**Universidad de Puerto Rico**
Recinto de Rio Piedras

12 de febrero de 2026

CIRCULAR NUM. 1 2025-2026

**A LA COMUNIDAD UNIVERSITARIA**

Rubén Rodríguez Ocasio, MSc.
Director Ejecutivo

**AVISO DE SEGURIDAD INFORMÁTICA - CAMPAÑA ACTIVA DE *PHISHING* DIRIGIDA A LA COMUNIDAD UNIVERSITARIA**

En los pasados días, la Universidad de Puerto Rico ha observado un aumento inusual de mensajes asociados a una campaña de phishing, utilizando cuentas institucionales comprometidas, dirigidos a estudiantes, personal docente y empleados no docentes.

Como parte del monitoreo de seguridad realizado, para más de 61,000 casos identificados recientemente, se han observado los siguientes patrones y/o características comunes:

- Envíos originados desde Google Workspace.
- Mensajes con el campo *Subject* o Asunto vacío o con el texto "SOLO TEXTO"**.**
- Inclusión de imágenes con mensajes que hacen referencia a números telefónicos.
- Autenticaciones provenientes de direcciones IP de proveedores de servicio de datos locales.
- Mensajes que hacen referencia a cancelación de cuentas**,** ofrecimientos de empleo u otros escenarios diseñados para inducir urgencia.
- Inclusión de URLs externas cuyo propósito es recopilar información confidencial de los usuarios.

Es importante reiterar que la Universidad de Puerto Rico no cancela cuentas institucionales. Tampoco solicita información de acceso**,** tales como: contraseñas, respuestas a preguntas de seguridad o códigos de autenticación mediante correo electrónico, llamadas telefónicas, y/o mensajes de texto.

Las comunicaciones recibidas, así como los incidentes reportados, han sido referidos al personal encargado de seguridad de la Oficina de Sistemas de Información de la Administración Central para su análisis, investigación y manejo conforme a los protocolos institucionales.

**División de Tecnologías Académicas y Administrativas**
6 Ave. Universidad STE 601, San Juan, Puerto Rico, 00925-2526
Tel. (787) 764-0000 ext. 83800
Fax. 787-764-2755

Como medidas cautelares, se ejecutaron las siguientes acciones de seguridad:

- Eliminación de los mensajes identificados de los buzones de correo.
- Implementación de políticas de filtrado basadas en los patrones observados en el *Subject* o Asunto y las URLs.
- Restablecimiento de contraseñas (*password reset*) en las cuentas afectadas.
- Suspensión preventiva de cuentas a nivel de Google Workspace.

Exhortamos enfáticamente a toda la comunidad universitaria a:

- Nunca compartir sus contraseñas**,** respuestas a preguntas de seguridad ni códigos de autenticación.
- No completar formularios ni acceder a enlaces contenidos en correos sospechosos.
- Reportar cualquier mensaje similar directamente desde la aplicación de correo electrónico institucional (Outlook) utilizando la opción de *Report Junk o Report Phishing***.**
- Proteger su seguridad digital y no atender este tipo de correos**.**

Si usted completó algún formulario asociado a uno de estos correos fraudulentos, le recomendamos acceder de inmediato al portal institucional Portal UPR y utilizar el mecanismo de "Olvidé mi contraseña" para realizar el cambio correspondiente. Este proceso permitirá que la nueva contraseña se propague a todas las plataformas institucionales.

Este aviso se emite conforme a la Política Institucional sobre el Uso y Acceso a los Recursos de la Tecnología de la Información, aprobada mediante la Certificación Núm. 85 (2022-2023) de la Junta de Gobierno de la Universidad de Puerto Rico, la cual establece la responsabilidad de todos los usuarios de:

- Proteger la seguridad, integridad y confidencialidad de los recursos tecnológicos institucionales.
- Utilizar los sistemas de información de forma ética, responsable y segura.
- Reportar posibles incidentes o violaciones de seguridad a las entidades correspondientes.

Para información adicional y recursos educativos sobre cómo evitar ser víctima de fraude electrónico, le recomendamos visitar el Portal de Seguridad de la Tecnologia de Informacion de la Universidad de Puerto Rico. Por otro lado, de necesitar asistencia técnica, puede efectuar una orden de servicio en la Mesa de Ayuda de la DTAA.

La Universidad de Puerto Rico continuará fortaleciendo sus mecanismos de protección tecnológica y monitoreo continuo para salvaguardar la información institucional y los datos personales de nuestra comunidad.