AUDITORIA INTERNA
auditoria@meic.go.cr
Teléfono: 2549-1400 Ext 205, 208, 272

San José, 30 de agosto de 2022

AI-SPASE-ADV-005-2022

Señor
Francisco Gamboa Soto, Ministro
Ministerio de Economía, Industria y Comercio

ASUNTO: ***Servicio preventivo de advertencia sobre: CIBERSEGURIDAD***

Estimado señor:

Como parte de los servicios preventivos de asesoría que presta la Auditoría Interna y en cumplimiento de su obligación de advertir a los órganos pasivos que fiscaliza, de las posibles consecuencias de determinadas conductas o decisiones, de conformidad con lo establecido en el numeral 1.1.4 de las Normas para el ejercicio de la auditoría interna en el Sector Público, publicadas en La Gaceta N° 28 del 10 de febrero del 2010, así como las competencias otorgadas en el artículo 22 de la Ley General de Control Interno y el artículo 38 del Reglamento de Organización y Funciones de la Auditoría Interna del Ministerio de Economía Industria y Comercio, nos permitimos hacer un recordatorio sobre **la obligación que tienen las Instituciones del Gobierno Central de acatar los lineamientos emitidos por el MICITT, respecto a la Emergencia Nacional de Ciberataque.**

Sobre el tema de Ciberseguridad, la Estrategia Nacional de Ciberseguridad enfatiza que un régimen de seguridad cibernética eficaz: adopta o desarrolla un marco con un ciclo continuo de actividad de evaluación del riesgo, control del riesgo, desarrollo de políticas de seguridad generales, garantía de continuidad del negocio, asignación de responsabilidades, promoción de concienciación y seguimiento de la eficacia de los controles implementados.

Al respecto, la Contraloría General de la República (CGR), en el ejercicio de sus competencias, realiza un diagnóstico sobre las prácticas de seguridad de la información en las instituciones públicas, como parte del Seguimiento de la Gestión Pública.

Esta Auditoría Interna ha colaborado con la CGR en esta revisión en el Ministerio de Economía, Industria y Comercio y ha observado que la institución presenta oportunidades de mejora en este tema.

Como resultado de la revisión, se le recuerda a la Administración lo siguiente:

1. El MEIC debía **haber declarado, aprobado y divulgado el marco de gestión de las tecnologías de información y comunicación** a más tardar el **1° de enero del 2022**, según el **R-DC-17-2020** (Transitorio I) emitido por la Contraloría General de la Republica.

2. Ante la Emergencia Nacional de Ciberataque declarada mediante el Decreto **N°43542-MP-MICITT**, publicado en el Alcance N°94 a La Gaceta N°86 del 11 de mayo de 2022 y sus reformas, adoptar el protocolo para el desarrollo de las acciones que se deben implementar ante una amenaza de un ataque a la ciberseguridad nacional, emitido por el MICITT.

3. Implementar la Directriz 133-MP-MICTT “Directriz dirigida a la Administración Pública Central y Descentralizada sobre las mejoras en materia de Ciberseguridad para el Sector Publico del Estado” que en el artículo 2 indica:

> ***Artículo 2*** *- Se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada* ***a realizar los procesos internos para promover de manera inmediata las acciones que favorezcan la resiliencia de la infraestructura tecnológica,*** *sea que la misma corresponda a la Administración Pública directamente o esté contratada de manera total o parcialmente,* ***incluyendo 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. (Lo resaltado no corresponde al original)***

En relación a este mismo tema, las Normas Técnicas de Control Interno para el Sector Público **(N-2-2009-CO-DFOE)** emitidas por la Contraloría General de la República, literalmente indican:

Norma 1.2 Objetivos del SCI

"El SCI de cada organización debe coadyuvar al cumplimiento de los siguientes objetivos:

a. ***Proteger y conservar el patrimonio público contra pérdida, despilfarro, uso indebido, irregularidad o acto ilegal****. El SCI debe brindar a la organización una seguridad razonable de que su patrimonio se dedica al destino para el cual le fue suministrado, y de que se establezcan, apliquen y fortalezcan acciones específicas para prevenir su sustracción, desvío, desperdicio o menoscabo.*

b. ***Exigir confiabilidad y oportunidad de la información****. El SCI debe procurar que se recopile, procese y mantenga información de calidad sobre el funcionamiento del sistema y sobre el desempeño institucional, y que esa información se comunique con prontitud a las instancias que la requieran para su gestión, dentro y fuera de la institución, todo ello de conformidad con las atribuciones y competencias organizacionales y en procura del logro de los objetivos institucionales.*

c. ***Garantizar eficiencia y eficacia de las operaciones****. El SCI debe coadyuvar a que la organización utilice sus recursos de manera óptima, y a que sus operaciones contribuyan con el logro de los objetivos institucionales." (**Lo resaltado no corresponde al original.)***

Norma 3.1 Valoración del riesgo

*"**El jerarca y los titulares subordinados, según sus competencias, deben definir, implantar, verificar y perfeccionar un proceso permanente y participativo de valoración del riesgo institucional**, como componente funcional del Sistema de Control Interno. Las autoridades indicadas deben constituirse en parte activa del proceso que al efecto se instaure." (**Lo resaltado no corresponde al original.)***

Norma 4.2 Requisitos de las actividades de control

b. Respuesta a riesgos.

*"**Las actividades de control deben ser congruentes con los riesgos que se pretende administrar**, lo que conlleva su dinamismo de acuerdo con el comportamiento de esos riesgos" **(Lo resaltado no corresponde al original.)***

Norma 5.8 Control de sistemas de información

*"El jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación**, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información** que ostente ese carácter." **(Lo resaltado no corresponde al original.)***

Norma 5.9 Tecnologías de información

*"El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance. En todo caso, **deben instaurarse los mecanismos y procedimientos manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información**. En esa línea, de conformidad con el perfil tecnológico de la institución, órgano o ente, en función de su naturaleza, complejidad, tamaño, modelo de negocio, volumen de operaciones, criticidad de sus procesos, riesgos y su dependencia tecnológica, **el jerarca deberá aprobar el marco de gestión de tecnologías de información y establecer un proceso de implementación gradual de cada uno de sus componentes**.*

Para la determinación del perfil tecnológico institucional se podrán considerar variables como las siguientes: ***marco de procesos para la gestión de TI, mapeo de procesos y subprocesos de negocio, organigrama de la entidad, conformación del Comité de TI, proveedores de TI, servicios de TI, inventario y criticidad de tipos documentales, centros de procesamiento y almacenamiento de datos, inventario de equipos y sistemas de información que soportan los servicios, software, proyectos de TI, planes de adquisición sobre TI, canales electrónicos y riesgos de TI****.” (Lo resaltado no corresponde al original)***

Por lo anterior, la auditoría interna recomienda a la Administración sobre el enfoque de esfuerzos en:

a) Presupuestar recursos para contratar personal, capacitar y dotar de equipo y software especializado al Ministerio para protegerlo de ciberataques.

b) Establecer medidas que minimicen el riesgo de accesos no autorizados y maliciosos a los sistemas informáticos, con el fin de extraer datos y utilizarlos para fines no éticos.

c) Brindar una adecuada atención a los incidentes y ataques cibernéticos e implementar procesos correctivos efectivos, para lo cual se requiere de flexibilidad y rapidez la respuesta, además de la articulación con los marcos de referencia y procedimientos existentes.

d) Desarrollar campañas de concienciación y educación dirigidas a los funcionarios públicos sobre las mejoras prácticas de protección y aseguramiento de datos de acceso a sistemas de información y datos sensibles o personales contenidos en los sistemas institucionales.

e) Proteger las infraestructuras informáticas críticas de la institución, entendiéndose estas como el conjunto de instalaciones, sistemas, equipos, redes, datos y servicios cuya interrupción o destrucción tendrían un alto impacto negativo en los servicios esenciales de un país, afectando seriamente el bienestar social y económico de todos los habitantes.

Por lo expuesto, se *ADVIERTE* al Jerarca, con el propósito de que se tomen las medidas pertinentes a fin de fortalecer las prácticas de seguridad de la información y minimizar la probabilidad de materialización del riesgo de ciberataques al Ministerio.

Por último, recalcamos que la Auditoría realiza este servicio de carácter preventivo y constructivo, orientado a apoyar la gestión en apego al deber de probidad, ordenamiento jurídico y técnico, sanas prácticas y al sistema de control interno.

Además, es una forma en que la Auditoría Interna agrega valora a la gestión Institucional.

Agradecemos, que de las acciones que se dispongan, respecto al presente documento, remita copia a esta Auditoría Interna para efectos de nuestro seguimiento.

Atentamente,

LUIS ORLANDO ARAYA CARRANZA (FIRMA)

Firmado digitalmente por LUIS ORLANDO ARAYA CARRANZA (FIRMA)
Fecha: 2022.08.30 12:24:55 -06'00'

Luis Orlando Araya Carranza.
AUDITOR INTERNO

CC: Eduardo Arias Cabalceta, Director Administrativo Financiero
Archivo