Sistema Nacional de Acreditación de la Educación Superior
(SINAES)

Informe Auditoría de Sistemas y Tecnologías de Información.

Carta de Gerencia TI 2024

Informe Final

San José, 28 de marzo de 2025

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

Presente

Según nuestro contrato de servicios, efectuamos nuestra visita de auditoría externa del período 2024 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 2024.

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

GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)
Firmado digitalmente por GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)
Fecha: 2025.04.07 15:06:44 -06'00'

Lic. Gerardo Montero Martínez
Contador Público Autorizado No. 1649
Póliza de Fidelidad Nº 0116FID000680013
Vence el 30 de setiembre del 2025.

"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 2024.

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 determinaron hallazgos nuevos para el periodo auditado.

III. MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

CG 2023	
HALLAZGO 01: AUSENCIA DE UN COMITÉ DE SEGURIDAD DE INFORMACIÓN/CIBERSEGURIDAD EN EL SINAES. RIESGO MEDIO.	
RECOMENDACIÓN	***A la administración del SINAES en coordinación con el Departamento de Tecnologías de Información:*** 1. Establecer un comité de seguridad de la información que valore a su vez temas de ciberseguridad en el SINAES y que tome como base la política de seguridad de la información de la entidad. 2. Establecer un reglamento formal para el comité de seguridad de la información, asegurando que incluya al menos los siguientes elementos: a. Disposiciones generales. b. Objetivo y funciones del Comité. c. Integración y responsabilidades del Comité. d. Limitaciones del Comité. e. Políticas o marco de trabajo. f. Participantes de las sesiones. g. Condiciones de las sesiones. h. Periodicidad de las sesiones. i. Composición de las actas. 3. Presentar el reglamento ante las entidades correspondientes para su respectiva revisión y aprobación, y una vez aprobada comunicarla a todas las áreas involucradas. 4. Comunicar y divulgar al personal respectivo sobre la existencia del reglamento. 5. Definir responsables de gestionar el reglamento, frecuencia de la revisión y actualización de este. 6. Establecer mecanismos de control que ayuden a verificar el cumplimiento de los lineamientos establecidos, así como las acciones a seguir en caso de incumplir con el reglamento.
COMENTARIOS DE LA ADMINISTRACIÓN	El área de Tecnologías de información cuenta solo con dos personas, lo que ha dificultado la asignación de recursos para la creación de dicho comité sobre todo a que en dicho comité debería incluirse otros colaboradores con conocimientos técnicos que puedan desempeñar roles técnicos.

	La creación del comité de seguridad de la información y ciberseguridad debe responder al tamaño y capacidad de la institución, sobre todo cuando se tiene un equipo de TI reducido. La normativa ISO 20071 sugiere adaptar la gobernanza de seguridad a la estructura de la institución, por tanto, como alternativa se tienen definida el área de TI con un responsable que sería el Gestor de Tecnologías de Información, quien coordina directamente con la Dirección de Apoyo a la Gestión y la Dirección Ejecutiva para proponer las acciones necesarias y mecanismos de control en seguridad de la información. Se realizan además reuniones de seguimiento quincenales donde también se tratan temas relacionados a seguridad sin necesidad de un comité formal. Se ha creado el lineamiento de seguridad de la información y ciberseguridad (L-DSAG-PSYC), el cual se encuentra divulgado en el SINAES, el cual tiene como objetivo "Cumplir con los pilares fundamentales de la seguridad de la información, confidencialidad, integridad y disponibilidad a través del establecimiento de mecanismos y controles apropiados con el fin de asegurar la protección de los activos de información contra amenazas, accesos no autorizados, divulgación o interrupción." A pesar de la ausencia de un comité formal de seguridad y ciberseguridad, SINAES ha adoptado iniciativas para gestionar la seguridad de la información • La seguridad de la información es gestionada directamente por el área de TI en coordinación con la jefatura inmediata y la Dirección de la institución. • Lineamiento de Seguridad y Ciberseguridad: Se cuenta con un lineamiento de seguridad que define principios y directrices para la protección de la información institucional. • Seguimiento en reuniones de Dirección: Los riesgos y necesidades de seguridad informática se comunican en las reuniones de Dirección, permitiendo la toma de decisiones estratégicas. • Uso de Controles de Seguridad en la Infraestructura: Implementación de medidas de seguridad como autenticación multifactor (2FA), respaldos en la nube, respaldos 3,2,1, acceso por VPN, segmentación de accesos, Firewalls de seguridad perimetral. • Adopción de Marcos de Referencia: Se sigue el lineamiento de marco de gestión emitido por el MICITT el cual se alinea al marco COBIT 2019.
ESTADO	**EN PROCESO**

	SINAES no cuenta con un Comité de Seguridad de la Información formalmente establecido debido a la limitación de personal en el área de TI. No obstante, se han implementado prácticas alineadas con la normativa ISO 27001, como la designación de un Gestor de Tecnologías de Información, quien coordina directamente con la Dirección Ejecutiva y la Dirección de Apoyo a la Gestión en la definición y aplicación de controles de seguridad. Asimismo, se realizan reuniones quincenales para dar seguimiento a temas de seguridad, y se ha establecido el Lineamiento de Seguridad de la Información y Ciberseguridad, donde se definen roles y responsabilidades en la gestión de la ciberseguridad. Dado que aún no se ha conformado un Comité de Seguridad de la Información, el hallazgo se encuentra en proceso.
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 Informática:*** 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 I&T. 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.

	3. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	SINAES cuenta con una Política de Comunicación Interna, la cual establece los lineamientos para la divulgación de información dentro de la institución, incluyendo el área de TI. Actualmente, esta política se encuentra pendiente de aprobación por parte del Consejo Nacional de Acreditación. La comunicación interna se realiza utilizando los canales oficiales tales como boletín "Así Vamos" que se envía semanalmente y por medio de circulares, adicionalmente en el lineamiento de arquitectura de TI y en el lineamiento de gestión de TI, se menciona que TI utilizará los canales oficiales para la divulgación de información en la institución. Dado el tamaño del equipo de TI (solo dos personas), la formalización de un procedimiento específico puede no ser prioritaria, ya que los mecanismos existentes permiten la difusión de información de manera efectiva.
ESTADO	**EN PROCESO** Según los comentarios de la administración y la evidencia suministrada, SINAES cuenta con una Política de Comunicación Interna que define los lineamientos para la divulgación de información en la institución, incluyendo el área de TI. Actualmente, esta política está pendiente de aprobación por parte del Consejo Nacional de Acreditación. Mientras tanto, la comunicación se realiza a través de canales oficiales como el boletín "Así Vamos" y circulares institucionales, tal como se menciona en el Lineamiento de Arquitectura de TI y el Lineamiento de Gestión de TI. Por lo anterior, el hallazgo se encuentra en proceso.
HALLAZGO 02: OPORTUNIDAD DE MEJORA EN LA GESTIÓN DE LAS CONTINGENCIAS DE TI. RIESGO BAJO.	
RECOMENDACIÓN	***Al Área de TI***: 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	De acuerdo con el plan de trabajo para la implementación del marco de gobierno y gestión, se tiene previsto la construcción y la formalización de los procedimientos que respondan a este hallazgo. Dicho plan de trabajo fue presentado al Consejo Nacional de Acreditación mediante el oficio SINAES-DSAG-TI-336-2024 (se adjunta como evidencia. La institución tiene implementada una contingencia de la infraestructura tecnológica en Microsoft Azure la cual fue implementada durante el año 2024 mediante el procedimiento en SICOP 2024LD-000012-0022400001, lo que demuestra que se han tomado medidas para garantizar la continuidad operativa y la recuperación ante incidentes, dicha solución se encuentra documentada la cual se aporta como parte de las evidencias a esta auditoria en la sección de “Aseguramiento”. La solución de contingencia está operativa, pero aún no ha sido documentada dentro de la normativa institucional la cual se estará desarrollando durante el año 2025.
ESTADO	**EN PROCESO** De acuerdo con lo indicado por SINAES, según el plan de trabajo **SINAES-DSAG-TI-336-2024** para la implementación del marco de gobierno y gestión, se tiene previsto la construcción y la formalización de los procedimientos que responden al hallazgo. De acuerdo con lo anterior, el hallazgo se encuentra en proceso de ser atendido.

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	El área de TI de SINAES reconoce la importancia de realizar un proceso de revisión y análisis del sistema para identificar oportunidades de mejora. En este sentido, se han implementado las siguientes acciones: • Monitoreo del desempeño del sistema para identificar debilidades y oportunidades de mejora. • Revisión de requerimientos técnicos y funcionales en conjunto con las áreas usuarias, con el fin de priorizar mejoras en la plataforma. Lo que ha llevado a la contratación de bolsas de horas para solventar necesidades. • Coordinación con proveedores y soporte técnico para atender las necesidades identificadas en el sistema, considerando los procedimientos de contratación administrativa establecidos. Se tiene contratos de soporte y mantenimiento del sistema financiero-contable que permite la corrección de errores y el desarrollar mejoras en los módulos que lo requieran. • Los usuarios expertos mediante el uso de las herramientas de Teams y correo electrónico establecen canales de comunicación con el área de TI para gestionar las solicitudes de mejora. • Los usuarios pueden documentar y canalizar sus necesidades con el área de TI, permitiendo priorizar mejoras.
ESTADO	**EN PROCESO**

	Según la administración, el área de TI ha implementado acciones como monitoreo del sistema, revisión de requerimientos y contratación de soporte para mejoras. También se han fortalecido los canales de comunicación con usuarios para gestionar solicitudes. Sin embargo, no se presentó evidencia escrita, ni se confirmó en entrevistas que se hayan atendido las debilidades del sistema Wizdom GRP. Solo se identificó que el sistema genera pistas de auditoría revisadas según escenarios específicos. Por lo anterior, la atención a las recomendaciones del hallazgo se encuentra en proceso.
CG 2021	
Hallazgo 01: Oportunidades de mejora en las gestiones asociadas a los procesos de TI en el SINAES.	
RECOMENDACIÓN	***Al comité responsable:*** 1. Revisar y aprobar por el comité respectivo, los lineamientos que contemplen la documentación de procedimientos operacionales. ***Al Área de Tecnologías de la Información*** 2. Producto de la atención de la *recomendación 1*, comunicar los lineamientos y/o procedimientos en cuestión a las partes involucradas. 3. Revisar y actualizar (esto último cuando sea necesario) los lineamientos al menos una vez al año y mantener el registro en el control de versiones. 4. Hacer uso de las buenas prácticas tales como la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como ISO, ITIL y COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	El área de TI desarrolla los lineamientos y procedimientos, asegurando que se alineen con las necesidades institucionales y son comunicados y formalizados a través del boletín institucional "Así vamos", garantizando su divulgación a las partes interesadas. El marco de gobierno y gestión de TI en SINAES esta alineado a la directriz emitida por el MICITT asegurando alineamiento con la normativa vigente, a su vez estas directrices siguen las buenas prácticas de COBIT 2019. La actualización de la documentación indicada se realiza conforme a lo establecido en el manual de procedimientos del SINAES, asegurando un proceso estructurado y normado. Este proceso es guiado y acompañado por el Área de Calidad.

ESTADO	**CORREGIDO** Como parte de la evidencia proporcionada para el estudio de auditoría, fue posible evidenciar la existencia de un marco para la gestión de TI desarrollado por el SINAES. Este documento, denominado **Marco COBIT SINAES vf**, toma como base los marcos de referencia COBIT 2019 e ITIL. Por otro lado, se nos suministró el **Lineamiento marco gestión de TI**, el cual contiene el marco utilizado para la gestión de tecnologías de información, donde se busca que la gestión de TI cumpla con los requerimientos establecidos por el marco de gobierno y gestión establecido por MICITT y contenga los controles adecuados que aseguren la confiabilidad de los servicios de TI. Además, en el **SINAES-DSAG-TI-336-2024** se incluye un plan de trabajo para la implementación de los procesos que forman parte del marco de gestión y gobierno de TI, se incluye el año propuesto para el cumplimiento y el porcentaje de avance. De acuerdo con lo anterior, el hallazgo queda corregido.
CG 2019	
2019.2.b	
RECOMENDACIÓN	2019.2.b Establecer el Plan de infraestructura (con vigencia según el plan estratégico institucional), que incluya necesidades de mantenimiento de la infraestructura instalada.
COMENTARIOS DE LA ADMINISTRACIÓN	SINAES cuenta con un Plan Estratégico de Tecnologías de Información y Comunicación (PETIC) 2024-2027 aprobado y divulgado (se adjunta como parte de las evidencias a esta auditoria), el cual establece las directrices para la evolución de la infraestructura tecnológica de la institución y el presupuesto estimado de las inversiones en este tema. A demás se ha desarrollado el lineamiento sobre infraestructura de TI (L-DSAG-PAIT Lineamiento administración infraestructura tecnológica), que define las mejores prácticas para la gestión y mantenimiento de los recursos tecnológicos. La planificación de infraestructura se realiza en concordancia con las necesidades institucionales y los recursos disponibles.
ESTADO	**CORREGIDO** Se verifica que la planificación de infraestructura tecnológica está contemplada en el **Plan Estratégico de Tecnologías de Información y Comunicación (PETIC) 2024-2027**, el cual detalla las inversiones proyectadas en infraestructura.

	Adicionalmente, se elaboró el documento **L-DSAG-PAIT Lineamiento administración infraestructura tecnológica** que establece directrices para la gestión y mantenimiento de la infraestructura tecnológica, asegurando la disponibilidad y continuidad de los servicios tecnológicos. Por lo anterior, el hallazgo se encuentra corregido.
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	La infraestructura de TI en SINAES está alineada con el Plan Estratégico de Tecnologías de Información y Comunicación (PETIC) y se ha desarrollado el lineamiento de arquitectura de TI (L-DSAG-PATIC) el cual se aporta como parte de las evidencias a esta auditoría.
ESTADO	**EN PROCESO** No se identificó un modelo de arquitectura formalmente documentado que describa explícitamente la integración entre negocio, datos, aplicaciones y tecnología. Aunque la arquitectura de TI está alineada con el PETIC, no se evidencia una estructura visual o metodológica aprobada que cubra todas las capas de la arquitectura empresarial. Por lo tanto, el hallazgo se encuentra en proceso.
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	SINAES está en proceso de construcción de las prácticas formales para la gestión de proyectos, las cuales serán fundamentales para garantizar que los proyectos de TI se gestionen de manera eficiente, cumpliendo con los plazos, presupuestos y objetivos establecidos. SINAES ha establecido prácticas formales para la administración de proyectos, asegurando que estos se desarrollen conforme a los objetivos institucionales y bajo los criterios de calidad, tiempo y presupuesto definidos. Estas prácticas incluyen lineamientos y metodologías respaldadas por normativas y procedimientos internos, los cuales garantizan una adecuada gestión de los proyectos tecnológicos. Procedimientos de Contratación Administrativa:

	La institución se rige por los procedimientos de contratación administrativa establecidos en la legislación vigente, los cuales incluyen la elaboración de términos de referencia, la decisión inicial del proyecto y la realización de estudios de mercado. Estos procesos, dictados por la Ley de Contratación Administrativa, aseguran que toda adquisición o contratación de bienes y servicios tecnológicos cuente con un análisis previo.
ESTADO	**EN PROCESO** De acuerdo con la respuesta al seguimiento de recomendaciones de cartas de gerencia anteriores se indicó que SINAES está en proceso de construcción de las prácticas formales para la gestión de proyectos. Por otra parte, se nos indicó que la institución se rige por los procedimientos de contratación administrativa establecidos en la legislación vigente, estos incluyen la elaboración de términos de referencia, la decisión inicial del proyecto y la realización de estudios de mercado. Estos procesos aseguran que toda adquisición o contratación de bienes y servicios tecnológicos cuente con un análisis previo. De acuerdo con lo anterior, el hallazgo se encuentra en proceso hasta que el SINAES concluya con la construcción e implementación de las prácticas para la gestión de proyectos.
2019.13	
RECOMENDACIÓN	2019.13 Disponer de lineamientos formales que permitan identificar y alinear necesidades y oportunidades de implementación de recursos tecnológicos como respuesta a la estrategia institucional.
COMENTARIOS DE LA ADMINISTRACIÓN	SINAES ha implementado una serie de lineamientos y procedimientos formales que permiten identificar y alinear las necesidades y oportunidades de implementación de recursos tecnológicos con la estrategia institucional. El Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC 2024-2027) es uno de los pilares fundamentales para la alineación de los recursos tecnológicos con los objetivos estratégicos de la institución. El PETIC establece las prioridades tecnológicas, define los proyectos y recursos necesarios y garantiza que todas las iniciativas tecnológicas estén en concordancia con la visión y misión institucionales. TI desarrolla planes individuales de trabajo que se alinean con las necesidades del PETIC y con los objetivos estratégicos definidos por la institución. Estos planes contemplan las acciones, recursos y tiempos necesarios para la implementación de proyectos tecnológicos específicos, asegurando su contribución a la estrategia institucional.

	Todos los lineamientos, el PETIC, los planes individuales de trabajo y el PAO están alineados con el Plan Estratégico Institucional. Esto garantiza que las decisiones tecnológicas no solo respondan a las necesidades operativas del área de TI, sino que también contribuyan al cumplimiento de los objetivos a largo plazo de SINAES.
ESTADO	**CORREGIDO** Según los comentarios de la administración y la evidencia suministrada, SINAES ha implementado lineamientos y procedimientos que permiten identificar y alinear las necesidades tecnológicas con la estrategia institucional. El Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC 2024-2027) establece las directrices para la gestión y evolución de los recursos tecnológicos, alineándolos con los objetivos estratégicos del Plan Estratégico Institucional (PEI). Este documento define proyectos clave, presupuestos estimados y riesgos asociados, asegurando que las decisiones en tecnología respondan a las prioridades institucionales. Adicionalmente, se verificó que el área de TI desarrolla planes individuales de trabajo y el Plan Anual Operativo (PAO), los cuales detallan acciones específicas alineadas con el PETIC y el PEI, permitiendo la planificación y control de la implementación de recursos tecnológicos. Por lo anterior, el hallazgo se considera como corregido.
2019.14	
RECOMENDACIÓN	2019.14 Establecer lineamientos formales que permitan definir y aplicar las actividades necesarias para identificar soluciones, su desarrollo/contratación e implementación; incluyendo la administración de cambios, control de versiones, actualización, así como obsolescencia.
COMENTARIOS DE LA ADMINISTRACIÓN	SINAES ha establecido una serie de lineamientos y procedimientos (se adjunta en evidencias) formales que permiten definir y aplicar las actividades necesarias para identificar soluciones, actualización y obsolescencia. El Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC 2024-2027) juega un papel clave en la identificación de soluciones tecnológicas necesarias, ya que establece las prioridades de TI alineadas con la estrategia institucional. El PETIC es un instrumento que guía la selección, desarrollo y contratación de nuevas soluciones tecnológicas, asegurando que sean coherentes con las necesidades institucionales y con el enfoque estratégico del SINAES.
ESTADO	**CORREGIDO**

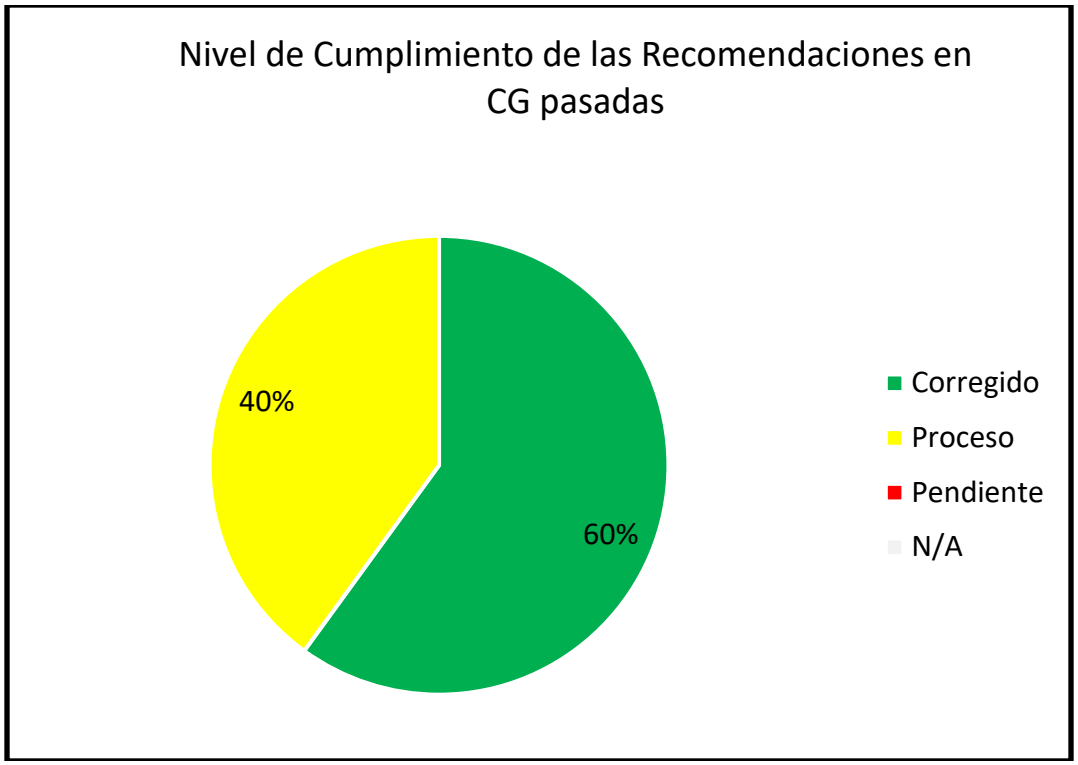
	El **Plan Estratégico de Tecnologías de la Información y Comunicaciones** establece las prioridades tecnológicas de SINAES y define los proyectos y recursos necesarios, garantizando su alineación con la estrategia institucional. Dentro de sus objetivos, se incluyen acciones estratégicas para la implementación de soluciones tecnológicas, fortalecimiento de la infraestructura, automatización de procesos y gestión de seguridad de la información. Asimismo, el **Lineamiento sobre Administración de Infraestructura Tecnológica** proporciona directrices para la gestión y control de los recursos tecnológicos, abordando aspectos como la configuración de servicios, activos e infraestructura, además del registro y actualización de elementos tecnológicos utilizados. Por lo anterior, el hallazgo se encuentra corregido.
2019.27	
RECOMENDACIÓN	2019.27 Establecer los lineamientos necesarios sobre la administración del acceso a los recursos, que implique la responsabilidad de los propietarios/custodios de la información para asignar los privilegios, según la necesidad de saber y utilizar, considerando la definición de perfiles, roles y niveles de privilegios que permitan controlar la identificación y autenticación para el acceso de información al nivel de usuarios y de recursos de TI.
COMENTARIOS DE LA ADMINISTRACIÓN	SINAES ha desarrollado y formalizado lineamientos necesarios para la administración del acceso a los recursos de TI, con el objetivo de garantizar que solo los usuarios autorizados puedan acceder a la información y a los recursos tecnológicos. El desarrollado del lineamiento de seguridad y ciberseguridad ha permitido establecer directrices necesarias para la protección de los activos de información, esto asegura que los usuarios solo tengan acceso a la información y los recursos necesarios para el desempeño de sus tareas y funciones. La identificación y autenticación de los usuarios es un componente fundamental para garantizar que el acceso se otorgue solo a aquellos que están debidamente autorizados. Se ha implementado procedimientos de autenticación robustos por medio de ActiveDirectory, que incluyen el uso de mecanismos de autenticación multifactor (2FA) en los sistemas más sensibles. Esto agrega una capa adicional de seguridad para prevenir el acceso no autorizado.
ESTADO	**CORREGIDO**

	En función de la evidencia proporcionada **SINAES-DSAG-TI-116-2025**, la institución a desarrollado y formalizado el Lineamiento de Seguridad y Ciberseguridad (incluido en las muestras solicitadas), en el cual se establece la administración del acceso a los recursos de TI. Este lineamiento define la responsabilidad de los propietarios y custodios de la información en la asignación de privilegios. Asimismo, contempla la gestión de cuentas y acceso lógicos, acceso físico de los activos de información, gestión de documentos sensibles, entre otros.
2019.28	
RECOMENDACIÓN	2019.28 Establecer las acciones de control sobre el acceso a información impresa, visible en pantallas o almacenada en medios físicos que permitan su debida protección.
COMENTARIOS DE LA ADMINISTRACIÓN	La institución aplica acciones de control de acceso a la información basado en los procedimientos definidos por CONARE. Se adjunta documentos en la carpeta “Requerimientos adicionales”: • OPES.P.32 Gestión de documentos de archivo V01.pdf • OPES.P.33 Administración Archivo Central V01.pdf • OPES.P.34 Gestión de documentos electrónicos V01.pdf
ESTADO	**CORREGIDO** Se identificaron lineamientos específicos en los documentos institucionales que regulan el acceso, gestión y resguardo de la información en distintos soportes. El **OPES.P.32 Gestión de documentos de archivo** establece medidas para la identificación, clasificación y almacenamiento seguro de documentos físicos. El **OPES.P.33 Administración Archivo Central** regula el acceso y préstamo de documentos, asegurando su conservación y trazabilidad. El **OPES.P.34 Gestión de documentos electrónicos** define normas para el almacenamiento y protección de documentos digitales, complementando la seguridad en medios físicos. Por lo anterior, el hallazgo se encuentra corregido.
2019.29	
RECOMENDACIÓN	2019.29 Establecer los lineamientos que permitan administrar la seguridad al nivel de desarrollo, mantenimiento, prueba e implementación y uso de software e infraestructura, así como el control de acceso y uso de programas fuentes y datos de prueba.

COMENTARIOS DE LA ADMINISTRACIÓN	SINAES ha desarrollado el lineamiento de Arquitectura Empresarial (se adjunta en evidencias), el cual establece bases para la seguridad en el desarrollo y custodia de software, códigos fuentes e infraestructura. Este lineamiento cubre diversas áreas de la seguridad informática tales como: • gestión del activo tecnológico • Licencias de software • Gestión de datos • Arquitectura empresarial de TI • Seguridad • Mejora continua
ESTADO	**CORREGIDO** El **Lineamiento de Arquitectura Empresarial** establece directrices para la gestión del activo tecnológico, licencias de software, gestión de datos y seguridad, abordando aspectos clave para la administración segura del software utilizado en la institución. Aunado a esto, según la evidencia suministrada, SINAES no realiza desarrollos de software internos, por lo que no aplica la implementación de controles específicos sobre el acceso a programas fuente o el uso de datos de prueba. Por tanto, el hallazgo se encuentra corregido.
2019.35	
RECOMENDACIÓN	2019.35 Definir y aplicar prácticas formales que permitan orientar la valoración del sistema de control interno aplicado al nivel de los recursos y servicios tecnológicos. Tales pueden ser mecanismos de autoevaluación, entre otros.
COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**CORREGIDO** En la evidencia suministrada se identifica el documento **Guía para el Establecimiento y Funcionamiento del SEVRI SINAES que** establece una metodología alineada con la normativa de la Contraloría General de la República (CGR) y la ISO 31000, la cual permite la identificación, análisis, evaluación y administración de riesgos en los procesos organizacionales, incluyendo los relacionados con la gestión de TI. Además, el **Informe Integrado ASCI - Riesgos SINAES** evidencia la aplicación de mecanismos de autoevaluación del control interno, detallando el registro y monitoreo de eventos de riesgo, la aplicación de estrategias de

	mitigación y la revisión periódica del nivel de cumplimiento en la administración de riesgos tecnológicos. Por lo anterior, el hallazgo se encuentra corregido.
2019.37	
RECOMENDACIÓN	2019.37 Establecer prácticas formales para el seguimiento sobre el nivel de cumplimiento de recomendaciones realizadas al área de TI.
COMENTARIOS DE LA ADMINISTRACIÓN	SINAES tiene implementado una serie de prácticas formales y mecanismos de evaluación que permiten asegurar la efectividad de dicho sistema y garantizar la eficiencia operativa del área de TI: • Evaluación del Desempeño y Seguimiento del Desarrollo de Tareas: La institución cuenta con un sistema de información DELPHOS para la evaluación del desempeño de los recursos y servicios tecnológicos, por medio de indicadores de gestión, que permite monitorear el cumplimiento de tareas y de ser necesario tomar medidas en aquellas que se están quedando rezagadas. • Retroalimentación por Parte de la Jefatura: Un aspecto clave en la valoración del sistema de control interno es la retroalimentación constante de la jefatura del área.
ESTADO	**CORREGIDO** El **Informe Integrado ASCI - Riesgos SINAES** documenta el seguimiento a las recomendaciones mediante la identificación de riesgos, la aplicación de medidas correctivas y la asignación de responsables para su cumplimiento. Se evidencia un registro estructurado donde se monitorean las acciones implementadas, sus fechas de ejecución y el avance en la mitigación de los riesgos identificados. Adicionalmente, la **Guía para el Establecimiento y Funcionamiento del SEVRI SINAES** establece un marco metodológico para la valoración de riesgos y el control interno, asegurando que los hallazgos y recomendaciones sean abordados de manera estructurada y con mecanismos de seguimiento en tiempo real. La implementación de un panel de control interactivo facilita la supervisión de las acciones derivadas de auditorías y autoevaluaciones. Por lo anterior, 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	2021	2022	2023	Total
Corregidas	8	1	0	0	**9**
En Proceso	2	0	3	1	**6**
Pendiente	0	0	0	0	**0**
No Aplica	0	0	0	0	**0**
Total	**10**	**1**	**3**	**1**	**15**

IV. ANEXO I

Análisis de Riesgos T.I.
Área de Tecnologías de Información
Periodo 2024

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.	✗		No cumple con la condición, se realiza seguimiento a hallazgo existente.	B

C. GESTIÓN DEL RECURSO HUMANO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
C.1.	Se cuenta con un plan de capacitaciones formalmente establecido.		✓	Se cumple con la condición.	B
C.2.	Las capacitaciones se encuentran justificadas (proyectos de TI, evaluaciones del desempeño).		✓	Se cumple con la condición.	B
C.3.	Se mantiene un manual de puestos actualizado con la descripción y las responsabilidades del personal de TI.		✓	Se cumple con la condición.	B
C.4.	Se realizan evaluaciones anuales del desempeño de los colaboradores de TI.		✓	Se cumple con la condición.	B
C.5.	Se realizan medidas correctivas para el personal que obtiene calificaciones deficientes en las evaluaciones del desempeño.		✓	Se cumple con la condición.	B

D. GESTIÓN DE PROVEEDORES DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
D.1.	Se establecen contratos formales para los servicios que son brindados por terceros.		✓	Se cumple con la condición.	B
D.2.	Para los contratos de servicios de TI, se establecen acuerdos de nivel de servicio con los respectivos indicadores de capacidad, disponibilidad, confiabilidad, etc.	✗		No se cumple con la condición, se genera el HALLAZGO 01: DEFICIENCIAS EN LA GESTIÓN Y SEGUIMIENTO DE CONTRATOS DE PROVEEDORES DE TI. RIESGO MEDIO.	M
D.3.	Se realiza un seguimiento al cumplimiento contractual de las responsabilidades de los proveedores.	✗		No se cumple con la condición, se genera el HALLAZGO 01: DEFICIENCIAS EN LA GESTIÓN Y SEGUIMIENTO DE CONTRATOS DE PROVEEDORES DE TI. RIESGO MEDIO.	M

II. IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

E. GESTIÓN DE DESARROLLOS DE SOFTWARE.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
E.1.	Se cuenta con una metodología para el desarrollo e implementación del software.		✓	SINAES no realiza desarrollos internos, adquiere sistemas y servicios por medio de contrataciones administrativas.	B

F. GESTIÓN DE ACTIVOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
F.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
F.2.	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
F.3.	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.

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 cuenta con una guía del proceso de contingencia, sin embargo, en plan de continuidad se encuentra en proceso de elaboración.	M
G.2.	Se realizan pruebas y capacitaciones sobre el plan de continuidad del negocio.	✗		Se cuenta con una guía del proceso de contingencia, sin embargo, en plan de continuidad se encuentra en proceso de elaboración.	M
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 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 de uso de recursos de TI (correo electrónico, equipos, red).		✓	Se cumple con la condición.	B

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
H.4.	Se cuenta con una política y/o procedimiento para la gestión de cuentas de usuario.	✗		Existe un hallazgo asociado al atributo, el cual se encuentra en proceso de ser atendido.	B
H.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
H.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
H.7.	Se inhabilitan las cuentas de los usuarios que cesan funciones en la organización (despidos, renuncias, jubilaciones, vacaciones, permisos, etc.).	✗		Se encontraron cuentas de usuarios que ya no laboran para la institución en la lista de usuarios activos, se emitió un nuevo hallazgo con el detalle de la situación.	M
H.8.	Se tiene implementado medidas de seguridad para la red institucional (firewall, estudios de vulnerabilidad, segmentación de redes).		✓	Se cumple con la condición.	B
H.9.	Se implementan medidas de seguridad para el acceso de la información desde fuera de las redes confiables.		✓	Se cumple con la condición.	B

IV. EVALUACIÓN DE TECNOLOGÍAS DE INFORMACIÓN.

I. VALORAR EL CONTROL INTERNO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
I.1.	Se han establecido normas para la evaluación del control interno de TI.		✓	Se cumple con la condición.	B
I.2.	Se realizan autoevaluaciones periódicas para que TI identifique de manera proactiva las debilidades de control.		✓	Se cumple con la condición.	B
I.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.

J. SEGURIDAD LÓGICA Y AUTOMATIZACIÓN DE PROCESOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
J.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
J.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
J.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 a hallazgo existente.	M
J.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 a hallazgo existente.	M
J.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 a hallazgo existente.	M
J.6.	Los sistemas de información cuentan con manuales de usuario y manuales técnicos.		✓	Se cumple con la condición.	B
J.7.	Los procesos de la organización están totalmente automatizados, evitando la realización de tareas manuales.		✓	Se cumple con la condición.	B
J.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

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
J.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
J.10.	Se brindan capacitaciones periódicas en el uso de los sistemas a los usuarios de la organización.		✓	Se cumple con la condición.	B

--Fin del documento-