GOBIERNO DE PUERTO RICO

19na. Asamblea Legislativa

6ta. Sesión Ordinaria

# SENADO DE PUERTO RICO

# P. del S. 1393

8 de noviembre de 2023

Presentado por el señor *Rivera Schatz*

*Referido a la Comisión de Innovación, Telecomunicaciones, Urbanismo e Infraestructura*

**LEY**

Para crear la "Ley de Capacitación para la Seguridad Cibernética del Gobierno de Puerto Rico"; establecer como política pública del Gobierno de 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 estos 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 nuestra responsabilidad anticipar y combatir. Uno de los principales problemas de índole tecnológico que enfrentan 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, el Gobierno de Puerto Rico, mediante la Ley 75-2019, según enmendada, 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 de Puerto Rico 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.

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 de sus miembros 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 PRITS, para el año 2022 se recibió 753,276,056 ataques cibernéticos detectados y bloqueados, cifra que resulta alarmante en comparación con el año 2021 donde se reportaron 13,731,41. De igual forma, al 31 de julio de 2023, se habían detectado casi 490,537,483 millones de intentos de ciberataques, lo que coloca a la Isla 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 el Pueblo de Puerto Rico ha sido testigo de los efectos de ataques cibernéticos perpetrados a varias entidades gubernamentales y privadas.

Han sido múltiples las gestiones de PRITS para prevenir y detener este tipo de ataques tanto en el sector gubernamental como en el privado. Recientemente, se anunció la creación de un "*Cyber Force*", el cual consiste de una alianza entre PRITS y diversas agencias federales y estatales bajo las cuales se busca capacitar y darles participación a ciudadanos de manera voluntaria en asuntos relacionados a seguridad cibernética. Lo anterior, con el fin de colaborar con entidades de seguridad en la prevención, intercambio de información, respuesta y recuperación de ataques, para así aumentar la resiliencia y disminuir las vulnerabilidades en los sistemas del Gobierno de Puerto Rico. De igual forma, la agencia ha sido responsiva en el establecimiento de políticas y en la creación de guías para los empleados sobre seguridad cibernética.

Aunque reconocemos los innumerables esfuerzos de PRITS para combatir los ataques cibernéticos, entendemos la necesidad de aprobar legislación a los fines de establecer como política pública del Gobierno de Puerto Rico la capacitación compulsoria sobre seguridad cibernética, en aras de garantizar la protección y el manejo adecuado de los sistemas y activos de información, mediante la creación de un programa a estos fines. Dicho programa está dirigido para adiestrar con el propósito de concientizar e implantar protocolos y controles para mitigar los riesgos de seguridad cibernética a través de la identificación y capacidad de respuesta oportuna a las amenazas o eventos que involucren irregularidades de seguridad. Así también, se establecen penalidades a toda persona que, mediante acción u omisión, incumpla con el reporte o manejo adecuado de un incidente cibernético, permitiendo el acceso no autorizado de información y afectando las operaciones de la entidad. De esta forma, se minimizan las posibilidades de amenazas internas dentro de todos los componentes del Gobierno de Puerto Rico, así como del sector privado.

Es por todo lo anterior, que esta Asamblea Legislativa entiende y reconoce los daños que los ataques cibernéticos provocan tanto en las operaciones gubernamentales como privadas, en los servicios que se brindan a la ciudadanía y la necesidad de identificar medidas preventivas para combatir esta actividad criminal.

**DECRÉTASE POR LA ASAMBLEA LEGISLATIVA DE PUERTO RICO:**

Artículo 1.- Título.

Esta Ley se conocerá como "Ley de Capacitación para la Seguridad Cibernética del Gobierno de Puerto Rico".

Artículo 2.- Política Pública.

Será política pública del Gobierno de Puerto Rico, el promover y concienciar sobre la seguridad cibernética a través de capacitaciones, talleres u orientaciones compulsorias con el fin de proteger la confidencialidad e integridad de los activos de

información de entidades gubernamentales y privadas, garantizando así, la implementación de medidas de seguridad y manejo adecuado para prevenir o mitigar el riesgo de eventos de seguridad cibernética y la divulgación involuntaria de información confidencial por parte de los empleados y /o personas que brinden servicios.

Artículo 3.- Programa de Capacitación para la Seguridad Cibernética.

Se ordena a la Puerto Rico Innovation and Technology Service del Gobierno de Puerto Rico (PRITS), a desarrollar y ofrecer un Programa de Capacitación para la Seguridad Cibernética. El mismo será ofrecido al menos una vez al año.

Para el desarrollo del Programa de Capacitación se deberá considerar lo siguiente:

(a) Concientizar e informar sobre seguridad cibernética y los sistemas de información que respaldan las operaciones y los activos gubernamentales y privados.

(b) Políticas de seguridad y tecnología, protocolos, procedimientos y controles físicos y técnicos promulgados por PRITS para el manejo adecuado de los sistemas y activos de información y protección de la confidencialidad, e integridad de los activos de información de entidades gubernamentales y privadas.

(c) Responsabilidad en el cumplimiento de las políticas y procedimientos de las entidades gubernamentales y privadas para la mitigación de riesgos, así como de requisitos legales y reglamentarios relacionados a la seguridad cibernética.

(d) Riesgos de seguridad cibernética asociados con su funciones y deberes.

(e) Prevención de daños para mitigar los riesgos de seguridad cibernética a través de la identificación y capacidad de respuesta oportuna a las amenazas, o eventos que involucren irregularidades de seguridad, o infracciones por el uso indebido y el acceso o divulgación no autorizada de la información.

(f) Diseño e implementación de planes y procedimientos para la recuperación y continuidad de las operaciones de los sistemas de información.

(g) Responsabilidad de divulgación de cualquier actividad o evento sospechoso, accidental o intencional que comprometa la integridad, disponibilidad y/o confidencialidad de la información.

Artículo 4.- Aplicabilidad.

Las disposiciones de esta Ley aplicarán de manera compulsoria a toda rama, agencia y/o instrumentalidad adscrita al Gobierno de Puerto Rico, incluyendo las corporaciones o instrumentalidades públicas, así como las instrumentalidades público privadas que funcionan como empresas o negocios privados, municipios y empresas privadas con un volumen de negocio de $100,000.00 o más.

La Rama Legislativa, la Rama Judicial, los municipios, y las empresas o negocios privados con un volumen de negocio de $100,000.00 o más, podrán coordinar la asistencia de PRITS o cualquier otra entidad gubernamental estatal, y/o federal, así como con otras entidades privadas con el peritaje para el asesoramiento e implementación del Programa de Capacitación en cumplimiento con las disposiciones de esta Ley.

Artículo 5.- Coordinación interagencial y/o colaborativo.

Se faculta a PRITS a llevar a cabo las gestiones necesarias para coordinar acuerdos de colaboración con agencias, departamentos, organismos gubernamentales estatales, federales y/o municipales, así como con otras instituciones públicas o privadas para adelantar los propósitos de esta Ley.

Artículo 6.- Conducta delictiva; Penalidades.

Toda persona que, mediante acción u omisión, a propósito, incumpla con el reporte o manejo establecido de un incidente cibernético y permita el acceso no autorizado de información con el propósito de afectar las operaciones del sistema de información y datos de cualquier entidad gubernamental o privada, o que compromete su confidencialidad, incurrirá en delito menos grave.

Artículo 7.- Reglamentación.

Se faculta a PRITS a que adopte la reglamentación necesaria para lograr el cumplimiento de las disposiciones de esta Ley. Disponiéndose además que, la reglamentación que se adopte deberá actualizarse, a tenor con los constantes avances tecnológicos.

Artículo 8.- Presupuesto.

Los fondos necesarios para cumplir con los objetivos de esta Ley se coordinarán con cada una de las agencias, en colaboración con PRITS, la Oficina de Gerencia y Presupuesto y la Autoridad de Asesoría Financiera y Agencia Fiscal, durante el proceso presupuestario de cada año fiscal para identificar los fondos necesarios dentro del Presupuesto Certificado, programas federales y/o cualquier otro fondo disponible.

Artículo 9.- Cláusula Derogatoria.

Cualquier disposición de ley o reglamentación que sea incompatible con las disposiciones de esta Ley queda por la presente derogada hasta donde existiere tal incompatibilidad.

Artículo 10.- Cláusula de Separabilidad.

Si cualquier cláusula, párrafo, subpárrafo, oración, palabra, letra, artículo, disposición, sección, subsección, título, capítulo, subcapítulo, acápite o parte de esta Ley fuera anulada o declarada inconstitucional, la resolución, dictamen o sentencia a tal efecto dictada no afectará, perjudicará, ni invalidará el remanente de esta Ley. El efecto de dicha sentencia quedará limitado a la cláusula, párrafo, subpárrafo, oración, palabra, letra, artículo, disposición, sección, subsección, título, capítulo, subcapítulo, acápite o parte de esta que así hubiere sido anulada o declarada inconstitucional. Si la aplicación a una persona o a una circunstancia de cualquier cláusula, párrafo, subpárrafo, oración, palabra, letra, artículo, disposición, sección, subsección, título, capítulo, subcapítulo, acápite o parte de esta Ley fuera invalidada o declarada inconstitucional, la resolución, dictamen o sentencia a tal efecto dictada no afectará ni invalidará la aplicación del remanente de esta Ley a aquellas personas o circunstancias en las que se pueda aplicar válidamente. Es la voluntad expresa e inequívoca de esta Asamblea Legislativa que los tribunales hagan cumplir las disposiciones y la aplicación de esta Ley en la mayor medida posible, aunque se deje sin efecto, anule, invalide, perjudique o declare inconstitucional alguna de sus partes, o, aunque se deje sin efecto, invalide o declare inconstitucional su aplicación a alguna persona o circunstancia. Esta Asamblea

Legislativa hubiera aprobado esta Ley sin importar la determinación de separabilidad que el Tribunal pueda hacer.

Artículo 11.- Vigencia.

Esta Ley entrará en vigor inmediatamente después de su aprobación. No obstante, la implementación del Programa se establecerá dentro de los próximos dieciocho (18) meses luego de la aprobación de esta Ley.