Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso
Contralora

Carta Circular
OC-24-03

Año Fiscal 2023-2024
25 de agosto de 2023

Al Gobernador, presidentes del Senado de Puerto Rico y de la Cámara de Representantes, jueza presidenta del Tribunal Supremo de Puerto Rico, secretarios de Gobierno, directores de organismos de las tres ramas del Gobierno del Estado Libre Asociado de Puerto Rico, incluidas las corporaciones públicas y sus subsidiarias; alcaldes, presidentes de las legislaturas municipales, de las juntas directivas de las corporaciones municipales, y de las juntas de alcaldes de las áreas locales de desarrollo laboral; directores ejecutivos de las corporaciones municipales y de las áreas locales de desarrollo laboral; presidente de la Universidad de Puerto Rico, directores de finanzas y auditores internos[1].

Asunto: Recomendaciones para la protección de los sistemas de información contra ataques cibernéticos

Estimados señores y señoras:

En los últimos años las entidades gubernamentales han incrementado el uso de los sistemas de información para efectuar sus operaciones principales y ofrecer servicios esenciales a la ciudadanía. Esto, ha aumentado el riesgo y los eventos relacionados con ataques cibernéticos que afectan la infraestructura tecnológica gubernamental y su información crítica. Mencionamos que los ataques cibernéticos tienen el propósito de acceder, modificar, destruir o apropiarse de información confidencial. También se utilizan para extorsionar a los usuarios o interrumpir la continuidad de las operaciones de una entidad, entre otras. Las amenazas cibernéticas representan un reto de gran importancia para el Gobierno del Estado Libre Asociado de Puerto Rico (Gobierno), por lo que es fundamental que se implementen las medidas de seguridad necesarias para proteger la infraestructura e información confidencial, tanto de los ciudadanos como de las mismas entidades.

[1] Las normas de la Oficina prohiben el discrimen por cualquier motivo prohibido por ley. Para propósitos de esta *Carta Circular*, se debe entender que todo término utilizado para referirse a una persona o puesto es sin alusión a géneros.

Los ataques cibernéticos pueden afectar la confidencialidad, la integridad y la disponibilidad de la información. Además, pueden ocasionar pérdidas económicas, afectar la reputación de las entidades y la confianza y la credibilidad que tienen los ciudadanos en estas. Por esto, es de suma importancia identificar las amenazas cibernéticas a las que se exponen los sistemas de información de las entidades gubernamentales. Algunas de estas amenazas son:

1. **Ransomware-** Programa malicioso que restringe el acceso a los sistemas comprometidos hasta que se satisfaga una demanda de rescate. Los atacantes solicitan el dinero en criptomonedas.

2. **Phishing -** Ataque en el que a través de un mensaje de correo electrónico o texto alguien suplanta a una entidad o servicio con el objetivo de obtener información confidencial para utilizarla con fines económicos. El atacante utiliza un enlace a un sitio *web* que suplanta al legítimo para engañar al usuario.

3. **Ataque de ingeniería social** - Conjunto de técnicas que los delincuentes usan para engañar a los usuarios con la intención de que revelen información sensitiva y confidencial para obtener dinero o acceder a los datos de los sistemas de información.

4. **Ataques de malware** - Programa malicioso como virus, gusano, *spayware* y *adware*, que tiene el objetivo de dañar o infiltrarse en un sistema de información, sin el consentimiento de su propietario.

5. **Amenazas persistentes avanzadas (APT)** - Ataque de varias etapas en el que los atacantes se infiltran en una red sin ser detectados y permanecen dentro durante una cantidad de tiempo para acceder a los datos sensitivos o interrumpir los servicios críticos.

6. **Ataques de denegación de servicios (DOS)** - Acción de impedir el acceso autorizado a información o sistemas de información, o de demorar la ejecución de las operaciones y las funciones de los sistemas de información, lo cual conlleva la pérdida de disponibilidad para los usuarios autorizados.

7. **Ataque de phishing ballenero (Whaling Phishing Attack)** - Ataque que utiliza el phishing para perseguir a un objetivo de alto perfil, como los ejecutivos de la alta gerencia o al ejecutivo de mayor jerarquía, con la intención de que revelen información sensitiva y confidencial para obtener dinero o acceder a los datos de los sistemas de información.

8. **Ataque de contraseña (Password Attack)** - Ataque que busca conocer u obtener contraseñas, mediante el uso de varias técnicas como la ingeniería social o herramientas para descifrar la contraseña (*passwords cracker*). Las técnicas más comunes son de ataques de fuerza bruta (*brute force attacks*), el ataque de diccionarios (*dictionary attacks*), y el ataque de registrador de tecla (*keylogger attacks*). Es recomendable que establezcan contraseñas seguras.

La ciberseguridad consiste en un conjunto de prácticas para proteger los datos, la información y los activos críticos de una entidad para reducir el riesgo de que pueden afectar la confidencialidad, la integridad y la disponibilidad de la información. Como parte de los esfuerzos para prevenir y mitigar los riesgos a los que pueden estar expuestos los sistemas de información del Gobierno y proteger la información, la *Puerto Rico Innovation & Technology Service* (PRITS) ha establecido políticas, guías y estándares de ciberseguridad aplicables a las agencias de la Rama Ejecutiva[2]. Además, publica periódicamente alertas para comunicar las vulnerabilidades identificadas[3].

Esta *Carta Circular* se emite para enfatizar a las entidades gubernamentales la importancia del uso de las directrices establecidas y de la verificación de las alertas de seguridad publicadas por el PRITS, según les aplique. Además, recomendar a aquellas entidades que no se les requiera cumplir con estas directrices, incluidos los municipios, que deben desarrollar, implementar y promover un programa de ciberseguridad.

Un programa de ciberseguridad ayuda a crear e implementar una estrategia, que incluye políticas, métodos y tecnologías para proteger y asegurar la información de las entidades y los sistemas que la procesan y almacenan. Además, tiene como objetivo evitar cualquier situación que ponga en riesgo la confidencialidad, la integridad y la disponibilidad de la información. Este debe incluir las medidas para identificar los riesgos y las vulnerabilidades para prevenir los ataques cibernéticos y reaccionar ante la posibilidad de que estos ocurran.

En el **Anejo** que se acompaña les ofrecemos varios elementos y aspectos que deben considerarse al desarrollar e implementar un programa de ciberseguridad.

Las amenazas y los ataques cibernéticos evolucionan constantemente, por lo que es importante que se realice un esfuerzo en conjunto a nivel de cada entidad y del componente gubernamental. Esto, para asegurar la protección de los datos confidenciales, de los sistemas de información, y mantener la continuidad de las operaciones gubernamentales. En nuestras auditorías verificaremos las iniciativas y los esfuerzos realizados por las entidades gubernamentales dirigidos a lograr estos objetivos.

---

[2] Significa cualquier junta, cuerpo, junta o tribunal examinador, comisión, corporación pública, oficina, división, administración, negociado, departamento, autoridad, funcionario, empleado, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Gobierno.

[3] Estas alertas y políticas se encuentran disponibles en *https://www.prits.pr.gov/ciberseguridad*.

Esta *Carta Circular* deroga la *Carta Circular OC-09-15* del 23 de enero de 2009.

Comprometidos en mejorar la fiscalización y administración de la propiedad y de los fondos del Gobierno, para generar valor público con buenas prácticas fiscalizadoras.

Cordialmente,

Yesmín M. Valdivieso

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

ASPECTOS PARA CONSIDERAR AL MOMENTO DE DESARROLLAR, IMPLEMENTAR Y PROMOVER UN PROGRAMA DE CIBERSEGURIDAD

Para desarrollar, implementar y promover un programa de ciberseguridad recomendamos lo siguiente:

1. Considerar como referencia las políticas, las guías y los estándares establecidos por el Puerto Rico Innovation & Technology Service (PRITS) o por agencias federales tales como, el National Institute of Standards and Technology (NIST) y el Cybersecurity & Infraestructure Security Agency (CISA).

2. Identificar detalladamente los recursos de los sistemas de información de la entidad (equipos, conexiones, sistemas y programas, información).

3. Realizar un análisis de los riesgos de seguridad informática para identificar las amenazas y las vulnerabilidades que pueden afectar los sistemas de información y los riesgos a los que podría exponerse. Como parte de este análisis, se debe incluir una evaluación de la efectividad de los controles existentes para atender las amenazas y las vulnerabilidades identificadas. Además, implementar los controles adicionales necesarios para proteger los sistemas de información, de forma costo efectiva, y responder adecuadamente a cualquier ataque cibernético.

4. Evaluar constantemente la infraestructura tecnológica de la entidad para determinar si cumple con las mejores prácticas de seguridad e implementar las actualizaciones recomendadas en la industria, conforme a sus necesidades. Como parte de esto, se deben considerar estrategias tales como la segmentación de la red basado en la criticidad de los sistemas de información de la entidad.

5. Revisar y actualizar periódicamente las políticas de seguridad para garantizar que estas consideran las amenazas de seguridad y los riesgos existentes y son suficientes para proteger los sistemas.

6. Establecer las siguientes políticas:

    a. **Política de privacidad de datos** - establece cómo se manejan y protegen adecuadamente los datos de la entidad.

    b. **Política de retención** - describe cómo, dónde y durante cuánto tiempo se deben almacenar los diferentes tipos de datos de la entidad.

    c. **Política de protección de datos** - establece cómo la entidad maneja los datos personales de sus empleados, clientes y proveedores y de terceros.

7. Establecer un plan de manejo de incidentes en el que se describan las responsabilidades y los procedimientos que se deben seguir para garantizar respuestas rápidas, eficaces y ordenadas a los ataques cibernéticos.

8. Promover una cultura de ciberseguridad dirigida a proteger la información confidencial de la entidad, sus proveedores y ciudadanos; y a reducir los errores o las fallas humanas que pueden afectar la seguridad. Como parte de las acciones que fomentan el desarrollo de esta cultura, recomendamos lo siguiente:

    a. Designar un encargado de la seguridad de los sistemas de información de la entidad, quien debe establecer y validar constantemente el programa de seguridad.

    b. Instruir al personal de la entidad para que evite abrir correos electrónicos o archivos adjuntos de fuentes desconocidas o no confiables que pudieran ser parte de ataques de modalidad *phishing* y conectar dispositivos de almacenamiento desconocidos.

    c. Proveer adiestramientos continuos al encargado de la seguridad de los sistemas y a todos los empleados para que puedan identificar y responder a las posibles amenazas cibernéticas.

    d. Mantener los programas y los sistemas operativos actualizados con los parchos de seguridad más recientes para garantizar que se encuentran protegidos contra las últimas amenazas y corrijan los errores y las vulnerabilidades. Además, establecer un plan de sustitución para los sistemas obsoletos que no se puedan actualizar.

    e. Utilizar programas de antivirus y mantenerlos actualizados. Esta herramienta protege de distintos ataques, como troyanos, gusanos, *adware*, *ransomware*, entre otros programas dañinos que amenazan la información. Estos programas pueden detectar, poner en cuarentena y eliminar, automáticamente, varios tipos de *malware*.

    f. Utilizar *firewall* o cortafuegos que permiten inspeccionar e identificar el tráfico de Internet, y restringir el acceso a desconocidos o usuarios no autorizados. Estos deben ser configurados según se establece en los manuales de usuario. Además, se deben adquirir herramientas, tales como sistemas de detección y protección contra intrusos (IPS/IDS), que faciliten el análisis y la revisión continua de los registros de tráfico en la red y alerten al personal a cargo de la seguridad de posibles irregularidades o comportamientos sospechosos.

    g. Realizar periódicamente copias de seguridad de los datos que permitan, en caso de pérdidas ocasionadas por ataques cibernéticos, tales como *ransomware* o *malware*, recuperar la información actualizada.

h. Implementar controles de acceso robustos y mecanismos de autenticación para evitar el acceso no autorizado a los sistemas y los datos. Estos deben requerir; (i) el uso de contraseñas seguras[4] y confidenciales; (ii) el cambio de estas contraseñas regularmente; (iii) la autenticación multifactor[5]; (iv) la eliminación de cuentas de accesos de exempleados y excontratistas; y (v) la limitación de los privilegios de administrador.

9. Realizar revisiones periódicas para evaluar la implementación, la efectividad y el cumplimiento del programa de ciberseguridad. Además, identificar las nuevas amenazas que deben incluirse en el mismo.

[4] Para diseñar contraseñas seguras se recomiendan que estas incluyan una combinación de letras, números y símbolos y un largo no menor de 10 caracteres. Incluso se recomienda el uso de contraseñas con modalidad de frase.

[5] Esta requiere ingresar al menos dos componentes de identidad para autenticar al usuario como un código único, otra contraseña, una biometría, o una característica física o de comportamiento única. Esto minimiza el riesgo de que un atacante obtenga acceso a una cuenta si conoce el nombre del usuario y la contraseña.