*or lo que la situación continúa vigente.*

3. Utilización de usuario genérico en transacciones

Durante la revisión de las bitácoras de las bases de datos se encontraron transacciones que mostraban al usuario *informix* como usuario que realizó un cambio en el caso. Este tipo de transacciones puede corresponder tanto a transacciones automáticas como a transacciones que están amparadas por un ticket, de acuerdo a los procedimientos que actualmente tiene el departamento de sistemas, sin embargo, no se puede identificar quién ha ejecutado dichas transacciones.

Riesgos:

- Transacciones que puedan afectar a la institución y que no se les pueda deducir responsabilidades.

Recomendación:

Es necesario identificar a los usuarios responsables de cada transacción dejando la evidencia necesaria en las bitácoras. Adicionalmente, para el caso de las transacciones automáticas, es necesario que quede la evidencia. En vez de que se mencione al usuario *informix* en la bitácora, puede existir un usuario denominado *operacionautomatica.*

Comentario de Actualización:

La situación se encuentra implementada, debido a que la utilización de este usuario en las transacciones prácticamente ya no se utilizó en el año 2010.

4. El ambiente de desarrollo está ubicado dentro del servidor DCFHA2, donde se encuentra también el ambiente de producción.

Los problemas que se puedan dar durante el desarrollo de las aplicaciones pueden causar molestias y/o problemas a los usuarios.

Riesgos:

- Sistemas lentos;
- Posible pérdida de información.

Recomendación:

Es necesario que se utilice un servidor dedicado para el ambiente de desarrollo, y uno dedicado al ambiente de producción.

Comentario de Actualización:

La situación se encuentra implementada, porque el ambiente de desarrollo fue trasladado al servidor DEVELOP, y las bases de datos de prueba se encuentran en el servidor DESA.

5. Debilidad en la seguridad física del cuarto de servidores

Se encontraron las siguientes debilidades de seguridad en el cuarto de servidores:

1. La puerta tiene una chapa simple con llave;
2. Las paredes del cuarto de servidores no están reforzadas;
3. Las ventanas que dan al exterior no están protegidas contra intrusos;
4. No se cuenta con detectores de humo, o alarma contra incendios;
5. No se cuenta con una bitácora de las visitas al cuarto de servidores.

Riesgos:

- Daños en los servidores centrales;
- Posible interrupción en el procesamiento de datos.

Recomendación:

Es necesario aumentar la seguridad física del cuarto de servidores de la siguiente manera:

1. Colocar un dispositivo electrónico que registre el acceso al cuarto de servidores;
2. Reforzar las paredes del cuarto de servidores;
3. Reforzar las ventanas que dan al exterior con alarmas de rotura de cristales, y/o con balcones internos;
4. Colocar detectores de humo, sensores de temperatura y humedad con alarma o alarma contra incendios dentro del cuarto de servidores;
5. Llevar una bitácora de las visitas realizadas por terceros al cuarto de servidores.

Comentario de Actualización:

Se implementaron nuevas medidas de seguridad física en el cuarto de servidores, incluyendo una reja metálica alrededor y en la parte superior. Adicionalmente se cambió la puerta por una metálica; se colocó una cámara de seguridad y una alarma. También se instaló un segundo equipo de aire acondicionado. Únicamente faltaría una bitácora de las visitas realizadas por terceros. *La situación se encuentra corregida e implementada.*

6. Debilidad en la realización de copias de respaldo de los servidores.

Actualmente se utiliza una herramienta para realizar copias de respaldo de los servidores. Sin embargo, el tamaño de las copias de respaldo sobrepasan 1 TB (terabyte = 1000 GB) de espacio, por lo que no es una solución que pueda sostenerse mucho tiempo.

Riesgos:

- Incremento en costo de la realización de backups por la adquisición de medios con mayor almacenamiento.
- Posible inhabilitación de realizar las copias de respaldo de los servidores.

Recomendación:

Es necesario considerar un cambio en la solución para la realización de copias de respaldo de los servidores centrales.

Comentario de Actualización:

Actualmente se han realizado cambios en las estrategias de elaboración de copias de respaldo, lo que ha ayudado en la administración y mantenimiento de los mismos, por lo que *la situación se encuentra corregida e implementada.*

C. PROCEDIMIENTOS APLICADOS PARA LA REVISIÓN DE LOS PRINCIPALES PROCESOS ELECTRÓNICOS DE INFORMACIÓN

Como parte de la revisión de los principales procesos electrónicos de información realizada, efectuamos una evaluación general del ambiente global de control interno de la institución, específicamente en todo lo relacionado con los sistemas informáticos.

A continuación se describen los procedimientos de revisión aplicados:

PLANEACIÓN Y METODOLOGÍA

Con el propósito de determinar adecuadamente el alcance de nuestras pruebas de la revisión de los principales procesos electrónicos de información, llevamos a cabo una evaluación del ambiente global de control interno de la institución y preparamos el programa de trabajo específico para cada área como sigue: estructura organizacional (recurso humano), tecnología (hardware y software), servicios internos y externos (proveedores) y seguridad física y lógica.

La evaluación del ambiente global de control interno incluyó las fases siguientes:

(i) Análisis de la estructura organizacional

(ii) Asignación de autoridad y responsabilidad

(iii) Prácticas y políticas de personal

(iv) Información externa de servicios con terceros

(v) Información administrativa del centro de cómputo

La evaluación antes mencionada, incluyó la aplicación de los procedimientos siguientes:

a) Obtuvimos un entendimiento del objeto, políticas y procedimientos para el manejo y control de las operaciones de la institución y lo relevante del control interno a través de los sistemas de software y hardware.

b) Verificamos si las políticas y procedimientos antes mencionados, se encuentran establecidos formalmente dentro de la institución (por escrito y debidamente aprobados por la autoridad correspondiente), y comunicados adecuadamente al personal de la misma.

c) Solicitamos la documentación relacionada con las principales políticas de seguridad informática, incluyendo reportes, revisiones, entre otros.

d) Solicitamos la documentación legal relacionada con los contratos de confidencialidad del personal de sistemas y contratos con otros proveedores.

e) Requerimos además, la documentación legal de las licencias de software vigentes para las aplicaciones de sistemas que actualmente utiliza la institución.

f) Obtuvimos un entendimiento general del software utilizado.

g) Así mismo solicitamos evidencia para el seguimiento de las auditorías de años anteriores.

PROCEDIMIENTOS ESPECÍFICOS DE REVISIÓN

De acuerdo con nuestro programa de trabajo, los procedimientos específicos que fueron efectuados en cada área de nuestra revisión, se detallan a continuación:

Estructura organizacional

1. Se examinó el organigrama general de la institución, con el propósito de verificar la relación que tiene el Departamento de Sistemas con otros departamentos de la institución.

2. Solicitamos los manuales de puestos y funciones del personal, con el objetivo de verificar que el personal del departamento realice las tareas que tiene asignadas.

3. Solicitamos los procedimientos del departamento, para verificar que todas las actividades del departamento estén documentadas, debidamente autorizadas y publicadas.

Tecnología (hardware y software)

1. Nos entrevistamos con el Jefe del Departamento de Sistemas para verificar la configuración de los servidores centrales, el tipo de red y su configuración.

2. Solicitamos el inventario del equipo de cómputo y de las aplicaciones de sistemas o software que utilizan, con el objetivo de verificar la tecnología que usan.

3. Revisamos la base de datos con el objetivo de verificar su integridad y capacidad para el manejo de la información.

4. Se verificaron las bitácoras de las actividades transaccionales dejadas por las aplicaciones, con el fin de identificar transacciones que puedan ser sospechosas.

5. Solicitamos un inventario de software instalado en las terminales de trabajo, para determinar si existe algún programa que no corresponda a las operaciones del FHA.

6. Verificamos los planes de trabajo, incluyendo informes de avance, de los proyectos informáticos.

7. Para el proceso de reclamos y liquidaciones, se verificó la forma cómo se calcula el sistema las estimaciones por pérdida en reclamos de seguro de hipoteca, y la estimación por pérdida en inmuebles adjudicados.

Servicios de tecnología internos y externos (proveedores)

1. Solicitamos la integración de los accesos de los usuarios a los diferentes sistemas, para comprobar que cada usuario tenga acceso únicamente a las opciones del sistema que se relacionan con sus actividades.

2. Verificamos los contratos y los acuerdos de niveles de servicio con terceros, con el objetivo de evaluar los alcances y beneficios de estos servicios para la institución.

3. Verificamos el proceso de trabajo y comunicación entre el Departamento de Sistemas y los diferentes departamentos de la institución que son usuarios del sistema, con el propósito de evaluar los procedimientos, tiempos de repuesta, control de calidad y bitácoras almacenadas de las modificaciones o procesos nuevos.

Seguridad

1. Solicitamos la documentación de las políticas de seguridad y respaldo, con el objetivo de verificar el área física, accesorios para casos de emergencia como fuego, inundaciones, terremotos u otro fenómeno natural, así como el resguardo de la información.

2. Solicitamos la documentación de los planes de contingencia y continuidad del negocio, con el objetivo de establecer si existen procedimientos previstos por la institución para hacer frente y asegurar la continuidad de las operaciones ante alguna eventualidad.

3. Validamos la seguridad de accesos de los diferentes usuarios a las áreas que les corresponde, con el objetivo de verificar la integridad de las claves de los usuarios y la confidencialidad de la información.

4. Realizamos una prueba de red para identificar las vulnerabilidades dentro de la misma, puertos abiertos y servicios que estén corriendo en las terminales de trabajo y los servidores, con la finalidad de detectar anomalías que puedan comprometer la información.