INSTITUTO COSTARRICENSE DE TURISMO

Auditoría Interna

16 de junio de 2022
AI-Ad-14-2022

Señor
Alberto López Chaves
Gerente

Asunto: *Servicio Preventivo sobre la gestión de riesgos sobre ciberataques y supervisión continua del control interno*

Estimado señor:

La Auditoría en cumplimiento del Plan Anual de Trabajo, analiza si se han comunicado a la Junta Directiva riesgos relacionados con los ciberataques que está viviendo el país y si existen eventos catalogados como catastróficos y emergentes. Además, se revisa si hay una supervisión continua por parte de los responsables sobre el cumplimiento de las actividades de control para mitigar los riesgos y se obtienen los resultados siguientes:

1. Gestión de riesgos por ciberataques, catastróficos y emergentes

Condición

La Gerencia no ha comunicado a la Junta Directiva:

a) Posibles riesgos relacionados con la emergencia que está viviendo el país sobre los ciberataques y que pueden afectar negativamente el logro de los objetivos institucionales.

b) Si en este año existen riesgos en nivel catastrófico u otros riesgos emergentes que requieran acciones inmediatas y que por su magnitud y cuantía deban ser analizados a nivel de Junta Directiva.

Criterio

El Gobierno de la República el 8 de mayo declara estado de Emergencia Nacional por los ciberataques que han afectado los sistemas de información de varias instituciones del país.

Auditoría Interna

La Política de valoración del riesgo institucional[1], establece que la Unidad de Planificación informará con una frecuencia proporcional a la gravedad y prioridad del riesgo, de manera que permita determinar el riesgo asumido, su pertinencia y la idoneidad de las medidas adoptadas o propuestas.

Los parámetros de aceptabilidad de riesgos[2] indican que los riesgos con nivel catastrófico deben contener medidas propuestas por el Director de la unidad que gestiona el riesgo y el visto bueno de la Junta Directiva.

La actividad de revisar los riesgos[3] de forma continua tiene como finalidad que la información que se genere sirva de insumo para los reportes de riesgos, ajustar las medidas para su administración y evaluar y ajustar los objetivos y metas institucionales en caso de requerirse.

Causa

La Gerencia y la UPI han seguido con la costumbre de solicitar a las unidades registrar y actualizar la información de riesgos y el seguimiento a las medidas propuestas con una fecha límite, por lo que las unidades realizan el ejercicio de riesgos de forma reactiva ante dicha solicitud y no como una actividad permanente o continua según lo estable el MOGERI.

Efecto

Las condiciones determinadas pueden provocar que las medidas propuestas por el Director para mitigar riesgos catastróficos pueden que:

a) No sean suficientes para la Junta Directiva lo que dejaría el riesgo descubierto y con un alto grado de ocurrencia.
b) No disponer de forma oportuna de los recursos necesarios para atención adecuada.

Lo anterior puede incidir que se materialicen riesgos valorados como catastróficos o los emergentes, por lo tanto, afectaría el cumplimiento de los objetivos del área o a nivel institucional.

[1] MOGERI, Prioridad vi)
[2] MOGERI, Resultado de la evaluación.
[3] Actividad Revisión de riesgos Procedimiento del SEVRI

2. Supervisión continua del control interno

Condición

La Gerencia no está realizando una supervisión continua del sistema de control interno durante el curso normal de las operaciones, que permita comprobar el cumplimiento de las actividades de control incorporadas en los procesos para mitigar los riesgos.

Criterio

La Ley General de Control Interno establece que los funcionarios responsables realicen continuamente las acciones de control y prevención en el curso de las operaciones normales integradas a tales acciones[4].

Las Normas de Control Interno para el Sector Público disponen que las actividades de seguimiento del SCI, deben incluir la comprobación durante el curso normal de las operaciones, del cumplimiento de las actividades de control incorporadas en los procesos[5] y que los funcionarios dentro de su labor cotidiana, deben observar el funcionamiento del SCI[6] con el fin de determinar las desviaciones en su efectividad, e informarlas oportunamente a las instancias correspondientes.[7]

El MISCI[8] establece que la Gerencia debe ejercer la supervisión del SCI, entre otras, mediante evaluaciones continuas, definir la frecuencia y el alcance considerando el ritmo de cambio en la Institución y en los procesos de negocio, éstas constituyen operaciones rutinarias, que se integran en los procesos y se realizan en tiempo real, para responder ante un entorno cambiante.

Causa

El Modelo Institucional del Sistema de Control Interno (MISCI) es aprobado[9] en junio de 2021; sin embargo a esta fecha la Administración no ha definido la frecuencia y

[4] Artículo 17, Seguimiento del sistema de control interno, inciso a)

[5] 6.3 Actividades de seguimiento del SCI inciso a).

[6] Componentes SCI: Ambiente de control, Valoración de Riesgo, Actividades de Control, Sistemas de Información y Seguimiento.

[7] 6.3.1 Seguimiento continuo del SCI.

[8] Principio 16, Punto Enfoque 16.1, documento probatorio.

[9] SJD-189-2021 del 15/6/2021, sesión del 14/6/2021.

el alcance de las evaluaciones continuas -en tiempo real-, ni éstas se han integrado en los procesos considerando el ritmo cambiante, el entorno, los riesgos y controles institucionales, según lo establece el MISCI en el principio 16, con el fin de determinar las desviaciones de su efectividad y comunicarlas de forma oportuna a las instancias correspondientes.

Efecto

La condición determinada puede provocar que al no revisarse de forma continua los controles:

a) los niveles de riesgo pueden aumentar debido a que los controles no surtan el efecto esperado.
b) algunos riesgos pueden no ser identificados.
c) que no existan controles asociados a algunos riesgos.

Lo anterior puede incidir que los controles no sean efectivos para mitiguen los riesgos, que éstos se materialicen, por lo tanto, afectaría el cumplimiento de los objetivos del área o a nivel institucional.

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:

a) La comunicación a la Junta Directiva por parte de la Unidad de Planificación y la Gerencia sobre los posibles riesgos por ciberataques que pueda enfrentar el ICT, según lo establece el MOGERI.

b) Los riesgos de nivel catastrófico y emergentes que requieren acciones inmediatas.

c) La frecuencia y alcance de las evaluaciones continuas al Sistema de Control Interno.

Se comunica lo anterior**,** con el propósito de que se tomen las acciones pertinentes y gestionar al menos los riesgos identificados en este servicio preventivo.

INSTITUTO COSTARRICENSE DE TURISMO

Auditoría Interna

Se solicita a la Gerencia, 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, artículos 33 y 35, la Ley General de Control Interno, artículo 22, inciso d), las “Normas para el Ejercicio de la Auditoría Interna en el Sector Público”, norma 1.1.4 y en atención del Plan Anual de Trabajo.

Atentamente,

Firmado por FERNANDO JOSE RIVERA SOLANO (FIRMA) PERSONA FISICA, CPF-03-0226-0040.
Fecha declarada: 16/06/2022 02:07 PM
Esta representación visual no es fuente de confianza. Valide siempre la firma.

Fernando Rivera Solano
Auditor Interno

C. Junta Directiva ICT
Sr. Víctor Quesada Rodríguez
Unidad de Planificación
Consecutivo

FRS / srch,mpa