

13 de enero de 2017

Arquitecto  
Héctor Daniel López Cordón  
Gerente General  
Instituto de Fomento de Hipotecas Aseguradas, -FHA-  
Ciudad

Estimado Arquitecto López:

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 que termina en esa fecha, efectuamos una revisión de los principales procesos electrónicos definidos por la Administración en el área de contabilidad.

Como parte de nuestros procedimientos revisamos la Resolución de Junta Monetaria JM 102-2011 Reglamento para la Administración del Riesgo Tecnológico, con el objeto de identificar oportunidades de mejoras para el FHA en la implementación de las mejores prácticas vigentes en el sector financiero con el objetivo de mitigar el riesgo de pérdidas financieras ocasionadas por la materialización del riesgo tecnológico.

Es importante señalar que la Superintendencia de Bancos mediante oficio No. 5023-2011 de fecha 5 de octubre de 2011 ratificó que dicho reglamento no es de observancia para el Instituto de Fomento de Hipotecas Aseguradas –FHA.

Sin embargo consideramos importante detallarles algunas oportunidades de mejoras que observamos en la revisión de sistemas automatizados de información al 31 de diciembre de 2016, las cuales se mencionan en el memorándum adjunto.

Atentamente



Licda. Olga Siomara Arévalo Iralda  
Socia de Auditoría

**INSTITUTO DE FOMENTO DE HIPOTECAS ASEGURADAS, -FHA-**Auditoria de Estados Financieros al 31 de diciembre de 2016

Como parte de nuestros procedimientos revisamos la Resolución de Junta Monetaria JM 102-2011 Reglamento para la Administración del Riesgo Tecnológico, que es de observancia para los bancos, sociedades financieras, entidades fuera de plaza o entidades off shore y empresas especializadas en servicios financieros que forman parte de un grupo financiero, con el objeto de identificar oportunidades de mejoras para el FHA en la implementación de las mejores prácticas vigentes en el sector financiero con el objetivo de mitigar el riesgo de pérdidas financieras ocasionadas por la materialización del riesgo tecnológico.

Dentro de este reglamento observamos las siguientes oportunidades de mejora para reforzar el área de tecnología e información:

1. *Administración del Riesgo Tecnológico*

Las instituciones deberán contar con una Unidad de Administración de Riesgos y un Comité de Gestión de Riesgos que se encargue de la implementación, funcionamiento y ejecución de las políticas y procedimientos que “les permitan realizar permanentemente una adecuada administración del riesgo tecnológico de la institución, considerando la naturaleza, complejidad y volumen de sus operaciones” cómo se indica en los artículos 5 y 6 del reglamento.

Dentro de las características con las que debe contar el Comité se pueden enumerar: debe estar integrado por al menos un miembro de Junta Directiva (la figura que aplica en el FHA del Consejo de Administración descrito en la norma) y por las autoridades y funcionarios que el consejo designe. Estas características están diseñadas para priorizar el impacto de las recomendaciones del comité en las decisiones de Junta Directiva.

2. *Manual de Administración del Riesgo Tecnológico*

El artículo 9 indica que las políticas y procedimientos a que se refiere el artículo 3 del reglamento deberán constar por escrito en un Manual de Administración del Riesgo Tecnológico que será aprobado por el Consejo. Así mismo menciona que el Consejo, o en su caso, Junta Directiva conocerá y resolverá sobre las propuestas de actualización del manual de administración del riesgo tecnológico y autorizará las modificaciones.

### 3. *Administrador de base de datos*

Tal como lo menciona el artículo 12 las instituciones deberán designar uno o más administradores de base de datos para gestionar los controles de accesos, la integridad, disponibilidad y confidencialidad de los datos, así como los procesos de creación, actualización o eliminación de estructuras en las bases de datos, entre otros.

### 4. *Continuidad de operaciones de Tecnología de la información*

El artículo 20 del reglamento menciona que las instituciones deberán contar con un Plan de Continuidad de Operaciones de TI que esté alineado a las necesidades de la institución para recuperar los procesos críticos de las principales líneas de negocio soportados por TI, así como la información asociada en caso de una interrupción.

### 5. *Capacitación del personal clave para la continuidad del negocio*

Las instituciones deberán mantener capacitado al personal clave y al listado de proveedores para activar o probar el plan de continuidad de operaciones de TI y sus modificaciones como se menciona en el artículo 22.

### Comentario de Administración

En relación a lo indicado y como parte de un proceso de adopción de mejores prácticas en el ámbito tecnológico, se contempló dentro del Plan Estratégico de Tecnología, aprobado por la Gerencia del FHA, la adopción de la metodología contemplada en la referida resolución, con el objetivo de implementar un sistema de gestión de Seguridad de la Información, de tal manera que pueda garantizarse la confidencialidad, disponibilidad e integridad de la información. El inicio de las actividades relativas a la implementación se encuentra contemplado a partir del mes de julio de 2017.