TEXTO APROBADO EN VOTACIÓN FINAL POR EL SENADO
(11 DE MAYO DE 2026)

GOBIERNO DE PUERTO RICO

20 ma Asamblea Legislativa

3 ra Sesión Ordinaria

SENADO DE PUERTO RICO

P. del S. 1126

9 de marzo de 2026

Presentado por el señor *Reyes Berríos*

Coautores la señora Barlucea Rodríguez; los señores Colón La Santa, González López; la señora Pérez Soto; y el señor Sánchez Álvarez

Referido a la Comisión de Ciencia, Tecnología e Inteligencia Artificial

LEY

Para enmendar los Artículos 2, 3, 4, 6, 7, 10 y añadir los nuevos Artículos 7-A y 11-A de la Ley Núm. 40-2024, según enmendada, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico", con el propósito de fortalecer el marco jurídico de ciberseguridad del Gobierno de Puerto Rico, reforzar la resiliencia digital y la continuidad de servicios esenciales, ampliar facultades regulatorias y establecer mecanismos de supervisión, notificación y financiamiento; y para otros fines relacionados.

EXPOSİCIÓN DE MOTIVOS

La transformación digital del Gobierno de Puerto Rico ha dejado de ser una aspiración programática para convertirse en una realidad operativa indispensable. La prestación de servicios públicos, la continuidad gubernamental, la protección de información sensitiva y el desarrollo económico sostenible son temas que se deben atender en esta transformación. La creciente interconexión de sistemas, la dependencia de infraestructuras tecnológicas y la utilización intensiva de plataformas digitales han ampliado significativamente la superficie de exposición a amenazas cibernéticas cada vez más sofisticadas, persistentes y coordinadas.

La aprobación de la Ley Núm. 40-2024, según enmendada, conocida como la "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico", constituyó un paso decisivo en la creación de un marco normativo para atender la seguridad de los recursos de información gubernamentales. Dicha legislación estableció estándares mínimos de ciberseguridad, creó la figura del Principal Oficial de Seguridad Cibernética (CISO) y formalizó la Oficina para la Evaluación de Incidentes Cibernéticos adscrita al Puerto Rico Innovation and Technology Service (PRITS). Con ello, se reconoció que la protección de los datos gubernamentales es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información pública.

No obstante, el entorno digital evoluciona a un ritmo que supera el ciclo ordinario de actualización legislativa. Los ataques mediante ransomware, la explotación de vulnerabilidades en la cadena de suministro tecnológica, el uso malicioso de herramientas basadas en inteligencia artificial, la suplantación digital y los ataques coordinados contra infraestructuras críticas evidencian que la ciberseguridad ya no es únicamente un asunto técnico, sino un componente estructural de la seguridad pública, la estabilidad económica y la gobernanza democrática.

La experiencia reciente demuestra que la interrupción de servicios esenciales tales como energía, agua, telecomunicaciones, sistemas financieros, salud o logística crítica puede generar efectos sistémicos inmediatos sobre la economía y la seguridad de la población. En ese contexto, la protección del ciberespacio y la resiliencia digital deben concebirse como elementos estratégicos de seguridad y desarrollo económico, no meramente como obligaciones administrativas de cumplimiento mínimo.

Las mejores prácticas internacionales han avanzado hacia modelos regulatorios que integran múltiples aspectos. Entre los aspectos antes referidos comúnmente se incluye la gestión de riesgos basada en criticidad, supervisión de operadores de infraestructuras críticas, obligación de notificación temprana de incidentes, fiscalización de la cadena de suministro digital y adopción de estándares técnicos armonizados con marcos como el National Institute of Standards and Technology (NIST) y estándares internacionales ISO.

Estos modelos reconocen que la resiliencia digital requiere coordinación centralizada, ejecución descentralizada y una clara delimitación de responsabilidades entre el sector público y el sector privado.

La Ley Núm. 40-2024, según enmendada, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico" (Ley 40), estableció un andamiaje inicial adecuado, pero su enfoque principal se circunscribe al ámbito gubernamental directo y a estándares mínimos de cumplimiento. Resulta necesario fortalecer dicho marco para incorporar un enfoque integral que atienda la clasificación de incidentes por niveles de severidad. Además, entendemos necesario que se reduzca el término de notificación para incidentes críticos, la supervisión de proveedores tecnológicos según su nivel de criticidad, la integridad de la cadena de suministro de software, la obligación de planes de continuidad de negocios y recuperación ante desastres, y un régimen sancionador proporcional que tenga verdadero efecto disuasivo.

Asimismo, se hace indispensable robustecer la autoridad técnica del Principal Oficial de Seguridad Cibernética y de la Oficina adscrita a PRITS. Para lograr lo antes dicho se deben dotar de facultades regulatorias claras para emitir normas técnicas vinculantes, coordinar respuestas interinstitucionales ante emergencias cibernéticas y fiscalizar el cumplimiento en sectores críticos. La gobernanza efectiva en materia de ciberseguridad exige claridad normativa, supervisión activa y capacidad de respuesta inmediata.

Por otro lado, la inversión en ciberseguridad debe concebirse como un habilitador del desarrollo económico. Un ecosistema digital seguro fomenta la inversión, fortalece la confianza en los servicios gubernamentales y posiciona a Puerto Rico como una jurisdicción confiable para la innovación tecnológica y la economía digital. La adopción de incentivos para certificaciones reconocidas internacionalmente, la creación de mecanismos de financiamiento para fortalecer la resiliencia digital y el desarrollo de talento especializado constituyen elementos esenciales de una política pública moderna en esta materia.

La presente medida tiene como propósito enmendar la Ley Núm. 40-2024 para actualizar y fortalecer el marco jurídico vigente, alinearlo con estándares contemporáneos, integrar un enfoque de resiliencia digital basado en riesgo y criticidad, reforzar la gobernanza centralizada de la ciberseguridad y establecer obligaciones claras, proporcionales y fiscalizables para entidades públicas y privadas cuya operación incida sobre servicios esenciales e infraestructuras críticas. Mediante estas enmiendas, la Asamblea Legislativa reafirma su compromiso con la protección de la información pública, continuidad gubernamental, estabilidad económica y seguridad digital de Puerto Rico. Reconociendo que en la era tecnológica la defensa del ciberespacio es inseparable de la defensa de la integridad institucional y del bienestar colectivo.

DECRÉTASE POR LA ASAMBLEA LEGISLATIVA DE PUERTO RICO:

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

"Artículo 2.- Aplicabilidad.

Las disposiciones de esta Ley son aplicables a la Rama Ejecutiva, incluyendo todo departamento, junta, dependencia, comisión, negociado, oficina, agencia, administración u organismo, subdivisión política, corporaciones públicas y municipios. De igual forma aplica a cualquier persona natural o jurídica que haga negocios o tenga contratos con el Gobierno, incluyendo, de forma no exhaustiva, a las personas privadas que desempeñan funciones y servicios públicos, pero solamente con respecto a las funciones y servicios públicos desempeñados; a todo ejercicio de administración pública o privada en el que se hubieren dedicado o invertido fondos o recursos públicos (directa o indirectamente),

o sobre la cual se hubiere ejercido la autoridad de cualquier servidor público, en cuanto a los datos que se generan como producto de tales actividades.

Las disposiciones de esta Ley también serán aplicables a todo operador de infraestructura crítica o proveedor de servicios esenciales, independientemente de que medie o no relación contractual directa con el Gobierno, cuando la interrupción, degradación o compromiso de sus sistemas pueda afectar la continuidad de servicios esenciales, la seguridad pública, la estabilidad económica o la continuidad gubernamental."

Sección 2.- Se enmienda el Artículo 3 de la Ley 40-2024, según enmendada, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico", para que lea como sigue:

"Artículo 3.- Política Pública.

Se establece como política pública en Puerto Rico lo siguiente:

1. …

…

10. Reconocer la resiliencia digital y la continuidad operacional de los servicios esenciales como componentes estratégicos de la seguridad pública y el desarrollo económico, adoptando un enfoque basado en riesgo y criticidad, armonizado con estándares reconocidos internacionalmente tales como *NIST, ISO/IEC 27001 e ISO 22301*."

Sección 3.- Se enmienda el Artículo 4 de la Ley 40-2024, según enmendada, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico", para que lea como sigue:

"Artículo 4. — Definiciones.

Para propósitos de esta Ley y salvo que otra cosa se disponga en la misma, los siguientes términos tendrán el significado expresado a continuación:

(a) …

(dd) "Servicios esenciales" — aquellos servicios cuya interrupción pueda afectar significativamente la salud, seguridad, economía o bienestar colectivo, incluyendo, sin limitarse, a energía, agua, telecomunicaciones, finanzas, salud, transporte, logística crítica y sistemas gubernamentales estratégicos.

(ee) "Operador crítico" — toda persona natural o jurídica, pública o privada, que administre, opere o controle infraestructura crítica o servicios esenciales.

(ff) "Cadena de suministro digital" — conjunto de procesos, componentes, software, hardware y servicios interconectados que intervienen en el desarrollo, provisión y mantenimiento de sistemas tecnológicos utilizados por el Gobierno.

(gg) "Gestión de riesgos cibernéticos" — proceso continuo de identificación, evaluación, mitigación y monitoreo de amenazas y vulnerabilidades que puedan afectar los Recursos de información.

(hh) "Plan de Continuidad y Recuperación" — documento formal que establece procedimientos para garantizar la continuidad operacional y la recuperación ante incidentes cibernéticos o desastres tecnológicos.

(ii) "Relación entre categorías" - Para efectos de esta Ley, los términos 'proveedor de servicios contratados', 'proveedor de servicios esenciales' y 'operador crítico' constituyen categorías distintas. El término 'proveedor de servicios contratados' se refiere a entidades con relación contractual directa con el Gobierno; el término 'proveedor de servicios esenciales' se refiere a entidades cuya operación impacta servicios esenciales independientemente de relación contractual; y el término 'operador crítico' comprende aquellas entidades, públicas o privadas, cuya operación o control de infraestructura crítica o servicios esenciales representa un riesgo significativo para la seguridad pública, estabilidad económica o continuidad gubernamental. PRITS establecerá mediante reglamento los criterios de clasificación y la interacción entre dichas categorías.

Se dispone que los términos definidos en este Artículo deberán utilizarse de forma consistente a través de toda la Ley. Cualquier referencia a entidades reguladas deberá interpretarse conforme a las categorías aquí definidas, evitando duplicidad o ambigüedad en su aplicación."

Sección 4.- Se enmienda el Artículo 6 de la Ley 40-2024, según enmendada, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico", para que lea como sigue:

"Artículo 6. – Principal Oficial de Seguridad Cibernética *(Chief Information Security Officer)* del Gobierno.

Se crea el cargo de Principal Oficial de Seguridad Cibernética *(Chief Information Security Officer)* del Gobierno, quien estará adscrito al PRITS, pero gozará de cierto nivel

de autonomía para llevar a cabo sus funciones de manera independiente utilizando los recursos provistos por PRITS. …

…

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

El Principal Oficial de Seguridad Cibernética tendrá facultad para emitir normas técnicas obligatorias y vinculantes aplicables a las Agencias y a los operadores críticos cubiertos por esta Ley, incluyendo estándares mínimos de seguridad, protocolos de notificación, requisitos de auditoría y medidas de mitigación. Asimismo, podrá recomendar al Gobernador la declaración de una emergencia cibernética cuando las circunstancias lo ameriten."

Sección 5.- Se enmienda el Artículo 7 de la Ley 40-2024, según enmendada, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico", para que lea como sigue:

"Artículo 7. – Estándares y principios mínimos de Ciberseguridad.

Toda Agencia y todo Proveedor de servicios contratados deberá cumplir y asegurarse que toda persona natural o jurídica que haga negocios o contrate con ellos cumpla con al menos los siguientes Estándares y principios mínimos de Ciberseguridad:

(1) **...**

...

(10) Los Proveedores de servicios contratados de tecnología de la información y comunicaciones compartirán información y notificarán en un término no mayor de veinticuatro (24) horas al PRITS y a la Agencia contratante cuando descubran un incidente de seguridad cibernética o un incidente potencial que pueda poner en Riesgo los datos, productos de software, Firmware o los servicios confidenciales del Gobierno o de cualquier persona natural o jurídica;

…

(20) PRITS adoptará mediante reglamento un sistema de clasificación de incidentes de seguridad cibernética en niveles bajo, medio, alto y crítico, conforme al impacto potencial sobre la confidencialidad, integridad, disponibilidad, continuidad operacional y seguridad pública, estableciendo para cada nivel obligaciones específicas de notificación, respuesta y mitigación.

(21) Todo proveedor clasificado como de alto o crítico impacto deberá mantener y proveer a PRITS un inventario actualizado de componentes de software (*Software Bill of Materials – SBOM*) conforme a estándares reconocidos, así como evidenciar un proceso formal de gestión de vulnerabilidades y aplicación de parchos de seguridad dentro de términos razonables establecidos por reglamento."

Sección 6.- Se enmienda el Artículo 10 de la Ley 40-2024, según enmendada, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico", para que lea como sigue:

"Artículo 10. – Sanciones.

PRITS podrá imponer multas administrativas, conforme a lo establecido en la "Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico", Ley 38-2017, según enmendada, que no excederán de cinco mil (5,000) dólares por cada incumplimiento con lo dispuesto en esta Ley.

…"

Sección 7.- Se añade un nuevo Artículo 7-A a la Ley 40-2024, según enmendada, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico", que leerá como sigue:

"Artículo 7-A. – Planes de Continuidad y Recuperación.

Toda Agencia y todo operador crítico deberá desarrollar, mantener y actualizar anualmente un Plan de Continuidad y Recuperación ante Incidentes Cibernéticos, el cual deberá ser sometido a PRITS para fines de evaluación y validación. Dichos planes deberán ser sometidos a pruebas periódicas no menos de una (1) vez al año o con mayor frecuencia según determine PRITS mediante reglamento."

Sección 8.- Se añade un nuevo Artículo 11-A a la Ley 40-2024, según enmendada, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico", que leerá como sigue:

"Artículo 11-A. — Fondo de Resiliencia Digital.

Se crea el Fondo de Resiliencia Digital adscrito a PRITS, con el propósito de financiar iniciativas de prevención, detección, respuesta y recuperación ante incidentes cibernéticos, así como programas de capacitación y certificación en ciberseguridad.

El Fondo podrá nutrirse de asignaciones legislativas, fondos federales, multas administrativas impuestas bajo esta Ley y cualquier otra fuente autorizada por ley. Las multas administrativas que nutran el Fondo tendrán como propósito exclusivo fortalecer la capacidad institucional de prevención, detección, respuesta y recuperación ante incidentes cibernéticos, y no se interpretarán como un mecanismo para la imposición indiscriminada de sanciones, sino como una herramienta para fomentar el cumplimiento y la sostenibilidad del sistema de ciberseguridad."

Sección 9.- Reglamentación.

Se ordena a la PRITS a enmendar aquella reglamentación que sea necesaria para cumplir con las disposiciones y propósitos de esta Ley en un término de noventa (90) días, luego de aprobada esta Ley.

Sección 10.- Vigencia

Esta Ley comenzará a regir inmediatamente después de su aprobación.