SINAES

Informe Auditoría de Sistemas y Tecnologías de Información.

Carta de Gerencia CG-TI 2021.

Informe Final.

San José, 18 de agosto de 2022

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 2021 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 los estándares establecidos según los Objetivos de Control para Información y Tecnología Relacionada – COBIT®., los cuales sometemos a consideración de ustedes en esta carta de gerencia CG-TI 2021.

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: 2022.09.08 12:05:47 -06'00'

Lic. Gerardo Montero Martínez
Contador Público Autorizado No. 1649
Póliza de Fidelidad Nº 0116 FIG 7
Vence el 30 de setiembre del 2022.

"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 basados en los Objetivos de Control de Tecnologías de Información (COBIT por sus siglas en inglés) emitidos por la "Information Systems Audit and Control Association" (ISACA por sus siglas en inglés) 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:

- ✓ Administración del área de tecnologías de información.
- ✓ Seguridad Física.
- ✓ Evaluación de políticas, procedimientos, normas, lineamientos y directrices internas en materia tecnológica.
- ✓ Funcionalidad e integración general de algunos sistemas.
- ✓ Seguimiento a recomendaciones emitidas en periodos anteriores.

PERIODO DEL ESTUDIO

El estudio se realizó durante los meses de julio y agosto del año 2022 y corresponde a la auditoría del periodo del 2021.

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: OPORTUNIDADES DE MEJORA EN LAS GESTIONES ASOCIADAS A LOS PROCESOS DE TI EN EL SINAES. RIESGO BAJO.

CONDICIÓN:

Producto de la revisión efectuada a la documentación suministrada por la adminsitración del SINAES, se determinó que la elaboración de procedimientos formales para algunas de las áreas evaluadas se encuentra en proceso de desarrollo y detalladas en el plan de trabajo respectivo, además en la respuesta a la solicitud de información inicial y en los requerimientos adicionales se menciona lo siguiente: *"El desarrollo de procedimientos y/o lineamientos forman parte del plan de trabajo 2022-2023."*

A continuación, se detallan las áreas que tienen pendiente la elaboración de un proceso formal:

- Gestión de activos.
- Gestión de proveedores.
- Gestión de proyectos.
- Gestión de aplicaciones y tecnologías.
- Gestión de respaldos.
- Seguridad de la información.
- Infraestructura de TI y telecomunicaciones.
- Plan de contingencia.
- Procedimiento para la gestión de roles y perfiles.
- Lineamientos para la gestión de bitácoras en los sistemas de información.

Dado que todas las actividades anteriores forman parte del plan de trabajo a desarrollar por el SINAES, actualmente el departamento de TI podría presentar dificultad para mantener los controles de gestión y seguridad dentro de diferentes ámbitos de TI. Lo que puede originar pérdidas financieras por una mala gestión de los recursos, tecnológicos, económicos y humanos que dispone la organización para llevar a cabo sus actividades.

CRITERIO:

El proceso **EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno**, presente en el estándar de Control Objectives for Information and related Technology 5 (COBIT 5), menciona: "Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa."

RECOMENDACIONES:

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.

III. MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

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	Sin comentarios.
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 2022-2023, por lo tanto, la recomendación se encuentra en proceso de ser atendida.
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 (considerando aplicativos, software y hardware) que soporta la operativa de cada uno de los procesos institucionales.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
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 2022-2023, por lo tanto, la recomendación se encuentra en proceso de ser atendida.
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	Sin comentarios.
ESTADO	**EN PROCESO** En la solicitud de información adicional se mencionó que se aplica la metodología SCRUM, con la cual realizan mediciones de avance por medio de los Sprints, sin embargo, el desarrollo de un procedimiento formal para la gestión

	de proyectos se encuentra en proceso como parte de la elaboración del plan de trabajo de TI. Además, fue posible verificar el seguimiento que se realiza a los proyectos desarrollados durante el periodo de auditoría, dado lo anterior, la recomendación se encuentra en proceso.
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	Sin comentarios.
ESTADO	**EN PROCESO** Se comenta por parte del departamento de TI que: "La institución está en proceso de levantamiento, actualización y aprobación de los lineamientos asociados. Se observa en el plan estratégico de TI la identificación de oportunidades de valor con la implementación de TI.". Por lo tanto, se considera el hallazgo en proceso.
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	Sin comentarios.
ESTADO	**EN PROCESO** Se comenta por parte del departamento de TI que: "La institución está en proceso de levantamiento, actualización y aprobación de los lineamientos asociados. Como parte del proceso de gestión de calidad, se ha establecido rehacer los lineamientos asociados a la gestión de TI.". Por lo tanto, se considera el hallazgo en proceso.
2019.15	
RECOMENDACIÓN	2019.15 Considerar en los lineamientos la definición de las especificaciones y requerimientos técnicos cuando sea requerida la adquisición e implementación de recursos tecnológicos.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**CORREGIDO**

	Esta práctica se lleva a cabo por medio del sistema SICOP. En donde se detallan los requerimientos de cada una de las contrataciones que se publican para la adquisición de un producto o servicio por parte de la organización.
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	Sin comentarios.
ESTADO	**EN PROCESO** Se notifica por parte del DTI que "la construcción de un procedimiento formal para la gestión de proveedores se encuentra en construcción como parte del plan de trabajo de TI.".
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	Sin comentarios.
ESTADO	**EN PROCESO** Se notifica por parte del DTI que "la construcción de un procedimiento formal para la gestión de proveedores se encuentra en construcción como parte del plan de trabajo de TI.".
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	Sin comentarios.
ESTADO	**EN PROCESO** Se comenta por parte del Departamento de Tecnologías de Información que las recomendaciones emitidas en periodos anteriores están siendo trabajadas por parte de la administración de TI como parte del plan de trabajo 2022-

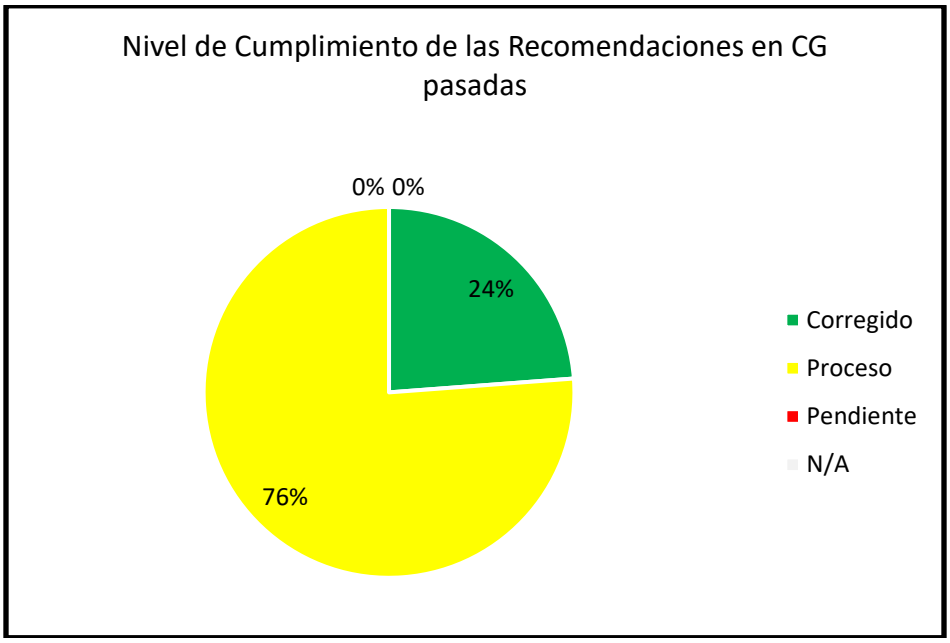
	2023 para la adopción del marco de gobierno y gestión emitido por el MICITT. Para el proceso de auditoría se suministró dicho marco como evidencia.
2019.1	
RECOMENDACIÓN	2019.1 Finalizar el levantamiento los lineamientos al nivel institucional que permitan gestionar la estrategia de SINAES, al nivel de creación, seguimiento de la ejecución y cierre de los planes. Estas directrices deben disponerse para todo el proceso de planificación a largo, mediano y corto plazo.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**CORREGIDO** Se identifican planes de acción para el cumplimiento de los objetivos y planes a corto, mediano y largo plazo que han sido definidos por el SINAES.
2019.3	
RECOMENDACIÓN	2019.3 Establecer formalmente en el lineamiento que regula las acciones del Comité Directivo las actividades relacionadas con la responsabilidad de valorar la adecuada gestión de TI en respuesta a la dirección institucional, así como definir las prioridades de implementación y mejora de la infraestructura tecnológica, de acuerdo con las necesidades y requerimientos institucionales.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**CORREGIDO** El marco de gestión de TI desarrollado por el SINAES define las actividades por realizar próximamente por la institución desde el departamento de TI con la intención de alcanzar los objetivos institucionales. Además, se determinan las actividades para velar por el cumplimiento jurídico en caso de que ocurra alguna incidencia en la gestión de TI.
2019.12	
RECOMENDACIÓN	2019.12 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	Sin comentarios.
ESTADO	**EN PROCESO** Se notifica por parte del DTI que “la construcción de un procedimiento formal para la gestión de proveedores se encuentra en construcción como parte del plan de trabajo de TI.”.
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	Sin comentarios.
ESTADO	**EN PROCESO** Se comenta por parte del Departamento de Tecnologías de Información que las recomendaciones emitidas en periodos anteriores están siendo trabajadas por parte de la administración de TI como parte del plan de trabajo 2022-2023 para la adopción del marco de gobierno y gestión emitido por el MICITT. Para el proceso de auditoría se suministró dicho marco como evidencia.
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	Sin comentarios.
ESTADO	**EN PROCESO** Se identifican actividades relacionadas a la concientización de los funcionarios en materia de seguridad de la información, sin embargo, dichas actividades no han sido formalizadas para ser aplicadas siempre.
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	Sin comentarios.
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 2022-2023, por lo tanto, la recomendación se encuentra en proceso de ser atendida.
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	Sin comentarios.
ESTADO	**EN PROCESO** Se evidencia que las recomendaciones efectuadas están siendo trabajados por la administración de Tecnologías de Información como parte del plan de trabajo 2022-2023 de la adopción del marco de gobierno y gestión emitido por el MICITT. Por lo tanto, se considera que el 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	Sin comentarios.
ESTADO	**EN PROCESO** Se evidencia que las recomendaciones efectuadas están siendo trabajados por la administración de Tecnologías de Información como parte del plan de trabajo 2022-2023 de la adopción del marco de gobierno y gestión emitido por el MICITT. Por lo tanto, se considera que el hallazgo se encuentra en proceso.
2019.33	
RECOMENDACIÓN	2019.33 Debe disponerse de un modelo formal que permita asegurar la adecuada gestión de los procesos de TI, tales como revisión y actualización (según aplique) de los lineamientos, actividades y responsabilidades en forma periódica, asegurando la adecuada respuesta según necesidades y prioridades institucionales.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**CORREGIDO** Es posible evidenciar un monitoreo periódico sobre las actividades por realizar que formar parte de los planes de acción para llevar a cabo cada objetivo del área de TI.
2019.34	
RECOMENDACIÓN	2019.34 Establecer actividades formales que permitan velar por el adecuado cumplimiento del marco jurídico que pueda tener incidencia sobre la gestión de TI (entre otros, licenciamiento, propiedad de los datos, propiedad intelectual sobre software y aplicaciones, etc.)

COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**CORREGIDO** El marco de gestión de TI desarrollado por el SINAES define las actividades por realizar próximamente por la institución desde el departamento de TI con la intención de alcanzar los objetivos institucionales. Además, se determinan las actividades para velar por el cumplimiento jurídico en caso de que ocurra alguna incidencia en la gestión de TI.
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	Sin comentarios.
ESTADO	**EN PROCESO** Se comenta por parte del Departamento de Tecnologías de Información que las recomendaciones emitidas en periodos anteriores están siendo trabajadas por parte de la administración de TI como parte del plan de trabajo 2022-2023 para la adopción del marco de gobierno y gestión emitido por el MICITT. Para el proceso de auditoría se suministró dicho marco como evidencia.
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	Sin comentarios.
ESTADO	**EN PROCESO** Se verificó que en el informe de auditoría del periodo anterior se realiza un seguimiento a las recomendaciones, sin embargo, no se evidenció la existencia de prácticas formales para realizar dichas tareas.

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	Total
Corregidas	5	**5**
En Proceso	16	**16**
Pendiente	0	**0**
No Aplica	0	**0**
Total	**21**	**21**

NOTA: los hallazgos 2019.5, 2019.7, 2019.9, 2019.18, 2019.32, 2019.30 y 2019.31, no fueron tomados en cuenta para realizar el gráfico y la tabla anteriores, debido a que no fue posible identificar cuál es el área responsable de realizar las recomendaciones emitidas.

IV. ANEXO I

Análisis de Riesgos T.I.
Departamento de Sistemas de Información
Periodo 2021

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.		✓		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.		✓		B
A.4.	Se le da seguimiento periódico al cumplimiento del PAO.		✓		B

B. GESTIÓN DEL PRESUPUESTO DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
B.1.	Se genera un plan anual presupuestario de TI formalmente aprobado.		✓	Se cumple con la condición.	B
B.2.	El presupuesto se encuentra categorizado y priorizado según las actividades críticas del plan anual operativo de TI.		✓		B
B.3.	Se mantiene un control de gastos y ejecuciones presupuestarias de TI y se le brinda informes de ejecución a la administración.		✓		B
B.4.	Se mantiene alineado el plan presupuestario de TI con el plan anual operativo.		✓		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, fue posible evidenciar un registro de las capacitaciones del periodo, así como evidencia de las evaluaciones del desempeño y manuales de puestos.	B
C.2.	Las capacitaciones se encuentran justificadas (proyectos de TI, evaluaciones del desempeño).		✓		B
C.3.	Se mantiene un manual de puestos actualizado con la descripción y las responsabilidades del personal de TI.		✓		B
C.4.	Se realizan evaluaciones anuales del desempeño de los colaboradores de TI.		✓		B
C.5.	Se realizan medidas correctivas para el personal que obtiene calificaciones deficientes en las evaluaciones del desempeño.		✓		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.		✓		B
D.3.	Se realiza un seguimiento al cumplimiento contractual de las responsabilidades de los proveedores.	✗		No se identifica información relacionada.	M

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 cuenta con una metodología para la gestión de proyectos de TI formalmente establecida.	✗		El desarrollo de una metodología formal se encuentra contemplado en el plan de trabajo 2022-2023, por lo que se mantiene en proceso, En el Hallazgo 1 menciona las respectivas recomendaciones.	M
E.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.)	✗			M
E.3.	Los usuarios o clientes de los proyectos aprueban formalmente los entregables de estos.		✓	Se cumple con la condición.	B
E.4.	Se les da seguimiento a los proyectos posterior a la implementación.		✓	Se cumple con la condición.	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.	✗		No se cumple con la condición.	B
F.2.	Las bases de datos poseen logs para registrar los cambios y mantener una trazabilidad de estos.	✗			M

G. GESTIÓN DE ACTIVOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
G.1.	Se mantienen controles para el ingreso y salida de equipo tecnológico a la organización.		✓	Se cumple con la condición.	B
G.2.	Se cuenta con un inventario de activos de TI (equipo en uso y desuso, periféricos, equipo de comunicación, dispositivos móviles, etc.), junto con información de su ubicación y responsable.		✓	Se cumple con la condición.	B
G.3.	Se genera plan de infraestructura de TI alineado a los proyectos establecidos en el plan anual operativo de TI.	✗		El plan de infraestructura se encuentra en proceso de elaboración en el plan de trabajo 2022-2023, las recomendaciones se incluyen en el Hallazgo 1.	M
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 una política y/o procedimiento para la realización de respaldos de información.	✗		El desarrollo de una metodología formal se encuentra contemplado en el plan de trabajo 2022-2023, por lo que se mantiene en proceso, En el Hallazgo 1 menciona las respectivas recomendaciones.	M
H.2.	Se realizan pruebas a los respaldos de información.		✓	Se cumple con la condición.	B
H.3.	Se tienen medidas de seguridad para los respaldos de información (acceso restringido, traslado de respaldos a un sitio externo).	✗		El desarrollo de una metodología formal se encuentra contemplado en el plan de trabajo 2022-2023, por lo que se mantiene en proceso, En el Hallazgo 1 menciona las respectivas recomendaciones.	M

H.4.	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.	✗		No se cumple con la condición.	A
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.	✗			A
I.3.	Se cuenta con una política de uso de recursos de TI (correo electrónico, equipos, red).	✗			A
I.4.	Se tiene implementado medidas de seguridad para la red institucional (firewall, estudios de vulnerabilidad, segmentación de redes).		✓	Se cuenta con un firewall, para la seguridad de la red.	B

IV. 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.	✗		El desarrollo de una metodología formal se encuentra contemplado en el plan de trabajo 2022-2023, por lo que se mantiene en proceso, En el Hallazgo 1 menciona las respectivas recomendaciones.	M
J.2.	Se revisan periódicamente las bitácoras de los sistemas de información para identificar comportamientos irregulares en las operaciones de la organización.	✗			M
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 tiene restricciones para inicios de sesión únicos.	A
J.4.	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.	A
J.5.	Los sistemas de información cuentan con manuales de usuario y manuales técnicos.		✓	Se cumple con la condición.	B
J.6.	Los procesos de la organización están totalmente automatizados, evitando la realización de tareas manuales.		✓		B
J.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.	✗		No se cumple con la condición, en la respuesta a la solicitud de información inicial se menciona que no hay una integración entre los sistemas de información actuales.	A
J.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
J.9.	Se brindan capacitaciones periódicas en el uso de los sistemas a los usuarios de la organización.		✓		B

V. ANEXO II

Valoración del nivel de satisfacción sobre la calidad funcional de algunos de los sistemas de información y soporte brindado por el Área de Tecnologías de la Información

OBJETIVO

Medir el nivel de satisfacción que posee el usuario con respecto al (los) sistema (as) que utiliza el SINAES y al soporte brindado por el Área de Tecnologías de la Información.

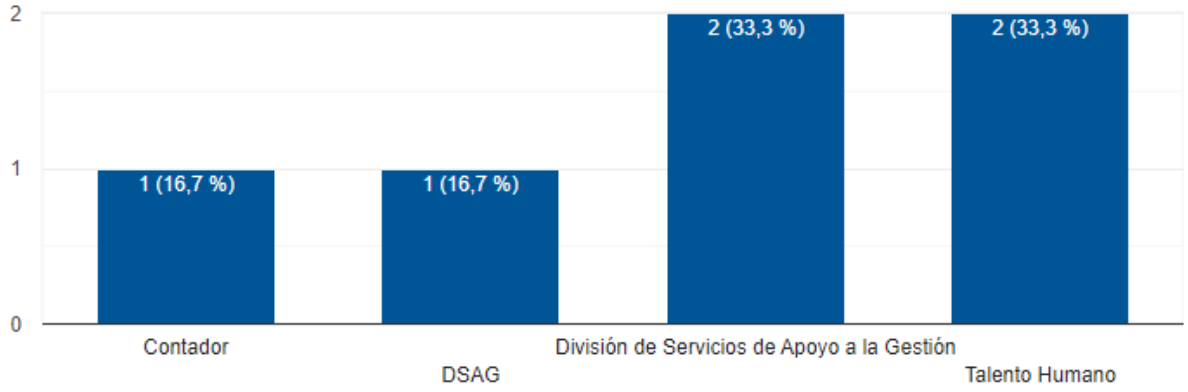
RESULTADOS

A continuación, se muestra el resultado de la evaluación realizada con respecto a la calidad funcional de algunos de los sistemas de información implantados en el SINAES, según la percepción de los usuarios finales.

En total, 6 colaboradores brindaron respuesta. Los sistemas de información/módulos que se indicaron en la evaluación pertenecen a las siguientes áreas de trabajo:

- El módulo de contabilidad.
- División de Servicio de Apoyo a la Gestión (DSAG), cabe mencionar que uno de los colaboradores identificó el mismo módulo con otro nombre por lo que se debe de sumar un total de 3 votos, para un total del 50%.
- Talento Humano.

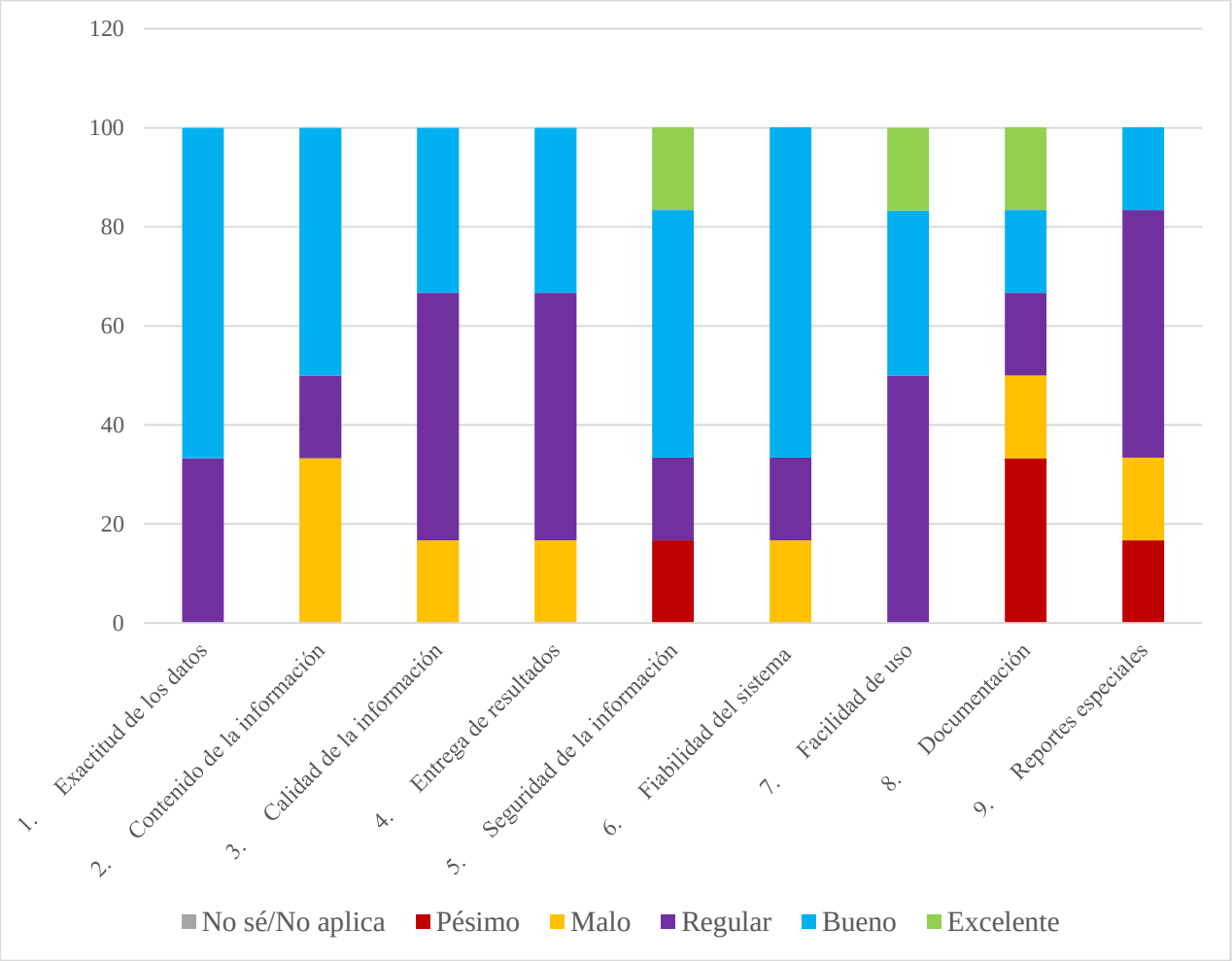
En el siguiente gráfico se muestra el porcentaje de respuestas por módulo.



En los siguientes apartados, se muestran las respuestas registradas según la sección evaluada.

Información sobre el sistema de información

El siguiente gráfico muestra el resumen de respuestas por categoría, esto para atributos relacionados propiamente con los sistemas/módulos utilizados.



Tal y como se observa en el gráfico, las respuestas brindadas en su mayoría se ubican entre las valoraciones de regular y bueno, los únicos atributos en los cuales se presentaron calificaciones de "pésimo" son *Seguridad de la información*, *Documentación* y *Reportes especiales*.

Para cada uno de los atributos, los usuarios tenían un espacio para brindar comentarios adicionales a su calificación (esto de forma opcional), entre las respuestas registradas indicaron que:

- El módulo de nómina presenta errores en acciones de personal, principalmente son errores visuales, ya que los cálculos se realizan de manera correcta.
- En el caso del GRP, no se hacen mejoras a reportes de históricos, en el flujo del gestor se considera que la información de las facturas no es fácil de acceder.
- Existen módulos que se consideran lentos, ya que el procesamiento tarda más de lo esperado.
- Algunos de los Sistemas de Información son desarrollos por empresas externas. No se podría dar certeza del nivel de seguridad empleada en los códigos fuentes que eviten la fuga de información.

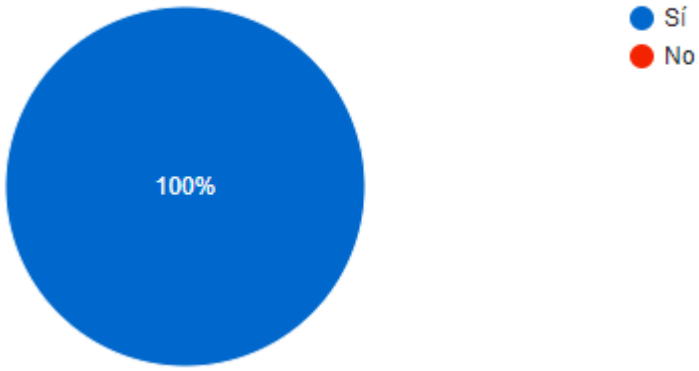
- Se menciona un caso en el cual se perdió toda la información almacenada, dicha situación le sucedió a un colaborador al momento de cambiar a la modalidad de teletrabajo. Se menciona que mucha información se respalda en SICOP, sin embargo, los expedientes con que se trabajaba no pudieron recuperarse, esto a pesar de haber guardado los datos en una red interna.
- No existen manuales de uso en la mayoría de los sistemas.
- En cuanto al módulo de nómina, se deben mejorar aspectos a la hora de generar reportes especiales.

En caso de que se desee indagar a profundidad sobre los atributos antes señalados u otros, es recomendable tomar una muestra de usuarios mayor y especifica (un solo sistema/módulo).

Opinión sobre el soporte brindado por el Departamento de Sistemas de Información

A continuación, se muestran las respuestas graficadas relacionadas con opiniones acerca del soporte brindado por el Departamento de Sistemas de Información.

El departamento brinda los resultados esperados

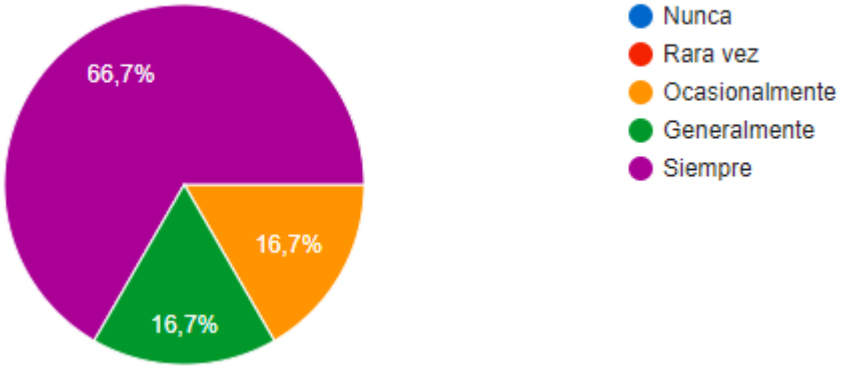


Al respecto amplían indicando que, se atienden los casos de excelente manera en tiempo y forma, además, a pesar de ser un departamento nuevo dentro del SINAES, se ha adaptado muy bien al entorno de la institución. Sin embargo, se destacan oportunidades de mejora en cuanto a la eficiencia de los sistemas actuales y la pérdida de información.

Servicio proporcionado por el departamento

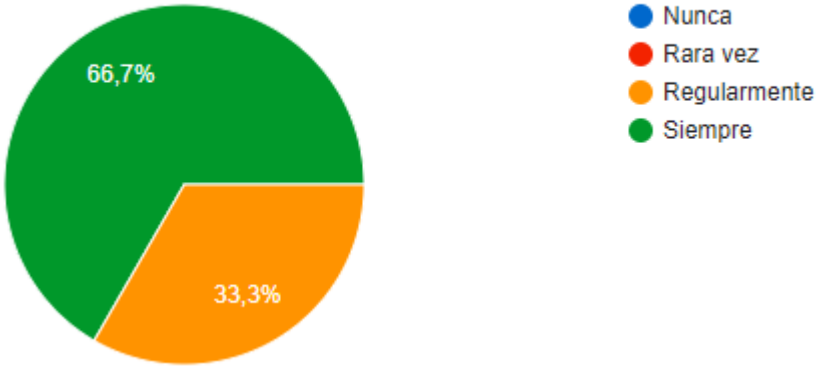
Al respecto amplían indicando que, el personal del departamento tiene un buen conocimiento y manejo de los procesos el negocio ya que se encargaron de la migración desde el sistema de CONARE, además de atender de excelente manera. Sin embargo, se considera por alguno de los usuarios que es necesario en otras necesidades y otros procesos del negocio que son más críticos.

Disponibilidad del departamento



Al respecto amplían indicando que, se tiene como objetivo en el departamento la creación de un ambiente de transformación digital del SINAES, y que el área de TI trabaja muy duro y con la mejor disposición para lograrlo, a pesar de contar con limitaciones de tiempo para realizar sus actividades.

Puntualidad con la entrega de solicitudes



Al respecto amplían recalcando que el trabajo que realizan y el control que implementan, han permitido que hasta el momento se atiendan los problemas e incidentes reportados de manera ágil.

Opinión sobre otros atributos adicionales

A continuación, se muestran las respuestas graficadas relacionadas con opiniones acerca de atributos adicionales.

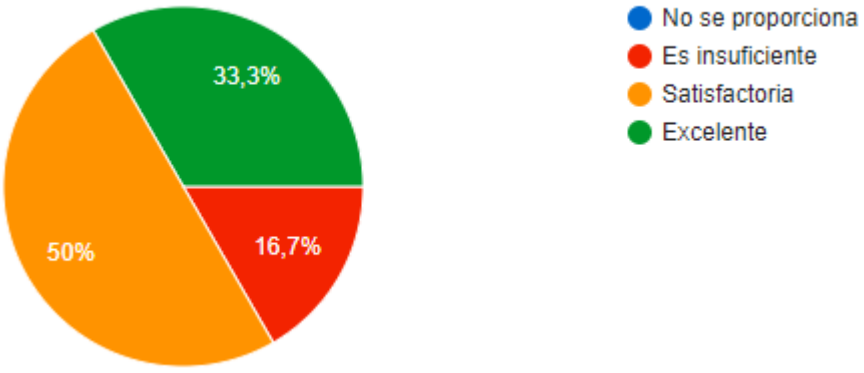
Cobertura de necesidades con el sistema proporcionado

Los usuarios señalan que debido a que es un área nueva, aún no ha logrado implementar todo lo necesario para la automatización de todos los procesos de la Institución, además, se menciona que aún es necesaria la adquisición de algunas licencias en sistemas de información que permitan modernizar el trabajo, por ejemplo, la parte de archivo o diagramas de procesos.
Se les consultó sobre nuevas funcionalidades que necesiten y el sistema actualmente utilizado no posee, al respecto indican:

- "Desarrollo de sistema para gestión de procesos de acreditación. Sistema de ventanilla única y gestión documental, automatización de procesos, implementación de mesa de ayuda para reporte de incidentes de TI".
- "Disponibilidad de nuevos auxiliares para el manejo de inversiones, derechos y garantías".
- "Autoservicio: que se pueda gestionar la reversión de vacaciones, que lleguen correos electrónicos con notificaciones cuando se hacen solicitudes o entregas de documentos".
- "Nómina: Que se pueda gestionar todo el proceso de nómina de inicio a fin en el sistema".
- "Ya se ha reiterado de solicitar mejoras e interfaces al GRP".
- "Analizar el cambio del sistema".
- "Sistema integrados, bases de datos apropiadas".

Como se denota, los comentarios anteriores reflejan varias necesidades de los usuarios a nivel del sistema que utilizan, es prudente analizarlos, pues, la mayoría contiene requerimientos que deberían considerarse (en caso de no haberlo realizado). A la hora de implementar mejoras a los sistemas actuales, o bien, adquirir uno nuevo, es de vital importancia considerar a los usuarios finales en la toma de requerimientos.

Capacitaciones recibidas en materia informática



El gráfico evidencia que más del 83% considera que las capacitaciones son excelentes (33.3%) o satisfactorias (50%). Y solamente un 16.7% determinó que las capacitaciones recibidas son insuficientes. A pesar de que solamente fue una respuesta, es prudente analizar -en conjunto con el Departamento de Recursos Humanos o equivalente- la necesidad de capacitar a las áreas usuarias con respecto al uso de sistemas, educación en temáticas tales como seguridad de la información, buenas prácticas relacionadas con TI, plataformas tecnológicas utilizadas u otras, las cuales, si bien son relacionadas al campo de TI impactan las labores de las otras áreas de la organización.

Comentarios adicionales

En la encuesta aplicada se proporcionó una sección final para que los usuarios agregaran (de manera opcional) comentarios, críticas u oportunidades de mejora que sirvan de retroalimentación para mejorar la calidad brindada por el Departamento de TI o de los sistemas en general, parte de las respuestas registradas fueron:

- ✓ Considero que se ha mejorado o se han apropiado algunas funciones al TI de SINAES, pero aún falta por seguir trabajando la calidad de los servicios.
- ✓ Las oportunidades de mejora radican en poder desarrollar los sistemas de información que se mencionan en la pregunta# 20:
  - Desarrollo de sistema para gestión de procesos de acreditación. Sistema de ventanilla única y gestión documental, automatización de procesos, implementación de mesa de ayuda para reporte de incidentes de TI.
  - Autoservicio: que se pueda gestionar la reversión de vacaciones, que lleguen correos electrónicos con notificaciones cuando se hacen solicitudes o entregas de documentos.

- Nómina: Que se pueda gestionar todo el proceso de nómina de inicio a fin en el sistema.

✓ Contar con personal especializado en desarrollo de Software, que permita agilizar proyectos en esta línea y agregar nuevas funcionalidades a los sistemas actuales.

En estos comentarios finales los usuarios recalcan la necesidad de contar con un mejor soporte para el desarrollo y personalización de los sistemas utilizados actualmente por la organización. Dado lo anterior, es recomendable, a nivel de sistemas, considerar las necesidades de los usuarios finales (tal y como se señaló en el apartado de *Cobertura de necesidades con el sistema proporcionado*), y, por otra parte, hacer un estudio de cargas laborales del Departamento de Sistemas de Información.

--Fin del documento--