SISTEMA NACIONAL DE ACREDITACIÓN DE LA EDUCACIÓN SUPERIOR

Informe Auditoría de Sistemas y Tecnologías de Información
Carta de Gerencia 2020
Informe final

CONSORCIO EMD
Contadores Públicos Autorizados

MIEMBRO ADHERENTE
ASOCIACIÓN INTERAMERICANA
DE CONTABILIDAD (AIC)

San José, 7 de marzo, 2021

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 2020 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 TI-2020.

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: 2021.04.19 09:25:23 -06'00'

Lic. Esteban Murillo Delgado
Contador Público Autorizado N° 3736
Póliza de Fidelidad No. 0116 FIG 7
Vence el 30 de setiembre del 2021

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

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 2020.

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.
- Seguimiento al nivel de implementación de las recomendaciones emitidas en auditorías de períodos anteriores.
- 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. RESULTADOS

La aplicación de buenas prácticas y estructura de responsabilidad de las áreas establecidas para la administración de los recursos tecnológicos implementados en las Instituciones se deben basar en una serie de atributos que apoyan su adecuada gestión.

La Unidad de Tecnología de Información entiende su relación con la institución y se esfuerza por mantener la adecuada operación de los servicios tecnológicos básicos.

Como resultado de esta evaluación, a continuación se presenta el nivel de implementación de las recomendaciones emitidas en informes de auditoría externa de períodos anteriores:

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.

Responsable: Dirección Servicios de Apoyo a la Gestión.

Estado: Pendiente.

2019.2 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

Estado: Atendida. Fue incluido en el PETIC 219-2023.

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)

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

Estado: Pendiente.

Consideraciones: El plan de Infraestructura sigue la línea de tiempo establecida para el PETIC y contiene al menos de los datos indicados en la recomendación para cada elemento de infraestructura: cantidad, años vida útil, nivel de criticidad, servicio que atiende, el período de ejecución (puede ser seccionado en trimestres), tipo de gestión (adquisición, renovación, mantenimiento, desecho, cambio, etc.), estado y observaciones generales según aplique.

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.

Estado: Aplicación parcial, ya que solo se ha definido para proyectos.

Consideraciones: El plan de inversiones sigue también la línea de tiempo establecida para el PETIC, de forma tal que permite poder establecer la previsión de fondos para responder a las inversiones. Considera en detalle la respuesta financiera a las necesidades establecidas en el plan de infraestructura. Puede considerarse trabajar con un plan consolidado, incorporando más detalle de inversión en el plan de infraestructura, tales como inversión estimada, partida asociada, relación con proyecto/iniciativa

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.

Responsable: Dirección Ejecutiva.

Estado: Pendiente.

Consideraciones: Para disponer de la formalidad requerida, las funciones específicas asociadas a TI deben estar incluidas en el funcionamiento del equipo directivo.

2019.4 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.

Estado: Pendiente.

Consideraciones: El plan debe contener curso/actividad de actualización, fecha estimada, costo estimado, nombre de participantes.

2019.5 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.

Estado: Pendiente.

2019.6 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.

Estado: Pendiente.

2019.7 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.

Estado: Pendiente.

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.

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

Estado: Pendiente. Se realizó una identificación inicial de la necesidad de su disponibilidad en el PETIC.

Consideraciones: El modelo de arquitectura empresarial considera cuatro componentes (puede usarse como referencia el Marco TOGAF/Cobit 2019 APO03), siendo recomendable en primer instancia identificar los procesos institucionales (capa 2), asociarle los sistemas de información que utilizan para su operativa (capa 3), la infraestructura que soporta la operativa (capa4) - servidores, sistemas operativos, administradores de bases de datos, comunicaciones, utilitarios, etc.- ligándolos a los sistemas de información y luego, validando contra la estructura de las bases de datos asociar los datos e información a los procesos (capa 1). Este modelo se representa gráficamente, utilizando herramientas funcionales para estos fines. Los lineamientos asociados a la administración de este modelo deben incorporar los estándares de modelado, simbologías, entre otros. Adicionalmente, debe establecer qué eventos hace que se active la necesidad de actualizar el modelo (incorporación/eliminación de componentes de cada capa, considerando actualización de la gestión de la organización, uso de sistemas de información e infraestructura tecnológica) lo que puede asociarse a la estrategia e iniciativas relacionadas.

2019.9 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.

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.

Responsable: Dirección Servicios de Apoyo a la Gestión.

Estado: Pendiente.

Consideraciones: Para disponer de estas prácticas se recomienda seleccionar un Marco y valorar las actividades por etapa que se adecúen a la institución, levantar los documentos base para respaldar el proceso (estudio de factibilidad, conformación de equipo de trabajo y roles asociados, acta constitutiva, presupuesto, plan de trabajo, plan de calidad, cierre, entre otros).

2019.11 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.

Estado: Atendida. Se levantó el inventario de infraestructura tecnológica.

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.

Responsable: Encargado de TI.

Estado: Pendiente.

Consideraciones:

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.

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

Estado: Pendiente.

Consideraciones:

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.

Responsable: Encargado de TI.

2019.15 Considerar en los lineamientos la definición de las especificaciones y requerimientos técnicos cuando sea requerida la adquisición e implementación de recursos tecnológicos.

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

Estado: En proceso.

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.

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

Estado: En proceso.

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. 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.

Estado: En proceso.

2019.18 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.

Estado: Atendida.

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.

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

Estado: Pendiente.

Consideraciones: La clasificación de datos entre otros incorpora su categorización (público, restringido, confidencial, etc.); el proceso que es responsable de su recopilación, registro, procesamiento, resguardo, eliminación; período de vigencia de forma tal que pueda establecerse términos de almacenamiento y desecho.

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.

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

Estado: Pendiente.

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.

Responsable: Encargado de RRHH y Encargado de TI.

Estado: Pendiente.

2019.22 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.

Estado: Pendiente.

2019.23 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.

Estado: Pendiente.

2019.24 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.

Estado: Pendiente.

2019.25 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.

Estado: Pendiente.

2019.26 Establecer los niveles formales de propiedad, custodia y responsabilidad sobre los recursos de TI instalados en la organización.

Responsable: Encargado de TI.

Estado: Pendiente.

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.

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

Estado: Pendiente.

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.

Responsable: Encargado de TI.

Estado: Pendiente.

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.

Responsable: Encargado de TI.

Estado: Pendiente.

2019.30 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.

Estado: Pendiente.

2019.31 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

Estado: Pendiente.

2019.32 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.

Estado: Pendiente.

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.

Responsable: Dirección Servicios de Apoyo a la Gestión.

Estado: Pendiente.

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.)

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

Estado: Pendiente.

Consideraciones: Recopilar las regulaciones y legislación pertinentes, coordinar con la asesoría legal las acciones a seguir.

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.

Responsables Dirección Servicios de Apoyo a la Gestión.

Estado: Pendiente.

2019.36 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.

Responsable: Encargado Auditoría Interna.

Estado: Pendiente.

2019.37 Establecer prácticas formales para el seguimiento sobre el nivel de cumplimiento de recomendaciones realizadas al área de TI.

Responsable: Encargado Auditoría Interna.

Estado: Pendiente.