ORIGINAL

GOBIERNO DE PUERTO RICO

20ma. Asamblea Legislativa

3ra. Sesión Ordinaria

CÁMARA DE REPRESENTANTES

Actas y Récord
2026 APR -9 P 4:10

P. del S. 24

INFORME POSITIVO

9 de abril de 2026

A LA CÁMARA DE REPRESENTANTES:

La Comisión de Gobierno de la Cámara de Representantes de Puerto Rico, previo estudio y consideración del Proyecto del Senado 24, tiene a bien rendir este Informe Positivo sobre el Proyecto del Senado 24, recomendando su aprobación con las enmiendas contenidas en el entirillado electrónico que se acompaña.

ALCANCE DE LA MEDIDA

El Proyecto del Senado 24 (P. del S. 24), según radicado originalmente, propone crear la "Ley de Capacitación para la Seguridad Cibernética en Puerto Rico". La medida busca establecer, como política pública, la capacitación compulsoria sobre seguridad cibernética para proteger la confidencialidad e integridad de los activos de información. Para ello, ordena al Puerto Rico Innovation and Technology Service (PRITS) desarrollar y ofrecer un Programa de Capacitación para la Seguridad Cibernética que se impartirá, al menos, una vez al año.

En su versión original, las disposiciones del proyecto aplicaban de manera compulsoria a toda rama, agencia e instrumentalidad pública, corporaciones públicas, municipios y empresas privadas con un volumen de negocio de $100,000 o más. Además, la pieza legislativa tipificaba en su Artículo 6 como delito menos grave el incumplimiento mediante acción u omisión en el reporte o manejo establecido de un incidente cibernético.

No obstante, **con las enmiendas introducidas por esta Comisión**, la medida enfocará sus esfuerzos de capacitación y obligatoriedad *exclusivamente en el sector gubernamental*, excluyendo a la empresa privada del mandato compulsorio y eliminando las disposiciones penales que entran en conflicto con las legislaciones federales aplicables a las diversas industrias.

ANÁLISIS DE LA MEDIDA

Los adelantos tecnológicos han provocado alteraciones estructurales en organizaciones públicas y privadas, creando vulnerabilidades sin precedentes frente a ataques cibernéticos. Durante el año 2022, el PRITS detectó y bloqueó más de 753 millones de ataques cibernéticos en Puerto Rico. Al 31 de julio de 2023, ya se habían detectado alrededor de 490.5 millones de intentos de ciberataques, colocando a la Isla en un nivel alto de alerta.

Entre las múltiples modalidades de ataques, las amenazas internas ("insider threats") constituyen el eslabón más débil dentro de las organizaciones. Los empleados o individuos no siempre actúan con mala intención, pero sus errores humanos pueden perjudicar la red y la información. Por ello, la capacitación y la educación continua son la primera línea de defensa para prevenir estas vulnerabilidades.

A pesar de los méritos innegables de la educación en ciberseguridad, esta Comisión reconoce que la imposición de un programa gubernamental uniforme al sector privado resulta contraproducente y legalmente conflictivo. Las empresas privadas, particularmente las industrias de telecomunicaciones, seguros, banca y comercio general, ya se encuentran cobijadas bajo un extenso y robusto marco regulatorio federal y estatal que rige la protección de datos, la capacitación de sus empleados y los procesos rigurosos de notificación de incidentes. Por tanto, esta Comisión ha determinado acoger las recomendaciones presentadas en los memoriales para enmendar la medida, centrando el mandato legislativo en robustecer la infraestructura y el capital humano del Gobierno de Puerto Rico, salvaguardando a la empresa privada de la duplicidad regulatoria.

ALCANCE DEL INFORME

Para analizar y evaluar esta medida, la Comisión de Gobierno de la Cámara de Representantes solicitó memoriales a las siguientes entidades gubernamentales y del sector privado:

1. Departamento de Justicia
2. Oficina del Inspector General de Puerto Rico (OIG)
3. Asociación de Industriales de Puerto Rico
4. Centro Unido de Detallistas de Puerto Rico
5. Asociación de Bancos de Puerto Rico
6. Asociación de Compañías de Seguros de Puerto Rico (ACODESE)
7. Cámara de Mercado, Industria y Distribución de Alimentos (MIDA)
8. Autoridad para las Alianzas Público Privadas
9. Oficina de Gerencia y Presupuesto (OGP)
10. Asociación de Farmacias de la Comunidad
11. Asociación de Constructores de Puerto Rico

12. Asociación de Contratistas Generales
13. Asociación de Restaurantes de Puerto Rico
14. Asociación de Ejecutivos de Cooperativas
15. Cámara de Comercio de Puerto Rico
16. Negociado de Telecomunicaciones
17. Liberty
18. T-Mobile Puerto Rico, LLC
19. Claro Puerto Rico

De igual manera, esta Comisión recibió el expediente de la Comisión de Gobierno del Senado de Puerto Rico con los siguientes memoriales:

1. Puerto Rico Innovation & Technology Service (PRITS)
2. Oficina de Presupuesto de la Asamblea Legislativa (OPAL)

Se recibieron los siguientes memoriales, los cuales se detallan a continuación:

1. Puerto Rico Innovation & Technology Service (PRITS)

El PRITS expuso en su memorial que no avala la aprobación de la medida según está redactada, argumentando que los objetivos principales del P. del S. 24 ya se encuentran contemplados dentro de la Ley 40-2024 (Ley de Ciberseguridad). La agencia indicó que dicho estatuto ya les delega la responsabilidad de mantener un programa integral de educación en ciberseguridad dirigido tanto a servidores públicos como a la ciudadanía en general, e incluso provee un régimen de sanciones para las agencias que incumplan.

En fiel cumplimiento con estas disposiciones, el PRITS detalló que actualmente ya se encuentra ofreciendo programas de capacitación en seguridad cibernética a través de su plataforma PRITS Academy. Explicaron que, en el ámbito del servicio público, este programa provee cuatro horas de crédito de educación continua, convalidadas por la Oficina de Ética Gubernamental, y mantiene acuerdos con la OIG para dichos fines.

A modo de recomendación, la agencia sugirió que, en lugar de crear una nueva ley, los aspectos valiosos del P. del S. 24 (como los elementos del sector privado y las disposiciones presupuestarias) fuesen evaluados como enmiendas a la legislación vigente (Ley 40-2024) para fortalecer el andamiaje jurídico y optimizar los recursos disponibles.

2. Oficina del Inspector General de Puerto Rico (OIG)

La OIG compareció favoreciendo plenamente la aprobación de la medida, expresando que la educación preventiva y compulsoria es la estrategia más costo-efectiva. La entidad argumentó detalladamente que los incidentes cibernéticos

representan gastos directos millonarios (como eliminación de malware) y costos indirectos incalculables (como la pérdida de confianza pública y pleitos legales), los cuales pueden evitarse drásticamente al educar anualmente al personal.

La OIG validó su capacidad y autoridad para fiscalizar el cumplimiento de esta ley gubernamental, explicando que pueden incorporar verificaciones en sus planes de trabajo de auditoría rutinarios. Sugirieron que es esencial asegurar la debida coordinación presupuestaria con la Oficina de Gerencia y Presupuesto (OGP) y la AAFAF para identificar fondos, recomendando además explorar fondos federales de DHS/FEMA para sufragar la iniciativa.

Para el éxito de la medida, la OIG propuso múltiples enmiendas de rigor: requerir una certificación anual de cumplimiento por parte de los jefes de agencias ante la OIG; rendir informes periódicos de progreso a la Asamblea Legislativa; institucionalizar un Comité de Cumplimiento Interagencial; y exigir la revisión y actualización periódica del currículo de capacitación para adaptarlo a las nuevas amenazas.

3. Negociado de Telecomunicaciones (NET)

El NET presentó un memorial otorgando deferencia a los comentarios del PRITS y las demás agencias con peritaje, explicando que el propósito específico de crear un programa educativo de seguridad cibernética gubernamental recae fuera de su competencia primaria de regulación sobre las telecomunicaciones.

A pesar de su falta de jurisdicción primaria, la agencia analizó los méritos de la pieza legislativa y reconoció que busca reforzar la política pública establecida en la Ley 40-2024. Destacaron que, desde la perspectiva de la industria que ellos regulan, las compañías de telecomunicaciones en Puerto Rico ya cuentan con sistemas de ciberseguridad sumamente rigurosos para la protección integral de sus consumidores y su información sensitiva.

4. Cámara de Mercadeo, Industria y Distribución de Alimentos (MIDA)

MIDA presentó una postura de fuerte objeción al proyecto según radicado, argumentando que resulta irrazonable forzar la aplicación de un programa diseñado por PRITS (cuya naturaleza es gubernamental) a un sector privado sumamente diverso y complejo. Señalaron que el sector empresarial cuenta con corporaciones de mayor sofisticación y preparación técnica de lo que el gobierno podría proveerles.

En su análisis, MIDA detalló exhaustivamente que las empresas privadas ya están sujetas a múltiples leyes federales muy estrictas que ocupan el campo de la protección de datos, como la Ley HIPAA, la Ley GLBA, COPPA, FCRA y CAN-SPAM. Como recomendación, solicitaron a la Asamblea Legislativa que el alcance de la legislación se

limite de forma exclusiva al sector público, objetando formalmente la obligatoriedad impuesta a empresas privadas.

Finalmente, MIDA objetó enfáticamente el Artículo 6 sobre las sanciones penales, describiéndolo como vago e irracional. Advirtieron que tipificar como delito el incumplimiento en el reporte de un incidente causaría graves conflictos y confusión, dado que cada industria tiene sus propios protocolos y responde a leyes federales preexistentes con sus propias sanciones civiles y normativas.

5. Asociación de Compañías de Seguros de Puerto Rico (ACODESE)

ACODESE reconoció que la medida constituye un paso en la dirección correcta, pero solicitó formalmente que la industria de seguros sea eximida por completo de la aplicación de las disposiciones. Argumentaron que su sector ya opera bajo un marco regulatorio altamente especializado y excesivamente robusto.

La entidad detalló su cumplimiento forzoso con leyes federales críticas, como HIPAA, HITECH y Gramm-Leach-Bliley Act (GLBA). Estos estatutos ya les obligan a implementar controles técnicos, encriptación, auditorías constantes, notificación estricta de brechas a agencias federales, y programas de adiestramiento compulsorio para todo el personal que maneja información protegida.

Además del cumplimiento federal, recalcaron su adherencia estricta a la Regla Núm. 108 de la Oficina del Comisionado de Seguros (OCS), la cual ya contempla normas específicas de ciberseguridad para aseguradoras. ACODESE advirtió categóricamente que someterlos a esta ley crearía una reglamentación paralela, generando duplicidad regulatoria y cargas innecesarias desde una agencia (PRITS) que no tiene jurisdicción primaria sobre la industria de seguros.

6. Asociación de Industriales de Puerto Rico (AIPR)

La AIPR concurrió con el propósito del proyecto de proteger la información confidencial de las empresas y ciudadanos, pero rechazaron enfáticamente que el Programa de PRITS sea compulsorio para las entidades del sector privado. Advirtieron que establecer un límite de $100,000 haría la ley obligatoria para la inmensa mayoría de las empresas en la Isla, añadiendo una carga irrazonable a una jurisdicción ya muy regulada.

Sugirieron y recomendaron, como alternativa, que el programa sea estrictamente voluntario para la empresa privada, proponiendo que el PRITS confeccione "guías generales" que sirvan de referencia, a discreción de cada patrono. De esta forma, las empresas pueden fortalecer sus sistemas sin verse forzadas por mandatos punitivos que desconocen las particularidades operativas de cada negocio.

Respecto al Artículo 6, la AIPR señaló que el lenguaje resultaba ambiguo. Recomendaron clarificar la redacción para garantizar que el delito tipifique exclusivamente la conducta intencional y deliberada de permitir accesos no autorizados o el encubrimiento intencional, asegurando que no se penalice criminalmente los errores humanos involuntarios.

7. Asociación de Bancos de Puerto Rico (ABPR)

La ABPR apoyó la iniciativa de establecer medidas para combatir agresivamente la actividad criminal cibernética, pero solicitaron formalmente la incorporación de una exclusión expresa para que la ley no sea aplicable a las instituciones de la banca comercial. Detallaron que los bancos operan bajo el Título V del *Gramm-Leach Bliley Act* (GLBA) y regulaciones promulgadas por agencias federales (FDIC, FRB y OCC).

Bajo estas normas, están obligados a mantener un Programa de Seguridad de Información de Clientes (WISP) altamente complejo. Este programa les requiere asignar Oficiales Calificados, auditar controles técnicos, como la encriptación, y mantener adiestramientos obligatorios, continuos y periódicos sobre riesgos emergentes de seguridad para todo su personal. Además, poseen estrictos planes de respuesta a incidentes, rigurosamente supervisados a nivel federal.

Finalmente, la ABPR esbozó recomendaciones muy puntuales sobre el Artículo 6 de penalidades. Sugirieron definir legalmente qué constituye un "incidente de ciberseguridad" para armonizarlo con la Ley 40-2024; circunscribir el delito única y exclusivamente a conductas maliciosas e intencionales (excluyendo la negligencia); y aclarar los términos legales de "persona" y "datos" (para especificar si abarca formatos físicos además de los electrónicos).

8. Centro Unido de Detallistas (CUD)

El CUD presentó su oposición institucional al proyecto según radicado, argumentando que los objetivos primordiales ya se encuentran atendidos mediante la Ley 40-2024. Expresaron que el PRITS ya posee la autoridad estatutaria y la plataforma (PRITS Academy) para coordinar la capacitación, por lo que resulta más eficiente enmendar la ley vigente en lugar de crear una nueva.

En la eventualidad de que la medida avanzara, el CUD formuló tres recomendaciones vitales de enmienda para mitigar el impacto negativo en el sector comercial. Primero, solicitaron exceptuar a los comercios que no requieren o conservan información personal de clientes. Segundo, establecer una excepción para eximir a las microempresas y pequeños negocios con un volumen menor a $3 millones. Y tercero,

dirigir la ley exclusivamente a las agencias de gobierno y municipios, debido a su mayor volumen de información ciudadana.

9. Puerto Rico Telephone Company, Inc. h/n/c Claro Puerto Rico

Claro se opuso enfáticamente al proyecto, sosteniendo que la industria de las telecomunicaciones debe ser eximida en su totalidad. Explicaron que operan bajo el marco regulatorio de la sección 222 de la Ley de Comunicaciones de 1934 y las estrictas reglas de la FCC, las cuales rigen la protección de la información propietaria de los clientes (CPNI) y establecen mandatos concretos sobre la capacitación disciplinaria del personal.

Claro levantó una bandera sumamente importante sobre el Artículo 6 (penalidades), advirtiendo que crearía un choque irrazonablemente punitivo con la Regla 64.2011 de la FCC. Dicha normativa federal exige que las telecomunicaciones notifiquen las brechas de seguridad al Servicio Secreto de los EE. UU. (USSS) y al FBI en un plazo de siete días, prohibiendo notificar al público hasta que se complete ese proceso investigativo.

Por estas razones, y destacando su actual cumplimiento inquebrantable con estatutos locales y estándares globales (PCI DSS, ISO/IEC 27001, NIST, OWASP), Claro sostuvo que someterlos a esta legislación resultaría redundante y crearía conflictos con responsabilidades federales, solicitando su exclusión expresa de la medida.

10. T-Mobile Puerto Rico, LLC

T-Mobile presentó una firme oposición al proyecto según redactado, alineando su postura con la de la asociación nacional de la industria inalámbrica, CTIA. Aunque aplaudieron la intención del Estado, indicaron que imponer obligaciones compulsorias a la empresa privada generaría duplicidad, confusión y cargas regulatorias injustificadas, dado que ya operan bajo estándares globales (ISO 27001, SOC 2, PCI DSS).

Para sustentar su petición, T-Mobile detalló que mantiene un programa interno de capacitación estructurado por su equipo de *Cybersecurity Awareness and Training*, el cual imparte adiestramientos obligatorios a empleados basados en sus roles, realiza simulaciones constantes de *phishing* y exige salvaguardas a proveedores externos.

La corporación presentó dos propuestas contundentes de enmiendas. En primer lugar, solicitaron enmendar el Artículo 4 para eliminar por completo todas las referencias a empresas privadas, centrando el programa exclusivamente en el gobierno. En segundo lugar, exigieron suprimir en su totalidad el Artículo 6 (penalidades), argumentando que criminalizar el manejo de incidentes desvirtúa el fin educativo central de la medida y choca con normas vigentes de notificación.

11. Asociación de Centros Comerciales Puertorriqueños (ACCP)

La Asociación de Centros Comerciales Puertorriqueños (ACCP) compareció ante la Comisión mediante memorial escrito expresando que no pueden endosar la aprobación del Proyecto del Senado 24, según fue aprobado por dicho cuerpo legislativo. Su objeción principal y fundamental se centra en el Artículo 4 de la medida, el cual dispone que los mandatos de la ley aplicarán de manera compulsoria a las empresas privadas que generen un volumen de negocio de $100,000 o más.

En su análisis de la pieza legislativa, la ACCP argumentó que no favorecen que las medidas o programas de ciberseguridad diseñados y establecidos por el Gobierno sean impuestos al sector privado de forma unilateral. Enfatizaron que las necesidades de seguridad cibernética de cada sector o empresa son muy particulares, por lo que cada entidad comercial debe tener la flexibilidad y discreción de diseñar sus propios mecanismos y programas internos para prevenir efectivamente los riesgos de ataques cibernéticos y accesos no autorizados a sus bases de datos.

Finalmente, la organización empresarial reconoció que resulta lógico y razonable que el gobierno diseñe, a través de los recursos del PRITS, sus propios sistemas de protección de data y prevención de riesgos cibernéticos para la estructura pública. Sin embargo, sostuvieron firmemente que este mandato no debe ser extensivo al sector privado, al cual se le debe brindar el espacio necesario para establecer sus propios sistemas de protección de ciberseguridad sin que el Estado tenga que intervenir de una forma tan invasiva en el ámbito de la actividad empresarial.

12. Liberty Puerto Rico

Liberty compareció ante la Comisión mediante memorial escrito reconociendo el loable esfuerzo de la Asamblea Legislativa de establecer medidas estrictas de ciberseguridad para proteger la información. No obstante, plantearon que la medida no es adecuada para la industria de las telecomunicaciones, al tratarse de un sector sumamente especializado y regulado. Advirtieron que la imposición de este mandato gubernamental resultaría en una contraproducente duplicidad de esfuerzos y en costos innecesarios para las empresas, por lo que solicitaron formalmente a la Comisión que su industria sea eximida del cumplimiento de esta ley.

Para sustentar su solicitud de exclusión, la empresa de telecomunicaciones explicó detalladamente que ya vienen obligados a cumplir con normativas federales rigurosas, particularmente la Sección 222 de la Ley de Comunicaciones de 1934 y las reglas de la FCC enfocadas en la protección de la Información Propietaria de la Red del Cliente (CPNI, por sus siglas en inglés). Destacaron que estas regulaciones federales, junto a los estrictos estándares de seguridad de la industria de tarjetas de pago (Payment Card

Industry Data Security Standard o PCI DSS), ya les exigen mantener programas continuos de capacitación y concienciación para sus empleados en áreas críticas como prevención de phishing, manejo y almacenamiento seguro de datos, y respuesta a incidentes. Además, enfatizaron que rinden una certificación anual ante la FCC para confirmar el cumplimiento con estas normativas y actividades de adiestramiento.

Finalmente, Liberty argumentó que los procesos de manejo y reporte de incidentes propuestos en el proyecto interferirían con los protocolos especializados que ya rigen a su industria. Explicaron que, ante una infracción que comprometa información sensitiva, las normas federales les exigen notificar de forma expedita al Servicio Secreto de los EE. UU. y al FBI. A nivel local, también deben dar estricto cumplimiento a la Ley 11-2005 y al Reglamento del DACO, que disponen plazos inalterables de notificación a los consumidores y multas de hasta $5,000. Al estar cobijados por estas regulaciones específicas y por la política pública ya delineada estatutariamente en la Ley 40-2024 de Ciberseguridad, Liberty reiteró que aplicarles esta medida crearía interferencias, por lo que solicitaron su exclusión expresa del proyecto.

IMPACTO FISCAL

13. Oficina de Presupuesto de la Asamblea Legislativa (OPAL)

La OPAL emitió su Informe 2025-120 concluyendo que el efecto fiscal de la medida "No Se Puede Precisar" (NPP). Basaron su determinación en que los costos reales dependerán enteramente de los términos específicos y alcance de los acuerdos colaborativos que el PRITS suscriba con las diferentes agencias gubernamentales y las empresas privadas.

En su análisis, la OPAL destacó que las obligaciones de impartir talleres recaen sobre el PRITS. El impacto principal radicaba en la inclusión mandatoria de las empresas privadas, ya que en Puerto Rico existen sobre 44,668 Pequeñas y Medianas Empresas (PyMEs) y resultaba imposible estimar la cantidad exacta con ingresos mayores al límite propuesto de $100,000. Al desconocer este universo, la OPAL no pudo estimar los inmensos gastos operativos y logísticos adicionales que enfrentaría el Estado.

ENMIENDAS ACOGIDAS POR LA COMISIÓN

Con el firme propósito de acoger las valiosas recomendaciones vertidas en los memoriales, especialmente las presentadas por las asociaciones del sector privado (MIDA, AIPR, ACODESE, ABPR, CUD, Claro y T-Mobile), esta Comisión de Gobierno ha integrado enmiendas fundamentales en el entirillado electrónico que acompaña este Informe. A continuación, las principales modificaciones adoptadas:

1. **Exclusión Absoluta del Sector Privado (Artículo 4):** Se enmendó el alcance de aplicabilidad de la Ley para eliminar toda referencia e imposición compulsoria sobre las empresas o negocios privados, independientemente de su volumen de ingresos. La capacitación compulsoria será aplicable única y exclusivamente a las entidades de las Ramas Ejecutiva, Legislativa y Judicial, corporaciones públicas y municipios, evitando así cargas regulatorias excesivas, duplicidad normativa, y respetando las regulaciones y campos ocupados a nivel federal.

2. **Supresión de las Sanciones Penales (Artículo 6):** Se eliminó el propuesto delito menos grave relacionado al manejo y reporte de incidentes cibernéticos. Se reconoce, tal y como esbozaron múltiples deponentes, que la criminalización de esta conducta desvirtúa el propósito genuino de capacitación y choca dramáticamente con los requerimientos federales de notificación y con las políticas de reporte interno, protegiendo a los empleados de ser castigados penalmente por errores humanos o negligencia no intencional.

3. **Fortalecimiento de la Fiscalización Pública:** Se acogieron las recomendaciones de la OIG, incorporando requisitos para que los jefes de agencias rindan una certificación anual de cumplimiento y se institucionalicen mecanismos de rendición de informes a la Asamblea Legislativa, para garantizar que la política pública en el sector gubernamental sea verdaderamente efectiva.

4. **Armonización con la Ley 40-2024:** Se aclaró y delimitó el alcance del mandato al PRITS para que la implementación de este Programa sea un complemento directo a las facultades, definiciones y plataformas (PRITS Academy) ya existentes en la Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico, logrando la economía de recursos señalada por el PRITS y la OPAL.

CONCLUSIÓN

La Comisión de Gobierno de la Cámara de Representantes revisó en detalle y de manera responsable los señalamientos presentados por las dependencias públicas y las entidades del sector privado en torno al Proyecto del Senado 24. A través de este análisis, quedó en evidencia la necesidad de brindar herramientas de capacitación y educación en ciberseguridad, pero reconociendo las profundas diferencias operativas y legales que separan al sector público del ecosistema empresarial privado.

Las enmiendas acogidas en el entirillado electrónico son el resultado directo de escuchar activamente a nuestros sectores productivos. Excluir a la empresa privada de este mandato compulsorio es un paso estrictamente necesario y justificado para evitar chocar con leyes y entes reguladores federales y estatales como el FDIC, la FCC, HIPAA, GLBA, y la OCS, los cuales ya imponen a las industrias controles técnicos sumamente rigurosos y planes de adiestramiento de clase mundial. De igual forma, la eliminación

del componente penal evita conflictos jurisdiccionales y de procesos de notificación investigativa.

Al enmendar el alcance del proyecto para enfocarlo exclusivamente en capacitar y fiscalizar al componente gubernamental implementando las recomendaciones de rendición de cuentas esbozadas por la OIG, la medida se transforma en una herramienta de avanzada pero respetuosa de la libre empresa. Con estas modificaciones, garantizamos que el Gobierno fortalezca su infraestructura y el conocimiento de sus servidores públicos de la mano de PRITS, sin imponer un clima punitivo o sobrerregulatorio en nuestra economía.

POR TODO LO ANTES EXPUESTO, la Comisión de Gobierno de la Cámara de Representantes de Puerto Rico, rinde este Informe Positivo sobre el Proyecto del Senado 24, recomendando su aprobación **con las enmiendas contenidas en el entirillado electrónico que se acompaña**.

Respetuosamente sometido,

Hon. Víctor L. Parés-Otero
Presidente
Comisión de Gobierno
Cámara de Representantes de Puerto Rico

ENTIRILLADO ELECTRÓNICO
TEXTO APROBADO EN VOTACIÓN FINAL POR EL SENADO
(27 DE MAYO DE 2025)

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*

Coautores la señora Román Rodríguez; y el señor Santos Ortiz

Referido a la Comisión de Ciencia, Tecnología e Inteligencia Artificial

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, 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

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 del 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.

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, el PRITS está comprometido 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 el 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. Ciudadanos puertorriqueños han sido testigos de los efectos de ataques cibernéticos perpetrados a varias entidades gubernamentales y privadas.

Han sido múltiples las gestiones del 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 en una alianza entre PRITS y diversas agencias federales y locales 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 electrónicos del Gobierno. 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.

Tras innumerables esfuerzos del PRITS para combatir los ataques cibernéticos, aún persiste la necesidad de aprobar legislación, a los fines de establecer como política pública en 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~~, 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,~~ y en los servicios que se brindan a la ciudadanía. Ante ello, es urgente e imperante 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 en 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 o por cualquier persona que brinden servicios.

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

Se ordena al *Puerto Rico Innovation and Technology Service*, a desarrollar y ofrecer un Programa de Capacitación para la Seguridad Cibernética. *El diseño e implementación de este Programa fungirá como un complemento directo a las facultades, definiciones y plataformas, tales como el PRITS Academy, ya existentes en la Ley 40-2024, conocida como la 'Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico', con el fin de lograr la mayor economía de recursos.* 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 el *Puerto Rico Innovation and Technology Service* 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 o la confidencialidad de la información.

Artículo 4.- Aplicabilidad.

Las disposiciones de esta Ley aplicarán de manera compulsoria a toda rama, agencia e instrumentalidad pública, incluyendo las corporaciones públicas, así como las público-privadas que funcionan como empresas o negocios privados~~,~~ *y* municipios. ~~y empresas~~

~~privadas con un volumen de negocio de cien mil dólares con cero centavos ($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 cien mil dólares con cero centavos ($100,000.00) o más~~, podrán coordinar la asistencia del *Puerto Rico Innovation and Technology Service* o cualquier otra entidad gubernamental local 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 colaborativo.

Se faculta al *Puerto Rico Innovation and Technology Service* a llevar a cabo las gestiones necesarias para coordinar junto con la Oficina del Inspector General los acuerdos de colaboración con agencias, departamentos, organismos gubernamentales locales, federales y municipales, así como con otras instituciones públicas o privadas para adelantar los propósitos de esta Ley.

A tenor con lo anterior se requerirá que el jefe de cada agencia, municipio y entidad cubierta certifique anualmente ante la OIG (y PRITS) el cumplimiento de la capacitación en su dependencia. Esta certificación documentará el porcentaje de empleados adiestrados, fechas de los adiestramientos y cualquier incidente de seguridad significativo ocurrido.

Además, PRITS, en coordinación con la OIG, rendirán informes anuales a la Asamblea Legislativa detallando la implementación de la ley. El informe incluiría estadísticas de cumplimiento por sector, uso de fondos destinados a capacitación y resultados en términos de reducción de incidentes.

Artículo 6.- ~~Conducta delictiva; Penalidades~~. *Revisión y actualización periódica de la capacitación*

~~Toda persona que, mediante acción u omisión, o 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 comprometa su confidencialidad, incurrirá en delito menos grave.~~

El programa de capacitación será revisado y actualizado cada dos años con el insumo de la OIG, PRITS y expertos del campo para garantizar que los contenidos se mantengan relevantes ante la evolución constante de las amenazas cibernéticas. Esta revisión continua tendrá como objetivo fortalecer el impacto del programa de capacitación y facilitar la fiscalización.

Artículo 7.- Reglamentación.

Se faculta al *Puerto Rico Innovation and Technology Service* a que adopte la reglamentación necesaria para lograr el cumplimiento de las disposiciones de esta Ley. La reglamentación que se adopte deberá actualizarse, a tenor con los constantes avances tecnológicos. Incluyendo, pero sin limitarse, a incluir la figura que hará el monitoreo de cumplimiento, imposición de sanciones *administrativas*, entre otros.

La Reglamentación incluirá mecanismos para reforzar las fiscalización, la rendición de cuentas y el logro de objetivos

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 el *Puerto Rico Innovation and Technology*

Service, 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 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 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 parte específica de esta que así hubiere sido anulada o declarada inconstitucional. Si la aplicación a una persona o a una circunstancia de cualquier 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 dieciocho (18) meses luego de la aprobación de esta Ley.