INSTITUTO COSTARRICENSE DE TURISMO

Auditoría Interna

25 de febrero de 2019
AI-Ad-007-2019

Señor
Alberto López Chaves
Gerente

Asunto: *Servicio preventivo sobre el plan de continuidad del negocio del ICT*

Estimado señor:

En cumplimiento del Plan Anual de Trabajo, la Auditoría evaluó el plan de continuidad del negocio institucional, con la finalidad de comprobar si se encuentra actualizado, implementado y debidamente probado.

El estudio determinó lo siguiente:

1. En el año 2015[1] la Junta Directica aprobó el plan de continuidad institucional y solicitó a la Gerencia su implementación y seguimiento.
2. La última actualización del plan de continuidad fue el 4 junio del 2015 (4 años desactualizado).
3. El administrador del plan de continuidad del negocio es el Sr. Roy Rojas Chaves y el Líder del plan es el Sr. Alberto López Chaves, Gerente General.
4. A la fecha no se han realizado pruebas al plan de continuidad.
5. La institución no cuenta con un sitio alterno para la recuperación de la información.

Al respecto, el Plan de Continuidad del Negocio, establece en sus políticas que al menos una vez al año se deberá actualizar lo siguiente:

- El análisis de impacto de negocio
- El análisis de riesgo
- Estrategias de continuidad de tecnología.

Además, establece que “al menos una vez al año el Administrador de continuidad de negocio establecerá pruebas en las cuales se considerará la totalidad de los procedimientos críticos definidos en el BIA.” Igualmente, indica que “el Administrador de continuidad de negocio establecerá el calendario de educación y entrenamiento del proceso de continuidad de negocio anualmente.”

[1] Comunicado de acuerdo SJD 196-2015 (04-06/2015)

De igual forma menciona que “el administrador de la continuidad de negocio es responsable de actualizar los repositorios físicos y lógicos la información correspondiente al Plan de continuidad de negocio.”

Por su parte, la norma 1.4.7 “Continuidad de los servicios de TI” de las NTGCTI[2] indica que “la organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y 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 organización”.

Por otra parte, y como mejor práctica, COBIT 5 en el punto DSS04.04 “Ejercitar, probar y revisar el BCP”, indica que se debe “probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera”.

Asimismo, la práctica de gestión en el punto DSS04.05 “Revisar, mantener y mejorar el plan de continuidad” menciona que se debe “realizar una revisión por la Dirección de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad” así como “gestionar los cambios en el plan de acuerdo al proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio”.

La razón por la cual el ICT no cuenta con el plan de continuidad de negocio actualizado y probado , se debe a que la Institución ha orientado sus esfuerzos a determinar y finiquitar un sitio alterno del Comité de Crisis, dado que estratégicamente resultaba de prioridad contar con este espacio físico, lo que permitirá completar totalmente los requerimientos de recursos para que este comité pueda operar eficazmente y posterior a esto se tiene previsto para el 2019, realizar pruebas correspondientes, una vez finalizado el equipamiento tecnológico propio o tercerizado, según lo indicado por la Gerencia.

[2] Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CODFOE) emitidas por la CGR.

La situación determinada, podría provocar que:

- En caso de desastre[3] el ICT no esté preparada de forma integral para minimizar los efectos de una interrupción de actividades, servicios críticos, ni se protejan bienes y equipos prioritarios de la institución.
- Pérdida de información financiera y operativa y documentación valiosa para el ICT.
- Pérdidas de recursos humanos y económicos.

Por la competencia que le asiste a la Gerencia como administrador general, jefe superior de la Institución y responsable del eficiente y correcto funcionamiento administrativo del Instituto, se advierte sobre lo determinado en el estudio en relación con el plan de continuidad del negocio del ICT, con la finalidad de que valore sobre si el no contar con acciones específicas para revisar, probar y mantener actualizado el plan de continuidad del negocio del ICT, contribuye a contar con una herramienta que garantice razonablemente la continuidad de los servicios en caso de incidentes

Se solicita a ese Despacho, informar a esta Auditoría Interna dentro de los próximos diez días hábiles, sobre las acciones tomadas en relación con este servicio preventivo, a efecto de determinar lo procedente.

El presente servicio preventivo se realiza con fundamento en las competencias conferidas a la Auditoría Interna en la Ley Orgánica del ICT, el inciso d) del artículo 22 de la Ley General de Control Interno, la norma 1.1.4 de las “Normas para el Ejercicio de la Auditoría Interna en el Sector Público” y en atención del Plan Anual de Trabajo.

Atentamente,

FERNANDO JOSE RIVERA SOLANO (FIRMA)

Firmado digitalmente por FERNANDO JOSE RIVERA SOLANO (FIRMA)
Fecha: 2019.03.04 12:35:46 -06'00'

Fernando Rivera Solano
Auditor Interno

C. Consecutivo
FRS / kbm

[3] Desastre: Incidente que puede ser anticipado (ejemplo huracanes) o no anticipado (ejemplo falla del fluido eléctrico, terremoto, ataque a la infraestructura de TI) que interrumpe el curso normal de las operaciones de la organización.