Contadores públicos y
consultores gerenciales

INSTITUTO DE FOMENTO DE HIPOTECAS ASEGURADAS –FHA

AUDITORÍA DE ESTADOS FINANCIEROS
AL 31 DE DICIEMBRE DE 2019

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

17 de enero de 2020

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

Estimados señores:

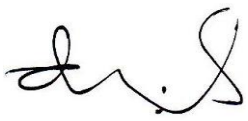
Como parte de la auditoría de los estados financieros del Instituto de Fomento de Hipotecas Aseguradas –FHA al 31 de diciembre de 2019 y por el año terminado en esa fecha, efectuamos una revisión en las áreas de los principales procesos electrónicos de información definidos por la Administración en el área de contabilidad.

Tanto las operaciones realizadas en el FHA, 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 consideremos deban ser reportados a su Administración. Así mismo, les informamos que los hallazgos observados en los procesos electrónicos de información al 31 de diciembre de 2018, fueron atendidos durante el año 2019. En el memorándum adjunto se describen los procedimientos de revisión efectuados.

Atentamente,



Lic. Hugo Arévalo Pérez
Socio Director

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

Tel (502) 2303-5050 | Email: arevalo@pkfguatemala.com
PKF | 3a. avenida 10-80 Zona 10, Edificio Forum Zona Viva, Torre II, Nivel 10 oficina 1001 | Guatemala 01010 | Guatemala, C.A.

INSTITUTO DE FOMENTO DE HIPOTECAS ASEGURADAS –FHA

Auditoría de estados financieros al 31 de diciembre de 2019

PROCEDIMIENTOS DE REVISIÓN EFECTUADOS AL 31 DE DICIEMBRE DE 2019

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*

Evaluamos la siguiente información:

- Organigrama de la entidad.
- Copia del acta de creación del Comité de Informática, Comité de Riesgos Informáticos, o equivalente.
- Copia de la última minuta o acta de reunión del Comité de Informática, Comité de Riesgos Informáticos, o equivalente.
- 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.

- Último Plan Estratégico de TI.
- 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 desvinculación de los mismos.
- 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.
- Planificación o cronograma de tareas para el año 2019
- 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*

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

Para esto revisamos 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*

Evaluamos la existencia de controles que reflejen una adecuada administración de la implementación de nuevos sistemas.

Para esto revisamos 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*

Evaluamos 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 revisamos 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*

Evaluamos la existencia de un programa de gestión de vulnerabilidades que se mantiene para la protección óptima de los sistemas, aplicaciones y datos.

Para esto revisamos 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*

Evaluamos 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 solicitamos 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

Verificamos que el Instituto aborde el respaldo y la recuperación para las necesidades de continuidad del negocio.

Para esto evaluamos 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*

Evaluamos la existencia de controles de acceso físico alrededor de los sistemas de información críticos para el negocio.

También solicitamos 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 y del sitio alterno (si aplica).
- Procedimiento de revisión de los controles de acceso al centro de procesamiento de datos y sitio alterno (si aplica).