VÍA CORREO ELECTRÓNICO

13 de agosto de 2024

CARTA CIRCULAR NÚM. 2024-005

A TODOS SECRETARIOS, DIRECTORES, PRINCIPALES OFICIALES DE INFORMÁTICA Y PERSONAL TÉCNICO DE LAS AGENCIAS DE LAS AGENCIAS DEL GOBIERNO DE PUERTO RICO

Antonio J. Ramos Guardiola
Principal Ejecutivo de Innovación e Información, Gobierno de Puerto Rico
Director Ejecutivo – PRITS

Poincare Díaz Peña
Principal Oficial de Seguridad Cibernética, Gobierno de Puerto Rico

Re: RECORDATORIO SOBRE PREPARACIÓN Y PROCEDIMIENTOS PARA LA PROTECCIÓN DE DOMAIN CONTROLLERS Y ARCHIVOS CRÍTICOS

BASE LEGAL

Esta Carta Circular se emite de conformidad con la Ley Núm. 75-2019, conocida como la "Ley de la Puerto Rico Innovation and Technology Service", y la Ley Núm. 40-2024, conocida como la "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico". Estas leyes establecen el marco normativo para la gestión y protección de la información y tecnología en el Gobierno de Puerto Rico, facultando a la Puerto Rico Innovation and Technology Service (PRITS) para liderar estos esfuerzos.

En virtud de la Ley 75-2019, PRITS está facultada para implantar, desarrollar y coordinar la política pública del Gobierno en materia de innovación y tecnología, así como para revisar y aprobar proyectos tecnológicos en las agencias gubernamentales. Además, PRITS tiene la autoridad para emitir órdenes administrativas y cartas circulares que aseguren el cumplimiento de dicha ley.

Por su parte, la Ley Núm. 40-2024, en su Artículo 5, asigna a PRITS la responsabilidad de velar por la administración segura de los recursos informáticos en todo el gobierno, estableciendo que toda agencia debe desarrollar, documentar e implementar un programa de ciberseguridad que, como mínimo, incluya la gestión integral de los activos de información, la realización anual de

evaluaciones de riesgos de ciberseguridad, y la evaluación de vulnerabilidades para validar la efectividad de los controles de seguridad implementados.

Además, el Artículo 7 de la Ley 40-2024 estipula que toda agencia debe establecer planes de resguardo y recuperación de datos que estén integrados al plan de contingencia de la agencia, asegurando la continuidad de las operaciones tanto en sistemas locales como en aquellos mantenidos por suplidores externos o en la nube. También, se requiere la implementación de controles automáticos para la detección de programas no deseados (como virus, adware, spyware, malware, y ransomware) y para prevenir actividades de intrusión que puedan comprometer la seguridad de la información.

APLICABILIDAD

Esta Carta Circular será aplicable a todas las agencias del Gobierno de Puerto Rico, según se definen en el Artículo 3(a) de la Ley Núm. 75-2019 y en el Artículo 4(c) de la Ley Núm. 40-2024. A aquellas agencias y entidades que estén exentas de estas leyes, se les recomienda implementar los procedimientos aquí descritos como una mejor práctica para garantizar la protección y seguridad de sus recursos tecnológicos y de información.

PROPÓSITO

MEDIDAS DE PREPARACIÓN Y PROCEDIMIENTOS

Todo sistema de información del Gobierno debe contar con medidas preventivas robustas para proteger nuestros sistemas críticos. Una preparación adecuada es clave para asegurar la continuidad operativa y la integridad de nuestros sistemas de información ante cualquier incidente, ya sea provocado por condiciones atmosféricas o cibernéticas.

Los componentes gubernamentales deben estar conscientes de que un incidente cibernético, como un ataque de "ransomware" durante una emergencia, puede tener serias consecuencias si cada agencia no toma las medidas preventivas adecuadas. Los "Domain Controllers" (en adelante "DC") y los archivos digitales críticos son elementos vitales de nuestras operaciones diarias, y su protección debe ser una prioridad máxima. A continuación, se detallan las medidas de seguridad preventiva que deben ser adoptadas por las agencias:

1. **Resguardo de DC:**
    - **"System State Backup":** Realizar un resguardo completo de la base de datos de "Active Directory" y otros componentes críticos a través del *Windows Server Backup* u otras herramientas de preferencia.
    - **"Complete DC Backup":** Crear una imagen completa del servidor, incluyendo todos los volúmenes y configuraciones esenciales.
    - **Almacenamiento Seguro:** Asegurarse de que los resguardos se almacenen en medios físicos o redes completamente aisladas de la red principal.
2. **Resguardo de Archivos Digitales Críticos:**
    - **Identificación de Archivos Críticos:** Identificar los archivos y configuraciones que son esenciales para la operación continua de la Agencia.

- **Uso de Herramientas de resguardo:** Utilizar la herramienta de resguardo que mejor se adapte a las necesidades de la agencia, como *Windows Server Backup* o "software" especializado, para realizar copias de seguridad de estos archivos.
- **Almacenamiento en Repositorios Seguros:** Asegurar que los respaldos de estos archivos estén en un medio seguro y aislado.

3. **Monitoreo y Supervisión:**
   - **Supervisión Activa:** Mantener un monitoreo constante de los DC y archivos respaldados, así como de las consolas del EDR, para detectar cualquier actividad sospechosa.
   - **Reporte Inmediato de Anomalías:** Reportar cualquier irregularidad detectada de manera inmediata para activar las acciones correctivas necesarias.

Para facilitar la verificación de estas medidas por parte de cada agencia, se adjunta un proceso que describe paso a paso el procedimiento para los resguardos mencionados anteriormente, así como su correspondiente trámite en redes o repositorios aislados.

Las Agencias deberán asegurarse de haber seguido rigurosamente los pasos descritos en el procedimiento adjunto y documentar todas las actividades relacionadas con la protección de los sistemas.

Para cualquier consulta adicional o asistencia técnica, pueden comunicarse a: support@prits.pr.gov

MULTAS

El incumplimiento con esta Carta Circular podrá resultar en la imposición de multas conforme al Artículo 10 de la Ley 40-2024. PRITS podrá imponer a la agencia, funcionario público o proveedor de servicios, previa notificación y oportunidad de ser oídos, multas de entre cincuenta (50) a cien (100) dólares diarios por cada día de incumplimiento con este estándar de ciberseguridad. En casos de obstrucción, negligencia, mala fe, temeridad o negativa caprichosa en el manejo o reporte de un ciberataque, las multas pueden oscilar entre mil (1,000) y cinco mil (5,000) dólares por violación. Además, las sanciones pueden incluir medidas disciplinarias como anotaciones en el expediente de personal del servidor público, prohibiciones de contratación por un periodo de cinco (5) años, y sanciones monetarias para los proveedores de servicios, incluyendo penalidades contractuales y legales aplicables. Todo incumplimiento también conllevará un proceso de reeducación y capacitación coordinado por PRITS en colaboración con la Oficina de Ética Gubernamental.

DEROGACIÓN

Esta Carta Circular no deroga ninguna Carta Circular, Memorando, Políticas, Normativas, comunicación escrita o instrucción anterior; y continuará en plena fuerza y vigor hasta su derogación expresa.

VIGENCIA

Esta Carta Circular tendrá vigencia inmediata.