PR ITS cyber security

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

GOBIERNO DE PUERTO RICO

PRITS 006-Guía para empleados

SOBRE SEGURIDAD CIBERNÉTICA

V1.1

PR ITS

Contenido

I. Trasfondo 1
II. Objetivos 1
III. Alcance 1
IV. Definiciones 2
V. Medidas de Seguridad 5
VI. Responsabilidades 6
Reconocimiento de la Política para la Seguridad de la Información del Gobierno de Puerto Rico 7

I. Trasfondo

La información es un componente crítico para el buen funcionamiento del Gobierno de Puerto Rico y brindar servicios a los ciudadanos. El uso de medidas de seguridad es importante para evitar el acceso no autorizado, divulgación, uso, daño, degradación y destrucción de la información electrónica, sus sistemas e infraestructura crítica. Con estos fines, el Puerto Rico Innovation and Technology Service (PRITS) está comprometido con el desarrollo de un enfoque moderno sobre asuntos de ciberseguridad, de tal modo que el gobierno tenga mayor visibilidad sobre aquellos aspectos concernientes a amenazas a la información y se garanticen controles efectivos para su seguridad.

La Política para la Seguridad Cibernética fue creada para definir roles y responsabilidades para la protección de la información y establecer estándares mínimos de seguridad que resulten en la reducción de los impactos y costos que surgen como resultado de las actividades maliciosas. Basado en dicha política, este manual se desarrolla para informar al empleado y orientar sobre aquellos aspectos en los cuales sus roles y responsabilidades pueden ayudar en la prevención de incidentes que pongan en riesgo la información manejada por el Gobierno de Puerto Rico. No obstante, para obtener información detallada sobre asuntos de ciberseguridad gubernamental se exhorta a leer la Política y ponerse en contacto con el personal encargado de los sistemas de información de su agencia.

II. Objetivos

- Proveer orientación a los usuarios sobre las medidas y principios para proteger los activos de información.
- Instruir a empleados nuevos y existentes sobre sus roles y responsabilidades para la protección de la información y asuntos de ciberseguridad.

III. Alcance

Por virtud de la Ley de la Puerto Rico Innovation and Technology Service (Ley 75-2019), la Política para la Seguridad Cibernética y, por consiguiente, esta guía aplica a todas las agencias gubernamentales y sus empleados, que utilizan o acceden cualquier recurso de tecnología de la información de PRITS u otra agencia. Del mismo modo aborda toda la información digital, independientemente de la forma o formato en el que se creó o utilizó en las actividades de apoyo y servicios proporcionados por todas las agencias gubernamentales.

Aquellos empleados cuyas funciones estén directamente asociadas con el manejo de sistemas de información y terceros (por ejemplo, consultores, suplidores y contratistas) deberán hacer referencia directa a la Política para la Seguridad Cibernética.

IV. Definiciones

Los siguientes términos tendrán el significado que se establece a continuación:

a. “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.

b. “Activos de información” - se refiere a una colección de elementos de datos o conjuntos de datos que pueden agruparse.

c. “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.

d. “Autenticación” - significa una medida de seguridad diseñada 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.

e. “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.

f. “Confidencialidad” - significa preservar las restricciones de acceso y divulgación, incluyendo los medios para proteger la privacidad personal e información confidencial.

g. “Credenciales” - el nombre de usuario y la contraseña únicos que se proporcionan a cada usuario autorizado para acceder los recursos y aplicaciones de los sistemas de información del gobierno.

h. “Cuenta administrativa” - significa una cuenta de usuario con privilegios completos destinada a realizar tareas de administración legítimas como la instalación de actualizaciones y programas, administración de cuentas de usuario, modificación del sistema operativo (SO) y configuración de aplicaciones, entre otros.

i. “Datos” - significa información registrada, sin importar la forma o el medio en el que se graban los datos.

j. “Disponibilidad”- significa garantizar el acceso y el uso oportuno y confiable de la información.

k. “Dispositivo móvil” - significa cualquier dispositivo de computación móvil como teléfono inteligente, otros teléfonos celulares, tableta, lector electrónico, dispositivo de medios portátil, dispositivo de computación portátil o cualquier otro dispositivo móvil con capacidad para almacenamiento de datos y conexión de red.

l. “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.

m. “Gobierno” - significa la Rama Ejecutiva del Gobierno de Puerto Rico.

n. “Incidente” o “incidente de seguridad de la información” - 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.

o. “Información sensitiva” - significa información, equipo o medios donde la pérdida, mal uso o acceso o modificación no autorizados pudieran afectar adversamente los intereses del Gobierno de Puerto Rico y/o la privacidad de los ciudadanos.

p. “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.

q. “Integridad” – significa proteger la información contra la modificación o destrucción indebida, incluyendo garantizar el no repudio y la autenticidad de la información.

r. "Información de identificación personal" (IIP) – significa cualquier representación de información que sea legible sin la necesidad de una clave criptográfica especial para acceder a ella, permita o facilite el rastreo de la identidad de un individuo, incluyendo el nombre o la primera inicial y el apellido paterno de un individuo combinado con otra información que está vinculada o que se puede vincular a un individuo específico, como:
    i. Número de Seguro Social
    ii. Licencia de conducir, tarjeta electoral u otra identificación oficial
    iii. Números de cuentas bancarias o financieras de cualquier tipo, con o sin las claves de acceso que puedan habérsele asignado
    iv. Nombres de usuario y claves de acceso a sistemas informáticos públicos o privados
    v. Información médica protegida por la Ley HIPAA
    vi. Información contributiva
    vii. Evaluaciones laborales

s. “Información protegida de salud” (IPS) – significa cualquier representación de información que sea legible sin la necesidad de una clave criptográfica especial para acceder a ella, que contenga al menos el nombre de una persona o la primera inicial y el apellido paterno combinado con información médica protegida por la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA), que incluye información demográfica, historial médico, resultados de análisis y laboratorio, afecciones de salud mental, información de seguros o cualquier otro dato que los profesionales de la salud recopilen para identificar a una persona y determinar la atención adecuada.

t. “Malware” – programa diseñado para obtener acceso no autorizado a un sistema de información y/o interrumpir, comprometer o dañar el funcionamiento de un sistema al realizar una función o proceso no autorizado que impacta la confidencialidad, integridad o disponibilidad de un sistema de información.

u. “Programa” o “software” – se refiere a los programas informáticos y datos asociados que pueden escribirse o modificarse dinámicamente durante la ejecución.

v. “PRITS” - significa el Puerto Rico Innovation and Technology Service.

w. “Recursos de información” - significa información y los recursos relacionados, como, por ejemplo, personal, equipo y tecnología de la información.

x. “Seguridad de la información” - 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.

y. “Sistema de información” - significa un conjunto discreto de recursos de información para la recopilación, procesamiento, mantenimiento, uso, intercambio, difusión o disposición de información.

z. *“*Tecnología de la Información*” (IT, inglés)*
   i. Para una agencia, significa cualquier sistema interconectado o subsistema de equipo utilizado en la adquisición, almacenamiento, análisis, evaluación, manipulación, gestión, 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 de ese equipo; o 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.

V. Medidas de Seguridad

1. Los sistemas de información gubernamentales no se utilizarán para la creación o distribución de ningún material que se considere inapropiado, irrespetuoso, ofensivo, amenazante, abusivo, difamatorio, ilegal, sexista, racista, sexualmente explícito, fraudulento o discriminatorio contra otros. Del mismo modo, está prohibido el uso del Internet para realizar actos ilícitos, incluido el acceso a sitios web con contenido ilegal, obsceno, odioso, difamatorio, indecente, objetable o inapropiado.

2. Bajo ninguna circunstancia la información confidencial (por ejemplo, información de identificación personal e información protegida de salud) quedará expuesta ni desprotegida.

3. Los usuarios deben evitar abrir y ejecutar archivos de fuentes desconocidas o no confiables. Deberán validar con el personal de sistemas de información de su agencia antes de descargar y ejecutar archivos de sitios web no gubernamentales.

4. No se instalará ningún programa (software) en los dispositivos y equipos del gobierno sin la aprobación del encargado de los sistemas de información de la agencia o personal designado. Solo se instalarán programas debidamente autorizados y con licencia. Se prohíbe el uso de programas no autorizados, sin licencia o copiados ilegalmente.

5. El uso de equipos fuera de la agencia deberá ser previamente autorizado por el encargado de los sistemas de información de la agencia o personal autorizado por éste. Las agencias deberán realizarán los controles y monitoreos necesarios para asegurar que el equipo que ha estado fuera de la agencia se esté utilizando legítimamente para cumplir con los roles y responsabilidades de los empleados o personal autorizado y que no represente un riesgo para sus sistemas. Esto incluye la evaluación del equipo y la realización de auditorías al ingresar a los sistemas de la agencia.

6. Se requerirá la aprobación del encargado de los sistemas de información de la agencia para la transferencia y relocalización de equipos.

7. Las personas que deseen utilizar dispositivos de propiedad personal para almacenar, acceder, transportar, transmitir, recibir o utilizar información gubernamental o realizar otras actividades relacionadas con sus labores, incluidos los servicios de correo electrónico, deberán reconocer las funciones, responsabilidades y riesgos que conlleva esta iniciativa. Este modelo, también conocido como “traiga su propio dispositivo” (*bring your own device*, BYOD, en inglés), requiere las siguientes medidas de seguridad mínima para proteger los activos de información al tiempo que brinda una mayor flexibilidad para acceder a los recursos de información del gobierno.

a. Los usuarios deben garantizar actualizaciones periódicas de los sistemas operativos y aplicaciones primarias (por ejemplo, navegadores web, software de productividad, aplicaciones de correo electrónico y programas de seguridad).
b. Si el dispositivo es utilizado por más personas, el altamente recomendado el uso de una cuenta separada para cada usuario, protegida con una contraseña.
c. Por motivos de seguridad, no se deberán utilizar dispositivos hackeados ("jailbroken"). Sólo se deberán utilizar aquéllos con sistemas operativos iOS, Android o Microsoft.

VI. Responsabilidades

Cada empleado gubernamental desempeña un papel fundamental para garantizar la seguridad de la información y es responsable de la protección de los activos de información. Se espera que todos los empleados actúen de forma 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 deberán actuar de forma profesional y responsable en el desempeño de sus funciones y deberán informar cualquier actividad o evento sospechoso, accidental o intencional que comprometa la integridad, disponibilidad y/o confidencialidad de la información. Para garantizar que todos los empleados comprendan sus funciones y responsabilidades, la capacitación anual en seguridad de la información será obligatoria.

El incumplimiento de la política y lo planteado en esta guía puede resultar en una acción disciplinaria.

Todos los empleados del gobierno serán responsables de:

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.

2. Ser cauteloso con los mensajes y tecnologías sospechosos que podrían tener la intención de atraer a un usuario a un incidente cibernético malicioso.

3. Usar los sistemas de información del gobierno sólo para tareas oficiales relacionadas con la agencia que correspondan a las funciones y responsabilidades del empleado.

4. Mantener las contraseñas secretas y seguras. Los empleados no se apropiarán, divulgarán o utilizarán las credenciales de inicio de sesión de alguien sin la autorización previa del supervisor del empleado o de Recursos Humanos.

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

6. Informar de inmediato al supervisor y al personal encargado de sistemas de información de la agencia si un dispositivo o equipo se ha perdido, robado o comprometido (ya sea una sospecha o se haya confirmado).

Reconocimiento de la Política para la Seguridad de la Información del Gobierno de Puerto Rico

Yo, _____, entiendo que como parte de mis funciones podría estar autorizado a acceder los sistemas de información del Gobierno de Puerto Rico. Reconozco que he recibido la Guía para Empleados sobre Seguridad Cibernética y entiendo que es mi responsabilidad de cumplir con todas las políticas de seguridad de la información, reglas de comportamiento, procedimientos y guías emitidas, ya sean provenientes directamente de PRITS o de la agencia en la cual desempeño mis funciones. Además, reconozco que he leído y comprendido los términos de la política y acepto cumplirlos.

Nombre (en letra de molde):		Fecha (dd/mm/yyyy):	
Firma:			
Agencia:			