GOBIERNO DE PUERTO RICO
PUERTO RICO INNOVATION AND TECHNOLOGY SERVICE

VÍA CORREO ELÉCTRONICO

6 de diciembre de 2021

CARTA CIRCULAR NÚM. 2021-007

Secretarios, Jefes de Agencias y Directores Ejecutivos, Departamentos, Agencias, Comisiones, Juntas, Administraciones, Autoridades, Corporaciones Públicas, Instrumentalidades y demás organismos o entidades componentes de la Rama Ejecutiva del Gobierno de Puerto Rico ("Entidad(es) Gubernamental(es)")

Enrique A. Völckers-Nin
Principal Ejecutivo de Innovación e Información, Gobierno de Puerto Rico
Director Ejecutivo, Puerto Rico Innovation and Technology Service

RE: ESTABLECIMIENTO DE LA POLÍTICA PARA LA SEGURIDAD CIBERNÉTICA

Base Legal

Esta Carta Circular se promulga en virtud de las facultades delegadas al Puerto Rico Innovation and Technology Service ("PRITS"), conforme la Ley Núm. 75 de 25 de julio de 2019, ("Ley-75"). El inciso (a) del Artículo 6 de la Ley-75, faculta a PRITS a implantar, desarrollar y coordinar la política pública del Gobierno sobre la innovación, información y tecnología. Mientras que, el inciso (x) del Artículo 6 otorga a PRITS la obligación de establecer e implantar las políticas y aplicaciones de seguridad del Gobierno para el uso del internet y de la red interagencial. Por otro lado, el Artículo 7, inciso (3) autoriza la promulgación órdenes administrativas, opiniones y/o cartas circulares por parte de PRITS con el fin de garantizar el cumplimiento de cualquier ley. De la misma forma, la Ley 151 del 22 de junio de 2004, según enmendada, Ley de Gobierno Electrónico ("Ley 151") faculta a PRITS a establecer las políticas de seguridad a nivel gubernamental sobre el acceso, el uso, la clasificación y la custodia de los sistemas de información.

Por su parte las Entidades Gubernamentales tienen el deber de cumplir con las políticas emitidas por PRITS e impartir las instrucciones necesarias para garantizar su cumplimiento, y asegurarse que las políticas establecidas sean comunicadas de manera rápida y efectiva al personal correspondiente, ello conforme a los incisos (g) y (h) del Artículo 7 de la Ley 151.

Propósito y Determinación

Los activos de información del Gobierno de Puerto Rico son fundamentales para su misión de brindar servicios de calidad a los ciudadanos. Por lo tanto, es esencial establecer medidas de seguridad adecuadas para evitar el acceso no autorizado, divulgación, uso, daño, degradación y destrucción de la información electrónica, de sus sistemas e infraestructura crítica. Por tanto, PRITS en cumplimiento con su responsabilidad de implementar los controles efectivos con relación a la seguridad de los sistemas de información que sustentan

las operaciones y los activos gubernamentales aprobó el 29 de octubre de 2021 la Política para la Seguridad Cibernética versión 1.0 y su Anejo A titulado Estándares para la Seguridad Cibernética versión 1.0. [1]

La Política para la Seguridad Cibernética tiene como objetivo:

1. Apoyar un marco gubernamental integral de seguridad cibernética y garantizar la implementación de medidas sólidas para proteger los activos de información, incluyendo procedimientos, directrices, controles físicos y técnicos y los requisitos mínimos de seguridad cibernética para todas las agencias.

2. Describir los principios que guiarán las actividades del gobierno relacionadas con la seguridad cibernética, incluyendo el enfoque y la metodología para proteger la confidencialidad, integridad y disponibilidad de los activos de información del gobierno.

3. Abarcar todas las demás políticas de seguridad y tecnología y sus estándares y procedimientos asociados definidos por el PRITS para la seguridad, operación y manejo adecuado de los sistemas y activos de información.

4. Definir y asignar roles y responsabilidades para el manejo de la seguridad cibernética y describir la gestión de desviaciones y excepciones a la política.

5. Proporcionar orientación a empleados nuevos y existentes, personal temporero, contratistas, socios y terceros sobre la importancia de sus funciones y responsabilidades relacionadas con la seguridad cibernética y la protección de los activos de información del gobierno.

La política aprobada aplica a todas las agencias gubernamentales, sus empleados y terceros (tales como consultores, proveedores y contratistas) que utilicen o accedan cualquier recurso de tecnología de la información del Gobierno y/o de una entidad gubernamental. También aplica a todos los sistemas de tecnologías de información automatizados y manuales que son responsabilidad administrativa del Gobierno de Puerto Rico o de cualquier otra agencia, incluyendo aquellos que son administrados o alojados por terceros en nombre del Gobierno de Puerto Rico. Incluye, además, toda la información digital, independientemente de la forma o formato en que se creó o se utilizó.

De igual forma, la política establece los requerimientos generales que deben cumplir las agencias, concienciación sobre la política, comunicación y capacitación de los empleados nuevos y existentes, de los contratistas y terceros. Así como enumera las responsabilidades de todos los empleados gubernamentales, del equipo de manejo de riesgos y seguridad cibernética y del personal ejecutivo de las agencias.

Mediante la política aprobada se instauran los estándares de seguridad cibernética y es la base y modelo inicial para políticas más integrales y específicas. Por tanto, cada agencia puede desarrollar políticas de seguridad especificas considerando sus necesidades, entornos tecnológicos sistemas, infraestructura crítica y leyes aplicables, pero debe, alcanzar los niveles de seguridad requeridos y delineados dentro de la política aprobada.

Por otro lado, el Anejo A titulado *Estándares para la Seguridad Cibernética (Estándares)* dispone los requisitos técnicos diseñados para respaldar la política establecida y delinear los principios y procedimientos para proteger los sistemas y activos de información. En la misma se enumeran los requisitos técnicos para el internet, software y aplicaciones, autenticación multifactorial, servicios contratados, controles de tecnología de información y controles para los dispositivos móviles propiedad del Gobierno.

Conforme a los Estándares, las agencias según sea requerido por PRITS, realizarán evaluaciones periódicas de ciberseguridad que deben incluir, entre otras, la evaluación de amenazas y vulnerabilidades, controles de la tecnología e información existentes e inventarios de estas. Una vez que se descubre un incidente o amenaza de seguridad de la información, la agencia deberá notificar inmediatamente al PRITS y enviará el Informe de Incidente de Ciberseguridad que incluirá la información descrita en la *Guía para informar incidentes de*

[1] La Política para la Seguridad Cibernética y los Estándares para la Seguridad Cibernética están disponibles en www.prits.gobierno.pr/documentos

ciberseguridad. De igual forma, las agencias que no son monitoreadas por PRITS deberán enviar informes mensuales de ciberseguridad, con la información requerida en el acápite 3.8.2 de los Estándares.

Reiteramos que es mandatorio que toda Entidad Gubernamental lleve las acciones necesarias para cumplir con lo dispuesto en la Política para la Seguridad Cibernética y con los Estándares según aprobados. Tanto la Ley 75 como la Ley 151, facultan a PRITS a llevar a cabo las investigaciones necesarias, y tomar toda medida que entienda pertinente para asegurar el cumplimiento de sus directrices. Fuera del ámbito investigativo, la Ley 75 establece un deber afirmativo de la Entidades Gubernamentales bajo la jurisdicción de PRITS de cumplir con las leyes aplicables y las directrices impartidas en la presente Carta Circular.

Es responsabilidad del Gobierno tomar las medidas de seguridad adecuadas y esenciales para proteger sus sistemas de información electrónica. PRITS está comprometido con dirigir un enfoque moderno sobre la ciberseguridad, aumentar la visibilidad del Gobierno sobre las amenazas a la información y garantizar controles eficientes de seguridad.

Se recomienda que tanto la Rama Legislativa como la Rama Judicial adopten políticas para la seguridad cibernética que incorporen las medidas de seguridad conforme lo dispuesto en esta Carta Circular.

Derogación

Esta Carta Circular deja sin efecto cualquier otra Carta Circular, Memorando, Orden Administrativa, Políticas, en particular las Políticas Núm. ATI 003 Seguridad de los Sistemas de Información y ATI 014, Manejo de Firewalls, Normativas, comunicación escrita o instrucción anterior de PRITS o publicada por la OGP como su predecesora antes de la aprobación de la Ley-75, que en todo o en parte sea incompatible con ésta, hasta donde existiera tal incompatibilidad.

Vigencia

Las Entidades Gubernamentales tendrán un término de noventa (90) días calendario a partir del 1 de enero de 2022 para dar cumplimiento con lo dispuesto en la Política para la Seguridad Cibernética y los Estándares para la Seguridad Cibernética.

En la consecución de tal objetivo las Entidades Gubernamentales cuentan con la colaboración y asistencia de PRITS.

Esta Carta Circular tendrá vigencia inmediata.

Puerto Rico
Innovation & Technology Service