ORIGINAL

GOBIERNO DE PUERTO RICO

20ma Asamblea Legislativa

2da Sesión Ordinaria

CÁMARA DE REPRESENTANTES

P. de la C. 825

INFORME POSITIVO

13 de noviembre de 2025

Actas y Récord
2025 NOV 13 P 2:45

A LA CÁMARA DE REPRESENTANTES DE PUERTO RICO:

La Comisión de Gobierno, previo estudio y consideración, tiene a bien someter a este Honorable Cuerpo el informe sobre el Proyecto de la Cámara 825, recomendando su **aprobación con las enmiendas** contenidas en el entirillado electrónico que acompaña este Informe.

ALCANCE DE LA MEDIDA

El Proyecto de la Cámara 825 propone enmendar los Artículos 6, 9, 12 y 13, añadir un nuevo Artículo 16 y reenumerar los subsiguientes artículos de la Ley 75-2019, conocida como la *"Ley de la Puerto Rico Innovation and Technology Service"*; así como enmendar los Artículos 7, 8 y 10, añadir un nuevo Artículo 11 y reenumerar los subsiguientes artículos de la Ley 40-2024, conocida como la *"Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico"*.

El propósito de esta medida es fortalecer las facultades de la Puerto Rico Innovation and Technology Service (PRITS) para identificar vulnerabilidades, evaluar la capacidad de respuesta de las entidades gubernamentales y asegurar que estén preparadas para enfrentar posibles ataques cibernéticos. Además, armoniza ambas leyes, tanto la de PRITS y como la de Ciberseguridad, para garantizar una gobernanza tecnológica sólida y coherente en todo el aparato gubernamental.

INTRODUCCIÓN

Surge de la Exposición de Motivos que, a pesar de los esfuerzos realizados mediante la aprobación de la Ley de Gobierno Electrónico, la Ley 75-2019 y la Ley 40-2024, los ataques cibernéticos a entidades públicas continúan representando un riesgo significativo para la seguridad, la información y la continuidad de las operaciones gubernamentales.

La medida parte de la premisa de que la protección cibernética es un elemento indispensable de la infraestructura del Estado moderno, y que PRITS debe contar con las herramientas y la autoridad necesarias para ejercer su función fiscalizadora y coordinadora.

Asimismo, se reconoce la necesidad de establecer mecanismos más ágiles para la detección, monitoreo y mitigación de vulnerabilidades, y de reforzar los estándares de cumplimiento y respuesta de todas las agencias, corporaciones públicas y municipios del Gobierno de Puerto Rico.

ÁNALISIS DE LA MEDIDA

Como parte del trámite legislativo de esta medida, se les solicitó ponencia al Departamento de Hacienda, el Departamento de Justicia, el Departamento de Seguridad Pública (DSP), la Federación de Alcaldes de Puerto Rico, PRITS, a la Oficina de Presupuesto de la Asamblea Legislativa (OPAL), a la Universidad de Puerto Rico (UPR) y a la Asociación de Alcaldes de Puerto Rico (Asociación).

Se evaluaron los memoriales explicativos presentados por la PRITS, UPR, Asociación y OPAL. A continuación, se detallan sus respectivas posturas:

Puerto Rico Innovation and Technology Service

PRITS expresó su firme apoyo a la aprobación del Proyecto de la Cámara 825, destacando que la medida refuerza sus facultades como ente rector en materia de innovación, información y tecnología. Subrayó que la legislación armoniza los marcos normativos de la Ley 75-2019 y la Ley 40-2024, lo que facilitará una coordinación efectiva entre las dependencias del Gobierno y promoverá una política pública uniforme de ciberseguridad.

La agencia apoyó la incorporación de nuevos subincisos que fortalecen sus funciones, señalando que la adopción de estándares internacionales de seguridad garantiza uniformidad y eleva la calidad de los controles, alineando a Puerto Rico con las mejores prácticas internacionales.

Por otro lado, recomendó que la referencia a los estándares técnicos se exprese de manera genérica y flexible, ya que las normas como NIST, ISO/IEC o CIS son revisadas periódicamente. De este modo, la medida se mantendría vigente sin requerir enmiendas legislativas constantes, permitiendo que PRITS adopte los estándares más actualizados mediante guías.

En cuanto a la creación del Comité sobre Ciberseguridad adscrito a PRITS, planteó que ya existe una estructura operativa bajo la Oficina de Evaluación de Incidentes Cibernéticos y la figura del Principal Oficial de Seguridad Cibernética, por lo que un comité adicional podría representar un nivel de burocracia innecesario.

No obstante, esta Comisión no acoge dicha objeción, por entender que la intención legislativa es precisamente fortalecer la colaboración interagencial y multisectorial en el área de la ciberseguridad. La participación de la academia, los municipios y las asociaciones que agrupan a los gobiernos locales añade valor y diversidad de perspectivas a los procesos de planificación y prevención. Lejos de duplicar funciones, el Comité propone una estructura consultiva que potencia la coordinación y la respuesta colectiva ante amenazas cibernéticas, sin afectar la autoridad ni las funciones actuales de PRITS.

En suma, varias de las recomendaciones de PRITS fueron acogidas por esta Comisión en el entirillado electrónico que acompaña este informe. PRITS reconoció que las disposiciones propuestas fortalecen la gobernanza tecnológica, alinean la política pública con estándares internacionales y mejoran la capacidad de respuesta del Estado ante amenazas digitales.

Universidad de Puerto Rico

La UPR destacó la importancia de reforzar la gobernanza tecnológica y la ciberseguridad gubernamental. Reafirmó su compromiso con la innovación y la formación de recursos humanos especializados en estas áreas.

Destacamos que su participación en el Comité sobre Ciberseguridad se considera esencial para fomentar la educación continua, la investigación aplicada y la adopción de mejores prácticas tecnológicas en el sector público.

Asociación de Alcaldes de Puerto Rico

La Asociación expresó no tener mayores reparos al proyecto, pero planteó preocupación respecto a la disposición que requiere que los municipios presenten anualmente a la PRITS su Plan Estratégico de Tecnología, conforme a la Ley 40-2024.

La Comisión reconoce y valora la preocupación de la Asociación, pero considera que la medida no impone cargas administrativas adicionales, sino que promueve la asistencia técnica y la capacitación municipal en materia de ciberseguridad.

Puntualizamos que los municipios administran sistemas con información crítica sobre finanzas, infraestructura y servicios esenciales. Por tanto, su integración a la red de seguridad tecnológica del Gobierno no es opcional, sino necesaria para proteger la información ciudadana y garantizar la continuidad de los servicios públicos.

Además, el proyecto dispone que la PRITS podrá establecer guías y metodologías uniformes para facilitar el cumplimiento de los municipios, lo que asegura apoyo técnico sin imponer obligaciones desproporcionadas.

En síntesis, la inclusión de los municipios en este proceso fortalece la protección digital del país, promueve la equidad tecnológica y permite una respuesta integral ante incidentes cibernéticos que puedan afectar tanto a agencias estatales como a gobiernos locales.

Oficina de Presupuesto de la Asamblea Legislativa (OPAL)

La OPAL señaló que la aprobación de la medida no tendrá un impacto fiscal directo sobre el Fondo General. Indicó que el proyecto fomenta nuevas formas de seguridad, eficiencia y transparencia en el uso de la tecnología gubernamental, sin crear estructuras ni compensaciones adicionales.

Es importante destacar que OPAL señala que, a pesar de que la medida establece un nuevo Artículo 11 en la Ley 40, supra, para integrar un Comité sobre Ciberseguridad en PRITS, el mismo no establece compensación ni dietas para sus integrantes, por lo que no se anticipa costo fiscal en ese aspecto. Sin embargo, aluden a que en la medida que el cumplimiento con las nuevas normas de ciberseguridad y cooperación entre agencias resulte en una pérdida de eficacia laboral que requiera de la contratación de recursos adicionales, el impacto fiscal derivado de la aprobación de la medida de reflejará en los costos asociados a los salarios y beneficios de dicho personal.

La Comisión entiende que el fortalecimiento de la PRITS como autoridad principal en asuntos tecnológicos es esencial para garantizar la resiliencia digital del Gobierno de Puerto Rico.

La creación del Comité sobre Ciberseguridad fomentará la coordinación interagencial e intermunicipal, incorporando a la academia y las asociaciones municipales en los esfuerzos de planificación y prevención.

De igual forma, las enmiendas que autorizan la imposición de sanciones y la adopción de estándares internacionales constituyen herramientas necesarias para promover la rendición de cuentas, la estandarización y la mejora continua en los sistemas de información del Estado.

La Comisión coincide en que el Proyecto de la Cámara 825 responde a una necesidad apremiante y que su aprobación representa un paso firme hacia la modernización y la protección de los sistemas digitales del Gobierno de Puerto Rico.

IMPACTO FISCAL

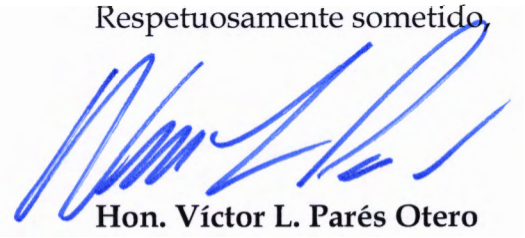
La OPAL concluye que la aprobación del P. de la C. 825 no conllevará un Impacto Fiscal sobre el Fondo General.

CONCLUSIÓN

Este proyecto consolida la estructura de gobernanza tecnológica del Gobierno, refuerza la capacidad institucional para atender incidentes cibernéticos, y fortalece la seguridad y continuidad de los servicios públicos en beneficio del país.

Por tanto, la Comisión de Gobierno, tras evaluar los méritos del Proyecto de la Cámara 825 y considerar las ponencias recibidas, **recomienda su aprobación con las enmiendas contenidas en el entirillado electrónico que acompaña este informe**.

Respetuosamente sometido,



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

ENTIRILLADO ELECTRÓNICO
GOBIERNO DE PUERTO RICO

20ma Asamblea Legislativa — 2da Sesión Ordinaria

CÁMARA DE REPRESENTANTES

P. de la C. 825

26 DE AGOSTO DE 2025

Presentado por el representante *Aponte Hernández*

Referido a la Comisión de Gobierno

LEY

Para enmendar los artículos 6, 9, 12 y 13, añadir un nuevo Artículo 16 y reenumerar los subsiguientes artículos de la Ley 75-2019, conocida como "Ley de la Puerto Rico Innovation and Techonology Service"; enmendar los artículos 7, 8 y 10 , añadir un nuevo Artículo 11 y reenumerar los subsiguientes artículos de la Ley 40-2024, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico"; a los fines de fortalecer las facultades de la Puerto Rico Innovation and Technology Service para identificar vulnerabilidades, evaluar la capacidad de respuesta de las entidades gubernamentales y asegurar que estén preparadas para enfrentar posibles ataques cibernéticos; y para otros fines relacionados.

EXPOSICIÓN DE MOTIVOS

Por virtud de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico", se adoptó como política pública la incorporación de las tecnologías de información a los procedimientos gubernamentales, a la prestación de servicios y a la difusión de información, mediante una estrategia enfocada en el ciudadano, orientada a la obtención de logros y que fomente activamente la innovación. Así las cosas, se estableció que la Puerto Rico Innovation and Technology Service (PRITS) será la agencia responsable de administrar los sistemas de información e implantar las normas y los procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental, además, asesorará a las agencias, actualizará y desarrollará las transacciones gubernamentales electrónicas, y se asegurará del funcionamiento correcto de las mismas.

Así también, la Ley 75-2019, conocida como "Ley de la Puerto Rico Innovation and Technology Service", otorgó a la PRITS la facultad de implantar, desarrollar y coordinar la política pública del Gobierno sobre la innovación, información y tecnología. También le confirió el deber de ofrecer servicios a los departamentos, agencias, corporaciones públicas, municipios y cualquier otra dependencia o instrumentalidad pública del Gobierno en relación a la integración de la tecnología a la gestión gubernamental y a la presentación de servicios a la ciudadanía.

No obstante, la integración y utilización de la tecnología trae consigo una serie de retos y situaciones. Así, por ejemplo, el uso de la Internet conlleva riesgos de ataques, de estrategias de infiltración y accesos no autorizados a los sistemas de información. Ciertamente, el Gobierno ha implementado diversos esfuerzos para atender estos problemas relacionados con la seguridad cibernética, entre los que podemos mencionar, la promulgación de la Ley Núm. 40-2024, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico". Con la referida Ley Núm. 40, se pretendió establecer un marco regulatorio para formular una política pública de ciberseguridad que propicie y fomente el desarrollo económico en un ambiente seguro y confiable.[1] Por virtud de dicha Ley, la PRITS es responsable de velar por la administración segura de los Recursos de información e implementar las normas y procedimientos relativas a la seguridad de las tecnologías de la información a nivel gubernamental, y de ofrecer asesoramiento a las agencias y actualizar y desarrollar las estrategias y planes de seguridad cibernética del Gobierno y asegurar del cumplimiento de las agencias con los mismos.[2]

A pesar de los esfuerzos implementados por el Gobierno, los ataques cibernéticos continúan. Conforme a información publicada en el portal de internet de la PRITS, en el 2022, fueron detectados y bloqueados unos 753,276,059 ataques. Para el 2023, la cantidad disminuyó a 517,885,218, y para el 2024 a 82,491,332. Durante el presente año, 2025, hasta 1 de mayo se habían registrado unos 1,505,488.

En efecto, el Gobierno de Puerto Rico ha estado expuesto a ataques cibernéticos. Entre los que han trascendido públicamente, podemos mencionar los suscitados en el 2017 que afectaron el sistema electrónico del Departamento de Hacienda y del Centro de Recaudaciones de Ingresos Municipales. En el 2020, ocurrió un ataque cibernético a diversas cuentas de agencias gubernamentales estatales, incluyendo la Compañía de Fomento Industrial de Puerto Rico (PRIDCO) y la Administración de Sistemas de Retiro. En el 2022, el Senado de Puerto Rico, así como la Oficina de Servicios Legislativos fue blanco de un ciberataque en sus sistemas de informática. Durante ese mismo año, también se registró un ataque al sistema de AutoExpreso, el cual, lo mantuvo inoperante

[1] Véase la Exposición de Motivos de la Ley 40-2024.
[2] Véase Artículo 5 de la Ley Núm. 40-2024.

durante un tiempo. En el 2023, la Autoridad de Acueductos y Alcantarillado sufrió un ciberataque a los sistemas de servicio al cliente. En días más recientes, el Departamento de Justicia, en específico el Sistema de Información de Justicia Criminal (SIJC-PR), fue objeto de un ciberataque.

Es menester señalar que, además de los costos que estos incidentes pueden conllevar para el Gobierno, también pueden poner en riesgo información sensitiva y comprometer la seguridad y continuidad en las operaciones gubernamentales.

Por lo cual, se hace necesario continuar implementando medidas para detectar, monitorear y mitigar vulnerabilidades en aplicaciones y servicios que permitan no tan solo asegurar la continuidad de los servicios públicos, sino, además, proteger la integridad de los sistemas, así como la información que contiene. Es necesario reforzar las estrategias para fortalecer y maximizar los esfuerzos encaminados para aumentar los niveles de seguridad cibernética en cada dependencia del Gobierno de Puerto Rico. Debemos priorizar la identificación y mitigación de vulnerabilidades en los sistemas de información. Se trata un enfoque proactivo que permita un esfuerzo concertado para reducir el impacto de ataques cibernéticos que ocurran contra el gobierno.

Con esta legislación, se enmienda la Ley Núm. 75, *supra,* para, entre otras cosas, reforzar las facultades de la PRITS como agencia encargada de todo lo relacionado a tecnología en el Gobierno de Puerto Rico, estableciendo el deber de las agencias de proveer información esencial que le permita a la PRITS identificar vulnerabilidades y evaluar la capacidad de respuesta de las entidades gubernamentales, para asegurar que estén preparadas para enfrentar posibles amenazas y/o ataques cibernéticos. Además, se busca armonizar las disposiciones de la Ley Núm. 75, antes citada, y la Ley Núm. 40-2024. En el caso de esta última Ley, se enmienda a los efectos de disponer que las agencias deben reportar inmediatamente a la Oficina para la Evaluación de Incidentes Cibernéticos adscrita a PRITS, cualquier sospecha de incidente de seguridad de manera que se puedan tomar las acciones correspondientes. También se realizan enmiendas técnicas a la referida Ley Núm. 40. Ambas leyes son complementarias, pero requieren ajustes para lograr una armonización plena que permita una gobernanza tecnológica sólida y una ciberseguridad efectiva.

DECRÉTASE POR LA ASAMBLEA LEGISLATIVA DE PUERTO RICO:

Sección 1.- Se enmienda el Artículo 6 de la Ley Núm. 75-2019, para que lea como sigue:

"Artículo 6. — Funciones, facultades y deberes de la Puerto Rico Innovation and Technology Service y del Principal Ejecutivo de Innovación e Información del Gobierno (PEII).

a) …

…

ff) …

gg) Velar por la adopción de estándares internacionales ~~(NIST CFS, ISO/IEC 27001, CIS Controls)~~ de seguridad de la información y ciberseguridad, según determine PRITS, mediante la adopción de guías en todos los departamentos, agencias, corporaciones públicas, municipios y cualquier otra dependencia o instrumentalidad pública del Gobierno.

hh) Auditar y validar configuraciones tecnológicas y de seguridad, imponer plazos de remediación y suspender temporalmente sistemas que representen riesgos graves, en coordinación con la Oficina para la Evaluación de Incidentes Cibernéticos, y de conformidad con la Ley 40-2024.

ii) Establecer, junto al Departamento de Hacienda y la Oficina de Gerencia y Presupuesto, la metodología y procedimientos que permitan identificar la inversión del Gobierno en tecnología, incluyendo: infraestructura, servicios profesionales, suscripciones y licenciamiento, entre otros."

Sección 2.- Se enmienda el Artículo 9 de la Ley Núm. 75-2019, para que lea como sigue:

"Artículo 9. — Plan Estratégico de Innovación y Tecnología para el Gobierno de Puerto Rico.

La Puerto Rico Innovation and Technology Service creará un Plan Estratégico que articule una visión exhaustiva, congruente, abarcadora y duradera sobre la utilización de las tecnologías de información y comunicación del Gobierno. El Plan Estratégico incluirá un mecanismo efectivo de integración de los múltiples sistemas de las tecnologías de información y comunicación utilizadas por las diferentes agencias; se nutrirá de las mejores prácticas identificadas en las agencias estatales, y federales e internacionales, así como en el sector privado; y establecerá prioridades para los proyectos tecnológicos actuales y futuros. A su vez, la Puerto Rico Innovation and Technology Service evaluará y analizará anualmente los planes de trabajo en todas las agencias, relativo a la administración, el uso, el análisis, el despliegue y la inversión de las tecnologías de información y comunicación del Gobierno. Además, la Puerto Rico Innovation and Technology Service, en colaboración con las agencias, creará e implementará un plan estratégico de recuperación tecnológica en situaciones de desastres o emergencias. *Todos los departamentos, agencias, corporaciones públicas, municipios y cualquier otra dependencia o instrumentalidad pública del Gobierno deberán presentar anualmente a PRITS su Plan Estratégico de Tecnología, alineado con la Ley 40-2024, y la política pública relacionada a tecnología."*

Sección 3.- Se enmienda el Artículo 12 de la Ley Núm. 75-2019, para que lea como sigue:

"Artículo 12. - — Deberes y Responsabilidades de las Agencias.

Para cumplir cabalmente con los objetivos y la política pública establecida en esta Ley, las agencias tendrán que cumplir con los siguientes deberes y responsabilidades:

(a) ...

(b) Proveer y divulgar a la Puerto Rico Innovation and Technology Service, en el tiempo requerido, aquella información, datos, documentos y servicios necesarios y esenciales que les sean requeridos por la Puerto Rico Innovation and Technology Service, salvo que la divulgación requerida esté expresamente prohibida por ley o reglamento. *Así también, las agencias deberán proveer anualmente, a la Puerto Rico Innovation and Technology Service, lo siguiente:*

i. Inventario de activos y dispositivos de informática que posee la agencia.

ii. Informar las aplicaciones o programas (software) utilizados por la agencia, incluyendo su funcionalidad.

iii. Planes de resguardo y recuperación de datos que tenga la agencia.

iv. Evaluaciones de vulnerabilidad realizados por la agencia.

v. Programa de educación de Ciberseguridad para el personal y sus contratistas.

vi. Plan o Protocolo de contingencia para atender incidentes.

vii. Plan de Continuidad de Negocio.

viii. Plan de recuperación de Desastres.

ix. Plan interno de respuesta a incidentes de ciberseguridad.

La entrega de inventarios, planes y evaluaciones debe estar alineada a los estándares reconocidos ~~(NIST SP 800-61r2, ISO /IEC 27001, CIS Controls) y los formatos, métricas y frecuencia de actualización que, mediante guías, la PRITS determine.~~ internacionalmente de seguridad de la información y ciberseguridad, según determine PRITS, mediante la adopción de guías.

(c) …

…

(l) Adoptar las herramientas de seguridad informática establecidas por la PRITS.

(m) *Cumplir con lo dispuesto en la Ley Núm. 40-2024, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico"."*

Sección 4.- Se enmienda el Artículo 13 de la Ley Núm. 75-2019, para que lea como sigue:

"Artículo 13. — Oficial Principal de Informática de las agencias.

Para cumplir cabalmente con los objetivos y la política pública establecida en esta Ley, el Oficial Principal de Informática de cada agencia, o en su defecto, el director o directores de información y tecnología de toda agencia, tendrán que cumplir con las políticas, protocolos, guías operacionales dispuestas por el PEII y los siguientes deberes y responsabilidades:

(a) …

…

(l) *Cumplir con lo dispuesto en la Ley Núm. 40-2024, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico".*

(m) Coordinar, participar y alinear sus planes, recursos y prioridades con los proyectos estratégicos liderados o apoyados por PRITS, tanto en materia de tecnología como de seguridad de la información, garantizando la implementación uniforme y eficiente en todo el Gobierno.

(n) Será el Oficial de Seguridad de Sistemas de Información de la Agencia a cargo de lo siguiente:

i. Cumplimiento normativo y regulatorio establecido por PRITS.

ii. Supervisar la creación y manejo de cuentas.

iii. Detectar, analizar y responder a incidentes de ciberseguridad.

iv. Coordinar planes de contingencia y recuperación ante desastres.

v. Mantener bitácoras y evidencias de incidentes de ciberseguridad.

vi. Ofrecer adiestramientos de seguridad a empleados y usuarios.

vii. Fomentar buenas prácticas de ciberseguridad.

viii. Participar en el diseño de nuevos sistemas, asegurando que incluyan controles de seguridad desde el inicio.

ix. Evaluar periódicamente la efectividad de las medidas de seguridad.

x. Recomendar mejoras tecnológicas y procesos para fortalecer la seguridad digital."

Sección 5.- Se añade un nuevo Artículo 16 a la Ley Núm. 75-2019, para que lea como sigue:

"Artículo 16.- Penalidades

Si alguna Agencia incumpliese con lo dispuesto en la presente Ley, la Puerto Rico Innovation and Technology Services podrá imponer a la Agencia y/o autoridad nominadora, una multa de hasta mil (1,000) dólares por cada violación, previa notificación y oportunidad de ser escuchada. Se faculta a PRITS a adoptar la reglamentación necesaria o enmendar la vigente, que disponga el procedimiento para la imposición de multas administrativas.

Se podrá recurrir en revisión de la multa administrativa de conformidad con las disposiciones de la Ley 38-2017, según enmendada, conocida como "Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico."

Sección 6.- Se reenumeran los artículos 16 al 37 de la Ley Núm. 75-2019, como artículos 17 al 38, respectivamente.

Sección 7. Se enmienda el Artículo 7 de la Ley Núm. 40-2024, 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 todo persona natural o jurídica que haga negocios o contrate con ellos cumpla con al menos los siguientes Estándares y principios mínimos de Ciberseguridad:

(1) ...

...

(8) Para garantizar las mejores prácticas de ciberseguridad, las agencias deben establecer un mecanismo de clasificación de datos basado en su criticalidad

para el gobierno y los ciudadanos, después de esta clasificación se establece *como requisito* el uso de autenticación multifactorial (MFA, en inglés) para todo usuario, *independientemente que la Agencia haya realizado clasificación de los datos.*

(9) …

…

(19) Las Agencias deberán mantener un plan interno de respuesta a incidentes de ciberseguridad, el cual deberán someter a la PRITS, en la frecuencia que esta disponga.

[19] *(20)* Cualquier otro estándar y principio de Ciberseguridad que la PRITS determine sea necesario.

..."

Sección 8.- Se enmienda el Artículo 8 de la Ley Núm. 40-2024, para que lea como sigue:

"Artículo 8.- Oficina para la Evaluación de Incidentes Cibernéticos.

Se crea la Oficina para la Evaluación de Incidentes Cibernéticos (Oficina) adscrita a PRITS. La misma será dirigida por el Principal Oficial de Seguridad Cibernética.

La Oficina se encargará de:

(1) …

…

(15) …

Toda Agencia deberá cumplir con los requisitos y solicitudes de la Oficina y se deberá acoger e implementar cualquier recomendación o directriz notificada por la Oficina.

Toda Agencia tendrá la obligación de informar, *inmediatamente tenga conocimiento,* cualquier sospecha de Incidente de seguridad a la Oficina para que, en coordinación con la Agencia, la Oficina lleve a cabo el proceso de Gestión de incidente, el tomar medidas para aislar el Incidente, tomar acciones para mitigar el impacto del Incidente, participar en la coordinación con agencias locales y federales que tengan injerencia sobre el Incidente, así como resolver el Incidente, documentar el mismo e identificar lecciones aprendidas. *La Oficina determinará la forma en que las agencias harán la notificación sobre la sospecha del Incidente. El Principal Oficial de Informática (OPI) y/o los responsables de seguridad cibernética deberán alinear su planes, recursos y prioridades con los proyectos estratégico de PRITS en infraestructura tecnológica, seguridad de la información y resiliencia cibernética.*

La Oficina preparará un informe trimestral, el cual deberá ser radicado tanto en la Cámara de Representantes como en el Senado de Puerto Rico, en el cual divulgará los resultados de sus gestiones e investigaciones el cual será publicado en las páginas de la PRITS y del Instituto. PRITS deberá adoptar políticas y estándares en cuanto al contenido y formato de estos informes."

Sección 9.-Se enmienda el Artículo 10 de la Ley Núm. 40-2024, para que lea como sigue:

"Artículo 10.- Sanciones.

Si alguna Agencia incumpliese con lo dispuesto en esta Ley, la PRITS podrá imponer a la Agencia, previa notificación y oportunidad de ser oída, una multa no menor de cincuenta (50) dólares ni mayor de cien (100) dólares diarios por

Incidente, por cada día que incumpla con los Estándares y principios de Ciberseguridad según establecidos en el Artículo **[6]** *7* de esta Ley.

Cuando medie obstrucción, negligencia, mala fe, temeridad o negativa caprichosa en el manejo o reporte de un Ciberataque, la PRITS podrá imponer a la Agencia, previa notificación y oportunidad de ser oída, una multa no menor de mil (1,000) dólares ni mayor de cinco mil (5,000) dólares por cada violación.

…"

Sección 10.- Se añade un nuevo Artículo 11 a la Ley Núm. 40-2024, para que lea como sigue:

"Artículo 11.- Comité sobre Ciberseguridad

Se crea el Comité sobre Ciberseguridad, adscrito a la PRITS. El Comité estará integrado por los representantes de las siguientes agencia y entidades:

1. *Oficina de Evaluación de Incidentes Cibernéticos, adscrito a la PRITS,*
2. *Universidad de Puerto Rico,*
3. *Departamento de Justicia,*
4. *Oficina de Gerencia y Presupuesto,*
5. *Departamento de Seguridad Pública,*
6. *Federación de Alcaldes,*
7. *Asociación de Alcaldes,*
8. *Cámara de Representantes y*
9. *Senado de Puerto Rico.*

En el caso de las agencias o entidades gubernamentales, la persona que participará en el Comité debe ser el Secretario, Director, Comisionado o Administrador de dicha agencia o el representante en quien este delegue, en cuyo caso, la persona deberá tener preparación académica y/o amplio conocimiento en el asunto de la Ciberseguridad. Por decisión de la mayoría de los miembros del Comité, se podrá integrar cualquier otra persona que sea necesaria incluir para adelantar los propósitos de esta Ley.

El Comité será presidido por el Principal Oficial de Seguridad Cibernética de la Oficina de Evaluación de Incidentes Cibernéticos. El Comité tendrá la responsabilidad de identificar, estudiar y, evaluar todos los problemas y necesidades relacionadas con ciberseguridad. Además, deberán coordinar y realizar ejercicios conjuntos y compartir los indicadores de compromisos.

Toda Agencia cooperará con el Comité en todos aquello que le sea requerido relacionado al asunto de Ciberseguridad."

Sección 11.- Se reenumeran los artículos 11 al 17 de la Ley Núm. 40-2024 como artículos 12 al 18, respectivamente.

Sección 12.- Esta Ley entrará en vigor inmediatamente después de su aprobación.