SISTEMA NACIONAL DE ACREDITACIÓN DE LA EDUCACIÓN SUPERIOR

Informe Auditoría de Sistemas y Tecnologías de Información
Carta de Gerencia 2019

San José, 25 de mayo, 2020

Señores
Alto Jerarca
Sistema Nacional de Acreditación de la Educación Superior
Presente

Estimados señores:

Según nuestro contrato de servicios, efectuamos la visita de auditoría externa del período 2019 al Sistema Nacional de Acreditación de la Educación Superior - SINAES y en el examen efectuado, revisamos 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 la información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, cuyo resultado sometemos a consideración de ustedes en esta carta de gerencia CG 1-2019.

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. Los resultados indicados en este informe no son puntuales a los diferentes funcionarios de la Institución y por el contrario debe ser considerado como una base para el mejoramiento y fortalecimiento de los procedimientos de control interno y los aspectos relacionados el Área de Tecnologías de la Información.

Agradecemos una vez más la colaboración brindada por los funcionarios y colaboradores del SINAES y estamos en la mejor disposición de ampliar o aclarar el informe adjunto en una sesión conjunta de trabajo.

CONSORCIO EMD
CONTADORES PÚBLICOS
AUTORIZADOS

ESTEBAN MURILLO DELGADO (FIRMA)
Firmado digitalmente por ESTEBAN MURILLO DELGADO (FIRMA)
Fecha: 2020.07.14 20:36:10 -06'00'

Lic. Esteban Murillo Delgado
Contador Público Autorizado N° 3736
Póliza de Fidelidad No. 0116 FIG 7
Vence el 30 de setiembre del 2020

"Timbre de Ley 6663 por ¢25,00 del Colegio de Contadores Públicos de Costa Rica, se adhiere y cancela en el original".

INFORME DE CUMPLIMIENTO Y CONTROL INTERNO DE TENOLOGÍAS DE INFORMACIÓN

CONTENIDO

I. OBJETIVO

Como parte de la evaluación de los estados financieros de la Organización, procedimos a realizar la evaluación de los controles generales de la gestión de Tecnología 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 a luz de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la Contraloría General de la República, y en general las mejores prácticas de la industria de tecnología de información.

II. ALCANCE

El trabajo de evaluación fue enfocado principalmente a las siguientes áreas:

- Valoración de la implementación actual de las normas técnicas emitidas por la Contraloría General de la República en lo que respecta a la gestión de tecnologías de información instaladas.
- Oportunidades de mejora identificadas en la evaluación.

III. PERÍODO DEL ESTUDIO

El estudio se realizó durante el mes de mayo del 2020 y corresponde a la auditoría del período 2019.

IV. ENFOQUE Y METODOLOGÍA

El enfoque general utilizado para llevar a cabo esta evaluación, se enmarcó dentro los términos establecidos en las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información según Resolución R-CO-26-2007 del 7 de junio de 2007 de la Contraloría General de la República, Publicadas en la Gaceta N° 119 del jueves 21 de junio de 2007.

Para el desarrollo del trabajo de campo, se emplearon una variedad de instrumentos metodológicos, dentro de los que destacan los siguientes:

- Delimitación del marco conceptual, legal, administrativo, organizacional y de ejecución por medio del cual se efectuará la evaluación.
- Identificación y obtención de documentación que resultara relevante para la evaluación.
- Otras técnicas, herramientas o métodos necesarios para mejorar la comprensión o el análisis de la información obtenida, a utilizar según criterio profesional de los consultores asignados a este proyecto.

V. ANTECEDENTES

El Sistema Nacional de Acreditación de la Educación Superior – SINAES, es la institución a la que desde 1999 el Estado costarricense le otorgó la potestad de dar fe pública de la calidad de las instituciones, carreras y programas de educación superior que voluntariamente se sometan a su riguroso proceso de evaluación y demuestren el cumplimiento de los criterios de calidad establecidos. En el 2002 el SINAES es reconocido como un órgano adscrito a CONARE.

A través del Acuerdo para el Apoyo de la Gestión Administrativa del SINAES por parte de CONARE y su Oficina de Planificación de la Educación Superior (OPES) presta los servicios en las áreas financiero contable, recursos humanos, proveeduría, tecnología de información, servicios generales, archivo y biblioteca, además de servicios jurídicos. Esta disposición rige mientras el SINAES asume su gestión administrativa y operativa en su transición de desconcentración máxima.

Específicamente, en la cláusula Sétima del acuerdo mencionado, se establece que CONARE prestará los servicios de tecnologías de información y comunicación, incluyendo mantenimiento y soporte técnico. Como parte de sus objetivos estratégicos, a partir del 2019, SINAES ha contratado un recurso en tecnologías de información para conformar un área a la que se vaya transfiriendo las facultades de administración de los recursos tecnológicos utilizados en esta institución y lograr así la autonomía tecnológica requerida conforme su ordenamiento jurídico.

VI. RESULTADOS

SINAES entiende la importancia de una adecuada gestión de las tecnologías de información, por lo que sus esfuerzos, debidamente alineados con la estrategia institucional, se están basando en lograr su autonomía en este proceso durante el período 2019-2020. Para lo cual se han levantado planes de introducción, implementación y adecuación de la administración de los recursos tecnológicos en producción y requeridos para soportar la operativa institucional.

Debido a la dependencia que se ha mantenido con CONARE y para completar este proceso de transición a la gestión autónoma, debe considerarse la definición de una estructura administrativa formalizada mediante lineamientos que consideren buenas prácticas y estructuras de responsabilidad de las áreas establecidas para la administración de los recursos tecnológicos implementados en la institución, basándose en una serie de atributos que apoyen su adecuada gestión y en alineación con los requerimientos regulatorios. Con base en el oficio SINAES-DSAG-41-2020, que especifica los lineamientos que están en proceso de levantamiento y revisión. Con respecto a los lineamientos asociados a la gestión de tecnologías de información, se indica que serán desarrollados conforme se avance en la migración de la infraestructura desde ATIC-CONARE a SINAES.

De esta forma, esta auditoría pretende aportar elementos de apoyo para que el proceso tanto de migración como de la definición de los lineamientos y aplicación de prácticas para fortalecer la gestión institucional y de TI.

Con el fin de orientar mejor este proceso de transición, se presentan los requerimientos, resultado de la evaluación se presentan por dominio expresado en la Norma técnica de la CGR, según se detalla a continuación:

I. Marco Estratégico de TI (Planificación y Decisiones)

La institución ha levantado el plan estratégico tanto al nivel institucional como de TI, y principalmente en este último, se avoca a la transición de la administración de los recursos tecnológicos que se utilizan en la institución para soportar sus operaciones.

Se cuenta adicionalmente con planes anuales operativos que explican proyectos y metas a desarrollar durante el período para cumplir con las acciones estratégicas definidas.

Según las especificaciones de cumplimiento del PAO 2019, hay un porcentaje de avance sobre el diseño de procedimientos y herramientas para el seguimiento de la evaluación del PAO y el Plan estratégico.

Según se explica, no se cuenta formalmente con un Comité de TI. Sin embargo, al nivel de Equipo Directivo, periódicamente se analizan y consolidan prioridades incluyendo los temas relacionados con la gestión de TI. Esto es una buena práctica, debido a que es importante que estos elementos sean parte integral de la gestión y administración institucional.

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.

   Responsable : Dirección Servicios de Apoyo a la Gestión

2. Al nivel de tecnologías de información, se recomienda que la línea estratégica de esta área sea incorporada en el plan estratégico institucional, según lo dictan las buenas prácticas y para administrar la gestión tecnológica, siguiendo la línea actual de trabajo, definir:

   a. Planes a mediano plazo (asociados a los programas de proyectos), en los que se especifiquen las iniciativas donde TI

   b. Plan de infraestructura (con vigencia según el plan estratégico institucional), que incluya necesidades de mantenimiento de la infraestructura instalada (sostenibilidad, actualización, mejora, licenciamiento, sustitución por obsolescencia) y adquisición de nueva infraestructura (basado en los programas de proyectos)

   c. Plan de inversiones al nivel de TI (con vigencia según el plan estratégico institucional) que responda a las necesidades establecidas en el plan de infraestructura

   Responsable : División Servicios de Apoyo a la Gestión / Encargado de TI

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.

   Responsable: Dirección Ejecutiva

   Comentarios de la Administración: actualmente no existe un comité formal, sin embargo, semanalmente hay una reunión de equipo directivo donde se consolidan las prioridades de la semana para la institución en general, incluyendo los proyectos y actividades a desarrollar en el área de TI.

II. Independencia y Recurso Humano de la Función de TI

Con base en la estructura organizativa definida y el manual de puestos, se observa que la gestión de tecnologías de información ha sido establecida de forma adecuada y que le permitiría generar sus servicios en una forma independiente y a toda la institución.

Adicionalmente, se está trabajando en el levantamiento de los lineamientos asociados a la gestión de recursos humanos.

Aunque se observa que se dispone de una partida para capacitación al nivel institucional, no se identificó la asociación de las necesidades específicas en este rubro para el área de TI.

4. Disponer de un plan formal y detallado de los requerimientos de capacitación del personal de TI sobre la administración de los recursos tecnológicos (hardware, software y comunicaciones), así como para usuarios en cuanto al uso de herramientas y otros relacionados con las tecnologías de información.

   Responsable: División Servicios de Apoyo a la Gestión

II. Gestión de Riesgos

5. Disponer de los lineamientos y metodología que les permita gestionar adecuadamente los riesgos, basándose en el SEVRI. Las directrices deben contener las actividades relacionadas a la identificación, valoración/medición, establecimiento de las acciones de gestión, documentación del portafolio de riesgos y monitoreo de su gestión.

   Responsable: División Servicios de Apoyo a la Gestión

6. Es recomendable disponer de un Comité de Riesgos (puede ser el Comité Directivo en forma ampliada), así como un oficial de riesgos que apoye en la administración de este proceso.

   Responsable: Dirección Ejecutiva

7. Por su parte, el área de TI debe aplicar en forma consistente las directrices establecidas y gestionar los riesgos asociados a las Tecnologías de información

   Responsable: Encargado de TI

III. Modelo de Arquitectura de Información

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.

   Responsables: Dirección Servicios de Apoyo a la Gestión / Encargado de TI

IV. Administración de los Recursos Financieros

La institución gestiona adecuadamente el proceso de administración de recursos financieros, estableciendo los respaldos documentales que lo soportan. Adicionalmente, se encuentran en proceso de finalización de los lineamientos asociados para dicha gestión.

9. Finalizar el levantamiento los lineamientos al nivel institucional que permitan gestionar la administración de los recursos financieros de SINAES.

   Responsables: Dirección Servicios de Apoyo a la Gestión

V. Gestión de proyectos

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.

    Responsable: Dirección Servicios de Apoyo a la Gestión

VI. Infraestructura Tecnológica

Debido al proceso de transición que atraviesa actualmente la institución con respecto a logro de la autonomía sobre la gestión del CONARE, se ha desarrollado un plan de migración que visualiza las necesidades y actividades requeridas para poder administrar directamente desde el SINAES los recursos tecnológicos que soportan su operativa.

11. Asegurar que el proceso de transición quede adecuadamente documentado, considerando inventario de activos tecnológicos, licenciamiento, topología de red, herramientas y aplicativos, según aplique, las versiones vigentes, la asociación de los procesos institucionales que se soportan con dicha infraestructura (este tema se puede integrar con el punto IV – Arquitectura de información, de este informe).

    Responsable: Encargado de TI

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.

    Responsable: Encargado de TI

VII. Implementación de TI (Infraestructura, Software y Aplicaciones)

13. Disponer de lineamientos formales que permitan identificar y alinear necesidades y oportunidades de implementación de recursos tecnológicos como respuesta a la estrategia institucional.

    Responsables: Dirección Servicios de Apoyo a la Gestión / Encargado de TI

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.

    Responsable: Encargado de TI

VIII. Contratación de Terceros para la Implementación y Mantenimiento de Software e Infraestructura

La institución está desarrollando los lineamientos asociados a la gestión y administración del proceso de contratación administrativa.

15. Considerar en los lineamientos la definición de las especificaciones y requerimientos técnicos cuando sea requerida la adquisición e implementación de recursos tecnológicos.
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.
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. Adicionalmente, es recomendable considerar al menos el análisis sobre el perfil del proveedor, su estabilidad en el mercado (tiempo de operación y de representación y comercialización del bien/servicio ofrecido), indagación sobre niveles de satisfacción de clientes que han adquirido bienes y/o servicios a los que eventualmente pueda requerir la institución, estableciendo los parámetros mínimos de cumplimiento para calificación del proveedor.

Responsables: Dirección Servicios de Apoyo a la Gestión / Encargado de TI

Comentarios de la Administración: Con respecto a la recomendación N°16, me surge la inquietud de qué tan apropiada sea llevarla a cabo ya que al ser una institución de carácter gubernamental estamos obligados por la Ley de Fortalecimiento a que todas las contrataciones sean llevadas a cabo por medio de Sicop, y por ende el tener un catálogo de proveedores no nos garantiza que a la hora de una contratación pueda ser efectivo.

Se realiza el ajuste a la recomendación.

IX. Definición de niveles de acuerdo de servicio

18. Establecer los términos formales que permitan definir, mantener y monitorear niveles de servicio tanto del área de TI hacia las unidades institucionales, como de proveedores externos de bienes y servicios; de forma tal que tenga claro los tiempos de respuesta, disponibilidad sobre estos servicios.

    Responsable: Encargado de TI

X. Administración de Datos

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.

    Responsables: Dirección Servicios de Apoyo a la Gestión / unidades institucionales

XI. Gestión de la Seguridad de la Información

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.

    Responsables: Dirección Servicios de Apoyo a la Gestión / Encargado de TI

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.

    Responsable: Encargado de RRHH y Encargado de TI

22. Establecer los lineamientos que permitan definir y aplicar las prácticas de seguridad sobre los recursos tecnológicos instalados en la institución (al nivel de configuración, dispositivos de control y resguardo, acceso interno y externo, entre otros) para proteger los datos e información que se procesan en las diferentes áreas de la institución.

    Responsable: Encargado de TI

23. Establecer lineamientos que permitan salvaguardar al nivel físico y ambiental los recursos tecnológicos instalados en la institución, tales como control de acceso autorizado, movilización (ingreso, salida y traslado), resguardo contra agentes tales como fuego, humedad, fallas eléctricas, entre otros.

    Responsable: Encargado de TI

24. Desarrollar prácticas formales a través de planes de continuidad, contingencia y recuperación que permitan administrar la continuidad de los servicios tecnológicos requeridos para la operación de los procesos institucionales. Estos planes también deben incluir las prácticas de administración, validación y prueba, de forma tal que se mantengan vigentes y disponibles para su aplicación en forma efectiva.

    Responsable: Encargado de TI

25. Disponer de lineamientos que permitan administrar adecuadamente la disponibilidad de datos e información (física, medios digitales), a través de recursos para almacenamiento apropiados y métodos de respaldo y recuperación.

    Responsable: Encargado de TI

26. Establecer los niveles formales de propiedad, custodia y responsabilidad sobre los recursos de TI instalados en la organización.

    Responsable: Encargado de TI

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.

    Responsable: Encargado de TI / Responsables de áreas funcionales de la institución

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.

    Responsable: Encargado de TI

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.

    Responsable: Encargado de TI

XII. Administración y operación de la plataforma tecnológica

30. Disponer de lineamientos formales que permitan administrar y monitorear el adecuado funcionamiento de la plataforma tecnológica instalada, en cumplimiento de las necesidades de operación de la institución

    Responsable: Encargado de TI

XIII. Atención de requerimientos de los usuarios de TI (Solicitudes, Incidentes, Problemas)

31. Establecer lineamientos y mecanismos formales que permitan gestionar adecuadamente los requerimientos de los usuarios sobre servicios y recursos de TI, tanto para el reporte y respuesta a incidentes, como para el tratamiento de nuevas necesidades y mejoras.

    Responsable: Encargado de TI

XIV. Gestión de la Calidad

32. Establecer los lineamientos que permitan asegurar que los productos y servicios brindados por la institución cumplen con los requerimientos mínimos de calidad en su proceso y entrega. Estas actividades de calidad se asocian al sistema de control interno y a la clara definición de los productos/entregables establecidos formalmente para cada proceso institucional (incluido TI).

    Responsable: Dirección Servicios de Apoyo a la Gestión

XV. Seguimiento de los procesos de TI

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.

Responsable: Dirección Servicios de Apoyo a la Gestión

XVI. Cumplimiento de Obligaciones relacionadas con la gestión de TI

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.)

Responsables: Dirección Servicios de Apoyo a la Gestión / Responsable de TI

XVII. Seguimiento y evaluación del control interno de TI

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.

Responsables Dirección Servicios de Apoyo a la Gestión

XVIII. Participación de la Auditoría Interna

36. Incorporar en los planes de trabajo, evaluaciones periódicas de la gestión de tecnologías de información, ya sea incorporando habilidades en el recurso interno para desempeñar dichas auditorías, o apoyándose en recursos externos.

37. Establecer prácticas formales para el seguimiento sobre el nivel de cumplimiento de recomendaciones realizadas al área de TI.

Responsable: Encargado Auditoría Interna