RESUMEN

En el Ecuador, la Secretaría Nacional de Administración Pública determinó la implementación de la norma ISO/IEC 27001:2005, en respuesta a los continuos ataques y delitos informáticos presentados. Sin embargo, la normativa solo establece directrices para la gestión de riesgo en la seguridad de la información, mas no una guía paso a paso de cómo llevar a cabo un análisis y evaluación de riesgo. Debido a lo anterior, se establece en el presente trabajo elaborar una guía metodológica práctica para la gestión de riesgo de TIC en entidades del sector público conforme normativa NTE INEN ISO/IEC 27005 para mejorar la administración de la seguridad de la información. Para lograr el objetivo fue necesario conocer la normativa ISO/IEC 27005 y determinar el nivel con el cual se administran los riesgos tecnológicos en entidades públicas, por lo cual se realizó un estudio cuali-cuantitativo de alcance descriptivo y se consideró un muestreo no probabilístico. Se aplicó la técnica encuesta, a través de un cuestionario a 18 jefes de área de tecnología de las entidades públicas ubicadas en la ciudad de Esmeraldas. Obteniendo principalmente que, a pesar de la incorporación de la normativa internacional es todavía complejo el proceso debido a que los estándares fueron creados para empresas desarrolladas en otro contexto. En respuesta, se propone la guía detallada en la cual se desarrolla cada etapa con su conjunto de actividades, y su aplicación en una entidad del sector público con la finalidad de validar cada una de las etapas previamente definidas.

Palabras claves:

- **GESTIÓN DE RIESGO TECNOLÓGICO**
- **CULTURA DE ADMINISTRACIÓN DE RIESGOS TECNOLÓGICOS**
- **SEGURIDAD DE LA INFORMACIÓN.**

ABSTRACT

In Ecuador, through the National Secretariat of Public Administration, the implementation of ISO / IEC 27001: 2005 was determined in response to the continuous attacks and computer crimes presented. However, the regulation only establishes guidelines for risk management in information security, but not a step-by-step guide on how to carry out risk analysis and evaluation. Due to the above, it is established in the present work to elaborate a practical guide for the management of ICT risk in entities of the public sector according to NTE INEN ISO / IEC 27005 regulation to improve the administration of information security. In order to achieve the objective, it was first necessary to know the ISO / IEC 27005 standard and then to determine the level at which the technological risks are managed in public sector entities, for which a qualitative and quantitative study was carried out, and a non-probabilistic sampling. The survey technique was applied, through a questionnaire to 18 heads of technology area of the public entities located in the city of Esmeraldas. Obtaining mainly that, despite the incorporation of international regulations, the process is still complex because the standards were created for companies developed in another context. In response, the detailed guide is proposed in which each stage is developed with its set of activities, and its application in a public sector entity in order to validate each of the previously defined stages.

Keywords:

- **TECHNOLOGICAL RISK MANAGEMENT**
- **CULTURE OF TECHNOLOGY RISK MANAGEMENT**
- **SECURITY OF THE INFORMATION**