



Contadores públicos y
consultores gerenciales

**INSTITUTO DE FOMENTO DE
HIPOTECAS ASEGURADAS –FHA**

AUDITORÍA DE ESTADOS FINANCIEROS
AL 31 DE DICIEMBRE DE 2013

**REVISIÓN DE LOS PROCESOS
ELECTRÓNICOS DE INFORMACIÓN**

**Arévalo Pérez, Iralda
y Asociados, S.C.**

14 de enero de 2014

Licenciado
Sergio Irungaray
Gerente General
Instituto de Fomento de Hipotecas Aseguradas –FHA
Ciudad

Estimado Licenciado Irungaray:

Como parte de la auditoría a los estados financieros del Instituto de Fomento de Hipotecas Aseguradas –FHA al 31 de diciembre de 2013 y por el año terminado en esa fecha, efectuamos una revisión de los principales procesos electrónicos de información definidos por su administración.

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

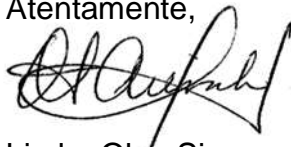
Nuestra responsabilidad se limita a expresar nuestras conclusiones sobre la eficacia de los procedimientos y controles que el Instituto tiene en operación para el manejo de cada área, y en general de la forma como opera el Instituto.

Derivado de dicha revisión, le informamos que no observamos hallazgos importantes que deban ser reportados a su Administración.

En las secciones siguientes se presentan:

- I Procedimientos de revisión de los sistemas automatizados de información al 31 de diciembre de 2013.
- II Seguimiento a las observaciones relacionadas con los sistemas automatizados de información derivadas de auditorías de años anteriores.

Atentamente,



Licda. Olga Siomara Arévalo Iralda
Socia de Auditoría

INSTITUTO DE FOMENTO DE HIPOTECAS ASEGURADAS –FHA

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

Auditoría al 31 de diciembre de 2013

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

I **PROCEDIMIENTOS DE REVISIÓN DE LOS SISTEMAS AUTOMATIZADOS DE INFORMACIÓN AL 31 DE DICIEMBRE DE 2013**

Se revisó lo siguiente:

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

No se encontró ningún hallazgo importante.

Seguridad física y lógica

No se encontró ningún hallazgo importante.

II SEGUIMIENTO A LAS OBSERVACIONES RELACIONADAS CON LOS SISTEMAS AUTOMATIZADOS DE INFORMACIÓN DERIVADAS DE AUDITORÍAS DE AÑOS ANTERIORES

Como parte de nuestros procedimientos de auditoría aplicados al 31 de diciembre de 2013, efectuamos seguimiento a los hallazgos y recomendaciones de auditorías anteriores, observando que los mismos algunos ya fueron implementados y otros se encuentran en proceso de implementación.

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

Actualización:

La situación está en proceso de regularización, puesto que ya se inició a elaborar los cuestionarios que darán inicio al proceso, además de que se tienen identificadas y documentadas las principales actividades a realizar para la puesta en marcha de los principales servidores y bases de datos.

Recomendación:

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.

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

Actualización:

Durante el segundo semestre de 2013, se elaboró el MANUAL DE POLITICAS Y ESTANDARES DE SEGURIDAD INFORMATICA DEL INSTITUTO DE FOMENTO DE HIPOTECAS ASEGURADAS, por lo que la situación se considera atendida.