

GOBIERNO DE PUERTO RICO

20^{ma}. Asamblea
Legislativa

1^{ra}. Sesión
Ordinaria

SENADO DE PUERTO RICO

P. del S. 527

10 de abril de 2025

Presentado por la señora *Soto Aguilú*

Referido a la Comisión de Asuntos Internos

LEY

Para enmendar el Artículo 6; añadir un nuevo Artículo 10 y reenumerar los actuales Artículos 10, 11, 12, 13, 14, 15, 16 y 17 como Artículos 11, 12, 13, 14, 15, 16, 17 y 18 de la Ley 40-2024, conocida como “Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico”, a los fines de ampliar las funciones de la Oficina de Seguridad Cibernética para incluir la promoción del desarrollo económico en el campo de la ciberseguridad y la tecnología de la información; establecer un Programa de Certificación y Formación Técnica en Ciberseguridad dirigido a estudiantes y pequeñas y medianas empresas (PyMEs); y para otros fines relacionados.

EXPOSICIÓN DE MOTIVOS

La acelerada transformación digital de los servicios gubernamentales, las empresas privadas y la vida cotidiana en general ha traído consigo enormes beneficios en términos de eficiencia, conectividad y acceso. No obstante, este nuevo entorno también ha aumentado exponencialmente los riesgos relacionados con la seguridad de la información, el manejo de datos sensibles y la protección de infraestructuras tecnológicas críticas. En este escenario, la ciberseguridad ya no es un asunto exclusivo de especialistas técnicos, sino un pilar esencial de la gobernanza pública, la competitividad económica y la estabilidad social.

Con la aprobación de la Ley 40-2024, el Gobierno de Puerto Rico adoptó una política pública integral para atender los riesgos cibernéticos en sus estructuras institucionales. Entre sus principales aciertos, la ley establece el cargo de Principal Oficial de Seguridad Cibernética de Puerto Rico, coordina protocolos de respuesta ante incidentes y establece obligaciones para las agencias y corporaciones públicas en cuanto a seguridad digital. Este andamiaje es fundamental para garantizar la continuidad de servicios públicos, proteger la integridad de los datos ciudadanos y responder eficazmente ante amenazas cibernéticas.

Sin embargo, el marco legal actual no aborda de manera suficiente la dimensión económica y formativa de la ciberseguridad. En un mundo donde los ataques digitales no conocen fronteras y donde la demanda por talento en seguridad informática crece aceleradamente, Puerto Rico tiene la oportunidad y la responsabilidad de convertirse en un centro de desarrollo de capital humano, innovación tecnológica y negocios especializados en ciberseguridad. Esta industria global genera cientos de miles de empleos y representa miles de millones en actividad económica. No solo es una prioridad de defensa digital, sino también una vía concreta para la diversificación económica y la creación de empleos bien remunerados.

A nivel local, existe una brecha importante en la capacidad de las pequeñas y medianas empresas (PyMEs) para adoptar prácticas seguras en sus operaciones digitales. La mayoría de estas empresas no cuentan con los recursos para contratar personal experto o implementar herramientas de protección, quedando vulnerables a fraudes, filtraciones de datos, suplantación de identidad y ataques de ransomware. Estas amenazas no solo impactan sus finanzas, sino que debilitan la confianza del consumidor y comprometen la estabilidad del ecosistema empresarial.

De igual manera, muchas personas jóvenes interesadas en incursionar en carreras tecnológicas enfrentan barreras económicas, educativas y de acceso a certificaciones que les impiden desarrollarse en un campo con alta demanda. Sin intervención del Estado, este potencial humano se desperdicia, limitando las oportunidades de movilidad social ascendente y frenando el desarrollo de un sector estratégico para la Isla.

Por tanto, esta medida tiene un doble propósito. En primer lugar, enmienda la Ley 40-2024 para ampliar el alcance de las funciones del Principal Oficial de Seguridad Cibernética, incluyendo la promoción del desarrollo económico en el campo de la ciberseguridad y las tecnologías de información. Esta dimensión económica debe ser parte central de la política pública, con un enfoque en alianzas multisectoriales, apoyo a empresas emergentes, e integración del sistema educativo y universitario.

En segundo lugar, la medida crea el Programa de Certificación y Formación Técnica en Ciberseguridad, coordinado entre PRITS, el Departamento de Desarrollo Económico y Comercio (DDEC), el Departamento del Trabajo y Recursos Humanos (DTRH), la Universidad de Puerto Rico y los Centros de Gestión Única. Este programa permitirá a jóvenes, personas desempleadas y propietarios de negocios recibir capacitación accesible, práctica y alineada con estándares internacionales. Además, facilitará la adopción de buenas prácticas digitales entre las PyMEs y abrirá caminos a la profesionalización de sectores vulnerables.

La intención legislativa detrás de este proyecto es clara y decidida: fomentar una cultura de seguridad digital que sea inclusiva, productiva y orientada al desarrollo. La ciberseguridad no debe tratarse solo como una cuestión técnica o defensiva; debe concebirse como un eje de oportunidad, un campo de innovación, y una responsabilidad compartida entre el Estado, la academia, el sector privado y la ciudadanía.

En resumen, esta medida busca fortalecer el marco institucional existente, ampliar su proyección hacia el desarrollo económico, y preparar a Puerto Rico para asumir con liderazgo los desafíos y oportunidades del siglo XXI en materia de ciberseguridad.

DECRÉTASE POR LA ASAMBLEA LEGISLATIVA DE PUERTO RICO:

- 1 Sección 1.- Se enmienda el Artículo 6 de la Ley 40-2024, conocida como “Ley de
- 2 Ciberseguridad del Estado Libre Asociado de Puerto Rico”, para que lea como sigue:

1 "Artículo 6.- Principal Oficial de Seguridad Cibernética (Chief Information Security
2 Officer) del Gobierno.

3 Se crea el cargo de Principal Oficial de Seguridad Cibernética (Chief Information
4 Security Officer) del Gobierno, quien estará adscrito al PRITS, pero gozará de cierto
5 nivel de autonomía para llevar a cabo sus funciones de manera independiente
6 utilizando los recursos provistos por PRITS. Al momento de la creación de esta
7 posición, la Oficina de Gerencia y Presupuesto deberá autorizar y diligenciar la creación
8 del puesto del Principal Oficial de Seguridad Cibernética ("Chief Information Security
9 Officer") del Gobierno y notificará a la Oficina de Administración y Transformación de
10 los Recursos Humanos del Gobierno de Puerto Rico para garantizar que se cumplan con
11 todas las leyes y reglamentos aplicables.

12 El Principal Oficial de Seguridad Cibernética será nombrado por el Principal
13 Ejecutivo de Innovación e Información del Gobierno. La persona nombrada como CISO
14 deberá ser de reconocida capacidad profesional.

15 El Principal Oficial de Seguridad Cibernética será el encargado de establecer las
16 medidas de seguridad adecuadas para evitar el acceso no autorizado, divulgación, uso,
17 daño, degradación y destrucción de la información electrónica, sus sistemas e
18 infraestructura crítica. También será responsable de reducir el Riesgo, el impacto y el
19 costo de los Ciberataques al establecer un marco con requisitos mínimos de seguridad
20 de las tecnologías de la información (TI), definir roles y responsabilidades y establecer
21 los estándares para proteger la información.

1 El Principal Oficial de Seguridad Cibernética trabajará en coordinación con el
2 Instituto y con el personal que cada Agencia designe para llevar a cabo tales funciones,
3 en la confección y ejecución de las estrategias para proteger la información pública del
4 Gobierno.

5 *Además de las funciones aquí dispuestas, el Principal Oficial de Seguridad Cibernética*
6 *también tendrá el deber de promover el desarrollo económico de Puerto Rico en el campo de la*
7 *ciberseguridad y tecnologías de información, mediante la creación de alianzas estratégicas con*
8 *instituciones educativas, el sector privado, las organizaciones sin fines de lucro y los gobiernos*
9 *municipales. Esta función incluirá el diseño de incentivos, actividades de formación y*
10 *certificación, así como el apoyo a proyectos empresariales emergentes en estos sectores.”*

11 Sección 2.- Se añade un nuevo Artículo 10 a la Ley 40-2024, conocida como “Ley de
12 Ciberseguridad del Estado Libre Asociado de Puerto Rico”, para que lea como sigue:

13 *“Artículo 10.- Programa de Certificación y Formación Técnica en Ciberseguridad.*

14 *a) Se establece el Programa de Certificación y Formación Técnica en Ciberseguridad como*
15 *política pública del Gobierno de Puerto Rico.*

16 *b) El programa estará bajo la coordinación del Puerto Rico Innovation and Technology*
17 *Service (PRITS), en colaboración con el Departamento de Desarrollo Económico y Comercio*
18 *(DDEC), el Departamento del Trabajo y Recursos Humanos (DTRH), la Universidad de Puerto*
19 *Rico (UPR) y los Centros de Gestión Única para PyMEs.*

20 *c) El programa tendrá como objetivos:*

21 *1. Ofrecer cursos, talleres y certificaciones en ciberseguridad reconocidas a nivel*
22 *internacional, de forma gratuita o a bajo costo;*

- 1 2. *Priorizar la capacitación de estudiantes, personas desempleadas, mujeres en carreras*
- 2 *STEM, y propietarios de pequeñas empresas;*
- 3 3. *Fortalecer las capacidades de seguridad digital de las PyMEs mediante diagnósticos,*
- 4 *asesoramiento técnico y acompañamiento continuo;*
- 5 4. *Fomentar la creación de startups locales en el sector de ciberseguridad.*

6 *d) El programa será financiado con asignaciones presupuestarias, fondos federales disponibles*
7 *y alianzas público-privadas. Se le autoriza a PRITS a solicitar fondos bajo la Ley Bipartidista de*
8 *Infraestructura y otros programas federales aplicables.”*

9 Sección 3.- Se reenumeran los Artículos 10, 11, 12, 13, 14, 15, 16 y 17 como Artículos
10 11, 12, 13, 14, 15, 16, 17 y 18 de la Ley 40-2024, conocida como “Ley de Ciberseguridad
11 del Estado Libre Asociado de Puerto Rico”

12 Sección 4.- Se faculta a PRITS, al DDEC y al DTRH a adoptar la reglamentación
13 necesaria para la implementación de esta Ley en un término no mayor de ciento veinte
14 (120) días a partir de su aprobación.

15 Sección 5.- Si cualquier disposición de esta Ley fuera declarada inconstitucional, nula o
16 inválida por un tribunal competente, dicha declaración no afectará las demás
17 disposiciones de esta Ley, las cuales continuarán en pleno vigor y efecto.

18 Sección 6.- Esta Ley entrará en vigor inmediatamente después de su aprobación.