OFICINA DEL INSPECTOR GENERAL
GOBIERNO DE PUERTO RICO

Ivelisse Torres Rivera
Inspectora General

9 de marzo de 2020

CARTA CIRCULAR NÚM. 2020-01

A: Todos los Secretarios, Directores, Jefes De Agencia, Departamentos, Oficinas, Comisiones, Administraciones, Organismos, Corporaciones Públicas y demás Instrumentalidades de la Rama Ejecutiva del Gobierno de Puerto Rico, bajo la Jurisdicción de la Ley Núm. 15-2017, según enmendada.

RE: **MEDIDAS PREVENTIVAS ANTE POSIBLES ATAQUES CIBERNÉTICOS**

I. BASE LEGAL

La presente Carta Circular se emite en virtud de la Ley Núm. 15-2017, según enmendada, conocida como "*Ley del Inspector General de Puerto Rico*".

II. INTRODUCCIÓN

La Ley Núm. 15-2017, *supra*, creó la Oficina del Inspector General con el propósito de fortalecer los mecanismos de prevención, fiscalización, investigación y auditoría de la gestión gubernamental. En términos generales, la OIG tiene la responsabilidad de coordinar y fortalecer los esfuerzos gubernamentales para promover la integridad y eficiencia, así como prevenir y detectar oportunamente, toda actividad fraudulenta en el manejo de fondos públicos. A su vez, la OIG tiene el deber inherente como entidad fiscalizadora de evitar la corrupción en los organismos gubernamentales y desalentar las prácticas ilegales y fraudulentas en el servicio público.

Como es de conocimiento público, se han podido identificar varias entidades gubernamentales que han sido víctimas de ataques cibernéticos, tales como "hacking y/o phishing". Esto, principalmente debido a una falta de controles internos, ya que, en algunos casos estas entidades tomaron como cierto el contenido de correos electrónicos y depositaron de manera equívoca fondos públicos, en lo que resultaron ser cuentas fraudulentas.

En cumplimiento con nuestro deber ministerial[1], sugerimos la implementación de las siguientes medidas y recomendaciones como mecanismo de prevención a futuros ataques cibernéticos:

- Establecer un plan periódico de concientización de seguridad en los sistemas de información "security awarenes" entre los empleados de sus entidades a través de talleres y documentación escrita que incluya, pero no se limite a:
    - Deberes y responsabilidades de cada empleado en cumplimiento con las mejores prácticas de sistemas de información;
    - Como establecer políticas y procesos básicos de seguridad en los sistemas de información;
    - Controles generales para evitar acceso indebido a los sistemas de información;
    - Manejo de incidentes de seguridad en los sistemas;
    - Leyes y reglamentos vigentes.
- Identificar y clasificar las áreas que se encuentren más expuestas a posibles ataques cibernéticos y orientar a los Oficiales Principales de Informática para que puedan desarrollar eficazmente un análisis de riego en sus respectivas entidades.
- Invertir responsablemente y de ser necesario en equipos de tecnología, que se hayan identificados como obsoletos o de alto riego en la seguridad de los sistemas. Podrá realizar metas estratégicas que le permitan ir modernizando los sistemas por fases.
- Establecer un procedimiento para atender ataques cibernéticos e instruir a los Oficiales Principales de Informática y personal involucrado a tomar todas las medidas preventivas necesarias para proteger su entidad y cualquier otra que pueda estar en contacto.
- Solicitar informes a los Oficiales Principales de Informática para mantenerse informado sobre sus operaciones en las entidades.
- Actualizar oportunamente las políticas y procedimientos de los Sistemas de Información para ajustarlos a las diferentes modalidades de ataques cibernéticos.
    - Procesos para regular el acceso a los sistemas de información
    - Activación, modificación o desactivación de acceso a los sistemas de información
    - Control de Acceso a los sistemas de cómputos y servidores
    - Otros procedimientos que resulten pertinentes de acuerdo a la actividad que realiza la entidad
- Asegurar el debido cumplimiento de las leyes y reglamentos aplicables a los Sistemas de Información.
- Unificar esfuerzos y fortalecer la comunicación para evitar, identificar y atender de manera oportuna, posibles ataques cibernéticos en todas las entidades gubernamentales.
- Cumplir con las órdenes y comunicados que emita la Puerto Rico Innovation and Technology Service (PRITS), como cualquier entidad fiscalizadora, incluyendo la OIG, que ayude a reforzar, prevenir posibles ataques cibernéticos y evitar el mal uso de fondos públicos, entre otros.

---

[1] Véase Ar. 7, Ley Núm. 15-2017, *supra*.

La OIG tiene el compromiso de promover y ayudar en la coordinación de esfuerzos para atender asuntos y situaciones que requieren la participación o intervención de varias entidades gubernamentales. De usted necesitar capacitación, orientación o información sobre este tema puede comunicarse con la OIG a través del 787-679-7997. Así mismo, es el deber de cada funcionario que identifique una acción irregular, reportar la misma. Para esto puede comunicarse a nuestras oficinas a través del 787-679-7979 o través del correo electrónico informa@oig.pr.gov. Es responsabilidad de todos prevenir el mal uso de fondos públicos, por tal razón, se les exhorta a todos los funcionarios y empleados de las respectivas entidades gubernamentales a tomar conocimiento para poder cumplir adecuadamente con el estatuto legal.

Cordialmente,

Ivelisse Torres Rivera
Inspectora General