Resumen

La presente tesis tiene como objetivo analizar la factibilidad técnica financiera para la implementación de un Grupo de Respuesta a Incidentes de Seguridad Informática (CSIRT), para la Escuela Politécnica del Ejército (ESPE).

Para el cumplimiento de este objetivo, inicialmente se ha realizado una recopilación de los procesos definidos en los modelos de gestión de tecnología, en guías y estándares internacionales y en publicaciones técnicas referentes al manejo de incidentes de seguridad informática, con la finalidad de establecer el marco teórico sobre el cual se sustenta el dimensionamiento de la infraestructura tecnológica y organizacional del CSIRT de la ESPE.

Con el objetivo de establecer una línea base de la arquitectura de seguridad informática de la ESPE, sobre la que se apoyara el CSIRT para el cumplimiento de sus objetivos y servicios, se ha realizado una evaluación de las políticas, procedimientos y controles de seguridad existentes en la institución. Adicionalmente se evaluó la estructura organizacional de la ESPE, para determinar los factores de éxito crítico en función de los cuales se establecen la misión, visión y servicios del CSIRT, que apoyarán al cumplimiento de los objetivos estratégicos institucionales.

Basándose en los datos obtenidos del diagnóstico organizacional y tecnológico de la ESPE se dimensionó y estructuró el CSIRT académico, en proyección a una futura implementación del mismo en la Institución, se realizó el análisis del presupuesto referencial necesario y se evaluó el costo beneficio que se obtendría una vez que el CSIRT se encuentre operativo.

Finalmente para evaluar las mejoras en los tiempos de resolución, la distribución de carga de requerimientos y el número de incidentes de informáticos de seguridad resueltos exitosamente, por parte del personal de la UTIC de la ESPE, al contar con procesos estructurados y capacitación en seguridad informática, se realizaron simulaciones de diferentes escenarios con la herramienta SIMPROCESS.