Crowe Horwath CR, S.A.

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

Carta de Tecnología de Información

Al 31 de diciembre de 2020

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

1 de junio de 2021

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 los Sistemas de Información del Fondo de Subsidios para la Vivienda, referente a la auditoría de sus estados financieros al 31 de diciembre de 2020, 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. Este informe se estructura como resultado del cumplimiento de las NIA 315 y 330; no es ni debe interpretarse como una evaluación al Departamento de Tecnología de Información de forma específica ni tampoco a una evaluación del Banco Hipotecario de la Vivienda.

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 2020, 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

FABIAN ZAMORA AZOFEIFA (FIRMA)
Firmado digitalmente por FABIAN ZAMORA AZOFEIFA (FIRMA)
Fecha: 2021.06.01 16:31:25 -06'00'

c.c. Presidente Comité de Auditoría

Fondo de Subsidios para la Vivienda

Informe de tecnología de información

Al 31 de diciembre de 2020

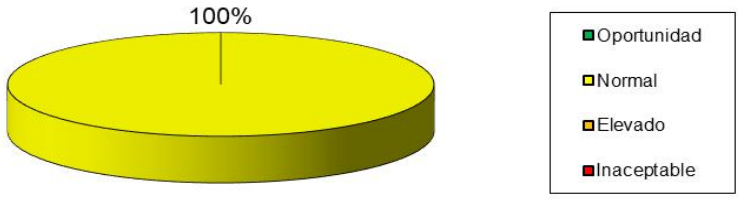
I. Resumen ejecutivo

Como parte del trabajo de la auditoría de estados financieros del periodo 2020 se llevó seguimiento de la evaluación de controles de Tecnología de Información (TI) en el Fondo de Subsidios para la Vivienda (FOSUVI) del periodo 2020, 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. Esta carta de gerencia no es ni debe tomarse como un informe sobre los sistemas de información del BANHVI.

Para la evaluación del periodo 2020 se encuentran en proceso de atención 1 observación que es clasificada de riesgo normal de acuerdo con la naturaleza y metodología utilizada.

Oportunidad de mejora de FOSUVI



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. 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.

V. 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.

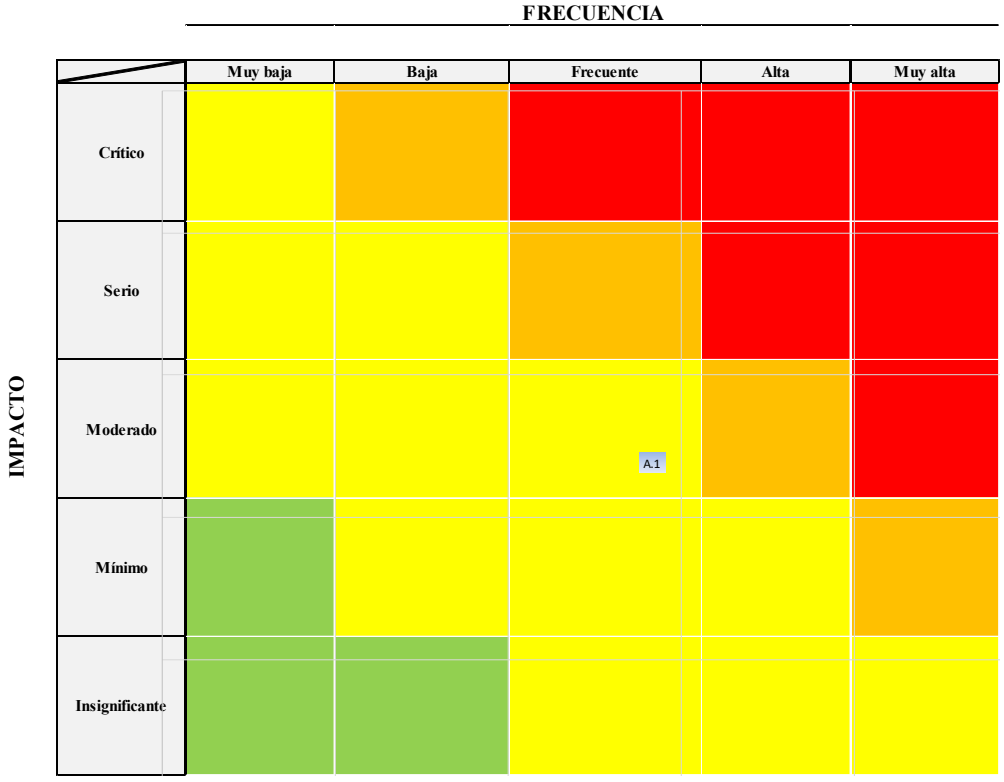
VI. Conclusiones generales 2020

Oportunidad de mejora del periodo 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 alto	Moderado	Frecuente	Normal

VII. 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.



VIII. 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 da seguimiento a las siguientes observaciones:

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

Normal
✔

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 han sido infructuosos, 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.

Comentario de la administración a marzo 2021

Los alcances de los proyectos denominados Sistemas de Apoyo a la Gestión Financiera y Capital Humano (SAGF-CH) y Rediseño del Sistema de Vivienda (RSV), fueron incluidos en el proyecto denominado **Optimización de Procesos y Tecnologías de Información Medulares para los Usuarios de Servicios BANHVI (OPTIMUS).** Dicho Proyecto fue conocido por la Junta Directiva el 12 de marzo de 2020 a partir del oficio GG-ME-0256-2020 remitido en esa misma fecha por parte del Lic. Dagoberto Hidalgo Cortés, Gerente General y patrocinador de este proyecto.

El oficio fue remitido en atención a lo requerido mediante Acuerdo No 16 de la Sesión No. 19-2020 del pasado 9 de marzo 2020, y al mismo adjuntó una propuesta de estrategia para la implementación de un nuevo proyecto de sistemas de información del Banco, a partir de lo cual se definió, oficializó e implementó el correspondiente Plan Maestro, conforme lo requerido por la Contraloría General de la República en la disposición 4.4 del Informe No. DFOE-EC-IF-00026-2019 denominado "Informe de auditoría de carácter especial sobre la calidad de la información de bonos de vivienda contenida en el sistema automatizado del BANHVI". En cumplimiento del acuerdo citado, el 28 de junio de 2020 la Gerencia General remitió el Plan Maestro del proyecto a la Junta Directiva, mediante el oficio *GG-ME-0577-2020 Plan maestro sistemas de información*.

El siguiente cuadro muestra un resumen actualizado de las acciones en proceso, a saber:

Cuadro 01 Hoja de ruta de la Propuesta de estrategia para la ejecución de un nuevo proyecto de sistemas de información del BANHVI (PROY-37-NP-INF-001).

Todas las actividades planteadas y definidas para el 2020, poseen un avance del 100%.

Situación actual

En proceso.

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 con 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.

Comentario de la administración a marzo 2021

Mediante el acuerdo No. 08-2020 del 30 de enero del 2020, la Junta Directiva aprobó el Plan de Acción para atender las debilidades y los riesgos identificados por la Auditoría Externa de Tecnologías de Información realizada en el 2019, conforme lo establecido en el Acuerdo SUGEF 14-17.

Situación actual de la auditoría

Concluido.

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.

Por medio del plan de acción aprobado mediante el acuerdo No. 08-2020 del 30 de enero del 2020 por Junta Directiva se da seguimiento y cumplimiento a las debilidades y los riesgos identificados por la Auditoría Externa de Tecnologías de Información realizada en el 2019, conforme lo establecido en el Acuerdo SUGEF 14-17.

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.

Por medio del plan de acción aprobado mediante el acuerdo No. 08-2020 del 30 de enero del 2020 por Junta Directiva se da seguimiento y cumplimiento a las debilidades y los riesgos identificados por la Auditoría Externa de Tecnologías de Información realizada en el 2019, conforme lo establecido en el Acuerdo SUGEF 14-17.

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.

Por medio del plan de acción aprobado mediante el acuerdo No. 08-2020 del 30 de enero de 2020 por Junta Directiva se da seguimiento y cumplimiento a las debilidades y los riesgos identificados por la Auditoría Externa de Tecnologías de Información realizada en el 2019, conforme lo establecido en el Acuerdo SUGEF 14-17.

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.

Por medio del plan de acción aprobado mediante el acuerdo No. 08-2020 del 30 de enero de 2020 por Junta Directiva se da seguimiento y cumplimiento a las debilidades y los riesgos identificados por la Auditoría Externa de Tecnologías de Información realizada en el 2019, conforme lo establecido en el Acuerdo SUGEF 14-17.