

RESUMEN

En el presente proyecto se pretende realizar un análisis de las vulnerabilidades del aplicativo Web del “SISTEMA INFORMATICO INTEGRADO DE SERVICIOS MUNICIPALES” del GADIC CAÑAR con el fin de detectar y prevenir las amenazas más comunes que ponen en peligro la estabilidad de los sistemas informáticos en la WEB, partiendo de un análisis comparativo entre diferentes metodologías de aseguramiento como son OWASP top 10, WASC Tc v2.0 Y CWE/SANS Top 25, los cuales presentan los riesgos más relevantes, sus vectores de ataque y los posibles controles de mitigación. Una vez determinada la metodología de aseguramiento a ser utilizada, se establece la metodología de auditoria con sus respectivos entregables por cada fase; luego se establece las herramientas que pueden ser utilizadas para la detección de las vulnerabilidades según los puntos de control establecidos por OWASP top 10, metodología seleccionada en un proceso anteriores. Las pruebas fueron diseñadas dentro de las pruebas sustantivas de auditoria, así también se tomó como referencia la ISO 27002 para realizar el análisis de los controles existentes y el diseño de las pruebas de cumplimiento. De los resultados obtenidos se emitió un informe detallado de los hallazgos con sus conclusiones y recomendaciones que fueron diseñados con el objetivo de brindar soporte al mejoramiento continuo de los servicios informáticos que brinda a la ciudadana el GADIC Cañar.

PALABRAS CLAVES: EVALUACIÓN TÉCNICA INFORMÁTICA, SEGURIDAD, VULNERABILIDADES, APLICACIONES WEB, OWASP TOP 10.