Instituto Costarricense de Turismo

Auditoría Interna

21 de junio de 2018
AI-P-Ad-09-2018

Dr. Alberto López Chaves, MBA.
Gerente

Asunto: Servicio Preventivo sobre la gestión de la seguridad de la información Institucional

Estimado señor:

En cumplimiento del Plan Anual de Trabajo, esta Auditoría Interna analizó la gestión de la seguridad de la información en el ICT, con el objetivo de corroborar que se garantiza de manera razonable la confidencialidad, integridad y disponibilidad de la información institucional, que contribuya a fortalecer y apoyar el cumplimiento de los objetivos institucionales.

El estudio determinó que la Institución cuenta con "Políticas en Tecnologías de Información[1]" y procedimientos, dentro de este compendio existen políticas de seguridad para el Departamento de TI, pero carece de un sistema de gestión de la seguridad de la información a nivel institucional.

Al respecto, la norma 1.4 "Gestión de la seguridad de la información" de las NTGCTI[2] indica que la organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales. Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos.

Asimismo, la norma 1.4.1 del mismo cuerpo normativo estipula lo siguiente:

[1] Actualizadas y aprobadas por acuerdo de Junta Directiva SJD-333-2013, sesión 5808 del 30 de julio del 2013

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

"La organización debe implementar un marco de seguridad de la información[3], para lo cual debe:

a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI[4], según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.
b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.
c. Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados. y considerar lo que establece la presente normativa en relación con los siguientes aspectos: La implementación de un marco de seguridad de la información"

Por otra parte, y como mejor práctica, el COBIT 5 en el punto APO013 "Gestionar la Seguridad", indica que "… se debe definir, operar y supervisar un sistema para la gestión de la seguridad de la información".

Además, también como mejor práctica, la norma ISO 27001, indica en el punto 5, que "la gerencia debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del Sistema de Gestión de la Seguridad de la Información (SGSI) al establecer una política de seguridad, asegurar que se establezcan objetivos y planes del SGSI, establecer roles y responsabilidades para la seguridad de la información."

La ausencia de un sistema de gestión de la seguridad de la información se debe a que el ICT no ha promovido las acciones necesarias para implementarlo, lo que puede exponer a la institución a que:

- No se garantice que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por el ICT de una forma

[3] Conjunto de componentes asociados a la gestión de la seguridad dentro de los cuales cuentan, entre otros: Principios y términos definidos para un uso uniforme en la organización; un sistema de gestión que implica la definición de actividades, productos y responsables del proceso de definición, implementación y seguimiento de acciones para la seguridad de la información; el conjunto de controles; las guías de implementación; métricas para seguimiento y la consideración de riesgos.
[4] Aplicaciones, información, infraestructura (tecnología e instalaciones) y personas que interactúan en un ambiente de TI de una organización.

documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

- No se identifiquen vulnerabilidades por uso indebido de información, alteración o pérdida de esta; sabotajes; fraudes, entre otros.

Por la competencia que le asiste a esa Gerencia, como administrador general del Instituto, responsable del eficiente y correcto funcionamiento administrativo, se comunica sobre lo importante que el ICT cuente con un sistema de gestión de la seguridad de la información institucional, que involucre a todas las dependencia con recursos de TI (aplicaciones, información, infraestructura y personas) y que contemple, al menos, lo mínimo establecido en la normativa, con la finalidad que contribuya a proteger los recursos de TI y garantizar la confidencialidad[5], integridad[6] y la disponibilidad[7] de la información.

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 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: 2018.06.22 08:20:20 -06'00'

Fernando Rivera Solano
Auditor Interno

FRS / kbm
C. Licda. Karen Hernández
Departamento de TI
Lic. Sergio Lira Valdivia
Jefe Departamento de TI
Consecutivo

[5] Protege los activos de información contra accesos o divulgación no autorizados.
[6] Garantiza la exactitud de los activos de información contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
[7] Se vincula con el hecho de que la información se encuentre disponible (v.gr. utilizable) cuando la necesite un proceso de la organización en el presente y en el futuro. También se asocia con la protección de los recursos necesarios y las capacidades asociadas. Implica que se cuente con la información necesaria en el momento en que la organización la requiere.