Resumen

El presente trabajo de investigación, busca analizar la situación actual de vulnerabilidad a la que está expuesta la infraestructura tecnológica digital de la Fuerza Terrestre a través de posibles brechas de seguridad físicas y lógicas en el servidor de correo electrónico institucional y el impacto que puede alcanzar en los aplicativos que mantiene en producción. Inicialmente se plantea el problema a resolver, luego se determina los objetivos de investigación. Se desarrolla una revisión bibliográfica respecto a la ciberseguridad y la ciberdefensa en el contexto militar a nivel mundial, regional y nacional mediante la utilización de fuentes primarias y datos estadísticos. La revisión exploratoria documental se desarrolla en la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre (DTIC FT). Se aplica el método científico con un enfoque cualitativo, planteando la hipótesis de investigación conjuntamente con las variables, posteriormente se aplica el método, técnicas e instrumentos de recolección de datos para su análisis e interpretación. Con los resultados y hallazgos se plantea implementar una propuesta de guía metodológica basada en la NORMA ISO/IEC 27001 y el Esquema Gubernamental de Seguridad de la Información (EGSI) en su última versión, lo cual permite evaluar la situación actual de vulnerabilidad, establecer una línea base para la implementación de políticas de seguridad que permitan incrementar la seguridad de la información que se almacena en los servidores de correo electrónico de la Fuerza Terrestre. La investigación ayuda a minimizar el impacto de los riesgos a través de conceptualizaciones doctrinarias, análisis de vulnerabilidades y concientización de los usuarios que administran y consumen la información disponible. Finalmente, la investigación concluye identificando las deficiencias tecnológicas, humanas y económicas que podrían ser causales de vulnerabilidad y de esta manera contribuir al fortalecimiento institucional y al desarrollo del país.

Palabras claves: vulnerabilidad, brechas de seguridad, servidor de correo electrónico, seguridad de la información

Abstract

This research work seeks to analyze the current situation of vulnerability to which the digital technological infrastructure of the Land Force is exposed through possible physical and logical security breaches in the institutional email server and the impact it can reach in the applications it maintains in production. A literature review regarding cybersecurity and cyber defense in the military context at global, regional and national levels is developed through the use of primary sources and statistical data. The exploratory documentary review is carried out in the Directorate of Information Technologies and Communications of the Land Force (DTIC FT). The scientific method is applied with a qualitative approach, raising the research hypothesis together with the variables, then the method, techniques and instruments of data collection are applied for analysis and interpretation. With the results and findings, it is proposed to implement a proposal for a methodological guide based on the ISO/IEC 27001 STANDARD AND THE GOVERNMENT INFORMATION SECURITY SCHEME (EGSI) in its latest version. Which allows to evaluate the current situation of vulnerability, establish a baseline for the implementation of security policies that allow to increase the security of the information that is stored in the email servers of the Ground Force. Finally, the research concludes by identifying the technological, human and economic deficiencies that could be causes of vulnerability and thus contribute to the institutional strengthening and development of the country.

Keywords: vulnerability, security gaps, email server, information security