BANCO HIPOTECARIO DE LA VIVIENDA (BANHVI)

Informe Auditoría de Sistemas de Información

Carta de Gerencia CG-I-TI 2025

Informe Final

San José, 08 de octubre del 2025

Señores
Banco Hipotecario de la Vivienda (BANHVI)

Estimados señores:

Según nuestro contrato de servicios, efectuamos nuestra primera 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-I-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: 09/12/2025 11:05:36 AM
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 septiembre y octubre del presente año y corresponde a l primera visita del periodo del 2025.

LIMITACIONES DEL ESTUDIO

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

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.

I. HALLAZGOS Y RECOMENDACIONES

HALLAZGO 01: OPORTUNIDADES DE MEJORA EN LA GESTIÓN DE LA CONTINUIDAD. RIESGO MEDIO.

CONDICIÓN:

Se comprobó que el BANHVI cuenta con un plan de continuidad del negocio y un plan de recuperación ante desastres. Sin embargo, no se suministró evidencia que permitiera verificar la realización de capacitaciones con las áreas involucradas con el plan para la gestión de la continuidad.

La falta de capacitación al personal involucrado en los planes de continuidad del negocio y recuperación ante desastres podría generar una respuesta inefectiva o descoordinada ante incidentes que afecten la operación institucional, aumentando el tiempo de recuperación y el impacto sobre los servicios críticos.

CRITERIO:

Además, en la práctica de gestión **DSS04.06 Realizar formación sobre el plan de continuidad** del proceso **DSS04 Gestionar la Continuidad**, menciona: "Proporcionar sesiones periódicas de formación sobre los procedimientos y sus roles y responsabilidades en caso de interrupción a todas las partes internas y externas involucradas".

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.

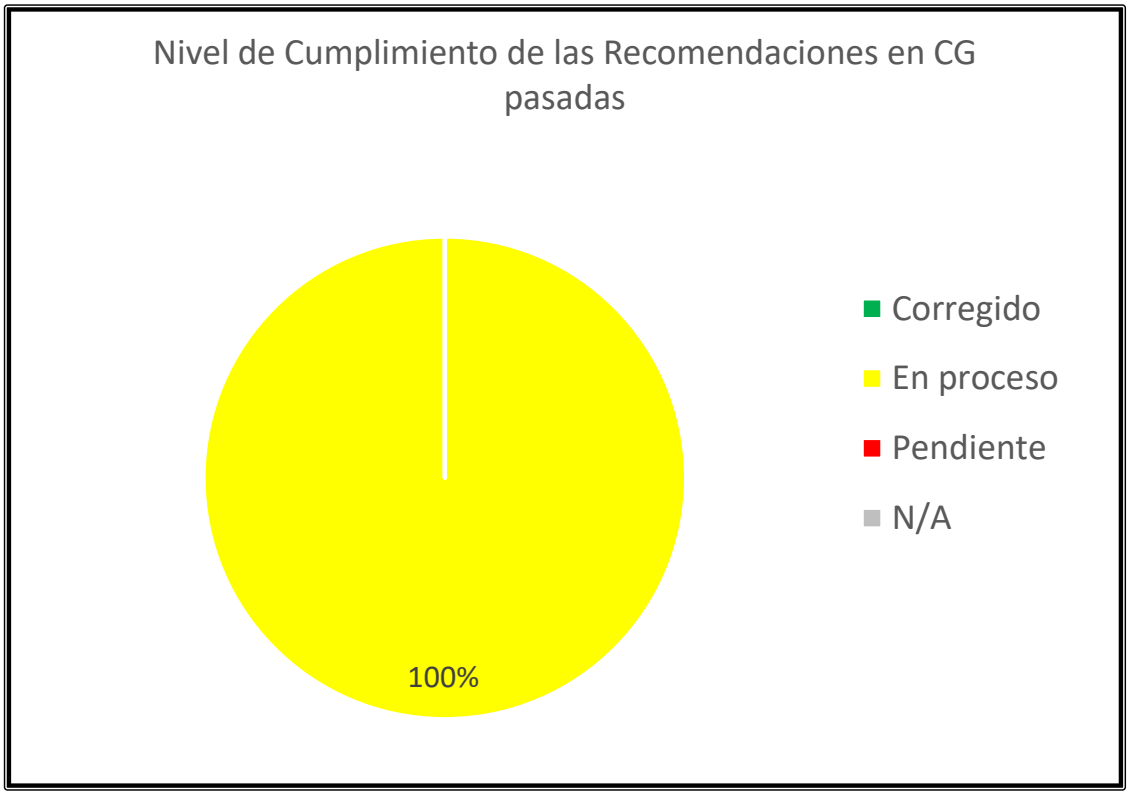
II. SEGUIMIENTO DE RECOMENDACIONES EMITIDAS EN CARTAS DE GERENCIA ANTERIORES

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	Sin comentarios.
ESTADO	**EN PROCESO** El BANHVI ha implementado mecanismos que permiten el control y monitoreo del software instalado en los equipos institucionales, tales como reportes mensuales de cumplimiento de actualizaciones para servidores y estaciones de trabajo, así como herramientas de seguridad y administración de parches. Adicionalmente, se cuenta con un inventario general de licencias que incluye el detalle de productos y cantidades adquiridas, lo que evidencia avances en la gestión administrativa del licenciamiento. Sin embargo, el inventario aún no incorpora todos los campos requeridos (proveedor, estado, licencias disponibles, fecha de adquisición y fecha de vencimiento) y no se ha documentado la conciliación anual entre licencias adquiridas y software instalado, con resultados y acciones corregidas.

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

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

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



III. ANEXO I:

Análisis de Riesgos T.I.

Departamento de Tecnología de Información I 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. PLANIFICACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

A. GESTIÓN DE PROVEEDORES DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
A.1.	Se establecen contratos formales para los servicios que son brindados por terceros.		✓	Se cumple con la condición.	B
A.2.	Para los contratos de servicios de TI, se establecen acuerdos de nivel de servicio con los respectivos indicadores de capacidad, disponibilidad, confiabilidad, etc.		✓	Se cumple con la condición.	B
A.3.	Se realiza un seguimiento al cumplimiento contractual de las responsabilidades de los proveedores.		✓	Se cumple con la condición.	B

B. GESTIÓN DE ACUERDOS DE NIVEL DE SERVICIO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
B.1.	Se cuenta con un catálogo de servicios de TI actualizado y aprobado por el Comité de TI.		✓	Se cumple con la condición.	B
B.2.	Se cuenta con una política o procedimiento para la gestión de los acuerdos de nivel de servicio (SLAs) de TI.		✓	Se cumple con la condición.	B
B.3.	Se tiene definido acuerdos de nivel de servicio para cada uno de los servicios activos que se encuentran definidos en el catálogo.		✓	Se cumple con la condición.	B
B.4.	Cada uno de los SLAs tiene establecido las responsabilidades de las partes, indicadores (disponibilidad, capacidad, confiabilidad, etc.) y requerimientos de soporte.		✓	Se cumple con la condición.	B
B.5.	Se verifica el cumplimiento, validez y actualización de los SLAs establecidos con las áreas usuarias de manera periódica.		✓	Se cumple con la condición.	B

II. IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

C. GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
C.1.	Se cuenta con una metodología para la gestión de proyectos de TI formalmente establecida.		✓	Se cumple con la condición.	B
C.2.	Se documenta cada una de las fases del ciclo de vida del proyecto para cada uno de los proyectos ejecutados por el área de TI (constitución, estimación de recursos, responsabilidades, cronograma, desempeño, riesgos, calidad, cambios y cierre del proyecto.)		✓	Se cumple con la condición.	B
C.3.	Los usuarios o clientes de los proyectos aprueban formalmente los entregables de estos.		✓	Se cumple con la condición.	B
C.4.	Se les da seguimiento a los proyectos posterior a la implementación.		✓	Se cumple con la condición.	B

D. GESTIÓN DE DESARROLLOS DE SOFTWARE.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
D.1.	Se cuenta con una metodología para el desarrollo e implementación del software.		✓	Los desarrollos son gestionados por medio de contrataciones a proveedores.	B

E. GESTIÓN DE LA CAPACIDAD Y DISPONIBILIDAD.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		

E.1.	Se cuenta con una política para la gestión de la capacidad y disponibilidad de la plataforma tecnológica.		✓	Se cumple con la condición.	B
E.2.	El equipo de TI es monitoreado periódicamente.		✓	Se cumple con la condición.	B
E.3.	Se realizan proyecciones del uso de recursos de acuerdo con el comportamiento o tendencia del consumo histórico para determinar la necesidad de ampliar la capacidad de la infraestructura.		✓	Se cumple con la condición.	B

F. GESTIÓN DE CAMBIOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
F.1.	Se cuenta con una política y/o procedimiento para la gestión de cambios de TI.		✓	Se cumple con la condición.	B
F.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
F.3.	La documentación de los cambios se mantiene de forma centralizada (mesa de servicios).		✓	Se cumple con la condición.	B
F.4.	Se evalúa periódicamente el estado de los cambios para verificar que todas las solicitudes hayan sido atendidas.		✓	Se cumple con la condición.	B

G. GESTIÓN DE ACTIVOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
G.1.	Se mantienen controles para el ingreso y salida de equipo tecnológico a la organización.		✓	Se cumple con la condición.	B
G.2.	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

G.3.	Se genera plan de infraestructura de TI alineado a los proyectos establecidos en el plan anual operativo de TI.		✓	Se cumple con la condición.	B
G.4.	Se mantiene un inventario actualizado de las licencias de software, así como un catálogo de software permitido en la organización.		✓	Se cumple con la condición.	B
G.5.	Se verifica periódicamente que el software instalado en los equipos corresponda a las licencias adquiridas y al software permitido en la organización.		✓	Se cumple con la condición.	B

III. SOPORTE Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN.

H. GESTIÓN DE INCIDENTES.

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

I. GESTIÓN DE PROBLEMAS.

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

J. GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
J.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
J.2.	Se realizan pruebas y capacitaciones sobre el plan de continuidad del negocio.	✗		Se realizan pruebas al plan, pero no se realizan capacitaciones. Se crea hallazgo Oportunidades de mejora para la gestión de la continuidad.	M
J.3.	Se cuenta con una política y/o procedimiento para la realización de respaldos de información.		✓	Es gestionado por el proveedor, las responsabilidades y requerimientos están debidamente documentadas en el contrato.	B
J.4.	Se realizan pruebas a los respaldos de información.		✓	Se cumple con la condición.	B
J.5.	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

K. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
K.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
K.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
K.3.	Se cuenta con una política de uso de recursos de TI (correo electrónico, equipos, red).		✓	Se cumple con la condición.	B
K.4.	Se utiliza programas de antivirus a nivel organizacional.		✓	Se cumple con la condición.	B
K.5.	Se monitorea y actualiza el antivirus periódicamente.		✓	Se cumple con la condición.	B

K.6.	Se cuenta con una política y/o procedimiento para la gestión de cuentas de usuario.		✓	Se cumple con la condición.	B
K.7.	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
K.8.	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
K.9.	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
K.10.	Se tiene implementado medidas de seguridad para la red institucional (firewall, estudios de vulnerabilidad, segmentación de redes).		✓	Se cumple con la condición.	B
K.11.	Se implementan medidas de seguridad para el acceso de la información desde fuera de las redes confiables.		✓	Se cumple con la condición.	B
K.12.	Se implementan medidas de seguridad para el acceso a la información desde dispositivos móviles.		✓	Se cumple con la condición.	B

IV. SISTEMAS DE INFORMACIÓN.

L. SEGURIDAD LÓGICA Y AUTOMATIZACIÓN DE PROCESOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
L.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
L.2.	Se revisan periódicamente las bitácoras de los sistemas de información para identificar comportamientos irregulares en las operaciones de la organización.	✗		No se presentó evidencia de la revisión de pistas de auditoria en el sistema SAP	M

L.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
L.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
L.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
L.6.	Los sistemas de información cuentan con manuales de usuario y manuales técnicos.		✓	Se cumple con la condición.	B
L.7.	Los procesos de la organización están totalmente automatizados, evitando la realización de tareas manuales.		✓	Se cumple con la condición.	B
L.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
L.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
L.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 --