QUESTIONS AND ANSWERS - REFERENCE : CO/2022-06

Nombre de la licitación: Auditoría del sistema informático
Referencia: CO/2022-06

Pregunta: 1.

Auditoría Técnica - Pentesting - Actividades de Hacking Ético: en el documento no se detalla el alcance de la auditoría técnica y en ningún momento se hace mención a realizar actividades de hacking ético, aunque en el Anexo 1, se establecen los criterios de valoración CVSS para las vulnerabilidades encontradas. ¿Nos podrían indicar cual es el alcance (volumen de sistemas, de servidores, Bases de datos, si la auditoría tiene un alcance de los sistemas internos o solo es perimetral)?

Respuesta 1:

- El COI no está certificado en la norma ISO 27001 ni es objeto de esta auditoría conseguir dicha certificación.
- El pliego de condiciones de la licitación en curso establece como marco de referencia el estándar ISO/IEC 27002, puesto que dicho estándar proporciona una buena metodología y orientación general sobre los objetivos comúnmente aceptados en la gestión de la seguridad de la información.
- En el pliego de condiciones se solicita analizar los controles que el COI considera más relevantes para su actividad, pero se valorará positivamente la inclusión de otros controles por parte de cada licitante.
- La comprobación de la tríada Confidencialidad, Integridad y Disponibilidad de la Información (CIA) es esencial para esta auditoría, y en este ámbito se debe realizar un “pentesting” de la red y de los sistemas del COI, así como un ejercicio de hacking ético, excepto DDoS, con el fin de aprovechar las debilidades e identificar posibles vulnerabilidades antes de que se produzcan incidentes.
- El uso de CVSS es la métrica exigida para valorar las vulnerabilidades que se analicen.

Pregunta 2:

Pueden explicar en más detalle el apartado de "Sistemas Analizados" dado que no queda claro todo el conjunto de herramientas y de sistemas que se debe hacer con ello. Es decir, a nuestro entender la licitación se centra en una auditoría de seguridad en donde en base al marco ISO 27002, evaluar el cumplimiento del COI frente a ese marco y las debilidades o incumplimientos detallarlos en el plan de acción o de mejoras. Entendemos que no es necesario realizar ninguna prueba técnica de los sistemas, en caso de ser así, ¿pueden especificar en más detalle qué pruebas y actividades se pueden hacer y sobre que alcance, detallando el alcance también?

Respuesta 2:

- En el capítulo SISTEMAS ANALIZADOS del ANEXO I, se detallan los componentes que se solicita analizar (funciones I/O, servlets, conectores de base de datos, códigos SSL, ….) en los Sistemas del COI (excepto el ERP, llamado SAGE). Y para ello, se entiende que serán necesarias herramientas tales como analizadores de tráfico, escáner de puertos, generador de paquetes IP, … (sugeridas también en ANEXO I)