PR iTS cyber security

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

Gobierno de Puerto Rico

POLÍTICA PARA LA SEGURIDAD CIBERNÉTICA

v. 1.0

Para la Rama Ejecutiva del Gobierno de Puerto Rico

Según establecido por el Puerto Rico Innovation and Technology Service por virtud de la Ley 75-2019.

Título:	**Política para la Seguridad Cibernética**		
Aprobado por:	Enrique A. Völckers Nin		10/29/2021
Jefe responsable:	N'gai Oliveras Arroyo	Revisado:	10/29/2021
Oficina responsable:	*Oficina de Ciberseguridad*, Puerto Rico Innovation and Technology Service (PRITS)	Contacto:	soc@prits.pr.gov

Contenido

1. Trasfondo

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, medidas de seguridad adecuadas son esenciales para evitar el acceso no autorizado, divulgación, uso, daño, degradación y destrucción de la información electrónica, sus sistemas e infraestructura crítica. El Puerto Rico Innovation and Technology Service (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. Esta política tiene la intención reducir el riesgo, el impacto y el costo de las actividades maliciosas 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.

2. Propósito

Esta política de 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.

3. Alcance

Según se define en la Ley de la Puerto Rico Innovation and Technology Service (Ley Núm. 75-2019), esta política 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 de PRITS u otra agencia. Esta política se aplica a todos los sistemas de tecnologías de información automatizados y manuales que son responsabilidad administrativa del PRITS o de cualquier otra agencia, incluyendo aquellos que son administrados o alojados por terceros en nombre del Gobierno de Puerto Rico. Aborda toda la información digital, independientemente de la forma o formato en el que se creó o utilizó en las actividades de apoyo y los servicios proporcionados por todas las agencias gubernamentales. Si existe un conflicto entre esta política y la política de una agencia, la política más restrictiva prevalecerá.

4. Autoridad

La ley 75 del 25 de julio de 2019, según enmendada, otorga al PRITS la responsabilidad y autoridad de establecer, supervisar, dirigir y coordinar el establecimiento de políticas, protocolos y estándares de tecnología de la información para el Gobierno de Puerto Rico. Además, La Ley 151 de 22 de junio de 2004, según enmendada, también conocida como Ley de Gobierno Electrónico, estipula que el PRITS puede establecer políticas de seguridad en todo el gobierno sobre el acceso, uso, clasificación y custodia de los sistemas de información. También designa a PRITS para liderar el desarrollo de un marco que garantice controles eficaces para la seguridad de los sistemas de información que sustenten las operaciones y los activos del gobierno.

5. Definiciones

Para esta política, los siguientes términos tendrán el significado que se establece a continuación:

5.1 *"Acceso no autorizado"* – ocurre cuando una persona obtiene acceso lógico o físico sin aprobación o consentimiento a una red de infraestructura crítica, sistema, datos, aplicación u otro recurso de tecnología de la información del gobierno.

5.2 *"Agencia"* – significa cualquier junta, organismo, junta examinadora, comisión, corporación pública, oficina, división, administración, negociado, departamento, autoridad, funcionario, empleado, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Gobierno de Puerto Rico.

5.3 *"Autenticación"* – significa una medida de seguridad diseñada para para proteger un sistema de información y verificar la identidad de un usuario, proceso o dispositivo. A menudo, es un requisito previo para permitir el acceso y proteger los recursos en un sistema de información.

5.4 *"Ciberseguridad"* – significa 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.

5.5 *"Ciclo de vida de la información"* – significa las etapas a través de las cuales pasa la información; que generalmente consisten en la creación o recopilación, procesamiento, diseminación, uso, almacenamiento y disposición, que incluye su destrucción y eliminación.

5.6 *"Confidencialidad"* – significa preservar las restricciones de acceso y divulgación, incluyendo los medios para proteger la privacidad personal e información confidencial.

5.7 *"Credenciales"* – el nombre de usuario y la contraseña únicos que se proporcionan a cada usuario autorizado para acceder a los recursos y aplicaciones de los sistemas de información del gobierno.

5.8 *"Cuenta de usuario estándar"* – significa una cuenta de usuario con privilegios limitados para tareas generales.

5.9 *"Datos"* – significa información registrada, independientemente de la forma o el medio en el que está registrada.

5.10 *"Disponibilidad"*- significa garantizar el acceso y el uso oportuno y confiable a la información.

5.11 *"Equipo"* – significa cualquier propiedad tangible y duradera del gobierno relacionada con las tecnologías de la información y la comunicación, que es útil para llevar a cabo las funciones de comunicación o manejar la información de una agencia.

5.12 *"Gobierno"* – significa la Rama Ejecutiva del Gobierno de Puerto Rico.

5.13 *"Incidente" o "incidente de seguridad cibernética"* – significa un suceso que (i) pone en riesgo real o inminente, sin autoridad legal, la integridad, confidencialidad o disponibilidad de la información o un sistema de información; o (ii) representa 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.

5.14 *"Infraestructura crítica"* – se refiere a los servicios, sistemas 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.

5.15 *"Integridad"* – significa proteger la información contra la modificación o destrucción indebida, incluyendo garantizar el no repudio *y* la autenticidad de la información.

5.16 *"Programa" o "software"* – se refiere a los programas informáticos y datos asociados que pueden escribirse o modificarse dinámicamente durante su ejecución.

5.17 *"PRITS"* – significa el Puerto Rico Innovation and Technology Service.

5.18 *"Recursos de información"* – significa información y los recursos relacionados, como, por ejemplo, personal, equipo y tecnología de la información.

5.19 *"Seguridad cibernética"* – significa proteger la información y los sistemas de información para prevenir el acceso, utilización, divulgación, interrupción, modificación o la destrucción no autorizada que impida su confidencialidad, integridad y disponibilidad.

5.20 *"Sistema de información"* – significa un conjunto discreto de recursos de información para la recopilación, procesamiento, mantenimiento, uso, intercambio, difusión o disposición de información.

5.21 *"Tecnología de la Información" (TI)*

5.21.1 Para una agencia, significa cualquier sistema interconectado o subsistema de equipo utilizado en la adquisición, almacenamiento, análisis, evaluación, manipulación, manejo, movimiento, control, visualización, conmutación, intercambio, transmisión o recepción automática de datos o información por la agencia 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;

5.21.2 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.

6. Política

6.1 Requerimientos generales

Las agencias deberán:

6.1.1 Proteger y mantener la confidencialidad, integridad y disponibilidad de la información almacenada y/o administrada por los sistemas de información gubernamentales y los activos de infraestructura relacionados.

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

6.1.3 Potenciar las capacidades y los esfuerzos para impedir, detectar, prevenir, proteger y responder a las amenazas contra los sistemas de información y los datos del gobierno.

6.1.4 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 sistemas de información gubernamentales.

6.1.5 Definir los procesos para el cumplimiento del monitoreo de la seguridad cibernética.

6.1.6 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.

6.1.7 Documentar e implementar el programa de ciberseguridad de PRITS en los recursos de información y los sistemas de TI que respaldan las operaciones y los activos de la agencia.

6.1.8 Realizar evaluaciones periódicas 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 la agencia.

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

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

6.1.11 Mantener la seguridad de los sistemas de información aun cuando el manejo y control de algunos de los procesos hayan sido delegados a un tercero.

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

6.1.13 Asegurar el cumplimiento de los controles y procedimientos presentados en los Estándares de Seguridad Cibernética, disponibles en https://support.prits.pr.gov.

6.2 Concienciación sobre la política, comunicación y capacitación

Las agencias serán responsables de la promoción continua y concienciación sobre la seguridad cibernética a través de capacitaciones, talleres u orientaciones periódicas. Para mitigar el riesgo de eventos de ciberseguridad y la divulgación involuntaria de información confidencial por parte de los empleados y proveedores de servicios externos, se tomarán las siguientes medidas.

6.2.1 Empleados nuevos

Durante el proceso de incorporación, el personal de Recursos Humanos deberá:

- Proporcionar a todos los empleados nuevos acceso a la **Guía para empleados sobre seguridad cibernética** y asegurarse de que todos reconozcan formalmente que han recibido, leído y cumplirán con los todos los requisitos en este documento que se aplican a sus áreas de responsabilidad.
- Asegurarse de que todos los empleados completen las actividades de capacitación y concienciación sobre ciberseguridad, según su disponibilidad.

6.2.2 Empleados existentes

Al menos una vez al año, todos los empleados que hayan estado laborando por más de doce (12) meses, deberán completar una sesión anual de capacitación y concientización sobre ciberseguridad y reconocer formalmente la finalización de estos requisitos anuales.

6.2.3 Salidas o cambios en la situación laboral

Tras un cambio en la situación laboral (por ejemplo, promoción, transferencia o despido), el personal de Recursos Humanos se asegurará de que se informe al Oficial Principal de Informática o al personal designado por éste para que la cuenta del empleado y los privilegios de acceso físico se restrinjan de manera oportuna, según corresponda para garantizar el acceso con privilegios mínimos.

6.2.4 Contratistas y Terceros

Los vendedores, suplidores, socios, contratistas, proveedores de servicios y otros terceros con acceso a los sistemas de información del gobierno deben cumplir con los requisitos aplicables aquí presentados.

7. Responsabilidades

7.1 Todos los empleados gubernamentales

Cada empleado gubernamental desempeña un papel fundamental para garantizar la seguridad cibernética y es responsable de la protección de los activos de información. Se espera que todos los empleados se comporten de manera profesional y responsable en el desempeño de sus funciones y den a conocer cualquier actividad o evento sospechoso, accidental o intencional que comprometa la integridad, disponibilidad y/o confidencialidad de la información. Todos los empleados son responsables de garantizar que cumplan con esta política. El incumplimiento de esta política puede resultar en una acción disciplinaria.

Todos los empleados gubernamentales serán responsables de:

7.1.1 Actuar con precaución y cuidado al utilizar cualquier sistema de información, servicio o plataforma tecnológica para evitar la divulgación no autorizada o inadvertida de información sensible, confidencial o personal.

7.1.2 Ser cauteloso con los mensajes y tecnologías sospechosos, que podrían tener como objetivo atraer a un usuario a un incidente cibernético malicioso.

7.1.3 Usar los recursos de TI del gobierno solo para tareas oficiales relacionadas con la agencia que correspondan a los roles y responsabilidades como empleado.

7.1.4 Mantener las contraseñas secretas y seguras. Los empleados no se apropiarán, divulgarán ni utilizarán las credenciales de inicio de sesión de otra persona.

7.1.5 Tomar las precauciones adecuadas para evitar daños, pérdidas o robos de cualquier dispositivo o equipo gubernamental emitido para su uso.

7.1.6 Informar de inmediato al supervisor y al personal de TI si un dispositivo o equipo se ha perdido, robado o comprometido (sospechado o confirmado).

7.2 Equipo de manejo de riesgos y seguridad cibernética

Cada jefe de la agencia debe designar a una persona o equipo que será responsable de la seguridad cibernética y el manejo de riesgos de la agencia. Las responsabilidades de este equipo incluyen, entre otras, las siguientes:

7.2.1 Asegurar que los empleados y contratistas de la agencia protejan los sistemas de información que respaldan las operaciones y los activos bajo su control.

7.2.2 Evaluar el riesgo y el impacto que podría resultar del acceso no autorizado, la utilización, la divulgación, la interrupción, la modificación o la destrucción de la información o los sistemas de información.

7.2.3 Determinar los niveles de seguridad cibernética apropiados para proteger la información y sus sistemas mediante la implementación de políticas, procedimientos, estándares y controles promulgados por el PRITS.

7.2.4 Implementar procedimientos para reducir de manera rentable los riesgos a un nivel aceptable.

7.2.5 Probar y evaluar periódicamente los controles y técnicas de seguridad cibernética para asegurar su implementación efectiva.

7.2.6 Asegurarse de que todos los informes solicitados por el PRITS sean entregados e incluyan la información requerida, describiendo la eficacia del programa de seguridad cibernética en la agencia y el progreso de las acciones correctivas.

7.2.7 Realizar pruebas y evaluaciones periódicas de la efectividad de las medidas, procedimientos y prácticas de seguridad cibernética, que se realizarán en función del riesgo, pero no menos de una vez al año. Las pruebas deben incluir controles de manejo, operacionales y técnicos de cada sistema de información identificado.

7.2.8 Desarrollar un proceso para planificar, implementar, evaluar y documentar acciones correctivas que aborden los riesgos a los activos de TI y cualquier deficiencia en las políticas, procedimientos y prácticas de seguridad cibernética de la agencia.

7.2.9 Desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad cibernética, que deberán (i) ser consistentes con las políticas, guías y estándares establecidos por el PRITS; (ii) incluir la mitigación de los riesgos asociados con tales incidentes antes de que se produzcan daños sustanciales; (iii) notificar y consultar al PRITS; y (iv) notificar y consultar con, según corresponda, los organismos encargados de hacer cumplir la ley y otras oficinas pertinentes.

7.2.10 Diseñar e implementar planes y procedimientos para la recuperación tras desastres y asegurar la continuidad de las operaciones de los sistemas de información que apoyan las operaciones y los activos de la agencia.

7.2.11 Evaluar y manejar los riesgos de forma coherente en todos los activos y sistemas de información y garantizar que la tolerancia al riesgo se refleje de la misma manera en toda la agencia y en el ciclo de vida de la información.

7.2.12 Brindar apoyo al personal técnico sobre ciberseguridad y operaciones seguras (por ejemplo, codificación segura, configuración segura).

7.3 Personal ejecutivo de la agencia (Secretario, Director, Presidente, etc.)

El jefe de cada agencia y el personal de liderazgo serán responsables de:

7.3.1 Asegurar que los procesos de manejo de la seguridad cibernética se consideren e integren en las estrategias, operaciones, misión y planificación presupuestaria de la agencia.

7.3.2 Proporcionar protecciones de seguridad cibernética en proporción al riesgo y la extensión del daño resultante del acceso no autorizado, divulgación, utilización, interrupción, modificación o destrucción de (i) la información recopilada o mantenida por la agencia o en su nombre; y (ii) sistemas de información utilizados u operados por una agencia, por un contratista de la agencia u otra entidad en nombre de una agencia.

7.3.3 Evaluar y aceptar el riesgo en nombre de la agencia.

7.3.4 Asegurarse de que los recursos necesarios para mantenerse en cumplimiento con esta política estén disponibles.

7.3.5 Identificar las responsabilidades y objetivos de seguridad cibernética de la agencia e integrarlos en los respectivos procesos de TI.

7.3.6 Promover la implementación y mejora de políticas y estándares de seguridad cibernética.

7.3.7 Respaldar la seguridad dentro de la agencia proporcionando los recursos y la dirección necesarios.

7.3.8 Transmitir un mensaje constante de concienciación sobre las mejores prácticas de seguridad mediante la formación periódica de los empleados.

7.3.9 Identificar a las personas que actuarán como propietarios de activos de información.

7.3.10 Participar en la respuesta a incidentes de seguridad.

7.3.11 Cumplir con los requisitos de notificación en caso de filtración de datos.

7.3.12 Cumplir con todos los requisitos legales y reglamentarios relevantes relacionados con la seguridad cibernética.

7.3.13 Comunicar a los empleados de la agencia y a terceros los requisitos de esta política y los estándares asociados, incluyendo las consecuencias del incumplimiento.

7.4 Puerto Rico Innovation and Technology Service (PRITS)

7.4.1 Oficina del Principal Oficial de Ciberseguridad del Gobierno

Dentro de PRITS, la Oficina del Principal de Oficial de Ciberseguridad del Gobierno será responsable de las siguientes funciones.

7.4.1.1 Liderar los esfuerzos para proteger, defender y reducir las vulnerabilidades de los sistemas gubernamentales.

7.4.1.2 Monitorear la implementación de las políticas y estándares de seguridad cibernética de PRITS.

7.4.1.3 Convocar reuniones con funcionarios de las agencias para ayudar a garantizar la implementación efectiva de las políticas y prácticas de seguridad cibernética.

7.4.1.4 Coordinar los esfuerzos de todo el gobierno sobre políticas y prácticas de seguridad cibernética, incluyendo consultas con los jefes de información de las agencias, los grupos/asociaciones de seguridad y las autoridades pertinentes.

7.4.1.5 Desarrollar y realizar evaluaciones operacionales específicas de los sistemas de información, incluyendo evaluaciones de amenazas y vulnerabilidades.

7.4.1.6 Desarrollar el programa de ciberseguridad del gobierno y determinar y documentar cómo se medirá su eficacia.

7.4.1.7 Proporcionar orientación y pericia sobre operaciones relacionadas con la seguridad, la mitigación de vulnerabilidades y la respuesta a incidentes.

7.4.1.8 Asegurarse de que las redes y los recursos externos sean monitoreados adecuadamente y que las notificaciones de nuevas amenazas y vulnerabilidades sean puntuales.

7.4.1.9 Asegurarse de que la agencia cuente con materiales de capacitación relevantes y actualizados para la concientización sobre seguridad.

7.4.1.10 Apoyar a las agencias a través de la detección de intrusiones, análisis de incidentes y capacidades de respuesta cibernética para proteger los sistemas de información del gobierno.

7.4.1.11 Establecer políticas y estándares de seguridad mínimos para los sistemas de información gubernamentales.

7.4.1.12 Desarrollar y supervisar la implementación de directrices operacionales a las agencias para implementar las políticas, principios, estándares y guías de seguridad cibernética, incluyendo (i) los requisitos para informar incidentes de seguridad, (ii) los requisitos de contenido para los informes anuales, (iii) requisitos para la mitigación de riesgos críticos a los sistemas de información.

7.4.1.13 Difundir información sobre amenazas cibernéticas, vulnerabilidades, mitigación y otros asuntos para mejorar la seguridad y protección de los sistemas de información gubernamentales e infraestructura crítica.

7.4.1.14 Brindar asistencia operacional y técnica a las agencias en la implementación de políticas, principios, estándares y directrices sobre seguridad cibernética.

7.4.1.15 A solicitud de una agencia, implementar tecnología para ayudar en el diagnóstico continuo y mitigación contra las amenazas cibernéticas y vulnerabilidades.

7.4.1.16 Recopilar y analizar datos sobre seguridad cibernética de las agencias.

7.4.1.17 Realizar esfuerzos de capacitación al personal, contratistas y otros usuarios para concientizar e informar sobre seguridad y (i) los sistemas de información que respaldan las operaciones y los activos de la agencia, (ii) los riesgos de seguridad cibernética asociados con sus actividades, y (iii) sus responsabidades en el cumplimiento de las políticas y procedimientos de la agencia desarrollados para reducir estos riesgos.

8. Aplicación

8.1 Excepciones y desviaciones

Esta política establece los estándares mínimos de seguridad cibernética y es la base y modelo inicial para políticas más integrales y específicas. Cada agencia puede desarrollar políticas de seguridad específicas considerando sus necesidades, entornos tecnológicos, sistemas, infraestructura crítica y leyes y regulaciones aplicables; pero debe, como mínimo, alcanzar los niveles de seguridad requeridos y delineados dentro de esta política.

Si el cumplimiento de esta política no es alcanzable o técnicamente posible, o si una desviación de esta política es necesaria para respaldar cualquier proyecto, o cumplir con una ley o reglamentación, la agencia debe solicitar una excepción a través del Principal Oficial de Ciberseguridad (CISO, en inglés)

del Gobierno de Puerto Rico. Cualquier agencia que solicite una excepción o desviación debe explicar las circunstancias y un plan para mitigar los riesgos potenciales.

9. Cumplimiento

Esta política entrará en vigor a partir de su publicación y se revisará al menos cada veinticuatro (24) meses. Se requiere y se espera que todas las agencias gubernamentales cumplan con esta política y todos los estándares de apoyo del PRITS. El PRITS puede modificar sus políticas y estándares en cualquier momento. Las agencias deben seguir cumpliendo con las políticas y estándares enmendados.

Cualquier violación de esta política puede someter al empleado, proveedor externo o cualquier otra agencia afiliada a medidas disciplinarias, sanciones civiles y/o enjuiciamiento penal.

10. Historial de revisiones

La Política de Seguridad cibernética del Gobierno de Puerto Rico pertenece y es mantenida por la Oficina del Principal Oficial de Ciberseguridad del Gobierno de Puerto Rico adscrita a PRITS.

Fecha	*Descripción del cambio*	*Revisado por*	*Aprobado por*