INSTITUTO CIENTÍFICO Y TECNOLÓGICO DEL EJÉRCITO

ESCUELA DE POSGRADO

GRAL DIV EDGARDO MERCADO JARRIN

TESIS:

El Nivel de Ciberseguridad y su Relación con el Éxito de una Operación de Ciberdefensa en el Activo Critico Nacional de SEDAPAL, 2024.

PARA OPTAR EL GRADO ACADÉMICO DE:

Doctor en Gestión y Desarrollo

PRESENTADO POR:

Maestro Guillermo Usbalter Manrique Carmen (código ORCID 0009-0005-6684-0832)

ASESOR:

Doctor Roberto Edwin Ramos Ballarta (código ORCID 0000-0002-4273-8965)

LÍNEA DE INVESTIGACIÓN:

Gestión de Operaciones y Logística

Lima, abril del 2026

Dedicatoria

A mi amada familia, mis antepasados, mis padres Dina y Belisario, por su amor, su educación, por su apoyo incondicional y abnegado.

A mi esposa Isabel y a mi hija Kytzia, mis hermanos Gladys, Cesar, María, Alex, a mis sobrinos, Max, Alexander y a mi familia siempre presentes en mi corazón.

A nuestro amado Dios, por seguir permitiendo llegar a cada uno de mis sueños.

Agradecimiento

A cada uno de los catedráticos, los docentes, instructores y profesionales del Instituto Científico Tecnológico del Ejército (ICTE), que me enseñaron con I+D+i asumir desafíos con éxito.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Actualmente la digitalización está presentes en todos los ámbitos de la actividad humana, incluidos los Activos Críticos Nacionales (ACN), las Tecnologías de información y comunicaciones (TICs) compuestas de hardware y software, experimentan un avance vertiginoso, que al no actualizarse en un ACN, crean nuevas brechas y amenazas cibernéticas, que son aprovechadas por personas o grupos de cibercriminales y/o ciberinteligencia de los estados. La Presidencia del Consejo de Ministros (PCM), e el marco de la activación para la protección del ACN en caso de un ataque cibernético indica en que en un primer momento, la ciberseguridad del ACN está a cargo del propio operador; en un segundo momento, a solicitud del ACN, cuando se presente un incidente que no pueda ser gestionado por el operador del ACN, la Dirección Nacional de Inteligencia (DINI) complementa la capacidad; y en un tercer momento, a su solicitud del ACN y la DINI sea sobrepasada; el Ministerio de defensa, a través del Comando Operacional de Ciberdefensa del Comando Conjunto de las Fuerzas Armadas (COCID-CCFFAA). En un cuarto momento, cuando sea sobrepasado el ACN, la DINI y el COCID-CCFFAA, se encargara la Secretaria de Gobierno y Transformación Digital o la que haga sus veces, a través del Centro Nacional de Seguridad Digital (PCM, 2024).

La presente investigación evaluó el nivel de ciberseguridad del ACN, y estableció un marco teoríco, para realizar una ciberseguridad holística en todos los ACN en el Perú, en Tecnologías de Informaciones (TI) y las Tecnologías Operativas (TO) como el Control de Supervisión y Adquisición de Datos (SCADA).

Esta investigación, establece una defensa integral, holística y resiliente de ciberseguridad de un ACN, para el éxito de una operación de Ciberdefensa. El estudio es bajo enfoque del tipo básica de nivel correlacional no experimental de corte transversal que tuvo 18 participantes. Los resultados fueron examinados a través de la estadística inferencial, utilizando los cuestionarios. Los resultados empleando el coeficiente de Rho Spearman 0,934 de correlación positiva muy alta, concluyendo que a mayor ciberseguridad de un ACN, el mayor es el éxito de la operación de Ciberdefensa.

Palabras Claves: Ciberseguridad, Activos Críticos Nacionales, Recursos Claves, Ciberataques, Operación de Ciberdefensa.

ABSTRACT

Digitalization is currently present in all areas of human activity, including Critical National Assets (CNAs). Information and communication technologies (ICTs), comprising hardware and software, are advancing rapidly. Failure to update these technologies in CNAs creates new vulnerabilities and cyber threats, which are exploited by individuals, cybercriminal groups, and state cyber intelligence agencies.

This research evaluated the cybersecurity level of a CNA and established a theoretical framework for implementing holistic cybersecurity across all CNAs in Peru, encompassing both Information Technology (IT) and Operational Technology (OT) systems, such as Supervisory Control and Data Acquisition (SCADA).

The study establishes a comprehensive, holistic, and resilient cybersecurity defense strategy for CNAs to ensure the success of cyber defense operations. The research employed a basic, correlational, non-experimental, cross-sectional design with 18 participants. The results were analyzed using inferential statistics based on questionnaire data. Spearman's rank correlation coefficient was 0.934, indicating a very high positive correlation. It is concluded that higher levels of cybersecurity in a CNA are associated with greater success in cyber defense operations.

Keywords: Cybersecurity, Critical National Assets, Key Resources, Cyberattacks, Cyber Defense Operation.