INSTITUTO COSTARRICENSE DE TURISMO

Auditoría Interna

16 de mayo de 2022
AI-Ad-12-2022

Señor:
Alberto López Chaves
Gerente

Asunto: *Servicio Preventivo sobre posibles vulnerabilidades no detectadas.*

Estimado señor:

La Auditoría en cumplimiento del Plan Anual de Trabajo, analiza la situación que puede enfrentar el ICT ante un posible ataque informático, obteniéndose el resultado siguiente:

Condición:

La Auditoría en el 2019[1] realiza el análisis de vulnerabilidades sobre la infraestructura tecnológica[2] interna y externa de la institución, tiempo en el cual la tecnología de información ha cambiado radicalmente, así como, vulnerabilidades explotadas por los ciberdelincuentes.

El Departamento de TI[3] ha realizado acciones tendientes a fortalecer las medidas de seguridad existentes en la Institución, asimismo, solicita a la Gerencia recursos adicionales para hacer frente a posibles ataques cibernéticos, sin embargo no incluye actividades o recursos para los eventos siguientes:

- Evaluar rastros de comportamiento extraño o malicioso en la red que exista y no se hayan detectado por medio de pruebas de penetración o pentest.
- Análisis de vulnerabilidades de los equipos y la red interna y externa, además de las que ya se realizan con el “Forticlient”

[1] AI-C-10-2019 Informe de la auditoría de cumplimiento sobre la seguridad de la red, bases de datos, configuraciones y web del ICT (11-12-2019).
[2] Activos de información de la plataforma tecnológica donde figuran servidores, bases de datos, equipos de comunicación y equipos de usuario final, además, del sistema integrado de recursos humanos, planillas y pagos (SIRH)
[3] DTI-090-2022 del 04-05-2022Requerimientos para fortalecer la seguridad e integridad de la información instituciona

- Fraudes que se hayan realizado o se estén realizando, por página web, redes sociales, aplicaciones móviles, etc., principalmente para el equipo que no está en la institución.
- Verificar información expuesta -metadatos- en documentos publicados en la web o la red, que contengan datos sensibles en la información interna.
- Verificar posibles robos de contraseñas que no se han detectado.
- Directorios mal publicados.
- Pruebas de penetración.
- Solucionar las vulnerabilidades que presenta SIRH, que es un sistema que ha sido vulnerado en otras instituciones, aunque de momento está aislado de la red interna.

Criterio:

COBIT 2019 en la práctica de gestión “DSS05.02 Gestionar la seguridad de la conectividad”, actividades 7 y 8 indica que se deben hacer pruebas periódicas de penetración y de la seguridad del sistema para determinar la idoneidad de la protección del sistema y la red.

Causa:

Las acciones realizadas y planeadas por el Departamento de TI, si bien es cierto, mejoraran la protección de la seguridad de la información institucional, no incluyen recursos para pruebas de penetración y análisis de vulnerabilidades que permitan fortalecer aún más la seguridad de la configuración, ataques más sofisticados y la revisión de rastros de comportamientos, por posibles infiltraciones de atacantes no detectados.

Efectos

Se pueden materializar los riesgos siguientes:

- Pérdida de confiabilidad, disponibilidad e integridad de la información por actuaciones de software malicioso no detectado.
- Seguridad de la red comprometida por omisión en la configuración.
- Pérdida de disponibilidad de los sistemas por explotación de vulnerabilidades no detectadas.
- Exposición de la información de los sistemas de información.
- Posibles demandas por parte de la ciudadanía por la exposición de información sensible.

Auditoría Interna

- Posibles daños financieros, operativos y reputacionales a la Institución.

La Ley Orgánica, artículo 32, establece que el Gerente es el responsable del eficiente y correcto funcionamiento administrativo de la Institución y debe ejercer las funciones inherentes a su condición de administrador general y jefe superior del Instituto, vigilando la organización, funcionamiento y coordinación de todas sus dependencias y la observación de las leyes, reglamentos y resoluciones de la Junta Directiva, razón por la cual, se comunica lo determinado sobre la situación que puede enfrentar el Instituto **ante un posible ataque cibernético que no sea detectado por los recursos actuales ni por los requeridos por el Departamento de TI**, con el propósito de que se tomen las acciones pertinentes y gestionar al menos los riesgos identificados en este servicio preventivo.

Se solicita 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.

Atentamente,

Firmado por FERNANDO JOSE RIVERA SOLANO (FIRMA)
PERSONA FISICA, CPF-03-0226-0040.
Fecha declarada: 16/05/2022 08:00 AM
Esta representación visual no es fuente
de confianza. Valide siempre la firma.

Fernando Rivera Solano
Auditor Interno

C. Sra. Karen Hernández Bonilla
Consecutivo
FRS/kbm