Sistema Nacional de Acreditación de la Educación Superior
(SINAES)

Informe Auditoría de Sistemas y Tecnologías de Información.

Carta de Gerencia TI 2025

San José, 16 de marzo de 2026

Señores
Sistema Nacional de Acreditación de la Educación Superior (SINAES)
Dirección Ejecutiva
Área de Tecnologías de la Información

Estimados señores:

Según nuestro contrato de servicios, efectuamos nuestra visita de auditoría externa del período 2025 al SINAES 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 la gestión y el control de las Tecnologías de Información" del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), los cuales sometemos a consideración de ustedes en esta carta de gerencia CG-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.

GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)
Firmado digitalmente por GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)
Fecha: 2026.04.14 11:36:08 -06'00'

Lic. Gerardo Montero Martínez
Contador Público Autorizado No. 1649
Póliza de Fidelidad N.º 0116FID000680014
Vence el 30 de setiembre del 2026.

"Exento de timbre de Ley número 6663 del Colegio de Contadores Públicos de Costa Rica, por disposición de su artículo número 8"

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 SINAES, 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 con base en las normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el MICITT, y en general las 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 SINAES.

ALCANCE

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

- ✓ Evaluación de políticas, procedimientos, normas, lineamientos y directrices internas en materia tecnológica.
- ✓ Seguimiento a recomendaciones emitidas en periodos anteriores.

PERIODO DEL ESTUDIO

El estudio se realizó durante los meses de febrero y marzo del presente año y corresponde a la auditoría del periodo del 2025.

LIMITACIONES DEL ESTUDIO

No se presentaron limitaciones al estudio durante la visita de auditoría.

METODOLOGÍA

Para llevar a cabo este trabajo utilizamos una modalidad de análisis de la información suministrada por la administración del SINAES. Solicitamos la documentación que evidenciara las respuestas a las solicitudes y cuestionarios aplicados en formato digital o escrito para respaldo de las aseveraciones manifestadas.

II. HALLAZGOS Y RECOMENDACIONES

No se detectaron nuevos hallazgos ni recomendaciones durante el periodo auditado.

III. MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

CG 2022	
HALLAZGO 01: AUSENCIA DE UN PROCEDIMIENTO PARA LA DIVULGACIÓN DE INFORMACIÓN DE TI EN EL SINAES. RIESGO BAJO.	
RECOMENDACIÓN	***Al Área de Tecnologías de la Información:*** 1. Gestionar la definición, aprobación y divulgación de una política o procedimiento para la divulgación de información de TI. Aplicar una vez creada la política, procedimiento o lineamiento de divulgación de la información, lo siguiente: a. Comunicarla a todos los funcionarios del SINAES, con el fin de que estén enterados sobre su existencia y acatamiento. b. Definir las reglas básicas de comunicación, identificando las necesidades de comunicación e implementando planes basados en dichas necesidades, considerando la comunicación ascendente, descendente y horizontal. c. Comunicar continuamente los objetivos y la dirección de las TI. d. La información comunicada debe incluir una clara misión articulada, objetivos de servicio, controles internos, calidad, código ético/conducta, políticas y procedimientos, roles y responsabilidades, etc. Comunicar la información con el nivel de detalle adecuado a las audiencias respectivas dentro de la entidad. 2. Definir responsables de gestionar la política, la frecuencia de la revisión y actualización de este documento.
COMENTARIOS DE LA ADMINISTRACIÓN	El SINAES cuenta con mecanismos institucionales formales y vigentes para la comunicación y divulgación de información, los cuales son utilizados también para los temas de Tecnologías de la Información. Los canales oficiales de comunicación establecidos son: • El boletín semanal “Así Vamos”. • Las circulares institucionales emitidas por la Dirección y áreas de coordinación correspondientes. Adicionalmente, conforme a lo establecido en los lineamientos de arquitectura y gestión de TI del SINAES, toda información relacionada con tecnologías de información debe ser divulgada exclusivamente a través de los canales institucionales oficiales, asegurando consistencia, control, trazabilidad y acceso adecuado para todos los funcionarios.

	Estos mecanismos permiten la comunicación clara, documentada, oportuna y transversal de la información de TI, cumpliendo con lo señalado en el hallazgo respecto a: • Comunicación ascendente, descendente y horizontal. • Asegurar que todos los funcionarios tengan conocimiento de la información relevante de TI. • Establecer un marco institucional para la divulgación formal de contenidos tecnológicos. Además, en el manual de procedimientos de SINAES, se menciona en la página 13, el boletín como medio para realizar las comunicaciones en el SINAES. Con base en estos elementos, y considerando que los lineamientos de TI ya disponen que la divulgación debe realizarse mediante los canales oficiales del SINAES, el hallazgo se considera atendido, por existir un mecanismo formal de comunicación institucional plenamente aplicable a los temas de Tecnologías de Información.
ESTADO	**CORREGIDO** Para la atención del hallazgo, se verificó que el SINAES dispone de mecanismos formales que facilitan la comunicación y divulgación de información institucional, incluyendo temas relacionados con tecnologías de información. Aunado a ello, de conformidad con lo establecido en los Lineamientos de Arquitectura y Gestión de TI del SINAES, toda información vinculada con tecnologías de información debe ser divulgada exclusivamente a través de los canales institucionales oficiales. Lo anterior favorece una comunicación ascendente, descendente y horizontal, permitiendo que todos los funcionarios conozcan la información relevante en materia de TI y que exista, además, un marco institucional para la divulgación formal de contenidos tecnológicos. Como parte de la evidencia documental, se adjuntaron muestras de los contenidos del boletín semanal “Así Vamos”, así como de las circulares institucionales emitidas por la Dirección y por las áreas de coordinación correspondientes. De acuerdo con lo anterior, se verificó que las recomendaciones asociadas al hallazgo se encuentran atendidas con base en la evidencia suministrada, esto debido a que se comprobó que el SINAES dispone y ejecuta un proceso formal para la comunicación institucional.

HALLAZGO 02: OPORTUNIDAD DE MEJORA EN LA GESTIÓN DE LAS CONTINGENCIAS DE TI. RIESGO BAJO.	
RECOMENDACIÓN	***Al Área de Tecnologías de la Información***: 1. Definir, aprobar y divulgar un procedimiento para la gestión de la continuidad y contingencia de TI del SINAES. 2. Agregar a la estructura del procedimiento una matriz de control de cambios que permita identificar las fechas de las actualizaciones que se le realizan al documento y quién las realiza y aprueba. Además, considerar incluir en la estructura del documento secciones como: a. Análisis de impacto sobre el negocio. b. Análisis de riesgos. c. Identificar procesos críticos del negocio. d. Identificar las acciones de contingencia y controles preventivos previo a una incidencia. e. Definir los procesos de activación del plan. f. Documentar los procedimientos de comunicación entre los responsables de ejecutar el plan. g. Definir los procedimientos para recuperar los procesos de negocio incluyendo la infraestructura tecnológica. h. Definir los procedimientos posteriores a recuperación, considerando evaluación de daños y efectividad del plan de continuidad. 3. Definir un plan de pruebas para el plan de continuidad y contingencia, así como aplicar dicho plan al menos una vez al año y documentar los resultados.
COMENTARIOS DE LA ADMINISTRACIÓN	SINAES ha dado cumplimiento total a las recomendaciones mediante la elaboración, aprobación y divulgación del documento **"L01-DSAG-PCDTI Continuidad y disponibilidad servicios TI 23jun25 ultver.pdf"** Este lineamiento establece el procedimiento oficial para la gestión de la continuidad y contingencia de TI, e incorpora: • Identificación de procesos críticos, análisis de impacto, riesgos y disposiciones de recuperación. • Roles, responsabilidades, comunicación durante incidentes y condiciones de activación de los planes. • Procedimientos de continuidad y recuperación documentados. • Control de versiones, responsables de elaboración/aprobación y repositorio oficial en SharePoint. Asimismo, se definió el plan de pruebas anual del BCP y DRP, junto con los formatos institucionales F01 y F02 para documentar los resultados y acciones de mejora. Con la aprobación del lineamiento y sus anexos,

	el hallazgo queda atendido, debido a que ya cuenta con un procedimiento formal, completo y operativo para la continuidad y contingencia de TI.
ESTADO	**CORREGIDO** Se evidenció que la administración definió, aprobó y divulgó un procedimiento formal para la gestión de la continuidad y contingencia de Tecnologías de Información, el cual se encuentra vigente y operativo. Además, el procedimiento incorpora la identificación de servicios y procesos críticos, análisis de impacto al negocio, análisis de riesgos, roles y responsabilidades, mecanismos de comunicación y condiciones de activación de los planes, así como los procedimientos de continuidad, recuperación y evaluación posterior a la restauración de los servicios. Adicionalmente, se identificó que se estableció un plan de pruebas periódico para la continuidad y contingencia de TI, el cual fue ejecutado y documentado durante el periodo evaluado, evidenciando pruebas de recuperación, validación de tiempos de respuesta, acciones correctivas y mejora continua. Asimismo, se brindaron registros que respaldan la capacitación del personal involucrado y la difusión del procedimiento mediante repositorios institucionales y sesiones informativas. En consecuencia, el hallazgo se considera atendido y corregido.
HALLAZGO 03: OPORTUNIDADES DE MEJORA EN ALGUNOS DE LOS SISTEMAS DE INFORMACIÓN DEL SINAES. RIESGO MEDIO.	
RECOMENDACIÓN	***Al Área de Tecnologías de la Información del SINAES:*** 1. Realizar un proceso de revisión y análisis del sistema que permita recolectar la información necesaria para solventar las debilidades y/o oportunidades de mejora identificadas en este hallazgo. ***A los usuarios expertos del sistema:*** 2. Gestionar con el área de TI las necesidades que se identifiquen para la correcta funcionalidad de los módulos que utilicen, para realizar sus labores de la mejor forma posible.
COMENTARIOS DE LA ADMINISTRACIÓN	En atención al hallazgo se indica lo siguiente: 1. Acciones realizadas por el Área de Tecnologías de Información. El proceso de revisión y mejora de los sistemas de información del SINAES es continuo. Durante el 2025, el Área de TI ejecutó diversas acciones de análisis y mejora, entre ellas:

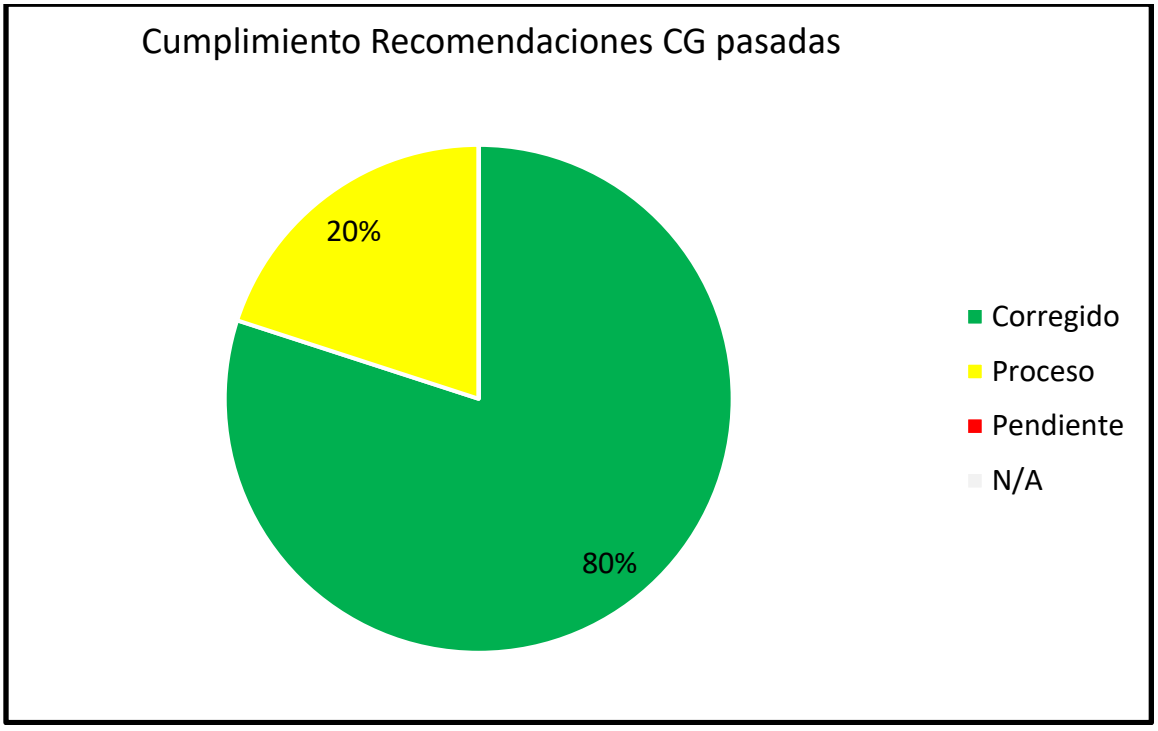
	• Ajustes y optimizaciones en el gestor de contenidos WordPress que soporta la página web institucional, orientados a mejorar estabilidad, rendimiento y usabilidad y la incorporación de herramientas de accesibilidad. • Mejoras funcionales y de experiencia de usuario en el flujo de PowerApps para la gestión de pagos de facturas, incorporando retroalimentación de usuarios y corrigiendo incidencias identificadas. Estas acciones responden directamente a la recomendación del hallazgo, ya que forman parte del proceso de revisión sistemática de los sistemas y módulos utilizados por la institución. Además, como parte del ciclo operativo del área, se continuará durante el 2026 con nuevos ajustes y mejoras conforme se identifiquen necesidades técnicas o funcionales, garantizando la evolución constante de los sistemas institucionales. 2. Acciones realizadas por los usuarios expertos: Los usuarios expertos han gestionado ante TI las necesidades identificadas en los módulos que utilizan, tanto para la web institucional como para las aplicaciones internas, siguiendo los canales formales establecidos. Estas solicitudes han sido incorporadas en el análisis y priorización de mejoras realizadas en 2025. En el marco de la mejora continua, el SINAES ha proyectado para las 2026 acciones adicionales que complementan y fortalecen este hallazgo, entre ellas: • Mejoras al sistema GRP institucional, incluyendo actividades de análisis, refactorización y proceso de integración con SICOP para optimizar la gestión administrativa y de contratación. • Contratación de un paquete de 1.000 horas de desarrollo para implementar mejoras y ajustes funcionales en el Sistema de Registro de Expertos (REX), atendiendo necesidades identificadas por los usuarios expertos y garantizando su evolución tecnológica. Estas acciones dan continuidad al proceso de revisión solicitado en el hallazgo y aseguran la mejora progresiva de los sistemas institucionales.

ESTADO	**EN PROCESO** El Área de Tecnologías de la Información ha ejecutado diversas acciones de mejora en los sistemas del SINAES durante el 2025, como ajustes y optimizaciones en WordPress y mejoras en el flujo de PowerApps. Además, los usuarios expertos han gestionado sus necesidades a través de los canales establecidos, lo que ha permitido identificar mejoras adicionales. No obstante, dentro del marco de la mejora continua, el SINAES ha proyectado para el periodo 2026 acciones adicionales, tales como mejoras en el sistema GRP institucional, refactorización e integración con SICOP, y la contratación de 1.000 horas de desarrollo para mejorar el Sistema de Registro de Expertos (REX). Por lo tanto, para el periodo auditado, dado que las acciones adicionales y mejoras están proyectadas para el 2026, se determina que el hallazgo se mantiene en proceso.
CG 2019	
2019.8	
RECOMENDACIÓN	2019.8 Debe establecerse el modelo de la arquitectura, de forma tal que refleje en sus diferentes componentes, la información requerida por cada uno de los procesos (ya sea como insumo procesamiento o salida, así como sus fuentes y "destinos") y la infraestructura tecnológica (considerandos aplicativos, software y hardware) que soporta la operativa de cada uno de los procesos institucionales.
COMENTARIOS DE LA ADMINISTRACIÓN	SINAES ha definido, aprobado y divulgado el documento "**L-DSAG-PATIC Lineamiento arquitectura de TI 26abr24 ultver.pdf** ", mediante el cual se establece el modelo de arquitectura que integra: • Procesos y flujos de información (insumos, procesamiento y salidas), su gobierno de datos y ciclo de vida, alineados a APO14 (estrategia, roles, glosario, calidad y depuración), permitiendo identificar fuentes y destinos de la información institucional. • Infraestructura tecnológica de soporte (aplicativos, software, hardware) y su gestión de activos bajo BAI09 (inventario, críticos, ciclo de vida, licencias), con repositorio y artefactos en SharePoint, y el servicio de arquitectura bajo APO03 (visión, arquitectura de referencia, plan de implementación y servicios de arquitectura). El lineamiento define el repositorio de arquitectura en SharePoint para almacenar artefactos (modelos, componentes, relaciones, estándares) que describen la operativa de cada proceso y su soporte tecnológico, y dispone la actualización continúa vinculada al PETIC/PAO. Con lo anterior, el hallazgo se considera atendido y cerrado

ESTADO	**CORREGIDO** Se proporciona el documento **L-DSAG-PATIC Lineamiento arquitectura de TI 26abr24 ultver**, el cual está definido, aprobado y divulgado por la administración. Este lineamiento establece el modelo de arquitectura empresarial en todas sus capas: arquitectura de negocio, arquitectura de información y datos (estrategia, roles, glosario, calidad y ciclo de vida, alineado a APO14), arquitectura de aplicaciones (relaciones, modelos, estándares y componentes en el repositorio), y arquitectura de tecnología (inventario de hardware/software, activos críticos, ciclo de vida y licenciamiento conforme BAI09). Además, define la visión, arquitectura de referencia, plan de implementación y servicios de arquitectura según APO03, con un repositorio oficial en SharePoint para almacenar los artefactos que describen procesos, flujos de datos, componentes tecnológicos y su interacción institucional. Igualmente se confirma en el documento **SINAES 2025-Seguimiento hallazgos** y la evidencia documental de implementación. Por lo anterior, se determina que el hallazgo se encuentra corregido.
2019.10	
RECOMENDACIÓN	2019.10 Disponer de prácticas formales, incluyendo lineamientos y metodologías formales que permitan administrar proyectos, de forma tal que se logren los objetivos, se satisfagan los requerimientos y se cumpla con los términos de calidad, tiempo y presupuesto establecidos.
COMENTARIOS DE LA ADMINISTRACIÓN	El SINAES administra sus proyectos bajo un marco formal compuesto por los procedimientos de Contratación Administrativa y los mecanismos institucionales de planificación y seguimiento establecidos. En primera instancia, todo proyecto que involucra adquisición o desarrollo de soluciones tecnológicas se gestiona conforme a la Ley de Contratación Administrativa, su reglamento y los procedimientos internos asociados. Esto incluye la elaboración de la Decisión Inicial, los Términos de Referencia, el estudio de mercado, la planificación presupuestaria y la gestión del concurso mediante SICOP, lo cual asegura el cumplimiento de criterios de trasparencia, calidad, tiempo y presupuesto definidos para cada proyecto. Adicionalmente, la institución utiliza el sistema para la gestión del desempeño DELPHOS para la administración y seguimiento de los proyectos incluidos en los Planes Operativos Anuales (PAO) y en los Planes Individuales de Trabajo (PIT). DELPHOS permite registrar proyectos, establecer responsables, definir metas e indicadores y realizar un seguimiento del avance. El sistema emite reportes automáticos, indicadores de cumplimiento y alertas sobre tareas o entregables atrasados, lo que facilita la supervisión continua y la toma oportuna de decisiones. Este conjunto de herramientas (Contratación Administrativa,

	SICOP, POA/PIT y DELPHOS) constituye una estructura formal y operativa para la administración de proyectos en el SINAES.
ESTADO	**CORREGIDO** En el SINAES, la gestión de proyectos se asocia directamente con los procesos de adquisición o desarrollo de soluciones tecnológicas. Para tales efectos, se aplican los procedimientos de contratación administrativa mediante el uso de la plataforma SICOP, lo que contribuye al cumplimiento de criterios de transparencia, calidad, control presupuestario y plazos de ejecución, conforme a las características particulares de cada proyecto. Como evidencia documental, se aportaron los lineamientos aplicables a la decisión inicial de contratación o adquisición, al estudio técnico y de mercado y a la elaboración de los términos de referencia. Adicionalmente, el SINAES utiliza la herramienta Delphos, la cual permite administrar y dar seguimiento a los proyectos incorporados en los Planes Operativos Anuales (PAO) y en los Planes Individuales de Trabajo. En herramienta es posible registrar proyectos, asignar responsables, definir metas e indicadores, así como monitorear su nivel de avance. Como respaldo documental, nos suministraron reportes generados desde la herramienta Delphos, en los cuales se observan los proyectos, planes de acción, tareas, fechas de inicio y conclusión, así como los indicadores asociados. A partir de la evidencia aportada por el SINAES, se comprobó que la gestión de proyectos se ejecuta operativamente conforme a los términos de referencia y a los estudios definidos para cada caso; por lo tanto, se determina que el hallazgo se encuentra corregido.

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



La siguiente tabla muestra el cumplimiento de recomendaciones por periodo.

Estado de Recomendaciones	2019	2022	Total
Corregidas	2	2	**4**
En Proceso	0	1	**1**
Pendiente	0	0	**0**
No Aplica	0	0	**0**
Total	**2**	**3**	**5**

IV. ANEXO I

Análisis de Riesgos TI Área de Tecnologías de Información
Periodo 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. PLANIFICACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
A.1.	Se tiene definido un plan estratégico de TI formalmente aprobado y alineado a los objetivos organizacionales.		✓	Se cumple con la condición.	B
A.2.	Se le da seguimiento al PETI por parte del Comité de TI.		✓	Se cumple con la condición.	B
A.3.	Se define anual un plan anual operativo de TI con los proyectos y actividades que realiza el área de TI y se encuentra alineado a las iniciativas y objetivos del PETI.		✓	Se cumple con la condición.	B
A.4.	Se le da seguimiento periódico al cumplimiento del PAO.		✓	Se cumple con la condición.	B

B. GESTIÓN DE LA ARQUITECTURA DE LA INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
B.1.	Se cuenta con un modelo de arquitectura de información formalmente establecido y aprobado.		✓	Se cumple con la condición.	B
B.2.	Se le realizan revisiones anuales al modelo de arquitectura para garantizar su actualización de acuerdo con los cambios generados a nivel organizacional.		✓	Se cumple con la condición.	B

C. GESTIÓN DE PROVEEDORES DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
C.1.	Se establecen contratos formales para los servicios que son brindados por terceros.		✓	Se cumple con la condición.	B
C.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
C.3.	Se realiza un seguimiento al cumplimiento contractual de las responsabilidades de los proveedores.		✓	Se cumple con la condición.	B

D. GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN.

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

E. GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
E.1.	Se les da seguimiento a los proyectos posterior a la implementación.		✓	Se cumple con la condición, por medio de la herramienta Delphos, a nivel operativo se realizan seguimientos a los proyectos.	B

F. GESTIÓN DE DESARROLLOS DE SOFTWARE.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
F.1.	Se cuenta con una metodología para el desarrollo e implementación del software.		✓	Se cumple con la condición, SINAES no realiza desarrollos internos, al momento de adquirir sistemas estos se realizan por medio del SICOP.	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 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.4.	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 LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
H.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
H.2.	Se realizan pruebas y capacitaciones sobre el plan de continuidad del negocio.		✓	Se cumple con la condición.	B
H.3.	Se cuenta con una política y/o procedimiento para la realización de respaldos de información.		✓	Se cumple con la condición.	B
H.4.	Se realizan pruebas a los respaldos de información.		✓	Se cumple con la condición.	B
H.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
H.6.	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

I. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
I.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
I.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
I.3.	Se cuenta con una política de uso de recursos de TI (correo electrónico, equipos, red).		✓	Se cumple con la condición.	B
I.4.	Se cuenta con una política y/o procedimiento para la gestión de cuentas de usuario.		✓	Se cumple con la condición.	B
I.5.	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
I.6.	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
I.7.	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. EVALUACIÓN DE TECNOLOGÍAS DE INFORMACIÓN.

J. VALORAR EL CONTROL INTERNO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
J.1.	Se han establecido normas para la evaluación del control interno de TI.		✓	Se cumple con la condición.	B
J.2.	Se realizan autoevaluaciones periódicas para que TI identifique de manera proactiva las debilidades de control.		✓	Se cumple con la condición.	B
J.3.	Se ejecutan estudios de auditoría periódicos (internos o externos) para identificar debilidades en el cumplimiento de obligaciones con normativas relativas a TI.		✓	Se cumple con la condición.	B

V. SISTEMAS DE INFORMACIÓN.

K. SEGURIDAD LÓGICA Y AUTOMATIZACIÓN DE PROCESOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
K.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
K.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
K.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.	✗		No se cumple con la condición. Se realiza seguimiento al hallazgo existente.	M
K.4.	Los sistemas de información cuentan con validación de usuarios a través de cuentas y contraseñas (Active Directory, LDAP, otros).	✗		No se cumple con la condición para el sistema financiero contable auditado. Se realiza seguimiento al hallazgo existente.	M
K.5.	Se han implementado medidas de seguridad lógica en los sistemas de información (vencimiento, histórico, tamaño y complejidad de la contraseña).	✗		No se cumple con la condición. Se realiza seguimiento al hallazgo existente.	M
K.6.	Los sistemas de información cuentan con manuales de usuario y manuales técnicos.		✓	Se cumple con la condición.	B
K.7.	Los procesos de la organización están totalmente automatizados, evitando la realización de tareas manuales.		✓	Se cumple con la condición.	B
K.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
K.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
K.10.	Se brindan capacitaciones periódicas en el uso de los sistemas a los usuarios de la organización.		✓	Se cumple con la condición.	B