Instituto Nacional Electoral

Análisis y respuesta del documento "CISQ Specifications for Automated Quality Characteristic Measures".

Análisis

Subdirección de Tecnología y Seguridad informática
Departamento de Seguridad Informática

1. Antecedentes

Durante la Tercera reunión ordinaria del COTAPREP se solicitó a la Subdirección de Tecnología y Seguridad Informática la revisión del documento "CISQ Specifications for Automated Quality Characteristic Measures" publicado por el Consorcio para la calidad del Software para las Tecnologías de información conocido como CISQ por su siglas en inglés (Consortium for IT Software Quality).

CISQ[1] es una organización líder dentro de la industria de TI fundada en 2009 y que es conformada por integradores de sistemas, proveedores de servicios y vendedores de tecnologías de software

El objetivo de este documento es determinar la aplicabilidad de las especificaciones descritas en las especificaciones publicadas por el CISQ.

2. Revisión de las especificaciones publicadas por el CISQ

Las especificaciones desarrolladas por el CISQ establecen un dominio o apartado de seguridad el cual toma como referencia los "25 Errores más Peligrosos del Software"[2] publicado por la organización norteamericana "Common Weakness Enumeration" conocida por sus siglas en inglés como CWE. CISQ toma como base para su especificación solo 19 tipos de error diferente.

Las especificaciones desarrolladas por CISQ tienen como objetivo establecer un framework que sirva como referencia para el desarrollo de la calidad del software. Asimismo cuentan también con otro objetivo el cual consiste en el desarrollo de herramientas que permitan la revisión de forma automática de la calidad del software.

De acuerdo a lo revisado por la Unidad Técnica de Servicios de Informática las herramientas desarrolladas por CISQ se encuentran en etapa de desarrollo y no pueden ser utilizadas de manera sistemática durante el ciclo de desarrollo del software establecido por la UNICOM.

Por otro lado CWE publica a través de su portal diversas herramientas que permiten llevar a cabo el análisis de calidad del software. De acuerdo a lo revisado por esta Unidad las herramientas publicadas con CWE son propietarias lo que significa que es necesaria la adquisición de licencias para su uso.

---

[1] http://it-cisq.org/
[2] http://cwe.mitre.org/top25/index.html

Para realizar la adquisición de las herramientas propuestas por el grupo CWE se requiere llevar a cabo el proceso de licitación establecido en la normatividad interna del Instituto. En este sentido el tiempo de adquisición de las herramientas sobrepasa los periodos establecidos para el desarrollo y puesta en producción de los sistemas del Programa de Resultados Electorales (PREP).

No obstante lo anterior cabe señalar que actualmente se cuenta con herramienta Acunetix WVS Enterprise Edition for Unlimited Websites para la cual la UNICOM cuanta con los derechos de uso así como con los servicios de actualización y suscripción vigentes. Esta herramienta es utilizada sistemáticamente como parte del ciclo de auditorías que se llevan a cabo a todas las aplicaciones desarrolladas al interior del Instituto incluyendo los aplicativos que se desarrollen como parte del PREP.

Como parte de las especificaciones de Acunetix WVS Enterprise Edition integra dentro de sus funcionalidades la verificación automática de los 25 errores más peligrosos del software publicados por CWE. En caso de identificarse alguno de los defectos señalados el software es actualizado por el grupo de desarrolladores. Lo anterior como parte del proceso de liberación en producción de las aplicaciones.

Por último el Instituto cuenta con el "ESTÁNDAR DE SEGURIDAD PARA EL DESARROLLO DE APLICACIONES DEL INSTITUTO NACIONAL ELECTORAL" el cual sirve como referencia para el desarrollo y la auditoría del software. El estándar en comento compila las mejores prácticas publicadas por organizaciones internacionales como SANS y NIST y OWASP. Se adjunta anexo a este informe dicho estándar.