



*Maestría en*

# **CIBERSEGURIDAD**

Tesis previa a la obtención del título de Magíster en Ciberseguridad

**AUTOR:** Ing. Alejandro Javier Santamaría Guayasamin

Ing. Cristian Hernán Sánchez Arias

Ing. Steven Jholaus Álava Guanopatín

Ing. Eddie Alexander Yánez Pinzón

**TUTOR:** Mtr. Martinez Gordon Ronie Stalin

Propuesta para el sistema de gestión de seguridad de la información basado en la norma ISO 27001 y la ley orgánica de protección de datos personales para la empresa “NEGOCIOS Y TELEFONÍA (NEDETEL) S.A” sede Quito

## RESUMEN

El presente documento desarrolla una propuesta para la implementación de un sistema de gestión de seguridad de la información (SGSI) en NEDETEL S.A., sede en Quito, basado en la norma ISO 27001 y la ley orgánica de protección de datos personales. NEDETEL, una empresa especializada en servicios de conectividad, infraestructura y seguridad ha reconocido la necesidad de fortalecer sus políticas y procedimientos de seguridad ante un entorno de amenazas cibernéticas cada vez más complejo. A través de la evaluación de la situación actual de la empresa y el análisis de vulnerabilidades, se identificaron diversas áreas críticas que requieren mejoras significativas en términos de políticas de seguridad, gestión de riesgos, y capacitación del personal.

El documento enfatiza la importancia de actualizar y adaptar continuamente las estrategias de seguridad para proteger la información sensible y garantizar la integridad y disponibilidad de los datos.

Palabras Clave: Seguridad de la Información, SGSI (Sistema de Gestión de Seguridad de la Información), ISO 27001, Ley Orgánica de Protección de Datos Personales, Análisis de Vulnerabilidades, Gestión de Riesgos, Capacitación de Seguridad, Mejora Continua.

## **ABSTRACT**

This document proposes the implementation of an Information Security Management System (ISMS) at NEDETEL S.A., based in Quito, guided by ISO 27001 standards and the personal data protection law. NEDETEL, a company specializing in connectivity, infrastructure, and security services, has identified an urgent need to enhance its security policies and procedures in response to an increasingly complex cyber threat environment. By assessing the current security status and conducting vulnerability analyses, critical areas requiring significant improvements in security policies, risk management, and staff training were pinpointed.

The document highlights the necessity of continuously updating and adapting security strategies to protect sensitive information and ensure the integrity and availability of data.

**Key Words:** Information Security Management System (ISMS), ISO 27001, Personal Data Protection Law, Cybersecurity, Vulnerability Analysis, Risk Management, Security Training, Continuous Improvement.