UNIVERSIDAD INTERAMERICANA DE PUERTO RICO
RECINTO DE SAN GERMÁN
Centro de Informática y Telecomunicaciones

A los usuarios de sistemas informáticos

P/C: José Luis Colón González, Ph.D.
Rector

Rogelio Toro Zapata
Director

RIESGO DE INTERRUPCIONES EN LA RED

Los sistemas de información son esenciales para transformar las experiencias de aprendizaje y, a su vez, constituyen componentes estratégicos de la infraestructura institucional que respaldan el desarrollo académico y facilitan la gestión administrativa. Por lo tanto, es fundamental garantizar la disponibilidad continua de estos servicios.

Sin embargo, se han enfrentado situaciones que han provocado interrupciones en los servicios. Por tal razón, es importante alertar a nuestra comunidad universitaria y promover la concienciación sobre prácticas que puedan representar una amenaza significativa para la seguridad y estabilidad de nuestros sistemas, para a prevenir que estos incidentes se repitan.

1. Conexión de dispositivos no autorizados a la red: esta práctica podría facilitar accesos no autorizados, ataques informáticos o fallas en el tráfico de la red, afectando procesos críticos que impactan tanto las actividades académicas como las administrativas.
   Por lo tanto, no está permitido instalar ni conectar dispositivos a la red institucional, particularmente a puntos de acceso o enrutadores (*routers*) inalámbricos, ni equipos periféricos o de telecomunicaciones que no hayan sido previamente configurados, instalados y administrados por personal técnico del CIT.

2. Fenómeno conocido como *network loop*: ocurre cuando ambos extremos de un mismo cable de red (*patch cord*) se conectan a la misma infraestructura por la que circula el tráfico de datos. Por ejemplo, esto sucede cuando un usuario conecta los dos extremos del mismo cable a dos puertos de un mismo *switch* o a dos puntos de red (*drops*) de pared pertenecientes al mismo segmento de comunicaciones. El tráfico de la red comienza a circular de manera redundante y exponencial, provocando la saturación y eventual bloqueo de los servicios. Aunque nuestros *switches* principales cuentan con mecanismos para detectar y desactivar los puertos involucrados en este tipo de incidente, en otras circunstancias los equipos pueden activar mecanismos de autoprotección que deshabiliten todos sus puertos, ocasionando interrupciones en los servicios de red para las computadoras, impresoras y demás dispositivos conectados.

   Ejemplo de un *network loop*: