Fondo de Subsidio para la Vivienda
(FOSUVI)

Informe Auditoría de Sistemas de Información

Carta de Gerencia

CG-TI 2023

San José, 01 de abril del 2024.

Señores
Fondo de Subsidio para la Vivienda (FOSUVI)

Estimados señores:

Según nuestro contrato de servicios, efectuamos nuestra visita de auditoría externa del período 2023 al Fondo de Subsidio para la Vivienda (FOSUVI) y con base en el examen efectuado observamos ciertos aspectos referentes al sistema de control interno y procedimientos de Tecnología de Información, basados en las "Normas técnicas para el gobierno y gestión de las tecnologías de la información" del MICITT y los estándares establecidos como buenas prácticas según los Objetivos de Control para Información y Tecnología Relacionada – COBIT®., los cuales sometemos a consideración de ustedes en esta carta de gerencia CG-TI 2023.

Considerando el carácter de pruebas selectivas en que se basa nuestro examen, ustedes pueden apreciar que se debe confiar en métodos adecuados de comprobación y de control interno, como principal protección contra posibles irregularidades que un examen basado en pruebas selectivas puede no revelar, si es que existiesen. Las observaciones no van dirigidas a funcionarios o empleados en particular, sino únicamente tienden a fortalecer el sistema de control interno y los procedimientos relacionados con la tecnología de información.

DESPACHO CARVAJAL & COLEGIADOS
CONTADORES PÚBLICOS AUTORIZADOS

MARIO RICARDO MONTENEGRO GUILLEN (FIRMA)
Firmado digitalmente por MARIO RICARDO MONTENEGRO GUILLEN (FIRMA)
Fecha: 2024.12.11 14:26:38 -06'00'

Lic. Ricardo Montenegro Guillén
Contador Público Autorizado No. 5607
Póliza de Fidelidad Nº 0116 FIG 7
Vence el 30 de setiembre del 2024.

Nombre del CPA: MARIO RICARDO MONTENEGRO GUILLEN
Carné: 5607
Cédula: 303430715
Nombre del Cliente: BANCO HIPOTECARIO DE LA VIVIENDA
Identificación del cliente: 3007078890
Dirigido a: BANCO HIPOTECARIO DE LA VIVIENDA
Fecha: 11-12-2024 02:23:47 PM
Tipo de trabajo: INFORME AUDITORÍA DE SISTEMAS DE INFORMACIÓN

Timbre de ¢25 de la Ley 6663 adherido y cancelado en el original.

MARIO RICARDO MONTENEGRO GUILLEN
Contador Público Autorizado No. 5607
COSTA RICA

COSTA RICA TIMBRE
25 COLONES 25

Código de Timbre: CPA-25-405739

TABLA DE CONTENIDO

INFORME DE CUMPLIMIENTO Y CONTROL INTERNO DE TECNOLOGÍAS DE INFORMACIÓN

I. INTRODUCCIÓN

ORIGEN DEL ESTUDIO

Como parte de la evaluación a los estados financieros del Fondo de Subsidio para la Vivienda (FOSUVI), evaluamos los controles generales de la gestión de tecnologías de información, con el objetivo de medir el grado de riesgo de la información en lo que respecta a seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica.

La evaluación la realizamos basados en las normas técnicas para el gobierno y gestión de las tecnologías de la información" del MICITT, y nos apoyamos en los Objetivos de Control de Tecnologías de Información (COBIT por sus siglas en inglés) emitidos por la "Information Systems Audit and Control Association" (ISACA por sus siglas en inglés) como marco de mejores prácticas de la industria de tecnología de información.

OBJETIVO DEL ESTUDIO

Con el propósito de cumplir con los requerimientos estipulados en la Norma Internacional de Auditoría 315, Entendiendo de la realidad y su entorno y evaluación de representación errónea de importancia relativa y en la Norma Internacional de Auditoría 330, Procedimientos del auditor en respuesta a los riesgos evaluados, realizamos un diagnóstico a la gestión de las tecnologías de información del Fondo de Subsidio para la Vivienda (FOSUVI).

ALCANCE

En esta visita el trabajo fue enfocado principalmente a las siguientes áreas:

- Planificación estratégica de TI.
- Gestión de respaldos y restauraciones.
- Gestión de activos de TI.
- Gestión de la calidad.
- Gestión de la seguridad de la información.
- Gestión de los roles y perfiles.
- Gestión de la seguridad lógica y automatización de procesos.
- Gestión de peticiones, incidentes y problemas.
- Gestión de cambios de TI.
- Gestión de riesgos.
- Seguimiento a recomendaciones emitidas en periodos anteriores.

PERIODO DEL ESTUDIO

El estudio se realizó durante el mes de marzo del año 2024 y corresponde a la auditoría del periodo del 2023.

LIMITACIONES DEL ESTUDIO

No se presentaron limitaciones durante el estudio.

METODOLOGÍA

Para llevar a cabo este trabajo utilizamos una modalidad de análisis de la información suministrada por la administración del FOSUVI y de las distintas áreas involucradas en el proceso de auditoría. Además, se formularon preguntas sobre la existencia de controles de las tecnologías de información, en todos los casos necesarios solicitamos a los funcionarios las evidencias en formato digital que respaldaran sus afirmaciones

II. HALLAZGOS Y RECOMENDACIONES

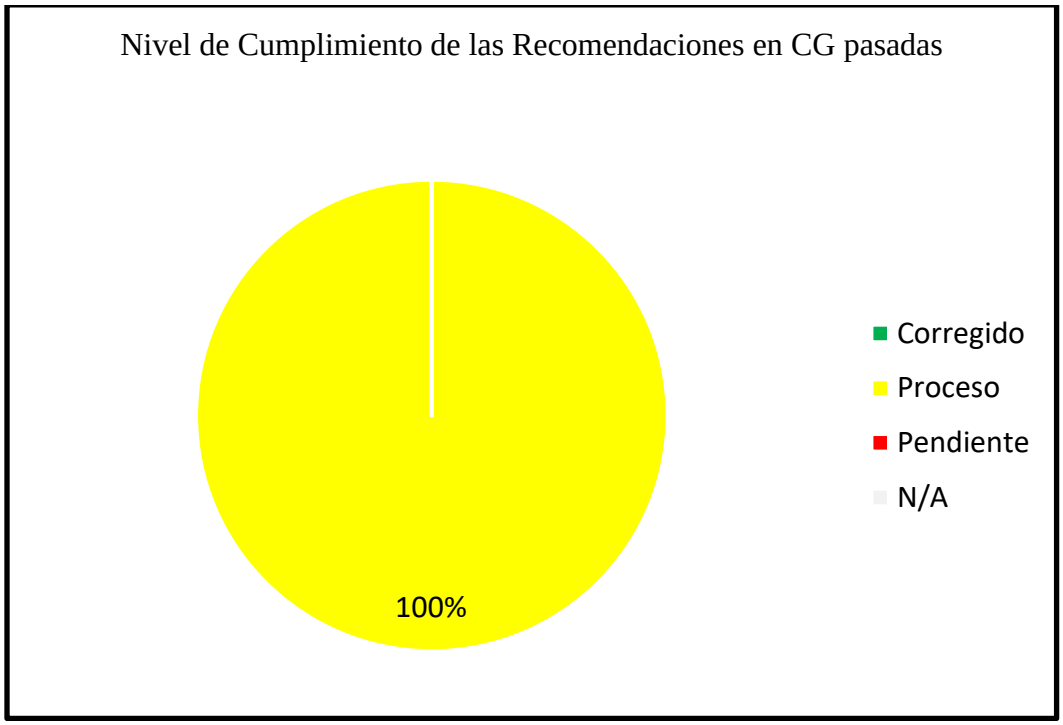
Producto de la revisión efectuada y el alcance establecido no se presentan nuevos hallazgos para el periodo evaluado.

III. SEGUIMIENTO DE RECOMENDACIONES EMITIDAS EN CARTAS DE GERENCIA ANTERIORES

Carta de Gerencia 2020	
A.1 Replanteamiento de proyectos para atender la ausencia de un Sistema integrado de Vivienda	
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	Al 31 de diciembre de 2023, se indica que el proyecto denominado OPTIMUS se encuentra en ejecución mediante la contratación 2022LN-000001-0016400001 (LA CONTRATACIÓN DE SERVICIO DE HOSPEDAJE, ADMINISTRACION, OPERACION, MONITOREO, SEGURIDAD E IMPLEMENTACIÓN, DE UNA PLATAFORMA INTEGRAL EN LA NUBE CON COMPONENTES ERP, CORE BANCARIO, RECURSOS HUMANOS, ADMINISTRACIÓN DE PROYECTOS Y ANALÍTICA, TODOS ESTOS DE CLASE MUNDIAL PARA EL BANCO HIPOTECARIO DE LA VIVIENDA), mediante este proyecto se pretende subsanar el hallazgo señalado. Según el cronograma la implementación se realizará en 3 fases, la implementación de FASE I registra un avance de 65% y se tiene previsto finalizar el proyecto en el mes de octubre de 2026.
ESTADO	**EN PROCESO** Según lo indicado por la administración y el cronograma de implementación suministrado, durante el 2024 se estará ejecutando la implementación de la plataforma OPTIMUS, la fase I presenta un avance del 65% y el cierre del proyecto está previsto para 2026, este proyecto incluye lo necesario para atender el hallazgo. Por tanto, la atención del hallazgo se encuentra en proceso.

A continuación, se resume el estado sobre el cumplimiento de las recomendaciones emitidas en informes de auditorías anteriores de manera gráfica:

ESTADO	2020	TOTAL
Corregido	0	**0**
Proceso	1	**1**
Pendiente	0	**0**
N/A	0	**0**
Total	**1**	**1**



IV. ANEXOS

ANEXO I: Análisis de Riesgos TI
Departamento de Tecnología de Información
Periodo 2023

Tipos de Riesgo	
ALTO	A
MEDIO	M
BAJO	B

Alto A	Requiere una atención inmediata por su impacto en seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. No se han establecido controles en este nivel de riesgo.
Medio M	Requiere una atención intermedia ya que su impacto representaría riesgos sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles insuficientes en este nivel de riesgo.
Bajo B	Requiere una atención no prioritaria ya que su impacto no es directamente sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles adecuados en este nivel de riesgo.

I. PLANIFICACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

A. GESTIÓN DE LA CALIDAD DE LOS SERVICIOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
A.1.	Se cuenta con una política, metodología o procedimiento para la gestión de la calidad de los servicios de TI.		✓	Se cumple con la condición, además, se pretende actualizar la información para el 2024.	B
A.2.	Se han definido indicadores clave de los procesos de TI realizados para determinar el rendimiento de los servicios brindados.		✓	Se cumple con la condición.	B

B. GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
B.1.	Se tiene una metodología formalmente establecida y aprobada para la gestión de riesgos de TI.		✓	Se cumple con la condición.	B
B.2.	La evaluación de riesgos de TI es periódica y se encuentra revisada y aprobada por la administración (de acuerdo con el nivel de tolerancia al riesgo organizacional).		✓	Se cumple con la condición.	B

II. IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

C. GESTIÓN DE CAMBIOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
C.1.	Se cuenta con una política y/o procedimiento para la gestión de cambios de TI.		✓	Se cumple con la condición.	B
C.2.	Los cambios se realizan a través de solicitudes formales y se documenta todo el proceso realizado (ciclo de vida).		✓	Se cumple con la condición.	B
C.3.	La documentación de los cambios se mantiene de forma centralizada (mesa de servicios).		✓	Se cumple con la condición.	B

D. GESTIÓN DE ACTIVOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
D.1.	Se cuenta con un inventario de activos de TI (equipo en uso y desuso, periféricos, equipo de comunicación, dispositivos móviles, etc.), junto con información de su ubicación y responsable.		✓	Se cumple con la condición.	B

III. SOPORTE Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN.

E. GESTIÓN DE INCIDENTES.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
E.1.	Se cuenta con un procedimiento para la gestión de incidentes de TI.		✓	Se cumple con la condición.	B
E.2.	La gestión de incidentes se mantiene centralizada (mesa de servicios).		✓	Se cumple con la condición.	B
E.3.	Se verifica periódicamente el estado de los incidentes para determinar si se atienden oportunamente los incidentes registrados.		✓	Se cumple con la condición.	B

F. GESTIÓN DE PROBLEMAS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
F.1.	Se cuenta con un procedimiento para la gestión de problemas de TI.		✓	Se cumple con la condición.	B
F.2.	Se identifica, clasifica y analiza la causa raíz de los problemas de TI.		✓	Se cumple con la condición.	B

G. GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
G.1.	Se cuenta con una política y/o procedimiento para la realización de respaldos de información.		✓	Se cumple con la condición.	B
G.2.	Se realizan pruebas a los respaldos de información.		✓	Se cumple con la condición.	B
G.3.	Se tienen medidas de seguridad para los respaldos de información (acceso restringido, traslado de respaldos a un sitio externo).		✓	Se cumple con la condición.	B

H. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
H.1.	Se cuenta con una política de seguridad de la información formalmente aprobado por la administración y divulgado a nivel organizacional.		✓	Se cumple con la condición.	B
H.2.	Se le brinda seguimiento al cumplimiento de la política de seguridad de la información (se aplican medidas correctivas) y se le comunica los resultados a la administración.		✓	Se cumple con la condición.	B
H.3.	Se cuenta con una política y/o procedimiento para la gestión de cuentas de usuario.		✓	Se cumple con la condición.	B
H.4.	La asignación de accesos a la plataforma tecnológica parte del principio de segregación de funciones y son aprobados por parte del dueño del sistema.		✓	Se cumple con la condición.	B
H.5.	Se revisan periódicamente los perfiles de los usuarios para determinar si estos poseen la cantidad de accesos mínimos necesarios.		✓	Se cumple con la condición.	B
H.6.	Se inhabilitan las cuentas de los usuarios que cesan funciones en la organización (despidos, renuncias, jubilaciones, vacaciones, permisos, etc.).		✓	Se cumple con la condición.	B

IV. SISTEMAS DE INFORMACIÓN.

I. SEGURIDAD LÓGICA Y AUTOMATIZACIÓN DE PROCESOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
I.1.	Existencia de pistas de auditoría o bitácoras en los sistemas de información que permitan tener una trazabilidad en las transacciones realizadas por los usuarios.	✗		Se encuentra en proceso de implementación debido a la migración al sistema OPTIMUS. Según lo indicado por FOSUVI, este punto será atendido con la implementación del nuevo ERP. Esto se incluye en las gestiones que se realizarán en la atención del hallazgo **A.1 Replanteamiento de proyectos para atender la ausencia de un Sistema integrado de Vivienda**.	M
I.2.	Se revisan periódicamente las bitácoras de los sistemas de información para identificar comportamientos irregulares en las operaciones de la organización.	✗		No se cumple con la condición debido a que las pistas de auditoría y bitácoras en los sistemas de información se encuentran en proceso de implementación. Esto se incluye en las gestiones que se realizarán en la atención del hallazgo **A.1 Replanteamiento de proyectos para atender la ausencia de un Sistema integrado de Vivienda**.	M
I.3.	Los sistemas de información permiten solo una única sesión simultánea por usuario, de modo que no se pueda abrir una sesión con un mismo usuario en lugares distintos al mismo tiempo.		✓	Se cumple con la condición.	B
I.4.	Se han implementado medidas de seguridad lógica en los sistemas de información (vencimiento, histórico, tamaño y complejidad de la contraseña).		✓	Se cumple con la condición.	B
I.5.	Los sistemas de información cuentan con manuales de usuario y manuales técnicos.	✗		Se encuentra en proceso de implementación debido a la migración al sistema OPTIMUS. Según lo indicado por FOSUVI, este punto aplica la documentación del BANHVI, el cual no ha actualizado los manuales actuales debido a la implementación del nuevo sistema OPTIMUS.	M
I.6.	Los procesos de la organización están totalmente automatizados, evitando la realización de tareas manuales.		✓	Se cumple con la condición, además los sistemas se encuentran integrados habilitando así la automatización de procesos.	B
I.7.	Los sistemas de información se encuentran integrados entre sí, de modo que no se deba enviar información a través de medios externos a los sistemas.		✓	Se cumple con la condición	B
I.8.	Se restringe la entrada de datos de modo que el registro de información sea lo más estándar posible.		✓	Se cumple con la condición	B

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
I.9.	Se brindan capacitaciones periódicas en el uso de los sistemas a los usuarios de la organización.		✓	Se cumple con la condición	B

Última línea.