27 de marzo del 2023
911-AI-2023-0913

SERVICIO PREVENTIVO DE ASESORIA

Señora
Adirman Miranda Mejía
Directora
Sistema de Emergencias 9-1-1

Cordial Saludo:

Asunto: Servicio Preventivo de Asesoría, acerca de aspectos mínimos que debe llevar un Marco de Gestión de TICs para fortalecimiento del SCI Institucional.

El servicio preventivo de asesoría, consiste en proveer a la Administración Activa (fundamentalmente al jerarca, aunque no de manera exclusiva, según determine el Auditor) criterios, opiniones, sugerencias, consejos u observaciones en asuntos estrictamente de la competencia de la Auditoría Interna, con la intención de que se conviertan en insumos para la administración activa, que le permitan tomar decisiones más informadas y con apego al ordenamiento jurídico y técnico, sin que se menos caben o comprometan la independencia y la objetividad de la Auditoría Interna en el desarrollo posterior de sus demás competencias. El servicio se suministra a solicitud de parte o por iniciativa del Auditor Interno. Una vez brindada, las manifestaciones que el Auditor realice mediante ella no tienen carácter vinculante, puesto que es un insumo entre varios para la toma de decisiones.

Es importante indicar que para brindar la presente Asesoría, implica realizar observaciones que previenen lo que legal, administrativa y técnicamente corresponde a un asunto determinado y se brinda a las autoridades correspondientes, que según lo manifestado por la Contraloría General de la República, este tipo de asesorías, se realiza en el entendido que se dan elementos de juicio para la preparación y formación de la voluntad administrativa y además está asesoría no compromete la independencia y objetividad en el desarrollo posterior de ese proceso en cuanto a las demás competencias que la Auditoría puede y debe ejercer en su papel de fiscalizador.

TEMA ASESORADO

Sobre la herramienta trasladada al Coordinador de T.I. referente a la implantación del Marco de Gestión de Tecnologías de Información de T.I. Institucional, ante la derogatoria de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) derogadas por la Contraloría General de la República mediante la resolución N°R-DC-17-2020 del diecisiete de marzo del dos mil veinte, se recibió respuesta el día veintitrés de marzo del dos mil veintitrés, donde el Coordinador del Proceso, emite respuesta, lográndose identificar los grandes esfuerzos que ha realizado la Institución para cumplir con los requerimientos mínimos requeridos que debe contar el Marco de Gestión de T.I., aun así a pesar de que la Institución procura el fortalecimiento del Sistema de Control Interno, se identifican aspectos que no se han considerado y, que podrían repercutir en la materialización de algún riesgo, y por ende al logro de los objetivos institucionales.

Asimismo, la resolución N°R-DC-17-2020, nos expresa claramente en su punto 11 lo siguiente:

> *"…Que la gestión de las tecnologías de información y comunicación (TIC) forma parte relevante de los sistemas de gestión institucionales de las entidades y órganos del sector público costarricense, los cuales, a su vez, son componentes orgánicos del sistema de control interno institucional. Por ende, tanto la Contraloría General de la República* ***como las Auditorías Internas del sector público****, mantienen su potestad de auditoría sobre dicha gestión de las TIC; la primera, en función de lo establecido en el artículo 183 de la Constitución Política y en el Capítulo II de su Ley Orgánica, N° 7428; y las segundas, en función de los artículos 21, 22 y 33 de la Ley General de Control Interno, y el ítem 1.1.4 sobre Servicios de la Auditoría Interna, de las Normas para el ejercicio de la Auditoría Interna en el Sector Público, N° R-DC-064-2014 del 11 de agosto de 2014"* El resaltado no es del original.

En el orden de ideas, el MICITT ente rector en la materia, ha señalado lo siguiente:

> *"Siguiendo el proceso de implementación de las Normas Técnicas para el gobierno y gestión de Tecnologías de la información para las instituciones del estado fiscalizadas por la Contraloría General de la*

República, se ha diseñado este modelo de trabajo que le va a permitir documentar a cada institución su situación actual con respecto a aquellos relevantes referentes a su Marco de Gestión de T.I.

La información incluida en el perfil de cada una de las instituciones es para su uso propio, va a ser relevante y de valor para la implementación de la normativa, inclusive les puede servir de apoyo para procesos de auditoría…"

Siendo que la Dirección del Sistema de Emergencias, en su Oficio 911-DI-2021-5184 del 25 noviembre del 2021, señaló lo siguiente: "...*esta instancia aprueba la implementación a lo interno de la Institución de dichas normas, en un plazo de dos años a partir de enero del 2022*…"

A partir de esto ya han transcurrido catorce meses, se puede visualizar en la matriz que se detalla, realizada por el Coordinador de TICs que existen procesos donde todavía no se ha incursionado, otros se encuentran en fase de diseño, algunos en operación menos del 50% y por último otros operan en más de un 50%

III. COMPOSICIÓN DEL MARCO DE GESTIÓN Y DE LA GESTIÓN ACTUAL DE TI

Para esta sección se requiere que todas las instituciones, sea que ya tengan definido o no su Marco de Gestión de TI, indiquen si cuentan con los siguientes aspectos en su organización, implementados o en proceso de implementación. Estos son algunos de los aspectos mínimos con que debería contar un Marco de Gestión de TI.

Funciones o aspectos relevantes	Porcentaje implementación				
	No se tiene	En fase de diseño	En operación menos del 50%	En operación más de un 50%	Operando al 100%
a) Organización formal de una unidad de TI	x				
b) Plan estratégico de TI alineado al Plan Estratégico Institucional					x
c) Gestión de la Arquitectura de información	x				
d) Gestión de la calidad	x				
e) Gestión de activos de información			x		
f) Gestión de riesgos de TI			x		
g) Gestión de la seguridad de la información		x			
h) Gestión de la ciberseguridad	x				
i) Gestión de incidentes de TI				x	
j) Gestión de servicios de TI a sus clientes internos				x	
k) Gestión de la continuidad de servicios de TI			x		
l) Gestión de proyectos de TI	x				
m) Gestión del desarrollo o adquisición de aplicaciones y tecnologías				x	
n) Gestión de proveedores de TI	x				
o) Gestión del cumplimiento	x				
p) Gestión de redes de telecomunicación		x			

Fuente: Coordinador de TICs.

Según el portafolio de riesgos emitidos por el MICITT, ante una ausencia de los puntos anteriores se podrían materializar los siguientes riesgos, aunque se parte que no todos pueden que se den, esto debido a la naturaleza del negocio y a la actividad que se realice, a continuación, se mencionan:

RIESGO EN LA GESTION DE LA INFORMACION
Abuso de derechos por parte de los usuarios del sistema
Acceso no autorizado a aplicaciones por parte de los usuarios
Conformación inadecuada de contraseñas (insegura, débiles)
Uso compartido de contraseñas por parte de los usuarios
Robo o perdida de información por controles inadeacuados
Capacitación inadecuada a los usuarios del sistema en la forma de administrar los recursoa asignados
Confidencialidad de la información comprometida
Privacidad de la información comprometida
Problemas en el acceso a las aplicaciones
Integridad de la Información comprometida por usuarios internos
Integridad de la Información comprometida por accesos externos no autorizados
No hay disponibilidad de la información
Clasificación inadecuada de la información
Etiquetado onadecuado de la in formación
Robo o perdida de información por ataques de Hackers, Malware

Fuente: Portafolio Riesgos del MICITT

RIESGOS EN LA GESTION DE LA CONTINUIDAD
Mala identificación de los respaldos de información
Respaldos de información no verificados
Respaldos de información almacenados en forma incorrecta
Inadecuado traslado y custodia de los respaldos
Técnicas de recuperación/restauración de los archivos no estandarizada
Errores en el respaldo y recuperación de los datos.
Interrupción del servicio por falta de capacidad de almacenamiento o por fallas en los dispositivos de almacenamiento
Plan de continuidad o contingencia no documentado
Plan de continuidad o contingencia incompleto
Plan de continuidad o contingencia no probado
Plan de continuidad o contingencia no aprobado por las altas autoridades
Plan de continuidad o contingencia desactualizado
Personal interno poco preparado para enfrentar una contingencia
No se cuenta con suficiente personal para enfrentar una contingencia
Plan de continuidad o contingencia no comunicado a las partes interesadas
Robo o pérdida de medios de almacenamiento
Desastres naturales (terremotos, inundaciones, tornados, huracanes, etc.)
Incendio
Epidemia
Electromanetismo
Técnicas de recuperación/restauración de los archivos no estandarizada
Desorden civil
Acciones emprendidas por empleados inescrupulosos que pueden causar daños tanto a las instalaciones
Interrupciones prolongadas de los servicios básicos como la electricidad, el agua potable y las comunicaciones
Actos criminales, como vandalismo, terrorismo, etc.
Robo o pérdida de medios de almacenamiento

Fuente: Portafolio Riesgos del MICITT

RIESGOS EN LA GESTION DE LAS COMUNICACIONES
Fallas en la infraestructura tecnológica de los proveedores externos (ICE. RACSA, CNFL) que soporta la prestación de servicios, afectando la disponibilidad
Fallas en las comunicaciones debido problemas internos
Fallas por eventos que afecten las lineas de transmision internas o externas
Falta de disponibilidad en las lineas de comunicaciones
Fallas producidas por errores o problemas en la transmisión
Errores en la configuración de equipos de comunicaciones
Monitoreo inadecuado de las comunicaciones

Fuente: Portafolio Riesgos del MICITT

RIESGOS EN CENTROS DE DATOS
Falta de disponibilidad del personal técnico (SO, base de datos, comunicaciones, etc.)
No existe de un plan formal, actulalizado y comunicado formalmente para la recuperación de las aplicaciones
Fallas eléctricas en el centro de cómputo
Daños que se presenten en los equipos por vandalismo, uso inadecuado o fallas en la administración
Datos se replican en forma incorrecta
Fallas en el equipo de aire acondicionado, UPS o planta eléctrica
Controles inadecuados para el monitoreo, seguimiento y protocolos formales para atención y escalamiento de incidentes
Aplicaciones anticuados que no soportan la carga de trabajo, el volumen, las funcionalidades
Inadecuado mantenimiento de los sistemas
Reprocesos en las pruebas y atrasos en la implementación por no contar con una infraestructura para la realización de las pruebas técnicas
Dependencia de los proveedores para el suministro de servicios, repuestos o de mantenimientos a los equipos donde corren los sistemas críticos
Utilización incorrecta de los equipos de cómputo
Mal funcionamiento de una base de datos
Daño en una base de datos o archivos críticos
Problemas de acceso a una base de datos
Administración inadecuada de procesos de actualización
Falta de capacitación o capacitación iadecuada de los encaragados de los procesos de actualización
Falta de procedimientos o procedimientos inadecuados para la ejecución de tareas críticas
Controles deficientes en ambientes de pruebas
Controles deficientes en ambientes de producción
Falla en un servidor o varios a la vez
Pérdidas o suspensión temporal del servicio por una incorrecta configuración de parámetros en los sistemas
Errores en la configuración de equipos (servidores)
Mal diseño de las aplicaciones generando problemas de funcionamiento
Problemas en la distribución del cableado eléctrico o de comunicaciones
Insuficiente personal capacitado para realizar las tareas de operación, monitoreo y soporte de los servicios en producción
Afectación en la gestión ylos programas de trabajo porque no se realizron las pruebas de aceptación dentro del tiempo planificado
Inundación por daño de tuberías internas del edificio
Fallas producidas por errores de programación que afectan la calidad del servicio
Afectación del servicio por generación de incidentes y problemas asociados a una mala implementación de cambios
Afectación del servicio por no tramitar oportunamente un cambio requerido urgente
Reprocesos en las pruebas y atrasos en la implementación por integración de aplicaciones incompletas o erróneas
Pérdida de información producidas por fallas en los controles de seguridad
Pérdida de información por la inadecuada utilización de los equipos de cómputo
No contar con las condiciones ambientales recomendadas por el fabricante para la operación adecuada de los equipos
Pérdida de información por la inadecuada utilización de los sistemas en utilización en la Institución

Fuente: Portafolio Riesgos del MICITT

RIESGOS EN LA GESTION DE PROVEEDORES
Incumplimiento de contratos por parte del proveedor
Incumplimiento de contratos por parte de la Institución
Deficiencias en los servicios de los proveedores
No contar con proveedores que estén preparados para ayudar a enfrentar una contingencia de tipo tecnológico.
Alta dependencia de proveedores claves a nivel de tecnología para proporcionar los servicios
Contratos obsolectos
Fallas en la gestión de licenciamientos
Fallas en el control de vencimiento de los contratos
Inexistencia de contratos
Contratos no alineados a niveles de servicio (SLA)

Fuente: Portafolio Riesgos del MICITT

RIESGOS DE CUMPLIMIENTO
Incumplimiento por entrega de información incompleta a entes reguladores
Incumplimiento de la legislación vigente
Incumplimiento de normativas externas
Incumplimiento en las fechas de entrega de la información a entes reguladores
No contar con el apoyo de las altas autoridades
Insuficientes recursos (humanos, equipos, espacio físico, etc.) para trabajar en la implementación
No contar con una cultura de riesgos en la institución
Los responsables de TI no cuentan con el suficiente apoyo de las altas autoridades para realizar su gestión
No se cuenta con políticas institucionales para la gestión de TI

Fuente: Portafolio Riesgos del MICITT

RIESGOS EN SEGURIDAD DE LA INFORMACION
Incumplimiento de políticas de seguridad
Falta de capacitación y concientizacion en seguridad de la información
Políticas de seguridad no documentadas o estan desactualizadas
Normativas de seguridad no documentadas o estan desactualizadas
Controles de seguridad no documentadas o estan desactualizadas
Procedimientos de seguridad no documentadas o estan desactualizadas
Procesos de seguridad no documentados o estan desactualizadas
Ataques de denegación de servicios
No se actualiza en forma adecuada la plataforma tecnológica que atiende los servicios de Internet
Plataforma de seguridad mal atendida, monitoreo inadecuado de incidentes de seguridad
Capacitación inadecuada en ingeniería social
Perdida de equipos de cómputo (principalmente portátiles) sin la debida protección, con la consiguiente perdida de información confidencial).
Perfiles de acceso no definidos o mal congigurados
Red interna puede ser vulnerada por parte de cibercriminales
Gestión inadecuada en el parchado de aplicaciones o equipos

Fuente: Portafolio Riesgos del MICITT

Así mismo, según nos menciona el Coordinador de T.I. con el llenado del instrumento , la Institución no cuenta con personal dedicado a la seguridad de la información, con personal dedicado a la ciberseguridad, aspectos relevantes para el buen actuar de los procesos en Tecnologías de Información, que puedan brindar una seguridad razonable a la institución en cuanto al proceso de Tecnologías de Información y Comunicación (TICs) y al cumplimiento de los requerimientos mínimos con que debe de contar el Marco de Gestión de las TICs.

	Si	No	Cuántos
1. ¿La institución cuenta con personal dedicado a la seguridad de la información?		x	

1. a. ¿Este personal se encuentra capacitado? (Marque todas las que apliquen)	Si	No
		x

	Institucional Interno
	Institucional Externo
	Apoyado por el CSIRT Nacional del MICITT
	Personal (autodidacta)
	Personal (autofinanciado)

	Si	No	Cuántos
2. ¿La institución cuenta con personal dedicado a la ciberseguridad?		x	

2. a. ¿Este personal se encuentra capacitado?	Si	No
		x

Fuente: Coordinador de TICs.

La Administración debe valorar que al ser una Institución de Servicios de primera línea resulta indispensable el fortalecimiento de estos procesos, por lo que se debe prestar la atención requerida a los puntos que todavía aún no se han podido cumplir, otros se encuentran en una fase de implantación y otros apenas tienen el 50% de operación.

Partiendo que se debe mantener una continuidad razonable de los procesos, donde su interrupción no debería afectar significativamente a los usuarios del Sistema, por lo que se debería poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la institución, la evaluación e impacto de los riesgos según su criticidad.

Por lo consiguiente, la Administración debería optimizar el uso de los recursos financieros para la gestión de las TICs en procura del logro de los objetivos institucionales, en forma efectiva sobre dichos recursos y, así mismo al

cumplimiento del ordenamiento jurídico que al efecto le resulte aplicable, con el fin de garantizar la operación del Sistema razonablemente en este proceso.

En el mismo orden de ideas, las Normas Técnicas de Control Interno para el Sector público (N°2-2009-CO-DFOE) en el ítem 5.9 señala (reformada), para que se analicen de la siguiente manera:

5.9 Tecnologías de Información.

> *"El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance. En todo caso, deben instaurarse los mecanismos y procedimientos manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información En esa línea de conformidad con el perfil tecnológico de la institución, órgano o ente en función de su naturaleza, complejidad, tamaño, modelo de negocio, volumen de operaciones, criticidad de sus procesos, riesgos y su dependencia tecnológica el jerarca deberá aprobar el marco de gestión de tecnologías de información y establecer un proceso de implementación gradual de cada uno de sus componentes. Para la determinación del perfil tecnológico institucional se podrán considerar variables como las siguientes: marco de procesos para la gestión de TI, mapeo de procesos y subprocesos de negocio, organigrama de la entidad, conformación del Comité de TI, proveedores de TI, servicios de TI, inventario y criticidad de tipos documentales, centros de procesamiento y almacenamiento de datos, inventario de equipos y sistemas de información que soportan los servicios, software, proyectos de TI, planes de adquisición sobre TI, canales electrónicos y riesgos de TI".*

CONCLUSIONES

Las observaciones emitidas en la presente asesoría se emiten con la intención de que se conviertan en insumos para la administración activa. Además, se aclara que, la asesoría no es un estudio donde se profundiza y revisa la normativa, sino que, es un insumo para que la administración activa pueda tomar decisiones más informadas y con apego al ordenamiento jurídico, técnico y a las sanas prácticas, sin que se menoscaben o comprometan la independencia y la objetividad de la Auditoría Interna en el desarrollo posterior de sus demás competencias.

Se solicita respetuosamente, que le indique a este ente fiscalizador en un plazo no mayor a diez días, las acciones que la administración realizará con respecto al tema asesorado.

Atentamente,
Auditoría

PEDRO MIGUEL JUAREZ GUTIERREZ (FIRMA)

Firmado digitalmente por PEDRO MIGUEL JUAREZ GUTIERREZ (FIRMA)
Fecha: 2023.03.27 14:58:32 -06'00'

Pedro M. Juárez Gutiérrez
Auditor Interno

PJG/pjg

🗁: secretarias
Coordinador T.I.
Archivo de gestión