BANCO HIPOTECARIO DE LA VIVIENDA (BANHVI)

Informe Auditoría de Tecnologías de la Información

Carta de Gerencia CG-II-TI 2025

Informe Final

San José, 10 de febrero del 2026

Señores
Banco Hipotecario de la Vivienda (BANHVI)

Estimados señores:

Según nuestro contrato de servicios, efectuamos nuestra segunda visita de auditoría externa del período 2025 al Banco Hipotecario de la Vivienda (BANHVI) 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-II-TI 2025.

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

IVAN GUSTAVO BRENES PEREIRA (FIRMA)
PERSONA FISICA, CPF-03-0353-0965.
Fecha declarada: 19/02/2026 09:56:01 a. m.
Esta es una representación gráfica únicamente,
verifique la validez de la firma.

Lic. Iván Brenes Pereira
Contador Público Autorizado N° 5173
Póliza de Fidelidad N° 0116FID000501714

Vence el 30 de setiembre de 2026.

Nombre del CPA: IVAN BRENES PEREIRA
Carné: 5173
Cédula: 303530965
Nombre del Cliente: BANCO HIPOTECARIO DE LA VIVIENDA (BANHVI)
Identificación del cliente: 3007078890
Dirigido a: BANCO HIPOTECARIO DE LA VIVIENDA (BANHVI)
Fecha: 09-12-2025 09:55:30 AM
Tipo de trabajo: Carta a la Gerencia

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

IVAN BRENES PEREIRA
Contador Público Autorizado No. 5173
COSTA RICA

COSTA RICA TIMBRE
25 COLONES 25

Código de Timbre: CPA-25-601279

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 Banco Hipotecario de la Vivienda (BANHVI), 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 Banco Hipotecario de la Vivienda (BANHVI).

ALCANCE

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

- Verificación del control interno en materia tecnológica con base en la normativa interna establecida.
- Oportunidades de mejora identificadas en la evaluación.
- Seguimiento a recomendaciones emitidas en cartas de gerencia de periodos anteriores.

PERIODO DEL ESTUDIO

El estudio se realizó durante los meses de enero y febrero del presente año y corresponde a la segunda visita del periodo del 2025.

LIMITACIONES DEL ESTUDIO

No se presentaron limitaciones al alcance durante el estudio de la auditoría.

METODOLOGÍA

Para llevar a cabo este trabajo utilizamos una modalidad de análisis de la información suministrada por el Departamento de Tecnología de Información del BANHVI 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

No se detectaron hallazgos o recomendaciones durante el periodo auditado.

III. SEGUIMIENTO DE RECOMENDACIONES EMITIDAS EN CARTAS DE GERENCIA ANTERIORES

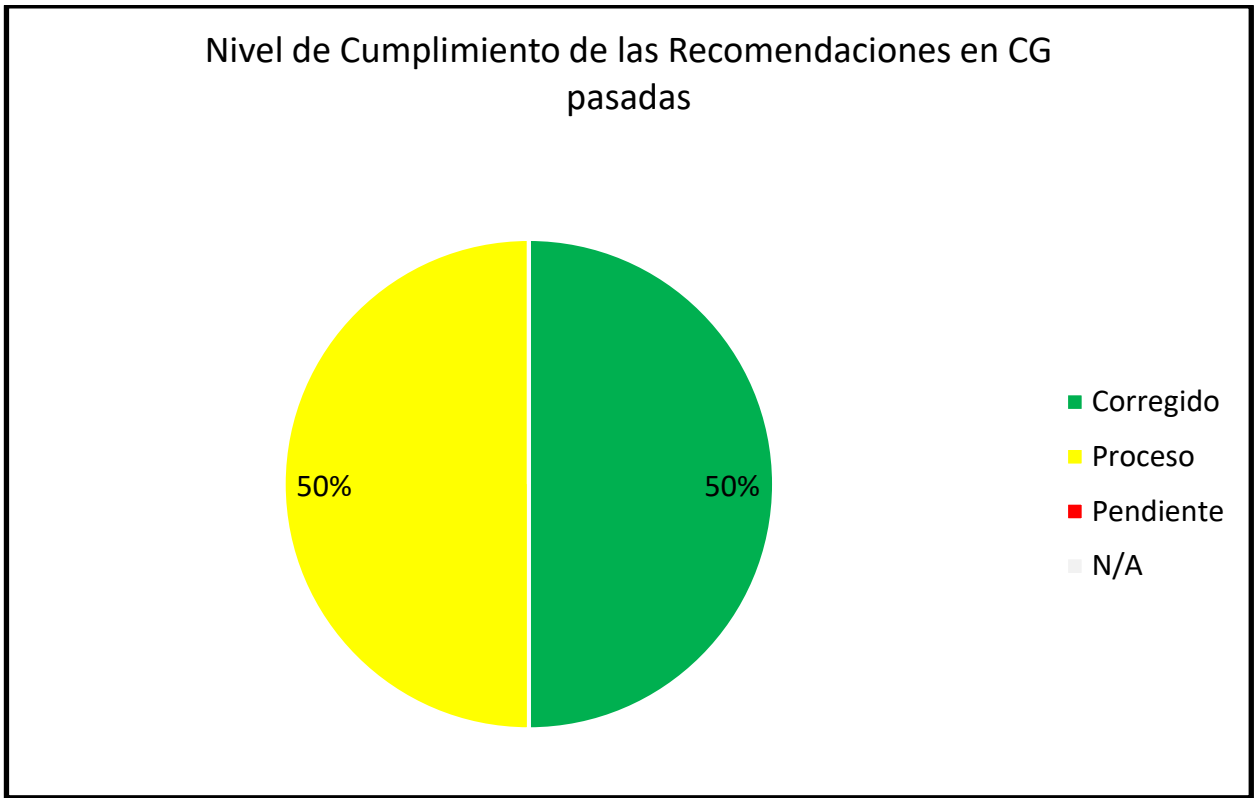
CG-I-TI 2025	
HALLAZGO 01: OPORTUNIDADES DE MEJORA EN LA GESTIÓN DE LA CONTINUIDAD. RIESGO MEDIO.	
RECOMENDACIONES	***A la directora Administrativa:*** 1. Programar y ejecutar capacitaciones periódicas sobre el Plan de Continuidad del Negocio y el Plan de Recuperación ante Desastres. 2. Mantener evidencia de las capacitaciones con las áreas involucradas con el plan para la gestión de la continuidad.
COMENTARIOS DE LA ADMINISTRACIÓN	Respecto a este tema, la institución cuenta con un Plan de sensibilización y capacitación vinculado a la implementación del Sistema de Gestión de Continuidad del Negocio, el cual fue desarrollado en septiembre de 2025. En dicho plan se identificaron tres grupos de funcionarios a los que se dirige la estrategia formativa: audiencia especializada, crítica y general, definidos según el rol y el nivel de responsabilidad que cada persona desempeña dentro del sistema. Asimismo, se incluyeron diversos contenidos, entre ellos: la política de continuidad del negocio (roles y responsabilidades), conceptos clave e importancia del sistema, identificación y declaración de crisis, así como otros temas relacionados. En cuanto a la periodicidad, se estableció que las capacitaciones se impartirán de forma semestral o anual, según la naturaleza del tema. Además, los contenidos se distribuyeron a lo largo del año calendario, con el fin de asegurar una cobertura integral de todos los tópicos contemplados en el plan. Finalmente, actualmente se está trabajando en el desarrollo de los materiales necesarios para iniciar las capacitaciones durante el primer trimestre del presente año, conforme a lo programado. Además, como evidencia se adjunta el plan de capacitación mencionado.
ESTADO	**EN PROCESO** Con base en la información suministrada por la administración, se constató la existencia del documento BANHVI - Plan de capacitación 2025_v2, el cual fue desarrollado en septiembre de 2025. No obstante, al momento de la revisión, se evidenció que las capacitaciones aún no han sido ejecutadas, dado que la

	institución se encuentra en la fase de desarrollo de los materiales necesarios para iniciar las sesiones conforme a lo programado durante el primer trimestre del presente año. Por lo anterior, se define el estado del hallazgo en proceso.
Informe 2019	
HALLAZGO 06: OPORTUNIDADES DE MEJORA EN LA GESTIÓN DE SOFTWARE. RIESGO BAJO.	
RECOMENDACIONES	***Al Departamento de Tecnología de Información:*** 1. Incluir en el inventario general de software al menos los siguientes aspectos: a. Proveedor. b. Estado. c. Licencias disponibles. d. Fecha de adquisición. e. Fecha de vencimiento / renovación. 2. Realizar conciliaciones al menos una vez cada año entre los inventarios de licencias de software general y el detallado, con los siguientes objetivos: a. Garantizar que el software instalado en los equipos es el autorizado por el BANHVI. b. Revisar que la cantidad de licencias instaladas corresponda a la cantidad de licencias adquiridas. En caso de identificar licencias que no se encuentra en uso, valorar la cancelación de estas considerando el ahorro en mantenimiento y otros gastos asociados.
COMENTARIOS DE LA ADMINISTRACIÓN	Se genera el Inventario de software Institucional con la información solicitada en la matriz “Inventario de Software Institucional" que se presentó como parte del Plan de Acción Conassif 05-17 en el proceso BAI09. Por lo cual se da por cumplida dicha recomendación.
ESTADO	**CORREGIDO** Como resultado del seguimiento realizado por el BANHVI, se verificó la elaboración de un inventario de software institucional, el cual fue presentado como parte del plan de acción asociado al proceso de gestión de activos. La evidencia documental revisada incluye un archivo en formato Excel correspondiente al Inventario de Software Institucional, el cual fue elaborado y validado por el Departamento de Tecnologías de Información en noviembre de 2025. Dicho inventario incluye los siguientes elementos: descripción de la licencia, proveedor, estado, fecha de adquisición, fecha de vencimiento o renovación, total de licencias contratadas, licencias asignadas, licencias disponibles, información de la licitación y responsable asignado. De acuerdo con la evidencia evaluada, se concluye que el hallazgo ha sido debidamente subsanado y se considera corregido.

A continuación, se resume por periodo el cumplimiento de las recomendaciones emitidas en periodos anteriores:

PERIODO	CORREGIDO	PROCESO	PENDIENTE	NO APLICA	TOTAL
2025	0	1	0	0	**1**
2019	1	0	0	0	**1**
TOTAL	**1**	**1**	**0**	**0**	**2**

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



IV. ANEXO I:

Análisis de Riesgos T.I. Departamento de Tecnología de Información
II Visita 2025

Tipos de Riesgo	
ALTO	A
MEDIO	M
BAJO	B

Alto ☑	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 ☑	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 ☑	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. SOPORTE Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN.

A. GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
A.1.	Se cuenta con un plan de continuidad del negocio (con el componente de TI), formalmente establecido y aprobado por la administración o el Comité de TI.		✓	Se cumple con la condición.	B
A.2.	Se realizan pruebas y capacitaciones sobre el plan de continuidad del negocio.	✗		No se cumple con la condición debido a que actualmente las recomendaciones relacionadas al hallazgo sobre capacitaciones en la gestión de la continuidad se encuentran en proceso de ser atendidas.	M
A.3.	Se cuenta con una política y/o procedimiento para la realización de respaldos de información.		✓	Se cumple con la condición.	B
A.4.	Se realizan pruebas a los respaldos de información.		✓	Se cumple con la condición.	B

B. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
B.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
B.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
B.3.	Se cuenta con una política y/o procedimiento para la gestión de cuentas de usuario.		✓	Se cumple con la condición.	B
B.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
B.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

B.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

II. SISTEMAS DE INFORMACIÓN.

C. SEGURIDAD LÓGICA Y AUTOMATIZACIÓN DE PROCESOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
C.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 cumple con la condición.	B
C.2.	Se revisan periódicamente las bitácoras de los sistemas de información para identificar comportamientos irregulares en las operaciones de la organización.		✓	Se cumple con la condición.	B
C.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
C.4.	Los sistemas de información cuentan con validación de usuarios a través de cuentas y contraseñas (Active Directory, LDAP, otros).		✓	Se cumple con la condición.	B
C.5.	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
C.6.	Los sistemas de información cuentan con manuales de usuario y manuales técnicos.		✓	Se cumple con la condición.	B
C.7.	Los procesos de la organización están totalmente automatizados, evitando la realización de tareas manuales.		✓	Se cumple con la condición.	B
C.8.	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
C.9.	Se restringe la entrada de datos de modo que el registro de información sea lo más estándar posible.		✓	Se cumple con la condición.	B
C.10.	Se brindan capacitaciones periódicas en el uso de los sistemas a los usuarios de la organización.		✓	Se cumple con la condición.	B

-- Última Línea --