INSTITUTO COSTARRICENSE DE TURISMO

Auditoría Interna

6 de mayo de 2022
AI-Ad-11-2022

Señor:
Alberto López Chaves
Gerente

Asunto: *Servicio Preventivo sobre la seguridad de la información Institucional ante un posible ataque cibernético*

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 diciembre de 2019[1] recomienda a la Gerencia, tomar las medidas necesarias para solventar las vulnerabilidades y riesgos relacionados con el acceso no autorizado desde la infraestructura externa del ICT y, a los sistemas críticos de la red interna como usuario interno o criminal cibernético, así como a la configuración de los puntos de acceso de la red inalámbrica institucional, además de la configuración de equipos que permitan reducir el ataque de los activos.

Las recomendaciones están en proceso de implementación según la Administración por falta de recursos y se tiene previsto implementarlas hasta el 31-12-2022, plazo que fue definido antes de presentarse la situación actual sobre los ataques cibernéticos.

El Departamento de TI[2] realiza medidas adicionales para resguardar la información institucional, además, indica que prepara una propuesta a la Gerencia para la adquisición de dispositivos para blindar aún más la plataforma tecnológica con

[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] DTI-083-2022

nuevas arquitecturas relacionadas con los servicios en la nube y actualización de dispositivos, por lo que necesitan ampliar el presupuesto del departamento, así como, establecer mecanismos de contratación ágiles y eficientes.

El Departamento de TI cuenta con presupueto para la operación normal, pero no cuenta con recursos específicos adicionales para hacerle frente a un posible ataque cibernético.

La Gerencia emite circular[3] referente a la *"actualización y seguimiento de riesgos 2022"*, solicitando incluir los nuevos riesgos que se requieran de acuerdo a la realidad institucional, **aunque no especifíca gestionar los posibles riesgos cibernéticos que puedan afectar la información que las unidades manejan.**

Criterio:

La Directriz[4] del Gobierno de la Republica y el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones sobre las mejoras en materia de ciberseguridad instruyen a la Administración Pública Central e insta a la Administración Pública Descentralizada a:

- Cumplir con las recomendaciones y medidas técnicas referentes a la mejora de las capacidades técnicas, de atención y de gestión de la ciberseguridad y seguridad de la información que emita el MICITT.
- Promover de manera inmediata las acciones que favorezcan la resiliencia de la infraestructura tecnológica[5] que incluya como mínimo:
    - Actualizaciones permanentes de todos los sistemas institucionales.
    - Cambiar contraseñas de todos los sistemas institucionales (correos electrónicos, sistemas operativos, servidores, VPN, redes sociales, entre otros posibles).
    - Deshabilitar servicios y puertos no necesarios y monitorear la infraestructura de red, con el fin de garantizar que los eventos adversos relacionados con incidentes de ciberseguridad sean detectados, registrados y gestionados de forma que se pueda limitar el impacto de los mismos en cada institución o entidad.

[3] G-1578-2022 del 26/04/2022
[4] Directriz N° 133- MP-MICITT del 21/04/2022
[5] Propia o contratada de manera total o parcialmente

- Autorizar a los equipos de TI, CSIRTs[6] internos o grupos que se hayan creado para atender la ciberseguridad institucional, para que asistan a las actividades de formación, capacitación, u otra actividad que organice el MICITT relacionada con la atención y mejora en las capacidades de ciberseguridad y seguridad de la información.
- Informar al CSIRT-CR[7] sobre los incidentes que afecten la confidencialidad, disponibilidad e integridad de servicios disponibles al público, o la continuidad de las funciones institucionales, o la suplantación de identidad de la institución en redes sociales, incluyendo los incidentes que a lo interno de la institución se consideren bajo control, además, de respaldar la información referente al incidente acontecido, para las investigaciones correspondientes.
- Informar al CSIRT-CR todos los dominios de sus sitios web con el fin de hacer un levantamiento de los sitios oficiales de las instituciones del Estado para generar y validar los sitios web oficiales de sus instituciones, para incluirlos dentro del validador de sitios oficiales de gobierno[8], con la finalidad de prevenir las acciones de suplantación y phishing contra las instituciones.
- Los sitios web reportados se le realizará al menos dos veces al año, un análisis de vulnerabilidades que se remitirá al contacto de ciberseguridad para que realicen las correcciones y acciones correspondientes, de conformidad con el resultado de este análisis, para disminuir el riesgo de sus sitios web públicos.

Causas:

a. Ataques a la infraestructura tecnológica en diferentes instituciones públicas y privadas[9].
b. Reducción presupuestaria al Departamento de TI en los años 2020 y 2021 producto de la pandemia y la aplicación de la regla fiscal.
c. No se ha alertado a todas las unidades que se debe gestionar el riesgo cibernético, ya que no es un riesgo exclusivo de TI.

Efectos

Se pueden materializar los riesgos siguientes:

[6] Centro de Respuesta de Incidentes de Seguridad Informática Institucionales
[7] Centro de Respuesta de Incidentes de Seguridad Informática de Costa Rica
[8] https://sitiosoficiales.gob.go.cr/
[9] Malware, virus, gusanos, troyanos, Spyware, ransomware, phishing, etc.

- Intrusión no autorizada a los diferentes servicios y componentes de la plataforma tecnológica de la institución y tercerizadas.
- Posibles demandas por parte de la ciudadanía por la exposición de información sensible vulnerada.
- Que la integridad de la información se vea comprometida porque usuarios externos o internos no autorizados tengan acceso.

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, con el propósito de que se tomen las acciones pertinentes y gestionar al menos los riesgos (efectos) 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: 06/05/2022 01:45 PM
Esta representación visual no es fuente
de confianza. Valide siempre la firma.

Fernando Rivera Solano
Auditor Interno

C. Sra. Karen Hernández Bonilla, Departamento de TI
Sr. Víctor Quesada Rodríguez, UPI.
Consecutivo
FRS/kbm