Universidad de Puerto Rico
Oficina de Sistemas de Información
Administración Central

Procedimiento Interno de Respuesta a Vulnerabilidades Críticas

Revisado y aprobado por el Comité Institucional de Seguridad en los Sistemas de Información
Abril 2024

Introducción

En la Universidad de Puerto Rico, la seguridad de la información es una prioridad que requiere la cooperación y el compromiso constante de todas las unidades académicas y administrativas. Dada la creciente sofisticación y frecuencia de las amenazas cibernéticas, es imperativo establecer mecanismos robustos y efectivos para proteger nuestros sistemas y datos.

Este documento presenta un protocolo diseñado para la identificación rápida, comunicación efectiva y resolución diligente de vulnerabilidades críticas dentro de nuestros sistemas de información. Al adherirnos a este protocolo, fortalecemos la seguridad en los sistemas de información con el fin de proteger la integridad, disponibilidad y confidencialidad de los datos y servicios institucionales.

Este protocolo aplica a las Oficinas de Sistemas de Información de todas las Unidades académicas y administrativas de la Universidad de Puerto Rico.

Definiciones

- **Vulnerabilidad Crítica**: Cualquier debilidad en los sistemas de información que pueda ser explotada para obtener acceso no autorizado, causar daños significativos, o exponer información confidencial o restricta de la institución.
- **CISO:** (Chief Information Security Officer) Principal Oficial de Seguridad de la Información de la Universidad de Puerto Rico.
- **Oficinas de Sistemas de Información**: Departamentos o unidades responsables de gestionar los sistemas de información en las distintas Unidades académicas y administrativas de la Universidad.
- **CISA**: Cyber Infrastructure and Security Agency

Procedimiento

1. Identificación y Comunicación de la Vulnerabilidad:
    a. El CISO, a través del "Cyber Hygiene Assessment" del CISA o cualquier otro método de detección, identifica vulnerabilidades críticas en los sistemas de información de la Universidad.
    b. Un informe detallado de la vulnerabilidad identificadas se envía a los directores y coordinadores de las Oficinas de Sistemas de Información correspondientes, incluyendo la criticidad, impacto potencial, y recomendaciones de mitigación. Este informe se envía cuando es identificada la vulnerabilidad.

2. Acuse de Recibo y Plan de Acción:
    a. Las Oficinas de Sistemas de Información deben acusar recibo del informe en un plazo razonable y proporcionar un plan de acción preliminar para la resolución de la vulnerabilidad, incluyendo plazos estimados.

3. Implementación de Medidas de Mitigación:
    a. Las unidades responsables deben comenzar la implementación de las medidas de mitigación según el plan de acción aprobado por el CISO.
    b. Si se requieren recursos adicionales o hay cambios significativos en el plan de acción, estos deben ser comunicados y aprobados por el CISO.

4. Verificación y Cierre:
    a. Una vez implementadas las medidas de mitigación, la Oficina de Sistemas de Información correspondiente debe informar al CISO, quien realizará o coordinará una verificación de la efectividad de las medidas.
    b. Si la vulnerabilidad ha sido resuelta satisfactoriamente, el CISO emitirá una confirmación. En caso contrario, se requerirá un ajuste de las medidas de mitigación y repetición del paso 4a.

5. Incumplimiento de los Plazos:
    a. En caso de que no se acuse recibo del informe, no se presente un plan de acción, o no se tomen las medidas de mitigación en los plazos establecidos, el CISO podrá ordenar la restricción de acceso en la red de comunicaciones del sistema identificado, hasta que se demuestre que la vulnerabilidad ha sido adecuadamente resuelta.