23 de octubre de 2023

CARTA CIRCULAR NÚM. 2023-006

Secretarios, Jefes de Agencias, Directores Ejecutivos y Oficiales Principales de Informática (OPI) de Departamentos, Agencias, Comisiones, Juntas, Administraciones, Corporaciones Públicas, Instrumentalidades y demás organismos o entidades de la Rama Ejecutiva del Gobierno de Puerto Rico

Antonio J. Ramos Guardiola
Principal Oficial de Tecnología
Subdirector
Puerto Rico Innovation & Technology Service

Actualización de los Sistemas de Gestión de Contenidos (CMS)

Base Legal

Esta Carta Circular se emite conforme a la autoridad conferida a PRITS por el artículo 7(3) de la Ley 75-2019, también conocida como "Ley del Puerto Rico Innovation and Technology Service". El inciso (a) del Artículo 6 atribuye a PRITS la responsabilidad de implementar, desarrollar y coordinar la política pública del Gobierno de Puerto Rico en los ámbitos de innovación, información y tecnología. Simultáneamente, el inciso (e) le asigna la tarea de optimizar el portal principal del Gobierno de Puerto Rico para mejorar su accesibilidad e integración, generando así beneficios tanto para la ciudadanía como para el Gobierno.

Además, el artículo 7 de la Ley 151-2004, "Ley de Gobierno Electrónico", según enmendada, establece que todos los organismos e instrumentalidades de la Rama Ejecutiva del Gobierno de Puerto Rico deben contar con una página electrónica con el propósito de proveer servicios y facilitar el acceso a la información. Concurrentemente, esta ley encomienda a PRITS la gestión de los sistemas de información y la implementación de normativas y procedimientos relativos al uso de las tecnologías de la información en el sector gubernamental.

Conforme al artículo 5(i) de la Ley 151 y el artículo 20 de la Ley 75, se establece que PRITS tiene la responsabilidad de implementar controles efectivos relacionados con la seguridad de los sistemas de información que respaldan las operaciones y los activos gubernamentales. Así también, la Ley 151 ordena la incorporación al quehacer

gubernamental de las tecnologías de la información con el propósito de transformar y agilizar las relaciones del Gobierno con los ciudadanos y empresas, así como las interacciones gubernamentales, buscando forjar un Gobierno más accesible, eficiente y transparente para el ciudadano. En consecuencia, PRITS está facultado para establecer la política pública y las directrices que guiarán la adquisición e implementación de los sistemas, equipos y programas de tecnología de la información para los entes gubernamentales.

Alcance y Jurisdicción

Conforme al artículo 3(a) de la Ley 75, esta Carta Circular es aplicable a toda junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina, división, administración, negociado, departamento, autoridad, y a cualquier funcionario, empleado, persona, entidad o instrumentalidad de la Rama Ejecutiva del Gobierno de Puerto Rico.

Para todas las entidades que, estando exentas de la Ley 75 y de la Ley 151, están sujetas a la Ley 229-2003, conocida como "Ley para Garantizar el Acceso de Información a las Personas con Impedimentos", se recomienda la adopción de esta Carta Circular.

Propósito

Mediante esta Carta Circular, se establecen directrices para la actualización de los Sistemas de Gestión de Contenidos (CMS) utilizados por las agencias del Gobierno de Puerto Rico. A pesar de la conveniencia y popularidad de los CMS de código abierto, como, por ejemplo, WordPress, hemos identificado vulnerabilidades significativas que comprometen la integridad de nuestra información y tecnología.

En la era digital contemporánea, las agencias gubernamentales de Puerto Rico se han esforzado por brindar a la ciudadanía un acceso inmediato y actualizado a información vital sobre servicios y actividades gubernamentales. En este proceso, se ha observado una inclinación hacia la utilización de sistemas de gestión de contenidos basados en código abierto, siendo WordPress un claro referente por su adaptabilidad y facilidad de uso.

No obstante, los desafíos de WordPress no solo radican en su configuración, sino también en el continuo mantenimiento requerido. Para garantizar una implementación segura de este tipo de plataforma, es imperativo que los usuarios instalen y configuren la aplicación de manera adecuada, acorde a los parámetros legales y normativos. Además, es esencial proteger y actualizar regularmente la plataforma ante cada nueva versión, parche o amenaza de seguridad detectada. Esta responsabilidad exige entidades fortalecidas con políticas, procedimientos y operaciones maduras en materia de ciberseguridad y privacidad, capacitadas para gestionar estos riesgos de forma ininterrumpida.
Aun tomando medidas preventivas, WordPress ha revelado diversas vulnerabilidades desde sus inicios debido a fallos en su configuración, monitoreo o gestión. Estas debilidades no han pasado desapercibidas para los actores maliciosos, que han aprovechado consistentemente estos fallos. La popularidad de WordPress agrava esta situación, al posicionarlo como blanco principal para quienes buscan explotar deficiencias de seguridad. Cabe destacar que, desde su lanzamiento inicial, el Instituto Nacional de

Estándares y Tecnología (NIST) ha identificado 6,878 vulnerabilidades vinculadas directamente con WordPress en su Base de Datos Nacional de Vulnerabilidades.[1]

A continuación, presentamos las principales vulnerabilidades asociadas a los sistemas de gestión de contenidos de código abierto que deben ser consideradas al evaluar dichas plataformas:

1. Inyección SQL: La inyección SQL en un gestor de contenido puede permitir a los hackers acceder y manipular la base de datos del sitio web, lo que puede resultar en la eliminación o corrupción de datos, y en algunos casos, en el control total del sitio.

2. Cross-site Scripting (XSS): Este tipo de ataque permite a los ciberdelincuentes inyectar scripts maliciosos en páginas web, que luego son ejecutados en los navegadores de los usuarios, comprometiendo sus datos y/o credenciales.

3. Cross-site Request Forgery (CSRF): Mediante esta vulnerabilidad, los atacantes manipulan a los usuarios para que ejecuten acciones involuntarias en un sitio web donde previamente se han autenticado, sin su conocimiento o consentimiento explícito.

4. Ataques de Fuerza Bruta: En este escenario, los atacantes intentan ganar acceso a un sitio web probando de manera repetida y sistemática diversas combinaciones de nombres de usuario y contraseñas hasta dar con la combinación correcta.

5. Inyección de Código: Los atacantes explotan vulnerabilidades presentes para inyectar código malicioso en el sitio web, facilitando así el control de este y/o la sustracción de datos.

6. Desbordamiento de Búfer (Buffer overflow): Esta vulnerabilidad permite a los atacantes sobrescribir la memoria del sistema, lo que puede conducir a la ejecución de código arbitrario, comprometiendo la integridad del sistema.

7. Divulgación de Información: Archivos y directorios que estén desprotegidos o mal configurados pueden llegar a revelar información crítica sobre la estructura e infraestructura del sitio web.

8. Seguridad de los Temas y Plugins: Temas y plugins desactualizados, o con códigos maliciosos, pueden ser puntos de entrada para ataques, comprometiendo el sitio web y sus datos.

[1]National Institute of Standards and Technology National Vulnerability Database (Last Accessed October 18, 2023). https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=wordpress&search_type=all

Determinación

Todas las entidades sujetas a la Ley 151 y la Ley 75 están obligadas a utilizar una plataforma web que utilice un sistema de gestión de contenidos (CMS) de código cerrado, siendo WebFlow la plataforma recomendada por PRITS. Aunque Webflow ha sido designada como la plataforma recomendada para todas las agencias del Gobierno de Puerto Rico, su adopción no es mandatoria. No obstante, cualquier agencia que opte por una plataforma diferente a la recomendada deberá obtener la autorización previa de PRITS.

Todas las agencias del Gobierno de Puerto Rico tienen un término de treinta **(30)** días para notificar a PRITS acerca de cualquier página web o aplicación que estén utilizando y que esté basada en un CMS de código abierto. Esta notificación se realizará mediante el formulario (RFI) que se adjunta en este documento.

En dicho RFI, deberán especificar detalles relacionados con el proceso de migración. Esto incluye si la entidad hará uso de sus recursos internos o contratará servicios externos. Además, las entidades deben presentar un plan de migración que asegure que la transición se complete en un término máximo de noventa **(90)** días desde la fecha de emisión de esta Carta Circular. Es importante que, durante este proceso, se priorice la adopción de sistemas de gestión de contenidos cerrado que posibiliten la publicación en la nube, siempre que satisfagan los estándares de viabilidad establecidos.

Favor de remitir el RFI a través del portal web: **www.prits.pr.gov/rfi-portales**.

Para concluir, es esencial enfatizar la importancia de que la implementación de la nueva página web cumpla rigurosamente con las normativas establecidas. Esto incluye adherirse a la Política de Seguridad Cibernética de PRITS, las Guías de Interfaz y Diseño (GUIDI) de PRITS, y las Guías de Accesibilidad para páginas WEB del Gobierno de Puerto Rico, conforme a las directrices proporcionadas por el Programa de Asistencia Tecnológica de Puerto Rico.

Derogación

Esta Carta Circular deja sin efecto cualquier otra carta circular, memorando, orden administrativa, políticas, 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

Esta Carta Circular tendrá vigencia inmediata.