Maestría en

CIBERSEGURIDAD

Trabajo de investigación previo a la obtención del título de

Magíster en Ciberseguridad

AUTOR:

León Jiménez Martín Darío

TUTORES:

Alejandro Cortés

Iván Reyes

TEMA:

Evaluación de vulnerabilidades mediante ejercicios prácticos de hacking ético y reporte a la Cooperativa de Ahorro y Crédito Luz del Valle

Quito, octubre 2024

RESUMEN

El proyecto analiza vulnerabilidades en la red interna de la Cooperativa de Ahorro y Crédito Luz del Valle, segmento 1 del sector financiero en Ecuador. Su objetivo es identificar debilidades en la infraestructura tecnológica, proponer medidas de mitigación y garantizar el cumplimiento de las normativas de la Superintendencia de Economía Popular y Solidaria (SEPS).

El estudio evalúa riesgos relacionados con gestión de software, permisos de acceso y controles deficientes, cuya falta de mitigación puede comprometer la confidencialidad, integridad y disponibilidad de los datos financieros. La metodología se basa en estándares internacionales de pruebas de penetración e incluye fases como reconocimiento, modelado de amenazas, análisis y explotación de vulnerabilidades, además de reportar hallazgos y recomendaciones.

Herramientas como Nessus, Metasploit y Shodan permiten detectar y explotar fallos en la red, bajo un enfoque ético. El trabajo se alinea con la Resolución SEPS-IGS-2022 y normas de gestión de riesgos, fortaleciendo la seguridad de los datos, la infraestructura tecnológica y fomentando una cultura de ciberseguridad en la organización.

Palabras clave: análisis de vulnerabilidades, hacking ético, pruebas de penetración, ciberseguridad, normativa SEPS, resiliencia tecnológica, gestión de riesgos.

ABSTRACT

This project analyzes vulnerabilities in the internal network of the Luz del Valle Credit Union, a segment 1 entity within Ecuador's financial sector. Its objective is to identify weaknesses in the technological infrastructure, propose mitigation measures, and ensure compliance with the regulations of the Superintendency of Popular and Solidarity Economy (SEPS).

The study evaluates risks related to software management, access permissions, and deficient controls, whose lack of mitigation could compromise the confidentiality, integrity, and availability of financial data. The methodology follows international penetration testing standards, including phases such as reconnaissance, threat modeling, vulnerability analysis, exploitation, and reporting of findings and recommendations.

Tools such as Nessus, Metasploit, and Shodan are used to detect and exploit network vulnerabilities ethically. This work aligns with SEPS-IGS-2022 Resolution and risk management standards, strengthening data security, technological infrastructure, and promoting a cybersecurity culture within the organization.

***Keywords*:** vulnerability analysis, ethical hacking, penetration testing, cybersecurity, SEPS regulations, technological resilience, risk management.