

Resumen

La Seguridad de la Información (S-I) es algo más que un antivirus, cortafuego o cifrado de datos, la S-I es el resultado de operaciones realizadas por personas y que son soportadas por la tecnología (Gonzalo Álvarez Marañon, Pedro Pablo Pérez García, 2004); bajo este contexto, la Escuela Politécnica del Ejército (ESPE) desde el año 2010 ha realizado adquisiciones considerables de equipamiento de seguridad perimetral y software de altas prestaciones, requiriéndose definir políticas, normas, procedimientos y controles que permitan gestionar correctamente los principios de la S-I (integridad, disponibilidad y confiabilidad).

El objetivo principal de esta investigación es presentar una propuesta formal para implementar políticas y controles de buenas prácticas que recomienda la Norma ISO/IEC 27002 enfocado a dos procesos de la UTIC: Base de Datos y Redes y Comunicaciones. Se pretende entregar una guía flexible, coherente e integral que permitirá minimizar o eliminar los ataques, vulnerabilidades, desastres naturales o disturbios sociales que destruyan la información, poniendo en peligro inminente a la Institución. Se propone un acercamiento a la metodología OCTAVE para gestionar el riesgo y a la norma de seguridad ISO/IEC 27002.

Se realizó un estudio real de las políticas, procesos, controles, planes y manuales existentes en la UTIC, para culminar con el Plan Maestro de Seguridad Informática con lineamientos de la norma ISO/IEC 27002. La utilización de estas políticas y controles permitirán ofrecer servicios de tecnología de calidad acorde a las exigencias Institucionales y tendencias Mundiales