Assignment 2: Security Assessment Questionnaire

Diseño y programación seguras

Amaia Echeandia

Para esta entrega de la asignatura, se detallarán algunos aspectos importantes de tres de los cuestionarios de evaluación de seguridad propuestos para analizar.

Cuestionario	Application Security Assessment Questionnaire	**ID**	Carnegie Mellon University	**Usuario objetivo**	Miembros del campus
Objetivo de cuestionario	El cuestionario está desarrollado para que un cliente reporte las posibles amenzas y vulnerabilidades que pueda sufrir para aclarar las necesidades que se tenga				
Descripcion	Al principio del cuestionario se lista el proceso a seguir para realizar una auditoría. A continuación, el documento se separa en varios cuestionarios que se enfocan en los escenarios más comunes de ataque				
Aspectos positivos	Analiza distintas vulnerabilidades en distintos servicios. El cuestionario también te deja desarrollar las respuestas ya que no son respuestas predefinida. De esta manera, se pueden dar más detalles que pueden ser claves en la evalución.				
Aspectos negativos	Lo que hace que sea positivo también puede jugar en contra, ya que al no haber respuestas predefinidas, hay aspectos que el usuario que completa el cuestionario puede dejar fuera de visión y no abordar el tema a posteriori por falta de conocimiento.				
Otros	A pesar de haber sido desarroyado por la Carnegie Mellon University para su propio uso, puede ser utilizado por más centros educativos.				

Cuestionario	VSAQ	**ID**	Github (2016)	**Usuario objetivo**	Proveedores de servicios
Objetivo de cuestionario	Es un metodo para verificar que los proveedores de servicio siguen las correctas prácticas de seguridad de información de manera que las empresas puedan confiar en delegar el manejo de su información y así minimizar las amenazas de ciberseguridad. También tiene como objetivo estandarizar los procesos de seguridad de proveedores				

Descripcion	Existen cuatro plantillas diferentes para realizar este tipo de cuestionario dependiendo del servicio que se esté ofreciendo. Estos incluyen las aplicaciones web, seguridad & privacidad, infraestructura y sistemas físicos & datacenters. En estas plantillas se pueden adjuntar tambien archivos por si se quisiera aportar alguna evidencia.
Aspectos positivos	El VSAQ es fácil de completar, intuituvo y cubre todas las áreas para la gestión de seguridad del proveedor. También permite la subida de evidencias para justificar respuestas y clarificar mejor la situación de lo reportado.
Aspectos negativos	Algunas respuestas predeterminadas pueden no reflejar la necesidad real del usuario que, además, no deja opción a detallar o justificar la respuesta seleccionada.
Otros	-

Cuestionario	Information Security Review Questionnaire - IT Support CUNY	**ID**	Departamento de soporte TI de City Univertsity of New York	**Usuario objetivo**	Responsables de proyectos, aplicaciones o sistemas que manejan información no pública de la Universidad.
Objetivo de cuestionario	Identifica los requisitos de seguridad carentes en los proyectos que manejan información, aplicaciones o sistemas físicos de la universidad que, además, puede atrasar la entrega programada de los proyectos.				
Descripcion	El cuestionario separa las preguntas en siete aspectos: clasificación de datos, servicios TI de proveedores, control de accesos, redes de comunicación y recuperación ante desastres. Además, si el usuario quiere añadir más información sobre cualquier aspecto de más, al final se podrán escribir comentarios.				
Aspectos positivos	El cuestionario da vía libre para completar las respuestas dando los detalles que el usuario vea necesario a parte de las prediseñadas. Parece un cuestionario muy completo para cualquier tipo de sistema o aplicación con preguntas faciles de leer y entender. Además, aunque lo haya desarrollado la CUNY para su propio uso, puede ser				
Aspectos negativos	El cuestionario ha sido desarrollado para un uso especifico de la CUNY, por ello hay opciones que sirven solo para esta universidad. En cambio, no son muchas las preguntas especificas para la CUNY y siempre se puede adaptar a la entidad que lo utilice.				
Otros	Puede ser utilizado por más centros educativos aplicando pequeños cambios.				

Todos estos cuestionarios analizados cumplen con objetivos muy parecidos pero enfocados a diferentes usuarios.

El cuestionario más completo que aborda bastantes aspectos y, a su vez, se puede completar con facilidad dando flexibilidad en las respuestas, me parece que es el "Information Security Review Questionnaire - IT Support CUNY", pero no podría elegirlo para mi proyecto ya que está enfocado a los requisitos de la universidad.

El cuestionario "Application Security Assessment Questionnaire" aunque haya sido desarrollado por otra universidad, no contiene preguntas especialmente enfocadas en ella, si no que es fácilmente aplicable a otras entidades. A pesar de ello, el cuestionario VSAQ me parece mejor para desarrollar una aplicación o servicio seguro/a, ya que los aspectos que se evaluan en el "Application Security Assessment Questionnaire" no son tan concretos. Además, como ya se ha comentado en la tabla anterior, el VSAQ tiene cuatro plantillas diferentes con una buena cantidad de preguntas dependiendo del tipo de servicio que se ofrezca, de manera que se puede detectar los problemas más fácil y se puede plantear un plan de acción concreto.