NO-43 GESTIÓN DE VULNERABILIDADES TÉCNICAS

1. Normatividad Relacionada

PO-00 Política de Seguridad de la Información

PO-02 Administración de Cambios

PO-03 Administración de la Seguridad de la Información

PO-08 Normas Procedimientos Operativos y Documentación

PO-15 Cumplimiento

2. Objetivo

Regular las actividades a realizar para la identificación, remediación, mitigación y seguimiento de vulnerabilidades técnicas en los Componentes Tecnológicos de la UAEAC.

3. Alcance

Esta norma aplica a todos los Componentes Tecnológicos de la UAEAC administrados por la Dirección de Informática.

4. Descripción

- Cuando se requiera realizar Análisis de Vulnerabilidades o Pruebas de Penetración sobre algún Componente Tecnológico de la UAEAC, sea con recursos internos o contratados, se debe tener en cuenta como mínimo los siguientes requisitos:

  ✓ Definir el Alcance del Análisis de Vulnerabilidades o Pruebas de Penetración.

  ✓ Definir y aprobar la metodología a utilizar.

  ✓ Aprobar las herramientas a utilizar, indicando la versión, nivel de actualización (Plugins, archivos identificadores de vulnerabilidades, entre otros) y demás características generales.

  ✓ Elaborar un informe ejecutivo y presentación de los resultados encontrados.

  ✓ Elaborar un informe técnico detallado, con el resultado generado por las herramientas utilizadas, el análisis de las vulnerabilidades encontradas con la codificación acorde al Common Vulnerability Score System - CVSS, impacto de la materialización del riesgo y las recomendaciones a implementar.

  ✓ Elaborar un Plan de Remediación con las actividades a realizar para remediar las Vulnerabilidades identificadas, el impacto de su implementación, el responsable de la implementación y las fechas acordadas. Si alguna vulnerabilidad no se puede remediar, debe ser justificada técnicamente y se debe evaluar la viabilidad de implementar controles adicionales que mitiguen el riesgo de explotación de la

vulnerabilidad identificada. Estos casos deben ser documentados y categorizados como excepciones en el proceso.

- La ejecución del Plan de Remediación es responsabilidad de la Dirección de Informática.

- Una vez sea realizada la remediación de las vulnerabilidades, se debe solicitar la ejecución de un nuevo Análisis de Vulnerabilidades o Pruebas de Penetración para validar el cierre de la brecha de seguridad.

- Una vez ejecutadas las validaciones por parte del Grupo Seguridad de la Información, se debe tomar el Plan de Remediación y dar cierre a las actividades asociadas en este.