Crowe Horwath CR, S.A.

Banco Hipotecario de la Vivienda
Fondo de Subsidios para la Vivienda
FOSUVI

Carta de gerencia de Tecnología de Información

Al 31 de diciembre de 2019

Banco Hipotecario de la Vivienda
Fondo de Subsidios para la Vivienda
FOSUVI

Índice

Crowe Horwath CR, S.A.
2442 Avenida 2
Apdo. 7108-1000
San José, Costa Rica
Tel + (506) 2221 4657
Fax + (506) 2233 8072
www.crowe.cr

30 de abril de 2020

Señores
Junta Directiva del Banco Hipotecario de la Vivienda
Atención: Irene Campos Gómez,
Presidente Junta Directiva
MBA. Marta Camacho Murillo,
Dirección de FOSUVI

ASUNTO: SISTEMA DE TECNOLOGÍA DE INFORMACIÓN

Al revisar la gestión de tecnología de información del Fondo de Subsidios para la Vivienda, referente a la auditoría de los estados financieros al 31 de diciembre de 2019, observamos asuntos relacionados con la administración del área de TI y los procesos de gestión sobre los cuales preparamos las conclusiones incluidas en el documento adjunto.

Al planear y ejecutar la revisión evaluamos la estructura de control interno existente y aplicamos pruebas selectivas de cumplimiento, con el fin de determinar el alcance de los procedimientos de auditoría para expresar opinión sobre los estados financieros al 31 de diciembre de 2019, y no para opinar sobre la estructura de control interno o los sistemas de información en su conjunto. Este informe no es ni debe interpretarse como una auditoría de los sistemas de información.

Es necesario señalar que nuestra evaluación es limitada para efectos de una revisión de controles generales, por lo que una revisión más detallada de controles de aplicación podría revelar más oportunidades de mejora de las que incluye este informe.

En este informe se incluyen comentarios de la administración que no modifican las revelaciones ni el criterio expresado y no son parte integral de los hallazgos.

Los temas tratados no se refieren a empleados en particular y tienen por objeto plantear medidas para fortalecer el sistema de tecnología de información.

Atentamente,

Fabian Zamora Azofeifa
Socio

c.c. Presidente Comité de Auditoría

Fondo de Subsidios para la Vivienda

Informe de tecnología de información

Al 31 de diciembre de 2019

I. Resumen ejecutivo

Como parte del trabajo de la auditoría de estados financieros del periodo 2019 se llevó a cabo la evaluación de controles de Tecnología de Información (TI) en el Fondo de Subsidios para la Vivienda (FOSUVI), la cual se basa en el Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) para las entidades fiscalizadas por la Contraloría General de la República (CGR), marco normativo interno y las buenas prácticas de control de TI.

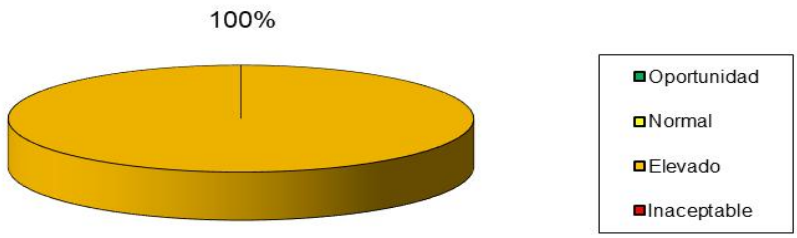
El Banco Hipotecario de la Vivienda (BANHVI) es el ente rector del Sistema Financiero Nacional para la Vivienda y brinda sus servicios mediante 24 diferentes Entidades Autorizadas.

El Sistema de Vivienda a la fecha de corte de este informe sigue presentando la falta de integración con otros sistemas, obsolescencia y falta calidad de la información a pesar del proyecto "Rediseño del Sistema de Vivienda (etapa I y II, conceptualización y determinación de requerimientos)" que no culminó satisfactoriamente. Se elaboró el "Plan de fortalecimiento del Sistema de Vivienda - Rediseño" con el objetivo de automatizar los procesos operativos de la Dirección FOSUVI junto con el proyecto "Sistema de Apoyo a la Gestión Financiera y Capital Humano", que tiene como objetivo fortalecer, modernizar, integrar y gestionar los procesos asociados con las operaciones del BANHVI, los cuales dependían uno del otro para lograr ambos objetivos (plan y proyecto). Sin embargo el informe de avance de proyecto "PROY-03 Rediseño del Sistema de Vivienda", con fecha 20 de diciembre de 2019, indica que "se tiene la limitación de que no podrá iniciar su etapa de diseño e implementación hasta tanto se conozcan los detalles de las interfases a desarrollar para integrar ambos sistemas", esto por debilidades indicadas en el informe N° DFOE-EC-IF-00026-2019 de la Contraloría General de la República, con fecha 09 de diciembre de 2019.

El Acuerdo N°5 de la Junta Directiva del BANHVI, de la sesión 09-2020 con fecha 03 de febrero de 2020, da por conocido el plan de trabajo de la Dirección FOSUVI para atender los acuerdos de Junta Directiva, recomendaciones de las auditorías externas e internas y el cierre de líneas de crédito a proyectos de vivienda, al existir compromisos en proceso de atención y pendientes superior a 350 al cierre del 2019.

Para la evaluación del periodo 2019 se identificaron observaciones que son clasificadas por riesgo de acuerdo a la materialización y posibilidad de presentarse el evento.

En la evaluación del área de TI se identifican 2 observaciones, que de acuerdo con la naturaleza del riesgo se distribuyen en un 100% de riesgo elevado.



Se utilizó como criterio de evaluación las Normas Internacionales de Auditoría 315 y 330, el Manual de Normas Técnicas y las buenas prácticas de control de TI, sin embargo, el informe no es ni debe tomarse como una auditoría de los sistemas de información.

En la sección de conclusiones de este informe se indican las observaciones identificadas.

II. Objetivo

Evaluar el cumplimiento de requerimientos de seguridad y control en Tecnología de Información (TI) en FOSUVI, de acuerdo con las Normas Internacionales de Auditoría 315 y 330, con el criterio del Manual de Normas Técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) para las entidades fiscalizadas por la CGR, publicado en La Gaceta Nº 119 del 21 de junio de 2007, marco normativo interno y las buenas prácticas de control para gobierno y control de TI, como referencia y no de cumplimiento regulatorio, con el propósito de determinar si cumple con los requerimientos de seguridad y control.

III. Alcance

El alcance incluyó aspectos relacionados con la gestión de control y sistemas de información de FOSUVI, respecto a la elaboración de procedimientos y aplicación de controles que fortalezcan la seguridad, integridad y funcionalidad de los procesos de gestión del área de TI, gestión de la seguridad de la información, sistemas de información, software y bases de datos, hardware, redes y comunicaciones, gestión de la continuidad y seguimiento de las recomendaciones anteriores. El informe no es ni debe tomarse como una auditoría de los sistemas de información.

IV. Procedimientos

A partir del alcance se elaboraron y utilizaron instrumentos para recopilar la información referente al alcance indicado; entre estos, entrevistas, cuestionarios, revisión documental, inspección física, levantamiento de minutas, selección de muestras, operación de los sistemas, pruebas de operación, normas de auditoría de aceptación general y buenas prácticas de control.

Para la evaluación del sistema de TI se utilizaron como referencia las Normas Internacionales de Auditoría NIA 315 y NIA 330, el Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información de la Contraloría General de la República, el marco normativo interno, la Biblioteca de Infraestructura de Tecnologías de Información (ITIL) y la Organización Internacional de Normalización (ISO), como marco de referencia y no de acatamiento regulatorio.

Con base en estos documentos se confeccionaron entrevistas para dar seguimiento a las respuestas, lectura de la evidencia solicitada y ejecución de las pruebas de cumplimiento y sustantivas.

Entre los temas evaluados en cada área se indican las oportunidades de mejora encontradas.

V. Criterios de evaluación

De acuerdo con la evaluación de control interno del área de TI y con base en el riesgo que representan para los recursos de TI (aplicaciones, información, infraestructura y personas), se presenta el mapa de riesgos que resume la relación entre el impacto para la organización y la posibilidad de materialización del riesgo que garanticen la alineación con los criterios de información (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad).

Los niveles de cumplimiento se describen a continuación:

Cumple	La entidad muestra desempeño adecuado respecto al factor evaluado.
Cumplimiento parcial alto	La entidad muestra algunas deficiencias, pero en general el desempeño respecto al factor evaluado es satisfactorio.
Cumplimiento parcial bajo	La entidad muestra débil desempeño respecto al factor evaluado.
No cumple	La entidad muestra desempeño crítico respecto al factor evaluado, por lo que no es aceptable clasificarlo en ninguno de los tres niveles anteriores.

Las categorías de riesgos se describen a continuación[1]:

Nivel de riesgo	Descripción
Inaceptable	Se estima que este nivel de riesgo es mucho más allá de su riesgo tolerable; cualquier riesgo que se encuentre en esta clasificación puede desencadenar una respuesta inmediata al riesgo.
Elevado	Riesgo elevado, por encima del riesgo tolerable; la entidad puede, como política interna, mitigar el riesgo u otra respuesta adecuada definida dentro de un tiempo límite.
Normal	Nivel aceptable de riesgo, por lo general sin realizar una acción en especial excepto para el mantenimiento de los actuales controles u otras respuestas.
Oportunidad	Nivel de riesgo muy bajo, en el cual las oportunidades de ahorro de costos pueden ser disminuir el grado de control o determinar en cuáles oportunidades pueden asumirse mayores riesgos.

El formato de este informe fue estructurado para proporcionar dos referencias específicas; Cumplimiento y Nivel de riesgo.

En la práctica el "apetito de riesgo" puede ser definido en términos de una combinación de frecuencia y magnitud de un riesgo descritos en bandas de significancia del riesgo. Hemos establecido niveles de riesgo en las bandas descritas anteriormente basándonos en la frecuencia y magnitud de los riesgos.

La frecuencia y magnitud de los riesgos no necesariamente están directamente relacionados con niveles de cumplimiento de la normativa, debido a que aunque haya incumplimiento, el impacto que puede ocasionar y la frecuencia de veces que puede ocurrir pueden tener efecto poco significativo en el proceso de administración integral de riesgos y en las operaciones.

VI. Determinación del cumplimiento y nivel de exposición al riesgo

Para obtener el nivel de exposición al riesgo nos hemos basado en la aplicación de una matriz de 25 cuadrantes (5 verticales y 5 horizontales), en la cual el riesgo de los factores es determinado por su ocurrencia e impacto.

Para cada acción evaluada que presenta incumplimiento hemos determinado el nivel de impacto y ocurrencia y obtuvimos el nivel de exposición al riesgo basados en la matriz indicada anteriormente.

[1] Datos tomados del Manual CRISC (*Certified in Risk and Information Systems Control*), emitido por el ISACA.

La frecuencia (cuadrantes horizontales) se basa en la verificación de las siguientes categorías:

Muy baja	La probabilidad de ocurrencia es insignificante, puede ocurrir solo en circunstancias excepcionales.
Baja	Tiene poca probabilidad de ocurrencia; no se espera que ocurra en cierto periodo de tiempo.
Frecuente	El evento ocurrirá más de una ocasión en un determinado lapso.
Alta	Se espera que suceda en muchas ocasiones en un periodo de tiempo dado, en circunstancias definidas.
Muy alta	Se materializa de forma continua y ocurrirá bajo muchas circunstancias.

El impacto (cuadrantes verticales) se basa en las siguientes categorías:

Insignificante	El costo no afecta la entidad. No es necesario tomar medidas al respecto.
Mínimo	La materialización podría traer un costo para la entidad; sin embargo, no es de importancia para los resultados de la entidad. Debe valorarse los motivos de la materialización del riesgo.
Moderado	Su materialización conlleva un costo para la entidad que puede incluir pérdidas. Deben establecerse medidas de prevención para posibles eventos.
Serio	Representa un costo elevado. Las medidas que deben tomarse son correctivas y preventivas.
Crítico	El costo asumido no es tolerable y es necesario tomar medidas correctivas inmediatas.

A continuación presentamos la matriz de 5 x 5 cuadrantes

		Frecuencia				
		Muy baja	**Baja**	**Frecuente**	**Alta**	**Muy alta**
Impacto	**Crítico**	5	10	15	20	25
	Serio	4	8	12	16	20
	Moderado	3	6	9	12	15
	Mínimo	2	4	6	8	10
	Insignificante	1	2	3	4	5

Calificaciones

Basado en los resultados de los análisis por acción se determina el nivel de exposición al riesgo de acuerdo con los siguientes rangos:

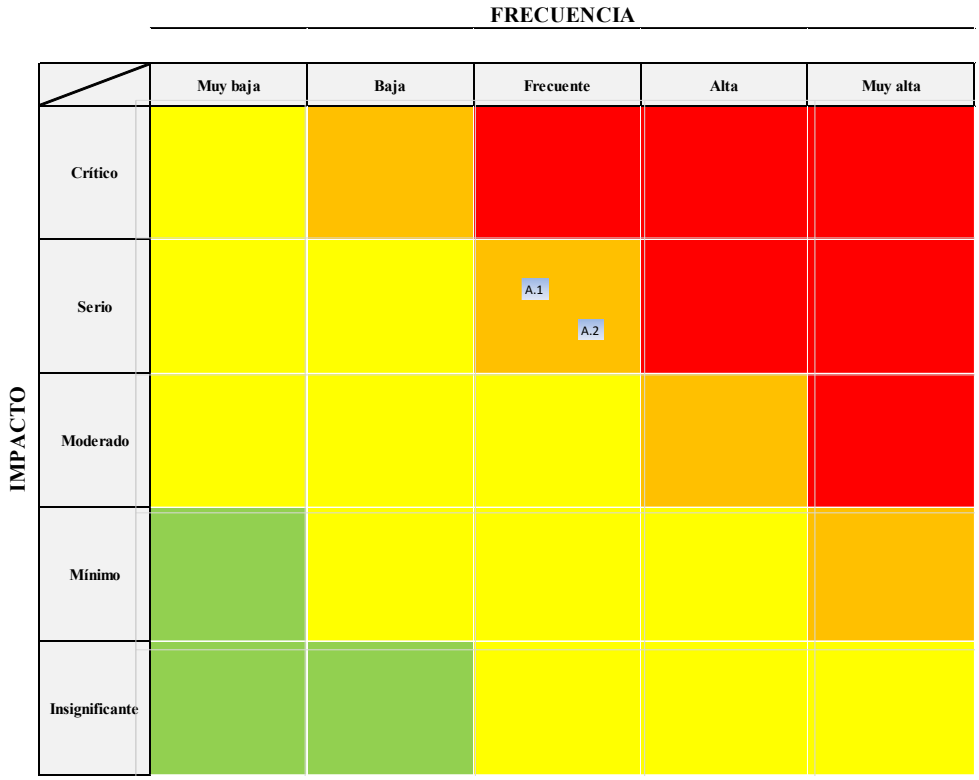
De 1 a 2:	El nivel de riesgo es de oportunidad.
De 3 a 9:	El nivel de riesgo es normal.
De 10 a 12:	El nivel de riesgo es elevado.
De 15 a 25:	El nivel de riesgo es inaceptable.

VII. Conclusiones generales 2019

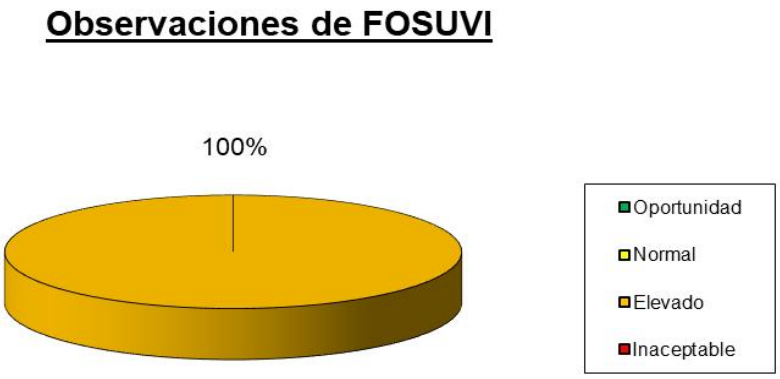
Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
A.1	Replanteamiento de proyectos para atender la ausencia de un Sistema Integrado de Vivienda	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
A.2	Mejoras a los procesos de gestión de TI y negocio para cerrar brechas según el Marco de Gestión de TI	Cumplimiento parcial bajo	Serio	Frecuente	Elevado

VIII. Mapa de calor de los riesgos evidenciados

De acuerdo con nuestra revisión y a la metodología de calificación del nivel de exposición al riesgo, presentamos a continuación la matriz de 25 cuadrantes donde se resume de manera gráfica, las observaciones que incluimos en nuestro informe y su nivel de riesgo.



Mapa de riesgos identificado para la oportunidad de mejora para los sistemas de información de FOSUVI.



Como resultado de la revisión se comunican 2 observaciones que son clasificadas en la categoría de riesgo ubicada en las áreas revisadas en la siguiente forma:

- 2 de riesgo elevado

IX. Procesos evaluados

A. Administración del área de TI

En la revisión de estas actividades se verificó lo siguiente:

1. Planificación estratégica de TI.
2. Aplicación de políticas, procedimientos y metodologías para la gestión de TI y procesos del negocio.
3. Cumplimiento de la normativa regulatoria.
4. Gestión del portafolio de proyectos.
5. Gestión del gobierno corporativo de TI.
6. Administración del cambio.

Se determina la siguiente observación:

A.1 Replanteamiento de proyectos para atender la ausencia de un Sistema integrado de Vivienda

Elevado
✔

Condición

Los proyectos:

- 25 Sistemas de Apoyo a la Gestión Financiera y Capital Humano.
- 03 Rediseño del Sistema de Vivienda.

Se gestiona en contrataciones separadas, en donde han existido inconvenientes en el proceso de contratación administrativa, recomendaciones nuevas que deben incluirse en los sistemas y requerimientos nuevos que no permiten avanzar en el "Rediseño del Sistema de Vivienda" y "Sistemas de Apoyo a la Gestión Financiera y Capital Humano."

El resultado del informe N° DFOE-EC-IF-00026 2019 de la Contraloría General de la República de fecha 18 de diciembre de 2019 sobre "la calidad de la información de bonos de vivienda contenida en el Sistema Automatizado del BANHVI", concluye sobre varias debilidades que hasta que no se identifican las acciones por medio de actividades y requerimientos, no es viable avanzar en las mejoras del Sistema de Vivienda.

El proyecto "Sistemas de Apoyo a la Gestión Financiera y Capital Humano", recibe una única oferta (26 de noviembre de 2019) para la Licitación Pública 2019LN-000001-0016400001 (Contratación de servicios de licenciamiento o suscripción, así como la implementación de una plataforma integral ERP de clase mundial y Capital Humano en la Nube con modalidad de servicio SaaS), con un precio del 76% de más sobre el monto establecido para la contratación con base en el Estudio de Mercado recibido.

Por las razones indicadas y lo informado en carta de gerencia del periodo 2019 sigue existiendo un "Sistema de Vivienda" no integrado a los sistemas del Banco y con recomendaciones a ser desarrolladas al sistema.

Causa

Se han presentado tiempos de espera debido al cumplimiento del proceso de contratación administrativa que no han sido fructuosos, junto con la incorporación de otras recomendaciones de auditoría del ente regulador, han generado riesgos operativos en la ausencia de una integración de sistemas, falta de recurso humano con las competencias para el desarrollo de sistemas de información, posibles pérdidas financieras y de tiempo en el recurso humano que interviene en el proceso.

Efecto

Estas condiciones afectan directamente el avance de los proyectos, correspondiendo a una debilidad significativa al no poder cumplir con el cronograma inicial para el rediseño del Sistema de Vivienda y la dependencia de un ERP integrado al Sistema de Vivienda.

Criterio

Según el Manual de Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República, que en el apartado 1.5, Gestión de proyectos menciona:

"La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos."

Recomendaciones

Continuar con las actividades replanteadas y aceptadas para la implementación de un nuevo proyecto de sistemas de información del BANHVI de los proyectos:

- ✓ Sistemas de Apoyo a la Gestión Financiera y Capital Humano (SAGF-CH)
- ✓ Rediseño del Sistema de Vivienda (RSV)

Dar seguimiento y rendimiento de cuentas como lo han venido ejecutando en las actividades de los proyectos anteriores, para el nuevo proyecto sobre la integración, fortalecimiento y mejoras a los sistemas de información.

Comentarios de la administración

Se analizaron integralmente la atención de las recomendaciones del informe N° DFOE-EC-IF-00026 2019 de la Contraloría General de la República sobre "la calidad de la información de bonos de vivienda contenida en el Sistema Automatizado del BANHVI", porque impacta los 2 proyectos citados.

Se replantearon los proyectos en un solo proyecto, con el objetivo de atender las necesidades organizacionales tanto del Proyecto de los Sistemas de Apoyo a la Gestión Financiera como del Proyecto de Rediseño del Sistema de Vivienda, pero considerando el Informe de la CGR, las sanas prácticas en materia de proyectos y los riesgos de mantener por separado la implementación de dichos proyectos.

Fueron documentadas las lecciones aprendidas de cada etapa de los proyectos y realizar un informe integral de cierre, identificando las causas que originaron los rezagos para futuros proyectos y la estrategia de negociación con proveedores.

Se informó a los Órganos de Dirección por medio de un análisis de riesgos, las debilidades y las condiciones actuales para lograr implementar un sistema de vivienda integrado a los sistemas financieros del Banco; a pesar de los esfuerzos realizados por años será difícil cumplir con los plazos establecidos para cumplir el objetivo.

Se definió una ruta de implementación integral con las prácticas de gobierno corporativo de TI, los insumos de las lecciones aprendidas, los compromisos sin atender de auditorías internas, externas y regulatorias, y en mayo 2020 se incorporará un Plan Maestro que considere un informe de riesgos, la disponibilidad presupuestaria y la capacidad instalada de recurso para atender los planes operativos anuales y lograr la implementación de un sistema integrado de vivienda con atributos de seguridad, integridad, confidencialidad y disponibilidad de los datos, la integración requerida a los sistemas del BANHVI y el control de accesos con el fin de mitigar los riesgos existentes a la fecha, por la falta de un sistema integrado de vivienda para el Banco como ente rector del Sistema Financiero Nacional para la Vivienda.

A.2 Mejoras a los procesos de gestión de TI y negocio para cerrar brechas según el Marco de Gestión de TI

Elevado
✔

Condición

Se identificó por medio del informe de auditoría externa de TI con fecha 12 de noviembre de 2019 realizado por otros auditores oportunidades de mejora a los procesos del Marco de Gestión de TI del Banco Hipotecario de la Vivienda (BANHVI), los cuales presentan brechas para cumplir con las prácticas de gestión de cada proceso, según lo indicado en el marco de referencia de aplicación para el Marco de Gestión de TI.

Los resultados de los 32 procesos auditados según el criterio de evaluación fueron los siguientes:

3 procesos son aceptables:

1.4 Asegurar la optimización de los recursos
1.5 Asegurar la transparencia hacia las partes interesadas
2.11 Gestionar los riesgos de TI

14 procesos son mejorables:

1.1 Asegurar el establecimiento y mantenimiento del marco de gobierno
1.2 Asegurar la entrega de beneficios
2.1 Gestionar el marco de gestión de TI
2.2 Gestionar la estrategia
2.6 Gestionar los recursos humanos
2.7 Gestionar las relaciones entre TI y el negocio
2.9 Gestionar los servicios de los proveedores de TI
3.1 Gestionar los programas y proyectos
3.4 Gestionar la disponibilidad y capacidad
3.7 Gestionar los activos de TI
4.1 Gestionar las operaciones
4.4 Gestionar la continuidad
4.5 Gestionar los servicios de seguridad de la información
5.2 Supervisar, evaluar y valorar el sistema de control interno

15 procesos son débiles:

2.4 Gestionar el portafolio
2.5 Gestionar el presupuesto y los costos
2.8 Gestionar los acuerdos de servicio
2.10 Gestionar la calidad
2.12 Gestionar la seguridad
3.2 Gestionar la definición de requerimientos
3.3 Gestionar la identificación y construcción de soluciones

3.5 Gestionar los cambios
3.6 Gestionar la aceptación del cambio y la transición
3.8 Gestionar la configuración
4.2 Gestionar peticiones e incidentes de servicio
4.3 Gestionar los problemas
4.6 Gestionar los controles de los procesos de la empresa
5.1 Supervisar, evaluar y valorar el sistema de control interno
5.3 Supervisar, evaluar y valorar la conformidad con los requerimientos externos

Las observaciones identificadas afectan directamente a FOSUVI, porque sus sistemas de información, infraestructura tecnológica y de comunicación, la gestión de la seguridad, la continuidad de operaciones, atención de requerimientos, la administración de las bases de datos, entre otros, son recibidos por el área de TI del Banco y se requieren para dar mejora continua a los procesos del Marco de Gestión de TI.

Causa

En cumplimiento del Marco de Gestión de TI, se debe cumplir con prácticas de control bajo un criterio del marco normativo que empezó a regir a partir del 2017, mismo que estaba en proceso de implementación de recomendaciones de la autoevaluación interna, cuando llego el oficio de la aplicación de la auditoría externa de TI, cuyo alcance debía aplicarse un año hacia atrás para verificar la efectividad de los controles.

Efecto

Estas observaciones evidencian la ausencia de procedimientos de control en los procesos vinculantes a FOSUVI para gestionar los servicios internos y administrar el Sistema de Vivienda de forma integral y sin la mayor intervención manual.

Recomendación

Recomendamos a los Órganos de Dirección, de acuerdo a la planificación institucional seguir dando seguimiento y dotar al Departamento de TI de los recursos necesarios para la implementación del plan de acción que debe ser presentado en un plazo no mayor a 6 meses y que incluye las actividades necesarias para ir cerrando las brechas actuales en los procesos de gestión de TI y del negocio.

B. Gestión de las prácticas de seguridad de la información

En la revisión de estas actividades se verificó lo siguiente:

1. Políticas, procedimientos, herramientas y metodologías en la administración de la seguridad de la información.
2. Gestión de roles y perfiles de acceso.
3. Planes de acción para la implementación de mejoras o debilidades de seguridad.
4. Validación de perfiles de acceso.
5. Gestión en la atención de incidentes.

6. Estrategia y plan de seguridad de la información.
7. Políticas y procedimientos para la prevención, detección y corrección de virus.
8. Gestión de contraseñas para el ingreso a sistemas.

En el informe de auditoría externa de TI sobre el Acuerdo SUGEF 14-17 del BANHVI se informan observaciones vinculadas a la gestión de las prácticas y seguridad de la información, entre ellas, las siguientes:

- ✓ No existe un Sistema de Gestión de Seguridad de la Información (SGSI).
- ✓ Falta la definición y gestión del plan de tratamiento del riesgo de la seguridad de la información.
- ✓ No existe una política de prevención de software malicioso.
- ✓ Falta la documentación relacionada con los protocolos de seguridad para las conexiones de red.
- ✓ No se evidencia la ejecución de pruebas de intrusión.
- ✓ Ausencia de evidencia documental sobre la gestión de accesos físicos a los activos de TI.
- ✓ Faltan esquemas de clasificación de información, para una administración de la información que contiene datos sensibles o confidenciales.

Por medio del plan de acción para la atención de las recomendaciones del proceso "2.12 Gestionar la seguridad" y el proceso "4.5 Gestionar contra software malicioso) del informe con fecha 12 de noviembre de 2019 de la auditoría externa de TI sobre el Reglamento de Tecnología de Información, se estarían atendiendo las brechas y riesgos identificados.

C. Sistemas de información

En la revisión de estas actividades se verificó lo siguiente:

1. Metodología para el desarrollo de sistemas y atención de requerimientos.
2. Validación de la documentación de cada una de las etapas de la metodología cuando se desarrolla nuevos sistemas.
3. Funcionalidad de los sistemas de información.
4. Inventarios de licencias, sistemas y activos de información.
5. Integridad, seguridad y disponibilidad de los datos en los sistemas de información.
6. Diagrama sobre la integración de sistemas.

En el informe de auditoría externa de TI sobre el Acuerdo SUGEF 14-17 del BANHVI se informan observaciones vinculantes a la gestión de sistemas de información, entre las siguientes:

- ✓ Faltan criterios en las "Metodologías de Desarrollo" para la identificación, análisis y remediación de los riesgos para los requerimientos de las soluciones.
- ✓ Faltan criterios en las "Metodologías de Desarrollo" para la identificación, análisis y remediación de los riesgos para los requerimientos de las soluciones.
- ✓ Ausencia de integración entre los sistemas de información.

- ✓ Faltan controles para la correcta configuración de las soluciones.
- ✓ No se evidencia planes de aseguramiento de la calidad.

- ✓ Faltan controles para registrar y analizar los cambios a los diseños y evaluar el impacto de la personalización y configuración en el rendimiento y eficiencia de las soluciones adquiridas, podría ocurrir un inadecuado desarrollo de los componentes de la solución, lo que podría llevar a la puesta en producción de soluciones que no satisfagan las necesidades del Banco.

  Por medio del plan de acción para la atención de las recomendaciones del proceso "3.2 Gestionar la definición de requerimientos" y el proceso "3.3 Gestionar la identificación y construcción de soluciones" del informe con fecha 12 de noviembre de 2019 de la auditoría externa de TI sobre el Reglamento de Tecnología de Información, se estarían atendiendo las brechas y riesgos identificados.

D. Software y bases de datos

En la revisión de estas actividades se verificó lo siguiente:

1. La aplicación de políticas y procedimientos para instalación, administración, mantenimiento y seguridad de las bases de datos.
2. Documentación de los componentes de las bases de datos.
3. Políticas y procedimientos para la administración de las bases de datos.
4. Cronograma para el mantenimiento y monitoreo de la base de datos.

En el informe de auditoría externa de TI sobre el Acuerdo SUGEF 14-17 del BANHVI se informan observaciones vinculantes a la gestión de software y bases de datos, entre los siguientes procesos "3.2 Gestionar la definición de requerimientos" y "3.3 Gestionar la identificación y construcción de soluciones.

Por medio del plan de acción para la atención de las recomendaciones del proceso asociado, del informe con fecha 12 de noviembre de 2019 de la auditoría externa de TI sobre el Reglamento de Tecnología de Información, se estarían atendiendo las brechas y riesgos identificados.

E. Gestión de la continuidad de operaciones

En la revisión de estas actividades se verificó lo siguiente:

1. Aplicación del marco de continuidad de negocio.
2. Existencia del plan de continuidad de TI.
3. Plan de pruebas de continuidad de negocio y TI.
4. Capacitación a los colaboradores en continuidad de negocio.
5. Pruebas de validación a los respaldos.
6. Sitio alterno o alternativas de procesamiento.

En el informe de auditoría externa de TI sobre el Acuerdo SUGEF 14-17 del BANHVI se informan observaciones se vinculan a la gestión de las prácticas y seguridad de la información, entre las siguientes:

- ✓ Falta alineación entre el perfil tecnológico y el plan de continuidad, lo que podría llevar a la incapacidad de recuperar procesos, servicios e infraestructura considerada crítica durante un evento de continuidad.
- ✓ Falta actualización del análisis de riesgos de continuidad, lo que podría ocasionar la indisponibilidad de los servicios y/o procesos críticos del Banco.
- ✓ Análisis de impacto no actualizado, podría ocasionar la no recuperación en tiempo de los servicios y procesos identificados como críticos.
- ✓ Ausencia de estrategias de recuperación documentadas y probadas, podrían llevar a pérdidas económicas.

Por medio del plan de acción para la atención de las recomendaciones del proceso "4.4 Gestionar la continuidad" del informe con fecha 12 de noviembre de 2019 de la auditoría externa de TI sobre el Reglamento de Tecnología de Información, se estarían atendiendo las brechas y riesgos identificados.

F. Seguimiento de las recomendaciones anteriores

Existe una identificación de recomendaciones en proceso y pendientes de atender para la Dirección de FOSUVI, para lo cual confeccionaron un plan de trabajo que fue aprobado en febrero de 2020 por la Junta Directiva del cual deben rendir cuentas del avance por medio de informes mensuales a la Junta Directiva, por un tiempo estimado de 2 años, que hará la Dirección de FOSUVI con los recursos que el Gobierno Corporativo proporcione.