Sistema Nacional de Acreditación de la Educación Superior
(SINAES)

Informe Auditoría de Sistemas y Tecnologías de Información.

Carta de Gerencia TI 2023

Informe final

San José, 10 de abril de 2024

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 2023 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 2023.

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: 2024.04.29 17:27:24 -06'00'

Lic. Gerardo Montero Martínez
Contador Público Autorizado No. 1649
Póliza de Fidelidad Nº 0116 FIG 7
Vence el 30 de setiembre del 2024.

"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

I. INTRODUCCIÓN 4
ORIGEN DEL ESTUDIO 4
OBJETIVO DEL ESTUDIO 4
ALCANCE 4
PERIODO DEL ESTUDIO 4
LIMITACIONES DEL ESTUDIO 4
METODOLOGÍA 5
II. HALLAZGOS Y RECOMENDACIONES 6
HALLAZGO 01: AUSENCIA DE UN COMITÉ DE SEGURIDAD DE INFORMACIÓN/CIBERSEGURIDAD EN SINAES. RIESGO MEDIO. 6
III. MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES 8
IV. ANEXO I 23
I. PLANIFICACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN. 24
A. PLANIFICACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN. 24
B. GESTIÓN DE LA ARQUITECTURA DE LA INFORMACIÓN. 24
C. GESTIÓN DEL RECURSO HUMANO. 25
II. IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN. 25
D. GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN. 25
E. GESTIÓN DE DESARROLLOS DE SOFTWARE. 26
F. GESTIÓN DE ACTIVOS. 26
III. SOPORTE Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN. 27
G. GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN. 27
H. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. 28
IV. SISTEMAS DE INFORMACIÓN. 29
I. SEGURIDAD LÓGICA Y AUTOMATIZACIÓN DE PROCESOS. 29

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 el mes de marzo del presente año y corresponde a la auditoría del periodo del 2023.

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

HALLAZGO 01: AUSENCIA DE UN COMITÉ DE SEGURIDAD DE INFORMACIÓN/CIBERSEGURIDAD EN EL SINAES. RIESGO MEDIO.

CONDICIÓN:

Producto de la revisión efectuada, no se evidenció la existencia de un comité de seguridad de la información que contemple temas de ciberseguridad formalmente establecido en el SINAES, por ende, no existe documentación relacionada a una política, reglamento o documento formal donde se especifique la siguiente información: conformación, objetivos, roles, funciones, periodicidad de sesiones, etc.

Al no contar con un comité de seguridad de la información aumenta la posibilidad de incurrir en una dirección inadecuada y una coordinación deficiente en la implementación de estrategias de seguridad y ciberseguridad. Esto podría dejar a la institución vulnerable ante amenazas cibernéticas y dificultar la capacidad de respuesta efectiva ante incidentes de seguridad.

CRITERIO:

En las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el MICITT se encuentra el proceso **XI. SEGURIDAD Y CIBERSEGURIDAD** del **Marco de Gestión de TI**, donde se indica: "La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados".

RECOMENDACIONES:

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.

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 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	La comunicación en la institución es realizada por medio de correo electrónico específicamente a la lista de distribución llamada sinaleslist, donde se encuentran incluidos todos los funcionarios. Adicionalmente todas las semanas se envía el boletín institucional llamado “Así Vamos” donde se resumen todas las acciones realizadas por las diferentes divisiones, incluida el área de tecnologías de información. En cuanto a la política de comunicación, la institución se encuentra actualmente en el diseño y se cuenta con una versión desarrollada, lista para ser presentada ante el Consejo Nacional de Acreditación para su

	aprobación. Se adjunta el documento "Política de Comunicación del SINAES 1.docx "en la carpeta 4-Activos.
ESTADO	**EN PROCESO** Según lo indicado, la comunicación de información es realizada por medio de correo electrónico a todos los funcionarios del SINAES, además, todas las semanas se envían boletines con las acciones realizadas por las diferentes áreas o departamentos de la organización. Adicionalmente, se menciona que existe una versión de una Política de Comunicación del SINAES, la cual se presentará ante el Consejo Nacional de Acreditación para su respectiva aprobación. Sin embargo, no fue posible identificar la evidencia mencionada en los comentarios de la administración, sobre los boletines enviados y la política de comunicación.
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	Ante el desarrollo del marco de gobierno y gestión de las tecnologías de información es presentado al Consejo Nacional de Acreditación un plan para la construcción de los lineamientos y/o procedimientos para subsanar el hallazgo. Dicho plan requiere de la participación del área de Calidad, como responsable de brindar las pautas para la construcción de estos lineamientos. Se adjunta en la carpeta de **requerimientos adicionales** los oficios: • SINAES-DE-189-2023 CNA Auditoría Externa.pdf • SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002)
ESTADO	**EN PROCESO** Se comenta por parte del Departamento de TI que se estableció y se presentó ante el Consejo Nacional de Acreditación un plan de trabajo para la construcción de los lineamientos y/o procedimientos para la atención del hallazgo. Se nos suministró evidencia del calendario para el desarrollo de la documentación y los responsables respectivos, para la atención de las recomendaciones.
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	Se han realizado esfuerzos para solventar deficiencias de los sistemas de información. En la carpeta 7- Aplicaciones y tecnología se evidencia la contratación de bolsa de horas para aplicar mejoras a los flujos automatizados del gestor documental. Se ha buscado la integración de los sistemas de información con el active Directory para que se apliquen las políticas, como por ejemplo contraseña robustas, validación de usuarios, entre otros. Con respecto a los inicios de sesión múltiples y como consecuencia de tener una plataforma basada en Microsoft, se permite que los usuarios puedan realizar varios inicios de sesión. Para brindar capas de seguridad se tiene implementado el 2FA (Doble Factor de autentificación) el cual valida que realmente sea el usuario correcto el que está realizando el inicio de sesión. El sistema de información financiero contable GRP Wizdom, tiene como limitante que no posee integración con LDAP seguro, por lo que no es posible realizar la integración con Active Directory. Se han aplicado mejoras a los diferentes módulos que permiten agilizar los procesos internos.
ESTADO	**EN PROCESO** Según comentarios de la administración y la evidencia suministrada, se ha trabajado en la atención de las oportunidades de mejoras identificadas en el hallazgo. Sin embargo, aún existe una oportunidad de mejora pendiente de atención, las pistas de auditoría y su respectivo procedimiento de revisión. Por tanto, la atención 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	Actualmente en procesos de construcción de lineamientos.
ESTADO	**EN PROCESO** De acuerdo con el comentario de la administración y las pruebas realizadas, se determinó que este hallazgo se encuentra en proceso. Se nos suministró el documento SINAES-DE-189-2023 CNA Auditoría Externa, donde se indica el plan de trabajo para elaborar el lineamiento, procedimiento, guías o formularios y el año en que se va a realizar.

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	El plan de infraestructura se incluye en el Plan estratégico de Tecnologías de Información que está pendiente de aprobar. En la carpeta 3-Planes se incluye la versión del PETIC 2024-2027
ESTADO	**EN PROCESO** Se evidenció mediante el documento SINAES-DE-189-2023 CNA Auditoría Externa y el comentario de la administración, que este hallazgo se encuentra en proceso, ya que se indica que el Plan estratégico de TI y el documento referente a la Administración de la Infraestructura de TI, se elaboraran durante el 2024.
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	Ante el desarrollo del marco de gobierno y gestión de las tecnologías de información es presentado al Consejo Nacional de Acreditación un plan para la construcción de los lineamientos y/o procedimientos para subsanar el hallazgo. Dicho plan requiere de la participación del área de Calidad, como responsable de brindar las pautas para la construcción de estos lineamientos. Se adjunta en la carpeta de **requerimientos adicionales** los oficios: • SINAES-DE-189-2023 CNA Auditoría Externa.pdf • SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002)
ESTADO	**EN PROCESO** Mediante los documentos SINAES-DE-189-2023 CNA Auditoría Externa.pdf, SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002) y según el comentario de la administración, se evidencia que este

	hallazgo se encuentra en proceso, ya que se indica que el modelo Arquitectura de información se elaborará para el 2024, como parte del desarrollo del marco de gobierno y gestión de las tecnologías de información.
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	Ante el desarrollo del marco de gobierno y gestión de las tecnologías de información es presentado al Consejo Nacional de Acreditación un plan para la construcción de los lineamientos y/o procedimientos para subsanar el hallazgo. Dicho plan requiere de la participación del área de Calidad, como responsable de brindar las pautas para la construcción de estos lineamientos. Se adjunta en la carpeta de **requerimientos adicionales** los oficios: • SINAES-DE-189-2023 CNA Auditoría Externa.pdf • SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002)
ESTADO	**EN PROCESO** Mediante los oficios SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002) y -DE-189-2023 CNA Auditoría Externa, se establece un plan para la construcción de políticas y procedimientos para subsanar el hallazgo incluido el procedimiento para gestión de proyectos. Por tanto, el hallazgo se encuentra en proceso.
2019.12	
RECOMENDACIÓN	12. Establecer prácticas que permitan disponer de estándares en cuanto a la adquisición de recursos tecnológicos, según las necesidades reales institucionales y tendencias de la industria.
COMENTARIOS DE LA ADMINISTRACIÓN	Los procesos de contratación se realizan buscando tener un estándar de equipos tanto de usuario final como de infraestructura. En la carpeta 4-activos, 7- Aplicaciones y tecnologías se incluye los procesos de contratación donde se especifica el detalle de los requerimientos solicitados; se realiza un estudio de mercado, se realiza un análisis de situaciones previas a la adquisición del servicio, como lo son estudios de requerimientos, diseño de modelos e incluso tesis universitarias de referencia.

ESTADO	**CORREGIDO** Según las pruebas realizadas se evidenció el proceso de contratación según las necesidades de la institución, donde se evidencia la realización de un estudio de mercado, análisis de situaciones previas a la adquisición del servicio, como lo son estudios de requerimientos, diseño de modelos.
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	Ante el desarrollo del marco de gobierno y gestión de las tecnologías de información es presentado al Consejo Nacional de Acreditación un plan para la construcción de los lineamientos y/o procedimientos para subsanar el hallazgo. Dicho plan requiere de la participación del área de Calidad, como responsable de brindar las pautas para la construcción de estos lineamientos. Se adjunta en la carpeta de **requerimientos adicionales** los oficios: • SINAES-DE-189-2023 CNA Auditoría Externa.pdf • SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002)
ESTADO	**EN PROCESO** De acuerdo al comentario de la administración y la evidencia suministrada, se determinó que el hallazgo se encuentra en proceso, los documentos suministrados indican el plan de trabajo para elaborar los lineamientos formales que permitan identificar y alinear necesidades y oportunidades de implementación de recursos tecnológicos y el año en que se va a realizar.
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	Ante el desarrollo del marco de gobierno y gestión de las tecnologías de información es presentado al Consejo Nacional de Acreditación un plan para la construcción de los lineamientos y/o procedimientos para subsanar el hallazgo. Dicho plan requiere de la participación del área de Calidad, como responsable de brindar las pautas para la construcción de estos lineamientos.

	Se adjunta en la carpeta de **requerimientos adicionales** los oficios: • SINAES-DE-189-2023 CNA Auditoría Externa.pdf • SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002)
ESTADO	**EN PROCESO** Mediante los documentos SINAES-DE-189-2023 CNA Auditoría Externa.pdf, SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002) se evidencia que este hallazgo se encuentra en proceso, ya que se indica que el lineamiento que permita definir y aplicar las actividades necesarias para identificar soluciones, su desarrollo/contratación e implementación, se elaborará para el 2025.
2019.16	
RECOMENDACIÓN	2019.16 Considerar los parámetros de establecimiento de términos generales de aceptación de bienes/servicios al nivel tecnológico, control de garantías, licenciamiento según aplique, entre otros; considerando adicionalmente la aplicación de prácticas de evaluación del desempeño del proveedor en cuanto a la entrega de productos y servicios según sea requerido.
COMENTARIOS DE LA ADMINISTRACIÓN	Es considerado el Reglamento de contratación administrativa. Por tanto, todo el proceso de contratación administrativa es realizado por la plataforma de compras públicas de SICOP, aplicándose todos parámetros generales de aceptación de bienes y servicios, así como la aplicación de garantías.
ESTADO	**CORREGIDO** Se nos indicó por parte del DTI que el proceso de contratación administrativa se realiza por medio de la plataforma de compras públicas (SICOP), donde se aplican los parámetros de aceptación de bienes y servicios y garantías.
2019.17	
RECOMENDACIÓN	2019.17 Incorporar en los lineamientos el esquema para establecer los términos técnicos para la adquisición de bienes y servicios al nivel de tecnología de información, de forma tal que estén alineados a los estándares establecidos al nivel de infraestructura tecnológica, de forma que se pueda facilitar la valoración en la adquisición de bienes y servicios al nivel de TI.
COMENTARIOS DE LA ADMINISTRACIÓN	Por medio de la proveeduría institucional se tiene definido los lineamientos y procedimientos para los procesos de contratación los cuales aplican también al área de tecnologías de información.

	En la carpeta “Requerimientos adicionales” se adjunta evidencias
ESTADO	**CORREGIDO** Senos indicó que por medio de proveeduría se encuentran definidos los lineamientos y procedimientos para los procesos de contratación, lo cuales aplican también para el área de tecnologías de información. Se nos suministró evidencia de la documentación utilizada durante el proceso de contratación.
2019.20	
RECOMENDACIÓN	2019.20 Establecer una política de seguridad institucional que establezca las directrices a seguir al nivel institucional sobre las prácticas de seguridad que deben ser aplicadas por cada funcionario, tales como control de acceso y protección de los recursos tecnológicos críticos, manejo de los datos, información y documentación (física y digital), entre otros.
COMENTARIOS DE LA ADMINISTRACIÓN	Se ha desarrollado el lineamiento referente a la seguridad de TI, en la carpeta 1- Marco de TI, se aporta el documento “Lineamiento TI seguridad.pdf”
ESTADO	**CORREGIDO** Se nos suministró evidencia de la existencia de un lineamiento para la seguridad y la ciberseguridad de SINAES, por lo tanto, el hallazgo se encuentra corregido.
2019.19	
RECOMENDACIÓN	2019.19 Deben establecerse parámetros y medidas formales que permitan apoyar la clasificación de los datos, según su nivel de criticidad, propiedad y requerimientos de disponibilidad.
COMENTARIOS DE LA ADMINISTRACIÓN	En la carpeta 4- Activos de información, se incluye el listado de activos de la institución, así como su clasificación.
ESTADO	**CORREGIDO** De acuerdo con las pruebas realizadas y al comentario de la administración, se evidenció que la calificación de los activos se da de acuerdo con su criticidad, tipo, y otra información relacionada, por lo tanto, este hallazgo se encuentra corregido.
2019.21	
RECOMENDACIÓN	2019.21 Disponer de actividades formales asociadas a la capacitación y concientización de los funcionarios en materia de seguridad de la información y protección de los recursos tecnológicos utilizados para la

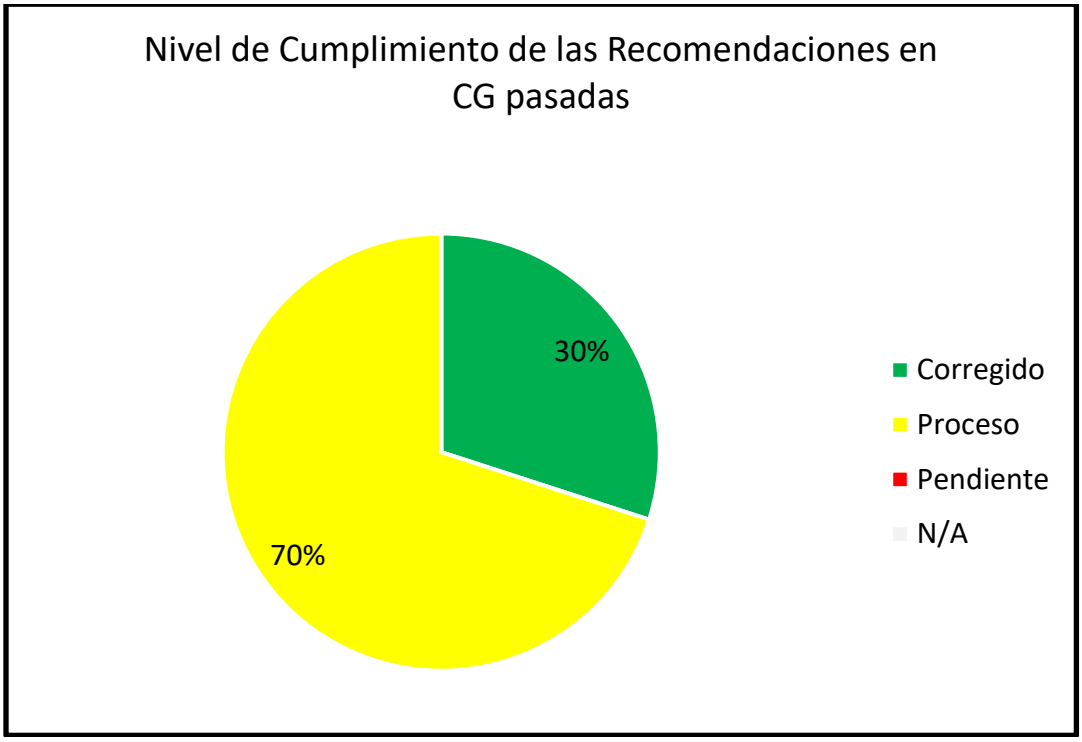
	operativa de la institución. Estas actividades se pueden incorporar a los procesos de inducción y retroalimentación de los funcionarios.
COMENTARIOS DE LA ADMINISTRACIÓN	Mediante el uso del aula virtual del SINAES se ha desarrollado un curso denominado "PROGRAMA DE INDUCCIÓN Y REINDUCCIÓN DE PERSONAL" de capacitación para el personal donde se incluye temas relacionados con todas las áreas y adicionalmente con tecnologías de información. Adicionalmente se realizan capacitaciones cuando se considere necesario para el personal, como por ejemplo la relacionada con el uso de la firma digital del BCCR, según se evidencia en la carpeta **4-Activos**, subcarpeta **capacitaciones**
ESTADO	**CORREGIDO** Según comentarios de la administración mediante el uso del aula virtual del SINAES se ha desarrollado un curso denominado "PROGRAMA DE INDUCCIÓN Y REINDUCCIÓN DE PERSONAL" de capacitación para el personal donde se incluye temas relacionados con todas las áreas y adicionalmente con tecnologías de información. Adicionalmente, se evidenció la realización de capacitaciones, campañas de concientización y certificaciones al personal sobre seguridad de la información.
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	Ante el desarrollo del marco de gobierno y gestión de las tecnologías de información es presentado al Consejo Nacional de Acreditación un plan para la construcción de los lineamientos y/o procedimientos para subsanar el hallazgo. Dicho plan requiere de la participación del área de Calidad, como responsable de brindar las pautas para la construcción de estos lineamientos. Se adjunta en la carpeta de **requerimientos adicionales** los oficios: • SINAES-DE-189-2023 CNA Auditoría Externa.pdf • SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002)

ESTADO	**EN PROCESO** En la respuesta suministrada por SINAES en la solicitud de información, se menciona que el desarrollo de lineamientos o procedimientos formales será parte del plan de trabajo presentado al Consejo Nacional de Acreditación, por tanto, la atención del hallazgo se encuentra en proceso.
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 está pendiente en el desarrollo de un procedimiento propio del SINAES. 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	**EN PROCESO** En la respuesta suministrada por SINAES en la solicitud de información, indican que se utilizan los procedimientos definidos por CONARE. Adicionalmente, se menciona que el desarrollo de lineamientos o procedimientos formales será parte del plan de trabajo presentado al Consejo Nacional de Acreditación, por tanto, la atención del hallazgo se encuentra en proceso.
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	Ante el desarrollo del marco de gobierno y gestión de las tecnologías de información es presentado al Consejo Nacional de Acreditación un plan para la construcción de los lineamientos y/o procedimientos para subsanar el hallazgo. Dicho plan requiere de la participación del área de Calidad, como responsable de brindar las pautas para la construcción de estos lineamientos.

	Se adjunta en la carpeta de **requerimientos adicionales** los oficios: • SINAES-DE-189-2023 CNA Auditoría Externa.pdf • SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002)
ESTADO	**EN PROCESO** Mediante los documentos SINAES-DE-189-2023 CNA Auditoría Externa.pdf, SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002) se evidencia que este hallazgo se encuentra en proceso, ya que se indica que el lineamiento referente a la gestión del desarrollo o adquisición de aplicaciones y tecnologías se elaborará para el 2025.
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	Ante el desarrollo del marco de gobierno y gestión de las tecnologías de información es presentado al Consejo Nacional de Acreditación un plan para la construcción de los lineamientos y/o procedimientos para subsanar el hallazgo. Dicho plan requiere de la participación del área de Calidad, como responsable de brindar las pautas para la construcción de estos lineamientos. Se adjunta en la carpeta de **requerimientos adicionales** los oficios: • SINAES-DE-189-2023 CNA Auditoría Externa.pdf • SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002)
ESTADO	**EN PROCESO** Mediante los oficios SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002) y -DE-189-2023 CNA Auditoría Externa, se establece un plan para la construcción de políticas y procedimientos para subsanar el hallazgo incluido el procedimiento para gestión del aseguramiento. Por tanto, el hallazgo se encuentra en proceso.
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	
ESTADO	**EN PROCESO** Se tiene establecido un plan de trabajo para seguimiento de desarrollo de las recomendaciones indicadas. Es posible validarlo según los oficios: • SINAES-DE-189-2023 CNA Auditoría Externa • SINAES-DSAG-257-2023 Respuesta SINAES-DE-158-2023 (002)

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	Total
Corregidas	6	0	0	6
En Proceso	10	1	3	14
Pendiente	0	0	0	0
No Aplica	0	0	0	0
Total	**16**	**1**	**3**	**20**

IV. ANEXO I

Análisis de Riesgos T.I.
Área de Tecnologías de Información
Periodo 2023

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 se cumple con la condición. Se encuentra en proceso según plan de trabajo establecido para la implementación de políticas y procedimientos en SINAES.	M

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 realizan evaluaciones anuales del desempeño de los colaboradores de TI.		✓	Se cumple con la condición.	B
C.4.	Se realizan medidas correctivas para el personal que obtiene calificaciones deficientes en las evaluaciones del desempeño.		✓	Se nos indicó que para el periodo auditado no se presentaron casos en que se necesitaran medidas correctivas.	B

II. IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

D. GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
D.1.	Se cuenta con una metodología para la gestión de proyectos de TI formalmente establecida.	✗		No se cumple con la condición. Se encuentra en proceso según plan de trabajo establecido para la implementación de políticas y procedimientos en SINAES.	M

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
D.2.	Se documenta cada una de las fases del ciclo de vida del proyecto para cada uno de los proyectos ejecutados por el área de TI (constitución, estimación de recursos, responsabilidades, cronograma, desempeño, riesgos, calidad, cambios y cierre del proyecto.)		✓	Se cumple con la condición.	B

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.	✗		No se cumple con la condición. Se encuentra en proceso según plan de trabajo establecido para la implementación de políticas y procedimientos en SINAES.	M

F. GESTIÓN DE ACTIVOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
F.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

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
F.3.	Se genera plan de infraestructura de TI alineado a los proyectos establecidos en el plan anual operativo de TI.	✗		No se cumple con la condición. Se encuentra en proceso según plan de trabajo establecido para la implementación de políticas y procedimientos en SINAES.	M
F.4.	Se mantiene un inventario actualizado de las licencias de software, así como un catálogo de software permitido en la organización.		✓	Se cumple con la condición.	B

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 nos indicó que el desarrollo del plan de contingencia es parte del plan de trabajo del Marco de Gobierno y Gestión de TI.	M
G.2.	Se realizan pruebas y capacitaciones sobre el plan de continuidad del negocio.	✗			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 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
H.6.	Se cuenta con una política y/o procedimiento para la gestión de cuentas de usuario.	✗		Se nos indicó que el desarrollo de la política para gestión de cuentas de usuario, es parte del plan de trabajo del Marco de Gobierno y Gestión de TI.	M
H.7.	La asignación de accesos a la plataforma tecnológica parte del principio de segregación de funciones y son aprobados por parte del dueño del sistema.		✓	Se cumple con la condición.	B
H.8.	Se revisan periódicamente los perfiles de los usuarios para determinar si estos poseen la cantidad de accesos mínimos necesarios.		✓	Se cumple con la condición.	B
H.9.	Se inhabilitan las cuentas de los usuarios que cesan funciones en la organización (despidos, renuncias, jubilaciones, vacaciones, permisos, etc.).		✓	Se cumple con la condición.	B

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 encuentra en proceso de atención en el hallazgo H03-2022.	M
I.2.	Se revisan periódicamente las bitácoras de los sistemas de información para identificar comportamientos irregulares en las operaciones de la organización.	✗			M
I.3.	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.4.	Se han implementado medidas de seguridad lógica en los sistemas de información (vencimiento, histórico, tamaño y complejidad de la contraseña).		✓	Se cumple con la condición.	B
I.5.	Los sistemas de información cuentan con manuales de usuario y manuales técnicos.		✓	Se cumple con la condición.	B
I.6.	Los procesos de la organización están totalmente automatizados, evitando la realización de tareas manuales.	✗		Se encuentra en proceso de atención en el hallazgo H03-2022.	M
I.7.	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 encuentra en proceso de atención en el hallazgo H03-2022.	M

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
I.8.	Se restringe la entrada de datos de modo que el registro de información sea lo más estándar posible.		✓	Se cumple con la condición.	B
I.9.	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-