ORIGINAL

GOBIERNO DE PUERTO RICO

20ma. Asamblea Legislativa

1ra. Sesión Ordinaria

SENADO DE PUERTO RICO

P. del S. 24

2 de enero de 2025

Presentado por el señor *Rivera Schatz*

Referido a

LEY

Para crear la "Ley de Capacitación para la Seguridad Cibernética en Puerto Rico"; establecer como política pública en Puerto Rico la capacitación compulsoria sobre seguridad cibernética para la protección y el manejo adecuado de los sistemas y activos de información; establecer el Programa de Capacitación para la Seguridad Cibernética; imponer penalidades; y para otros fines relacionados.

EXPOSICIÓN DE MOTIVOS

Los adelantos tecnológicos experimentados en los últimos treinta (30) años han provocado cambios vertiginosos en el estilo de vida e interacción de los seres humanos. El acceso a la información, el desarrollo de la inteligencia artificial, la impresión 3D, la robótica, entre otros, evolucionan a pasos acelerados. Esta revolución tecnológica ha requerido de alteraciones estructurales en organizaciones públicas y privadas, con efectos sin precedentes. Toda esta transformación tecnológica ha contribuido favorablemente en la calidad de vida de los seres humanos, ya que va dirigida a cubrir necesidades, tanto sociales como económicas.

A pesar de los múltiples beneficios que traen consigo, éstos han creado en algunas instancias una sociedad cada vez más dependiente, frágil y en ocasiones vulnerable a ciertos aspectos tecnológicos que no necesariamente se pueden prevenir, por lo que es imprescindible anticipar y combatirlos. Uno de los principales problemas de índole

tecnológico en la actualidad a nivel mundial son los ataques cibernéticos, mediante los cuales individuos o grupos organizados obtienen acceso no autorizado a los sistemas de información, para la divulgación, uso, daño, degradación o destrucción de la información electrónica, sistemas e infraestructura crítica.

Para cumplir a cabalidad con un modelo de desarrollo socioeconómico cónsono con los constantes cambios tecnológicos, mediante la Ley 75-2019, según enmendada, se creó el *"Puerto Rico Innovation and Technology Service"* (en adelante, PRITS). Uno de los objetivos primordiales de PRITS es liderar la transformación digital del Gobierno ante los desafíos y las tendencias de la era moderna, a través de la innovación y la tecnología con un enfoque colaborativo, desarrollando así un gobierno centralizado, ágil y transparente, y de forma tal que los servicios que se ofrecen al ciudadano se brinden eficientemente, esto por la implementación de nuevas tecnologías e innovaciones de clase mundial.

Adicionalmente, la información es un componente crítico para el buen funcionamiento del Gobierno y para brindar servicios eficientes a los ciudadanos. El uso de medidas de seguridad es importante para evitar el acceso no autorizado, divulgación, uso, daño, degradación y destrucción de la información electrónica, sus sistemas e infraestructura crítica. Con este fin, la PRITS está comprometida con el desarrollo de un enfoque moderno sobre asuntos de ciberseguridad, de tal modo que el gobierno tenga mayor visibilidad sobre aquellos aspectos concernientes a amenazas a la información y garantizar controles efectivos para su seguridad.

Cabe señalar, que se han identificado varias modalidades de amenazas tanto en individuos, grupos o entidades que llevan a cabo ataques cibernéticos con la intención de causar daño, explotar vulnerabilidades u obtener acceso no autorizado a sistemas informáticos, redes, datos u otros activos valiosos. Dichos grupos o individuos pueden abarcar una amplia gama de motivaciones, habilidades y recursos, y pueden operar en diversos contextos, entre los que se encuentran:

- Hactivismo *"Hacktivism"* - Utilizan técnicas de pirateo para promover agendas políticas o sociales, como difundir la libertad de expresión o exponer violaciones de los derechos humanos.
- Cibercriminales *"Cybercriminals"* - Cometen delitos cibernéticos para obtener beneficios económicos.
- Amenazas Internas *"Insider threats"* - En los casos de amenazas internas los individuos no siempre actúan con mala intención. Algunos perjudican a su organización por errores humanos, pero existen los empleados malintencionados o descontentos que abusan de sus privilegios de acceso para hurtar datos con fines lucrativos o dañan datos o aplicaciones como represalia.
- Ciberespionaje o *"Cyberespionage"* - Obtienen acceso no autorizado en sistemas y redes informáticas con el propósito de extraer datos confidenciales gubernamentales o corporativos para obtener información.
- Ciberterrorismo o *"Cyberterrorism"* - Lanzan ataques por motivos políticos o ideológicos que amenazan o conducen a actos de violencia.

De todas las modalidades antes mencionadas, son las amenazas internas las que resultan el eslabón más débil en una organización, y la única amenaza que se puede prevenir mediante el adiestramiento y capacitación a los fines de enfrentar y prevenir este tipo de ataque.

Lamentablemente, Puerto Rico no ha sido la excepción a la exposición de este tipo de práctica criminal. Según datos ofrecidos por la PRITS, para el año 2022 se detectaron y bloquearon 753,276,056 ataques cibernéticos, cifra que resulta alarmante en comparación con el año 2021 donde se reportaron 13,731,041. De igual forma, al 31 de julio de 2023, se habían detectado alrededor de 490,537,483 millones de intentos de ciberataques, lo que coloca a Puerto Rico como una jurisdicción de Estados Unidos con un nivel alto de alerta en este tipo de amenazas, virus y otras actividades cibernéticas maliciosas. Así mismo, durante los últimos meses los ciudadanos de Puerto Rico han sido testigo de los efectos de ataques cibernéticos perpetrados a varias entidades gubernamentales y privadas.

Han sido múltiples las gestiones de la PRITS para prevenir y detener este tipo de ataques tanto en el sector gubernamental como en el privado. Recientemente, se