Fondo de Subsidio para la Vivienda (FOSUVI)

Informe Auditoría de Sistemas de Información

Carta de Gerencia CG-TI 2022

Informe Final

San José, 21 de abril del 2023

Señores
FONDO DE SUBSIDIO PARA LA VIVIENDA (FOSUVI)

Estimados señores:

Según nuestro contrato de servicios, efectuamos nuestra visita de auditoría externa del período 2022 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 2022.

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: 2023.07.19 17:30:17 -06'00'

Lic. Ricardo Montenegro Guillén
Contador Público Autorizado No. 5607
Póliza de Fidelidad No. 0116 FIG0007
Vence el 30 de setiembre del 2023.

Nombre del CPA: MARIO RICARDO MONTENEGRO GUILLEN
Carné: 5607
Cédula: 303430715
Nombre del Cliente: FONDO DE SUBSIDIO PARA LA VIVIENDA
Identificación del cliente: 3007078890
Dirigido a: FONDO DE SUBSIDIO PARA LA VIVIENDA
Fecha: 19-07-2023 05:18:30 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

Código de Timbre: CPA-25-171441

TABLA DE CONTENIDO

I. INTRODUCCIÓN 4
ORIGEN DEL ESTUDIO 4
OBJETIVO DEL ESTUDIO 4
ALCANCE 4
PERIODO DEL ESTUDIO 5
LIMITACIONES DEL ESTUDIO 5
METODOLOGÍA 5
II. HALLAZGOS Y RECOMENDACIONES 6
III. SEGUIMIENTO DE RECOMENDACIONES EMITIDAS EN CARTAS DE GERENCIA ANTERIORES 7
IV. ANEXOS 10
ANEXO I: Análisis de Riesgos TI 10
I. PLANIFICACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN. 11
A. GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN. 11
B. GESTIÓN DE ACUERDOS DE NIVEL DE SERVICIO. 11
II. IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN. 12
C. GESTIÓN DE LA CAPACIDAD Y DISPONIBILIDAD. 12
D. GESTIÓN DE CAMBIOS. 12
III. SOPORTE Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN. 13
E. GESTIÓN DE INCIDENTES. 13
F. GESTIÓN DE PROBLEMAS. 13
G. GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN. 13
H. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. 14
IV. SISTEMAS DE INFORMACIÓN. 14
I. SEGURIDAD LÓGICA Y AUTOMATIZACIÓN DE PROCESOS. 14

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 la seguridad de la información.
- Gestión de cambios de TI.
- Gestión de respaldos y restauraciones.
- Gestión de la continuidad.
- Gestión de la capacidad y disponibilidad.
- Gestión de incidentes.
- Gestión de riesgos.
- Gestión de inventarios de activos de TI.
- Gestión de las Telecomunicaciones.
- Gestión de la Infraestructura Tecnológica.
- Gestión de contratos con proveedores de TI.

- Gestión de los servicios brindador por TI.
- Arquitectura empresarial.
- Gestión de la calidad.
- Seguimiento a recomendaciones emitidas en periodos anteriores.

PERIODO DEL ESTUDIO

El estudio se realizó durante los meses de marzo y abril del año 2023 y corresponde a la auditoría del periodo del 2022.

LIMITACIONES DEL ESTUDIO

Como limitación para la presente auditoría no fue posible comprobar si el Sistema de Vivienda cuenta con los parámetros adecuados para el formato de los datos que se ingresan al sistema, así como mensajes de error/ayuda y la modificación de campos de despliegue; dicha información se solicitó a la señora Lilia Podlisetski vía correo electrónico el día 14 de abril de 2023, posterior a la sesión realizada para la evaluación de sistemas de información.

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.

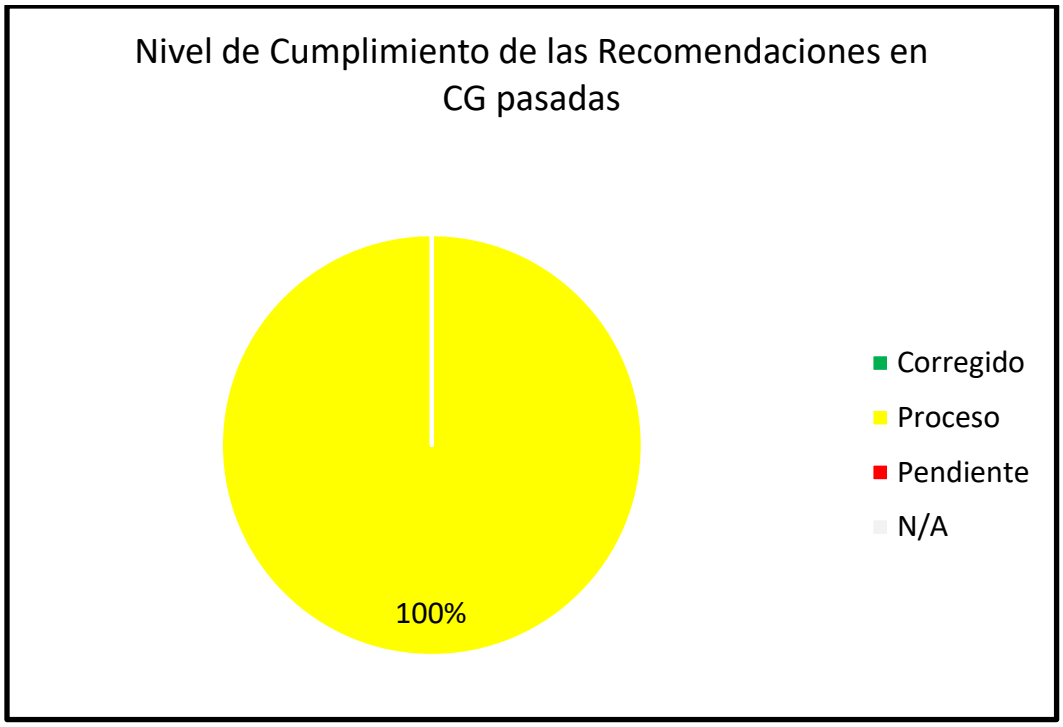
III. SEGUIMIENTO DE RECOMENDACIONES EMITIDAS EN CARTAS DE GERENCIA ANTERIORES

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 21 de marzo de 2023**, se indica que la contratación "2022LN-000001-0016400001 SERVICIO DE HOSPEDAJE, ADMINISTRAC, OPERAC, MONITOREO, SEGURIDAD E IMPLEMENTAC, DE UNA PLATAFORMA INTEGRAL EN NUBE CON COMPONENTES DE CLASE MUNDIAL", se encuentra en ejecución, con fecha de inicio 3 de octubre de 2022. Para este momento se cuenta con un cronograma de implementación que fue aprobado por el BANHVI acorde con lo establecido en el cartel. Por lo anterior el Plan Maestro fue actualizado y se tiene que la Implementación de la Solución para la fase I, finalizará en octubre del 2023, posteriormente se contemplará un periodo de estabilización de la solución para luego abordar las fases II y III. El cierre del contrato está previsto para setiembre de 2026. Acorde con el oficio "BANHVI-DTI-OF-0030-2023 Informe de Avance Proyecto y de labores del 24vo mes - Director de proyecto OPTIMUS informe" remitido a la Gerencia General el 2 de marzo de 2023 al 8 de febrero de 2023, la etapa de Implementación del Proyecto según el cronograma de implementación lleva un avance real de 20% contra un avance esperado de 21%, con una desviación negativa de 1%. Mientras que a nivel general se registra un avance de 48% de un 48% esperado, de manera que no se registran brechas, es decir, no hay variación a nivel general porque se compensa el avance de actividades atrasadas con actividades adelantadas.
ESTADO	**EN PROCESO** De acuerdo con la evidencia suministrada, el proyecto se encuentra en proceso y la fase 1 concluirá en octubre del presente año, el cierre del contrato está previsto para 2026. En la documentación adjunta se encuentra el informe de avance del proyecto, dicho documento describe a detalla la situación actual y las actividades a futuro, además se cuenta con una sección de seguimiento a las recomendaciones de informes anteriores, en la evidencia también se incluye el cronograma y reporte de brechas en el avance general del proyecto. Por lo anterior, se

	visualiza evidencia detallada de las gestiones que se realizan para subsanar las recomendaciones establecidas en periodos anteriores, así como recomendaciones internas, por lo tanto, el 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 2022

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 RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
A.1.	Se tiene una metodología formalmente establecida y aprobada para la gestión de riesgos de TI.		✓	Se cumple con la condición.	B
A.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

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

II. IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

C. GESTIÓN DE LA CAPACIDAD Y DISPONIBILIDAD.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
C.1.	Se cuenta con una política para la gestión de la capacidad y disponibilidad de la plataforma tecnológica.		✓	Se cumple con la condición.	B
C.2.	El equipo de TI es monitoreado periódicamente.		✓	Se cumple con la condición.	B
C.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

D. GESTIÓN DE CAMBIOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
D.1.	Se cuenta con una política y/o procedimiento para la gestión de cambios de TI.		✓	Se cumple con la condición.	B
D.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
D.3.	La documentación de los cambios se mantiene de forma centralizada (mesa de servicios).		✓	Se cumple con la condición.	B
D.4.	Se evalúa periódicamente el estado de los cambios para verificar que todas las solicitudes hayan sido atendidas.		✓	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 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
G.2.	Se realizan pruebas y capacitaciones sobre el plan de continuidad del negocio.		✓	Se cumple con la condición.	B
G.3.	Se cuenta con una política y/o procedimiento para la realización de respaldos de información.		✓	Se cumple con la condición.	B
G.4.	Se realizan pruebas a los respaldos de información.		✓	Se cumple con la condición.	B

G.5.	Se cuenta con un sitio alterno para el procesamiento de datos en una posición geográfica distinta a la ubicación del cuarto de servidores principal.		✓	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 y/o procedimiento para la gestión de cuentas de usuario.		✓	Se cumple con la condición.	B
H.2.	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.3.	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.4.	Se inhabilitan las cuentas de los usuarios que cesan funciones en la organización (despidos, renuncias, jubilaciones, vacaciones, permisos, etc.).		✓		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 cumple con la condición.	B
I.2.	Se revisan periódicamente las bitácoras de los sistemas de información para identificar comportamientos irregulares en las operaciones de la organización.		✓	Se realizan revisiones trimestrales de las bitácoras de eventos de los sistemas de información.	B
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.		✓	Los sistemas permiten un máximo de 3 sesiones simultaneas por usuario.	B

I.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
I.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, las claves cuentan con al menos 2 mayúsculas, 2 minúsculas, 2 números, 2 caracteres especiales y al menos 12 caracteres.	B
I.6.	Los sistemas de información cuentan con manuales de usuario y manuales técnicos.		✓	Se cumple con la condición.	B
I.7.	Los procesos de la organización están totalmente automatizados, evitando la realización de tareas manuales.		✓	Se cumple con la condición.	B
I.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
I.9.	Se restringe la entrada de datos de modo que el registro de información sea lo más estándar posible.	✗		No se recibió evidencia que permita evaluar el atributo.	M
I.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 --