(P. de la C. 1530)

LEY

Para crear la "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico"; establecer como principio de política pública que proveer seguridad a los datos gubernamentales es esencial para apoyar los procesos de innovación y el fomentar desarrollo y crecimiento económico sostenible de todos los sectores en Puerto Rico; crear el cargo del Principal Oficial de Seguridad Cibernética (Chief Information Security Officer) bajo la oficina del Puerto Rico Innovation and Technology Service ("PRITS") y establecer sus facultades y deberes, a los fines de garantizar la ejecución de la política pública establecida en esta Ley; establecer la obligación de las Agencias de colaborar con la PRITS y con el Principal Oficial de Seguridad de Información; crear la Oficina para la Evaluación de Incidentes Cibernéticos adscrita a la PRITS; ordenar a PRITS a adoptar y promulgar en todas las agencias reglamentación de conformidad con lo establecido en esta Ley; establecer relaciones patrono-empleados sobre el uso de sus sistemas; y para otros fines relacionados.

EXPOSICIÓN DE MOTIVOS

Contrario a lo que se puede pensar, la ciberseguridad ha existido desde la creación del Internet, la única diferencia es que en los últimos quizás 24 a 36 meses hay un incremento dramático en la cantidad de ataques, de estrategias de infiltración y accesos no autorizados a los sistemas de información que comprometen la seguridad y el comercio del país por el secuestro, robo o manipulación de la información.

La ciberseguridad se inscribe dentro del concepto más amplio de la seguridad de la información, cuyo objetivo es proteger la información de sistemas que se encuentran interconectados. Existen también otros conceptos relacionados a la ciberseguridad, como pueden ser el cibercrimen, las ciberamenazas o el ciberespacio, cuya característica principal y común reside en la existencia de estos en la red.

El Foro Económico Mundial y la Organización de las Naciones Unidas (ONU) han señalado al cibercrimen entre los principales riesgos para la humanidad, junto a los desastres naturales y el cambio climático, y en poco tiempo, la pandemia del COVID-19 ha exacerbado los riesgos virtuales para todas las industrias.

La crisis propiciada a principios del año 2020 por la pandemia del COVID-19 ha puesto en relieve la dependencia a una infraestructura vital que, para la gran mayoría de los ciudadanos, resulta invisible o su existencia pasa prácticamente desapercibida. La vida diaria gira alrededor de actividades cada vez más digitalizadas y, por consiguiente,

más sensibles a amenazas cibernéticas. Cadenas de suministro de alimentos, transporte, pagos y transacciones financieras, actividades educativas, trámites gubernamentales, servicios de emergencia, y hasta el suministro de agua y energía, entre un sinnúmero de actividades, operan en la actualidad a través de tecnologías digitales.

La pandemia de COVID-19 ayudó a reflexionar sobre el progreso en la expansión el uso de las tecnologías de la información y la comunicación, la conectividad a Internet y la ciberseguridad en Puerto Rico. La mayor dependencia del ciberespacio durante la crisis subraya la necesidad de extraer lecciones para lo que se espera en la transformación continua de la sociedad y economía, y en garantizar la ciberseguridad a nivel nacional.

En un sentido más general, en la última década los ataques cibernéticos han aumentado en frecuencia y complejidad. El bajo costo y el riesgo mínimo que conllevan estos delitos han sido factores clave en su crecimiento. Con el simple uso de una computadora y el acceso a Internet los cibercriminales pueden causar daños enormes mientras permanecen relativamente anónimos.

Tanto las personas como las instituciones están expuestas a la incertidumbre y la impredecible naturaleza del delito cibernético. Por lo tanto, es imprescindible abordar estas amenazas. Los esfuerzos para hacerlo deben ser de naturaleza multidimensional, porque se requiere una variedad de factores para construir una sociedad resiliente. Las políticas y los marcos legales deben ajustarse y todas las partes interesadas de la sociedad civil, así como los sectores público y privado, deben trabajar para crear una cultura de ciber conciencia y capacitar a profesionales calificados para construir una estrategia de ciberseguridad; por lo tanto, es un esfuerzo continuo y complejo.

El crecimiento en el número de ataques cibernéticos ha suscitado un mayor interés por la seguridad cibernética a nivel mundial. Para presentar un ejemplo simple, la búsqueda de la palabra ciberseguridad en línea, en uno de los *search engines* más conocidos, de marzo de 2016 a junio de 2019, aumentó de 20 a 100. En otras palabras, el interés por saber más sobre ciberseguridad se ha vuelto popular entre los usuarios de Internet. Casualmente, los usuarios que indagan sobre ciberseguridad tienden a buscar cursos y oportunidades de capacitación en el campo. Es decir: más personas están conscientes de la importancia de la ciberseguridad e investigan formas de mejorar sus conocimientos.

Las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la propiedad, así como para aumentar la confianza de los ciudadanos en las tecnologías digitales, y que estos puedan sentirse cómodos accediendo a dichas tecnologías. El crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo. A nivel agregado, las cifras adquieren aún mayor magnitud pues los daños económicos de los ataques cibernéticos podrían sobrepasar el 1% del Producto Interno

Bruto en algunos países. En el caso de los ataques a la infraestructura crítica, esta cifra podría alcanzar hasta el 6% del GDB.

El daño generado por fuentes internas puede ser difícil de detectar porque estas amenazas abarcan una amplia gama de comportamientos y motivos. Una amenaza podría provenir de un empleado descontento que intenta interrumpir las operaciones, un integrante del personal que busca ganar dinero extra vendiendo datos o un colaborador bien intencionado que simplemente pasa por alto una política de seguridad de la empresa para ahorrar tiempo.

Puerto Rico aún no está suficientemente preparado para enfrentar los ataques cibernéticos que se producen. El país sufrió más de 926 millones de intentos de ciberataques en 2021 y para mediados del 2022 ya sumaban sobre 12.4 millones de ataques confirmados. No obstante, identificar un peligro cibernético es tan sólo el primer paso. Tomar medidas contra las amenazas y crímenes del ciberespacio es un reto aún mayor para el país. La realidad es que los recursos son limitados para investigar los delitos que se cometen en el ciberespacio. Más aún, para lograr que dichos delitos resulten en juicio es todavía un reto mayor. Parte del problema comienza muchas veces en la propia ley: en un tercio de los países (incluyendo a Puerto Rico) no existe un marco legal sobre los delitos informáticos.

El 1 de febrero de 2021 se formalizó en Puerto Rico la oficina de Seguridad Cibernética del Gobierno con la contratación del Principal Oficial de Seguridad Cibernética (CISO). Esta oficina tiene le encomienda de proveer servicios centralizados de ciberseguridad para el Gobierno mediante acuerdos de colaboración con agencias federales y proveedores externos de servicios y de proteger y fortalecer la seguridad de los sistemas de información y los datos del Gobierno mediante controles, monitoreo y respuestas ágiles en cuanto a incidentes de ciberseguridad.

Contar con profesionales más capacitados se ha vuelto fundamental para diseñar e implementar las políticas y medidas de seguridad cibernética que son necesarias para garantizar la resiliencia del país frente a ciberataques cada vez más sofisticados y complejos.

Desde el punto de vista de ciberseguridad, se reconoce erróneamente que el tema de la ciberseguridad está en manos solo de expertos y tal vez en el sentido técnico más elevado sí. Sin embargo, la ciberseguridad es un tema crucial que debe estar bajo la responsabilidad de todos los ejecutivos y gerenciales y debe incluirse como requisito de educación para todos los usuarios de sistemas y tecnologías, como computadoras y dispositivos móviles. Cuidando que las aplicaciones que tienen en sus dispositivos móviles no sean aplicaciones que pueden llegar a extraer información sobre todo cuando están relacionadas íntimamente al trabajo, *Google Drive, Dropbox* o *One Drive*, por mencionar algunas aplicaciones.

El desarrollo de una estrategia abarcadora de seguridad cibernética otorga a un país un enfoque más integral que permite comprender y atender mejor los desafíos de la seguridad cibernética. Asimismo, esta planificación estratégica permite priorizar sus objetivos e inversiones en seguridad cibernética.

Los países deben estar preparados para adaptarse rápidamente al entorno dinámico que los rodean y tomar decisiones basadas en un panorama de amenazas en constante cambio. Pasar al siguiente nivel de preparación requerirá una política de ciberseguridad integral y sostenible, apoyada por una gestión pública asertiva, con asignación de recursos financieros y capital humano calificado para llevarla a cabo.

El reto de proteger el espacio digital continuará creciendo. Hay que ser proactivos, pero más certeros en desarrollar e implantar leyes que ayuden a mitigar los problemas de ciberseguridad en Puerto Rico. Todos los ciudadanos tienen una vida digital que hay que proteger por lo que el Gobierno tiene que servir de escudo para proteger la información de sus ciudadanos, salvaguardar su privacidad y que estos se sientan seguros en el mundo digital.

Por todo lo anterior, esta Asamblea Legislativa está convencida de que es hora de crear un marco regulatorio para formular una política pública de ciberseguridad robusta y abarcadora que propicie y fomente el desarrollo económico en un ambiente seguro y confiable. A tales efectos, se aprueba la presente Ley.

DECRÉTASE POR LA ASAMBLEA LEGISLATIVA DE PUERTO RICO:

Artículo 1.-Título.

Esta ley será conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico".

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.

Artículo 3.-Política Pública.

Se establece como política pública en Puerto Rico lo siguiente:

1. Establecer unos estándares y principios mínimos de ciberseguridad centrada en el concepto de "zero trust architecture" para que el Gobierno pueda incorporar al quehacer gubernamental las tecnologías electrónicas y cibernéticas con el propósito de transformar y agilizar las relaciones del Gobierno entre sí, con la ciudadanía en general, así como las empresas locales y extranjeras, de manera que el Gobierno resulte en uno más accesible, efectivo y transparente, pero de una manera segura y confiable;

2. Establecer como política una prohibición a toda agencia o persona natural o jurídica cubierta, así como a sus agentes, aseguradores, o garantizadores a realizar cualquier tipo de Pago por rescate en respuesta a un Ransomware y establecer colaboración con la Agencia de Ciberseguridad e Infraestructura del Departamento de Seguridad Nacional, según establecido por la "State and Local Government Cybersecurity Act" de 2021. A manera de excepción, y evaluando caso a caso, se permitirá el evaluar negociar un pago si se trata de:

    a. Infraestructura crítica; o

    b. Exista un riesgo inminente de perdida de vida;

    En caso de que un Pago por rescate en respuesta a un Ransomware se realice por alguna de las razones antes listadas y consultadas con la Oficina, no se considerará un incumplimiento con esta sección.

3. Proteger y mantener la confidencialidad, integridad y disponibilidad de la información almacenada y/o administrada por los Recursos de información gubernamentales y los activos de infraestructura relacionados, ya sea que esté en reposo (almacenada), que esté en movimiento (transmitida o recibida), o que está siendo creada o en proceso de transformación (procesada);

4. Incrementar las actividades para coordinar y mejorar la seguridad de las redes gubernamentales y la infraestructura crítica y proteger los datos que contienen;

5. Potenciar las capacidades y los esfuerzos para impedir, detectar, prevenir, proteger y responder a las amenazas contra los Recursos de información y los Datos del Gobierno;

6. Garantizar un entorno de Tecnología de la Información (TI) estable y seguro mediante la implementación de medidas adecuadas para reducir los riesgos de

seguridad cibernética a través de la prevención, reducción y limitación de la pérdida de información o la degradación operativa de los Recursos de información gubernamentales y accionar medidas correctivas y protocolos que aseguren la rapidez de atender y resolver cualquier ataque inminente;

7. Proteger los derechos de intimidad y privacidad de los ciudadanos, sin coartar los derechos de una sana convivencia en la red cibernética;

8. Detener y castigar el uso indebido de las personas de todo tipo de Tecnología de información utilizados en la comisión de actos delictivos;

9. Cumplir con las normas básicas de ciberseguridad establecidas en la Orden Ejecutiva emitida el pasado 12 de mayo de 2021 por el Presidente de los Estados Unidos, Hon. Joe Biden, y con cualquier orden subsiguiente que trate sobre el tema de ciberseguridad.

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) "Acceso no autorizado" — ocurre cuando una persona, grupo, código, programa, aplicación o cualquier otra entidad o proceso informático obtiene acceso lógico, digital o físico sin aprobación o consentimiento a una red de infraestructura crítica, sistema, datos, aplicación, "data room" u otro recurso de tecnología de la información del Gobierno o cuando se obtiene acceso o se intenta obtener acceso a información o recursos que no son necesarios para cumplir con su trabajo y o función, siguiendo el Principio de Privilegios Mínimos;

(b) "Activos sensitivos" — significará información, equipo o medios donde la pérdida, mal uso, acceso o modificación no autorizadas pudieran afectar adversamente los intereses del Gobierno y/o la privacidad de los ciudadanos;

(c) "Agencia" — significa el conjunto de funciones, cargos y puestos que constituyen toda la jurisdicción de una autoridad nominadora, independientemente de que se le denomine departamento, corporación pública, oficina, administración, comisión, junta o de cualquier otra forma;

(d) "Agencia de Ciberseguridad e Infraestructura (CISA)" - una agencia del Departamento de Seguridad Nacional de los Estados Unidos (DHS) que es responsable de fortalecer la seguridad cibernética y la protección de la

infraestructura en todos los niveles del gobierno, coordinar los programas de seguridad cibernética con los estados y demás jurisdicciones de los Estado Unidos , y mejorar las protecciones de seguridad cibernética del gobierno contra piratas informáticos privados y nacionales, según lo dispuesto por la "Cybersecurity and Infrastructure Security Agency Act" de 2018".

(e) "Arquitectura de confianza cero" (zero trust architecture, en inglés) – significa que se asume que ninguna conexión, usuario o activo es confiable hasta que esté verificado;

(f) "Autorización" – significa el proceso de otorgar a un usuario privilegios de acceso a la información o a un sistema de información siguiendo el Principio de Privilegios Mínimos;

(g) "Ciberataque" – El término "ciberataque" significa el uso de un Código no autorizado o malicioso en un sistema de información o el uso de otro mecanismo digital, como un ataque de denegación de servicios, con el propósito interrumpir o afectar las operaciones de un sistema de información o comprometer la confidencialidad, disponibilidad, o integridad de información digital almacenada en, procesada por, o que transita a través de un sistema de información;

(h) "Ciberseguridad" – significará la prevención de daños a, protección y restauración de computadoras, sistemas y/o servicios de comunicación electrónica, incluyendo la información contenida en ellos para garantizar su disponibilidad, integridad, autenticidad, confidencialidad y no repudio;

(i) "Confidencialidad" – significa preservar las restricciones de acceso y divulgación, incluyendo los medios para proteger la privacidad e información confidencial;

(j) Credenciales – significa los atributos únicos que se proporcionan a cada usuario autorizado para acceder a los recursos y aplicaciones de los sistemas de información;

(k) "Datos" – significa cualquier secuencia de uno o más símbolos a los que se les da significado mediante actos específicos de interpretación;

(l) "Estándares y principios mínimos de ciberseguridad" – significa un marco que proporciona unas prioridades y objetivos estratégicos de seguridad de las redes y Recursos de información;

(m) "Gestión de incidentes" — significa todos los procedimientos administrativos, físicos y técnicos aplicados para la investigación y mitigación ante la sospecha o el reporte de un Incidente. Incluyendo las notificaciones de violación o brechas a las partes o individuos impactados por el Incidente, según aplicables por las regulaciones federales y locales;

(n) "Gobierno" — significa el Estado Libre Asociado de Puerto Rico;

(o) "Incidente" o "Incidente de seguridad de la información" - significa un suceso que (i) pone en riesgo real o inminente, sin autoridad, la integridad, confidencialidad o disponibilidad de la información, sistema o proceso o un Recurso de información; o (ii) representa un uso indebido de un Recurso de información o una violación o amenaza inminente de violación de la ley, políticas de seguridad, procedimientos de seguridad, políticas de uso aceptable o prácticas estándar de seguridad informática;

(p) "Infraestructura crítica" — se refiere a los servicios, sistemas, recursos y activos esenciales, ya sean físicos o virtuales, cuya incapacidad o destrucción tendría repercusiones perjudiciales en la seguridad cibernética, la salud, la economía, la seguridad de Puerto Rico o cualquier combinación de esos asuntos.

(q) "Instituto" o "Instituto de Estadísticas" — se refiere al Instituto de Estadísticas de Puerto Rico, creado por la Ley 209-2003, según enmendada, conocida como "Ley del Instituto de Estadísticas de Puerto Rico".

(r) "Oficina" — se refiere a la Oficina para la Evaluación de Incidentes Cibernéticos creada por esta Ley.

(s) "Pago Por Rescate" — El término "Pago por rescate" significa la transferencia de dinero u otra propiedad o activo, incluyendo monedas virtuales, o cualquier fracción de estas, que se haya realizado en conexión a un ataque de Ransomware, excluyendo el pago legítimo de servicios por respuesta a un incidente.

(t) "Principal Oficial de Seguridad Cibernética (Chief Information Security Officer)" — significa el Principal Oficial de Seguridad Cibernética (Chief Information Security Officer) del Gobierno;

(u) "Principio de Privilegios Mínimos ("Principle of Least Privelage")" - Cada módulo (proceso, usuario, o programa, dependiendo del tema) solo puede acceder a la información y recursos necesarios para su propósito legítimo.

(v) "(PRITS)" – significa la Puerto Rico Innovation and Technology Service, Oficina de la Rama Ejecutiva encargada de implantar, desarrollar y coordinar la política pública del Gobierno sobre la innovación, información y tecnología, según lo dispuesto por la Ley 75 de 2019;

(w) "Programa" o "software" – se refiere a los programas informáticos y datos asociados que pueden escribirse o modificarse dinámicamente durante su ejecución;

(x) "Proveedor de servicios contratados" – significa una entidad, ya sea persona natural o jurídica, pública o privada que provee servicios como redes, aplicaciones, programas, infraestructura o medios de seguridad mediante el soporte continuo y habitual, así como servicios de administración activa ya sea en las instalaciones de una Agencia, en el centro de procesamiento de datos de la Agencia (hosting), o en el centro de procesamiento de datos de un tercero;

(y) "Ransomware" – El término "Ransomware"

i. significa un Ciberataque, que incluye una amenaza de utilizar un código no autorizado o malicioso en un Recurso de información, o una amenaza de utilizar otro mecanismo digital, como un ataque de denegación de servicios, con el propósito interrumpir o afectar las operaciones de un Recurso de información o comprometer la confidencialidad, disponibilidad, o integridad de información digital almacenada en, procesada por, o que transita a través de un Recurso de información, con el fin de exigir un Pago por rescate; y

ii. no incluye un evento en el cual el pago sea exigido por una entidad del Gobierno Federal, una investigación de seguridad bona fide, un pago legítimo de servicios por respuesta a un incidente o como respuesta a una invitación hecha por el dueño u operador del sistema de información a terceros para identificar vulnerabilidades en el sistema de información;

(z) "Recursos de información" – significa información y los recursos relacionados, como, por ejemplo, personal, equipos, programas y Tecnología de la información, entre otros;

(aa) "Riesgo" – significa toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y Recursos de información.

(bb) "Seguridad Informática" — significa el conjunto de controles, salvaguardas y otras medidas que toma una organización para proteger la información en cualquier formato. Esto implica la protección de los activos de informática, incluyendo la información, independientemente de si los activos están interconectados;

(cc) "Tecnología de la Información (TI)" — El término "Tecnología de la Información (TI)"

i. Para una Agencia, significa cualquier sistema o recurso interconectado o subsistema de equipo utilizado en la adquisición, almacenamiento, análisis, evaluación, manipulación, manejo, movimiento, control, visualización, conmutación, intercambio, destrucción, transmisión o recepción automática de datos o información, si el equipo es utilizado por la agencia directamente o por un tercero bajo un contrato con la agencia que requiere el uso (i) de ese equipo; o (ii) de ese equipo en una medida significativa para la prestación de un servicio o el suministro de un producto;

ii. incluye computadoras, equipos auxiliares (incluidos periféricos de imágenes, dispositivos de entrada, salida y almacenamiento necesarios para la seguridad y vigilancia), equipos periféricos diseñados para ser controlados por la unidad central de procesamiento de una computadora, software, firmware y procedimientos y servicios similares (incluyendo servicios de apoyo) y recursos relacionados.

Toda palabra o frase usada en singular se entenderá que también incluye el plural, salvo que del contexto se desprenda otra cosa. De igual forma, los términos usados en género femenino incluirán el masculino y viceversa.

Todas las definiciones aquí listadas deben ser evaluadas conforme a las definiciones promulgadas por el National Institute of Standards and Technology (NIST).

Artículo 5.- Implementación de la política pública.

La Puerto Rico Innovation and Technology Service (PRITS) será la responsable de, a tenor con la política pública establecida en la presente Ley, 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, a la vez que ofrecerá asesoramiento a las Agencias y actualizará y desarrollará las estrategias

y planes de seguridad cibernética del Gobierno y se asegurará del cumplimiento de las Agencias con los mismos.

Toda Agencia, en colaboración con PRITS, deberá desarrollar, documentar e implementar un programa de Ciberseguridad de acorde con esta Ley. El programa, como mínimo, deberá incluir todos los activos de información de la Agencia, incluyendo servicios de informática provisto por terceros, una evaluación de riesgos de Ciberseguridad que la Agencia llevará a cabo por lo menos una vez al año, un plan educativo que vele por la educación del personal, contratistas, y clientes (la ciudadanía), incluyendo cursos especializados para desarrollo de los administradores de sistemas y tecnologías sobre las mejores prácticas de Ciberseguridad y una evaluación de vulnerabilidades de seguridad tanto interno como externo ("penetration test") para validar la efectividad de los controles que la agencia haya implementado.

PRITS deberá revisar y evaluar los programas de Ciberseguridad a nivel de cada Agencia para validar que son afines a los estándares y principios adoptados por PRITS, así como el cumplimiento con lo estipulado en esta Ley y toda ley aplicable.

PRITS deberá identificar cuáles son los sistemas y servicios de informática críticos del Gobierno y deberá desarrollar y ejecutar planes para validar la efectividad de los controles de seguridad en esos sistemas y servicios de informática críticos.

PRITS deberá velar que toda Agencia tenga publicado en su portal de Internet el Aviso de Privacidad, disponible para el conocimiento de la ciudadanía.

PRITS deberá, en conjunto con cualquier otra Agencia que estime pertinente, desarrollar y divulgar un Protocolo de Ciberseguridad ante una Emergencia.

El Instituto y PRITS tendrán la obligación de divulgar en su portal de internet, para la disposición de la ciudadanía, estadísticas sobre los Incidentes reportados por las Agencias, velando por el cumplimiento de la protección de información Confidencial sobre los Recursos de información del Gobierno.

El Instituto y PRITS, además, coordinarán con el sector privado para publicar los Incidentes que estos reciban y que voluntariamente autoricen a divulgar.

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. Al momento de la creación de esta posición, la Oficina de

Gerencia y Presupuesto deberá autorizar y diligenciar la creación del puesto del Principal Oficial de Seguridad Cibernética ("Chief Information Security Officer") del Gobierno y notificará a la Oficina de Administración y Transformación de los Recursos Humanos del Gobierno de Puerto Rico para garantizar que se cumplan con todas las leyes y reglamentos aplicables.

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

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

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.

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) Establecer mecanismos de control para detener tráfico en el internet categorizado como inapropiado y una política de seguridad para al menos bloquear el acceso a sitios web con contenido pornográfico, programas malignos (malware), suplantación de identidad u obtener datos de la identidad de usuario (phishing) y otras amenazas identificadas a menos que sea requisito para el cumplimiento del deber;

(2) Establecer mecanismos de control en capas, que refuercen la confidencialidad, integridad y autorización con el fin de proteger la información;

(3) Establecer políticas de uso apropiado de equipos y sistemas de información y reforzar con controles administrativos y técnicos y establecer mecanismos de control, tanto administrativos como técnicos, para acceder a la red de información tanto interna como externa;

(4) Establecer controles administrativos que hagan requisito en el uso de cifrados, basado en mejores recomendaciones del National Institute of Standards and Technology (NIST) para reforzar la confidencialidad e integridad de la data en transporte y en almacén. Establecer mecanismos técnicos para forzar las políticas establecidas;

(5) Establecer las conexiones remotas a la red del gobierno se realizarán únicamente a través de una red privada virtual (VPN, en inglés) o cualquier otro programa de red privada virtual que el gobierno contrate exclusivamente para uso oficial cuando las tareas relacionadas con el trabajo sean necesarias. Para el uso de la aplicación VPN o cualquier otro programa de red privada virtual que el gobierno contrate o utilice se establecerá un acuerdo que incluya una autorización del administrador de datos y un reconocimiento de unas responsabilidades y deberes mínimos de protección y manejo de información.

(6) Todo desarrollo de programas o aplicación utilizado por una Agencia o mediante contrato con un Proveedor de servicios contratados, para brindar servicios a los ciudadanos a través de Internet o facilitar las operaciones internas de la Agencia, deberá asegurar que cumpla con los Estándares y principios mínimos de seguridad para su implementación;

(7) Cualquier agencia que acepte pagos con tarjeta de crédito en sus portales a través de un mecanismo de pago deberá cumplir con las mejores prácticas y estándares de seguridad de datos de la industria de tarjetas de pago (PCI-DSS o la mejor práctica), de la agencia no tener su propio sistema, debe exigir a su proveedor de servicios financieros informes de cumplimiento desarrollados por terceros, para determinar cumplimiento con los estándares antes de contratar;

(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 el uso de autenticación multifactorial (MFA, en inglés) para todo usuario.

(9) Los contratos con Proveedores de servicios contratados incluirán medidas para salvaguardar los Activos sensibles. Todo proveedor contratado debe cumplir con la Ley Federal de Administración de Seguridad de la Información y mantener no menos de tres (3) años de información. En el evento de ser requerida para ley y orden, deben tener la capacidad de producirla electrónica y en no menos de dos (2) días desde que se requiere la información;

(10) Los Proveedores de servicios contratados de tecnología de la información y comunicaciones compartirán información y notificarán en un término no mayor de cuarenta y ocho (48) 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;

(11) Para cualquier contrato de servicios de Ciberseguridad, el proveedor de servicios externo presentará a PRITS informes mensuales sobre el estado de la Ciberseguridad de los sistemas de información y cualquier Activo sensitivo administrado en nombre de la Agencia. Estos informes incluirán la información que se detalla a continuación:

a. Las amenazas detectadas, los actores de amenazas y las vulnerabilidades;

b. Las acciones de respuesta y remediación inmediata;

c. El número total de incidentes de seguridad de la información que se informaron al PRITS a través de la plataforma para el Informe de Incidentes de Ciberseguridad; y

d. El avalúo realizado sobre el estado de la Ciberseguridad;

(12) Los Proveedores de servicios contratados cuyos servicios estén relacionados con la Ciberseguridad o cuyos servicios requieran que información sensible de los ciudadanos resida en sus sistemas, deberán contar con todas las certificaciones de seguridad válidas que requiera PRITS al momento de firmar el contrato, deberán cumplir con las mejores prácticas en cuanto a certificación de industria de ciberseguridad y deberán cumplir con esta Ley y todas las leyes, reglas y estándares aplicables;

(13) Las Agencias instalarán controles automáticos para la detección de programas no deseados (por ejemplo, virus, adware, spyware, malware, Ransomware) y la prevención de eventos o actividades de intrusión que puedan afectar la seguridad de la información.

(14) Los sistemas de TI del gobierno se utilizarán estrictamente para realizar asuntos gubernamentales o para los propósitos que sean autorizados por el Gobierno, el acceso a los sistemas de TI del gobierno debe ser por roles, y solo incluir la información necesaria para su trabajo y o función, siguiendo el Principio de Privilegios Mínimos;

(15) Las instalaciones y activos de procesamiento de información (por ejemplo, servidores, armarios de cableado para redes, conexiones telefónicas, áreas de impresión para datos sensitivos o confidenciales) deberán estar alojados en áreas seguras, no rotuladas, protegidas con un perímetro de seguridad

apropiado y controles para evitar el acceso no autorizado y daños y deberán contar con un generador eléctrico para evitar fallas en caso de problemas con el servicio eléctrico, como parte de un protocolo de contingencia;

(16) La información confidencial (por ejemplo, IIP, IPS) no quedará expuesta ni desprotegida en ninguna circunstancia. Deberá estar encriptada en todos sus estados (es decir, en tránsito y en reposo);

(17) Establecer y mantener un programa de educación de Ciberseguridad para el personal y para la ciudadanía, incluyendo personal de entidades que provean servicios al Gobierno;

(18) Establecer planes de resguardo y recuperación de datos que deben ser integrado al plan de contingencia de la Agencia para velar por la continuidad de las operaciones considerando sistemas mantenidos localmente y los sistemas mantenidos por suplidores o terceros tipo "cloud";

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

Las Agencias deberán consultar con la PRITS antes de realizar cualquier contrato, enmienda, renovación o extensión de contrato con un Proveedor de servicios contratados sobre los requisitos mínimos de Ciberseguridad que deberá tener dicho proveedor para cumplir con los Estándares y principios de Ciberseguridad.

Todo contrato con un Proveedor de servicios contratados otorgado sin consultar con PRITS deberá ser enviado a PRITS para evaluación y podrá ser cancelado de PRITS encontrar que no cumple o que no puede ser enmendado para cumplir con los Estándares y principios de Ciberseguridad.

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. Llevar a cabo la gestión de incidentes cada vez que se produzca un Incidente o un Incidente de seguridad de la información;

2. Definir los procesos para el cumplimiento del monitoreo (24/7) de la seguridad cibernética;

3. Monitorear, identificar, responder y administrar los riesgos y eventos que involucran irregularidades de seguridad, infracciones o comprometen los activos de información, incluyendo la pérdida, el uso indebido y el acceso o divulgación no autorizados;

4. Realizar evaluaciones trimestrales del riesgo y la magnitud del daño que podría resultar del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados de la información y los sistemas de información que respaldan las operaciones y los activos de las Agencias;

5. Establecer controles para prevenir el inicio de ataques cibernéticos desde sus redes internas a otros sistemas de información externos;

6. Abordar la adecuación y eficacia de los procedimientos y las prácticas de seguridad cibernética en los planes e informes de manejo;

7. Apoyar a las Agencias en la investigación, mitigación y resolución de incidentes de seguridad, incluyendo la colaboración con agencias locales y federales que tengan injerencia sobre el incidente;

8. Informar al PRITS cualquier incidente de seguridad cibernética, intrusión o amenaza a la ciberseguridad utilizando las herramientas proporcionadas para tales fines;

9. Desarrollar y promulgar métricas sobre los ataques recibidos y confirmados;

10. Establecer un Protocolo de Ransomware;

11. Establecer un Protocolo de contingencia;

12. Establecer requisitos de capacitación para toda aquella persona que use un sistema de información electrónico;

13. Establecer requisitos mínimos para el uso y manejo de sistemas;

14. Establecer penalidades para el mal uso de sistemas de información; y

15. Establecer un programa que le de responsabilidad al usuario de sistemas y consecuencias de no cumplir.

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 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 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.

Artículo 9.- Obligación de informar y educar sobre la Política Pública de Ciberseguridad

La PRITS establecerá y mantendrá un programa de educación virtual para informar y educar al público sobre la Ciberseguridad. Este programa incluirá educación sobre los aspectos técnicos para la utilización segura y apropiada de los instrumentos electrónicos o cibernéticos que facilitan el acceso a la información pública. El material educativo deberá contener herramientas para la identificación y manejo de un posible ataque cibernético, así como donde y cuando informar dicho ataque. La información y educación que se presente estará disponible de manera virtual y asincrónica en el portal de la PRITS.

Además, la PRITS, en colaboración con la Oficina de Ética Gubernamental, establecerá y mantendrá un programa de educación continua para los Oficiales de Información y para los servidores públicos de las Agencias sobre las disposiciones de esta Ley y la Política Pública de Ciberseguridad. Como parte del referido programa, se requerirá que los Oficiales de Información y los servidores públicos del Gobierno tomen un curso de educación continua de Ciberseguridad anualmente. Además, la PRITS podrá programar el uso de ejercicios de capacitación y preparación como los llamados Table Top Exercises, entre otros.

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 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.

Si se identifica a un servidor público responsable de esta conducta, la PRITS, en coordinación con la Oficina de Administración y Transformación de los Recursos Humanos (OATRH) y con la autoridad nominadora correspondiente, ordenará, previa notificación y oportunidad de ser oído, la anotación de la determinación en el expediente de personal del servidor público. De dicha acción culminar en el despido de dicho servidor público, el mismo no podrá ser contratado por una Agencia o contratista del gobierno, ni como empleado, ni bajo una relación como contratista o subcontratista por un periodo de cinco (5) años.

Si se identifica a un Proveedor de servicios contratados responsable de esta conducta, le aplicaría sanciones monetarias conforme hasta un tope de la cuantía contratada, más cualquier otra contractual y por daños causados, incluyendo penalidades establecidas por leyes locales y federales aplicables. Además, ni ese Proveedor de servicios o cualquier entidad que tenga un número significante de la misma gente podrá ser contratado por una Agencia o contratista del Gobierno, ni como subcontratista por un periodo de cinco (5) años.

Todo incumplimiento con esta Ley conllevará un proceso de reeducación y capacitación que será coordinado por PRITS, en colaboración con la Oficina de Ética Gubernamental.

Artículo 11.- Asignación presupuestaria.

Los gastos que conlleve la aplicación de las disposiciones contenidas en esta Ley estarán sujetos a la disponibilidad de los fondos para sufragar los mismos, según certifiquen la Oficina de Gerencia y Presupuesto y la Autoridad de Asesoría Financiera y Fiscal a las Agencias concernidas. Así también, los fondos necesarios para su implantación deberán ser consignados en los presupuestos correspondientes por cada año fiscal.

Artículo 12.- 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 13.- Cláusula de Supremacía.

Ante cualquier inconsistencia entre la legislación, reglamentación, órdenes administrativas o cartas circulares vigentes y las disposiciones incluidas en esta Ley, se dispone la supremacía de esta legislación y la correspondiente enmienda o derogación de cualquier inconsistencia con este mandato, a menos que sea materia de campo ocupado federal o esté sustancialmente en conflicto con alguna ley federal, en cuyo caso prevalecerá lo dispuesto en la ley federal.

Artículo 14.-Reglamentación.

Se faculta a PRITS a adoptar la reglamentación necesaria o enmendar la vigente, con el fin de hacer cumplir las disposiciones aquí estatuidas. El procedimiento para adoptar esta reglamentación estará exento de cumplir con las disposiciones de la Ley 38-2017, según enmendada.

Además, el PRITS se asegurará que la reglamentación que se apruebe no será más restrictiva a los requisitos establecidos por el gobierno federal.

Artículo 15.- Cláusula de Transición.

El Gobierno tendrá un periodo de seis (6) meses para finalizar todos los trámites necesarios para cumplir con lo establecido en esta Ley.

Artículo 16.-Cláusula de separabilidad.

Si cualquier parte de esta Ley fuere declarada inconstitucional o defectuosa por un tribunal competente, la sentencia a tal efecto dictada no afectará, perjudicará, ni invalidará el resto de esta Ley. El efecto de dicha sentencia quedará limitado exclusivamente a la cláusula, párrafo, artículo, sección, parte específica de la misma que así hubiere sido declarada inconstitucional o defectuosa.

Artículo 17.-Vigencia.

Esta Ley comenzará a regir inmediatamente después de su aprobación.

.....
Presidente de la Cámara

.....
Presidente del Senado

Aprobada en 18 enero 2024

Gobernador