Resumen

El presente trabajo propone un modelo de ciberseguridad alineado a los objetivos empresariales de la Corporación Nacional de Telecomunicaciones (CNT) que permita minimizar el riesgo y aplicar gobernanza en un sistema de infraestructura crítica como caso de estudio el área de transmisiones de la CNT, la cual permite mantener la disponibilidad de conectividad e interconexión en el país. De esta manera, se ha planteado como objetivo: diseñar un modelo de ciberseguridad con el fin de evaluar e identificar procesos y controles que permitan mantener la integridad, disponibilidad y confidencialidad de la información a ser transportada en las redes de transmisión. La metodología empleada en este estudio se basó en la revisión bibliográfica y documental de estudios relacionados con temas de ciberseguridad alineados a la estrategia empresarial de un sistema de infraestructura crítica, utilización de marcos para análisis de riesgos, ciberseguridad y gobernanza. Los resultados de este diseño indican que seis objetivos de gobierno y gestión se alinean a los requerimientos de la alta dirección de la CNT, el nivel actual de ciberseguridad es riesgo informado y son necesarios 21 proyectos quick wins para optimizar los procesos con una inversión baja y de esta manera mejorar el nivel de ciberseguridad de la CNT. Este modelo propuesto es la base para que las actividades de gobierno y gestión generen valor a través del objetivo de asegurar la optimización del riesgo mediante un enfoque de mejora continua.

Palabras clave: modelo de ciberseguridad, riesgo, redes de transmisión, gobernanza

Abstract

The present work proposes a cybersecurity model aligned with the business objectives of the National Telecommunications Corporation (CNT) that allows minimizing risk and applying governance in a critical infrastructure system as a case study of the transmission area of the CNT, which It allows maintaining the availability of connectivity and interconnection in the country. In this way, the objective has been set: to design a cybersecurity model in order to evaluate and identify processes and controls that allow maintaining the integrity, availability and confidentiality of the information to be transported in the transmission networks. The methodology used in this study was based on the bibliographical and documentary review of studies related to cybersecurity issues aligned to the business strategy of a critical infrastructure system, use of frameworks for risk analysis, cybersecurity, and governance. The results of this design indicate that six governance and management objectives are aligned with the requirements of the CNT's senior management, the current level of cybersecurity is an informed risk and 21 quick wins projects are necessary to optimize processes with a low investment and in this way improve the level of cybersecurity of the CNT. This proposed model is the basis for governance and management activities to generate value through the objective of ensuring risk optimization through a continuous improvement approach.

*Keywords: c*ybersecurity model, risk, security networks, transmission, governance.