

**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 Crítico 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

CARATULA	
DEDICATORIA.....	ii
AGRADECIMIENTO.....	iii
ÍNDICE.....	iv
LISTA DE TABLAS.....	vi
LISTA DE FIGURAS.....	viii
RESUMEN.....	x
INTRODUCCIÓN.....	xii
CAPITULO I PLANTEAMIENTO DEL PROBLEMA.....	1
1.1 Descripción de la realidad problemática.....	1
1.2 Formulación del problema.....	7
1.2.1 Problema principal.....	7
1.2.2 Problemas específicos.....	7
1.3 Objetivos de la investigación.....	7
1.3.1 Objetivo principal.....	7
1.3.2 Objetivos específicos.....	8
1.4 Justificación e importancia de a investigación.....	8
1.4.1 Justificación teórica.....	8
1.4.2 Justificación práctica.....	8
1.4.3 Justificación metodológica.....	9
1.4.4 Importancia de la investigación.....	9
1.5 Delimitación de la investigación.....	10
1.5.1 Delimitación espacial.....	10
1.5.2 Delimitación temporal.....	11
1.5.3 Delimitación social.....	11
1.5.4 Delimitación conceptual.....	11
1.6 Limitaciones.....	11
CAPITULO II MARCO TEÓRICO	13
2.1 Antecedentes.....	13
2.1 Antecedentes internacionales.....	13
2.2 Antecedentes nacionales.....	19

2.2 Marco filosófico.....	25
2.3 Bases teóricas.....	27
2.4 Definición de términos básicos.....	36
2.5 Formulación de hipótesis.....	42
2.5.1 Hipótesis principal.....	42
2.5.2 Hipótesis específicas.....	42
2.6 Identificación y clasificación de las variables.....	43
2.7 Operacionalización de las variables.....	44
CAPITULO III METODOLOGÍA DE LA INVESTIGACIÓN.....	47
3.1 Tipo, diseño y nivel de la Investigación.....	47
3.2 Población y muestra.....	47
3.2.1 Población.....	47
3.2.2 Muestra.....	48
3.3 Técnicas e instrumentos de recolección de datos.....	45
3.4 Procesamiento de los datos.....	48
CAPITULO IV ANALISIS Y PRESENTACION DE RESULTADOS.....	50
4.1 Presentación, análisis e interpretación de resultados.....	50
4.2 Contrastación de hipótesis.....	80
4.3 Discusión de los resultados.....	85
CONCLUSIONES.....	88
RECOMENDACIONES.....	90
REFERENCIAS.....	91
ANEXOS.....	97
01 Matriz de consistencia.....	98
02 Aporte de investigación.....	101
03 Instrumento de recolección de datos.....	102
04 Declaración jurada de autenticidad y no plagio.....	104
05 Autorización para publicación de tesis en el repositorio del ICTE Reservado	105
06 Confiabilidad y validez de los instrumentos.....	106
07 Modelo Guía para evaluar la Ciberseguridad del Activo Crítico Nacional.....	115
08 Otros de Seguridad Nacional Acuerdo de Sigilo y Confidencialidad.....	138

LISTA DE TABLAS

Tabla 1	Evolución de la divulgación sobre la ciberseguridad en empresas.....	30
Tabla 2	Matriz de operacionalización de las variables.....	45
Tabla 3	Rango del Alfa de Cronbach.....	49
Tabla 4	Rasgos demográficos de los grados de instrucción y año de expertis..	50
Tabla 5	Prueba de Normalidad.....	51
Tabla 6	Distribución de frecuencias y los porcentajes de la variable Ciberseguridad y sus dimensiones.....	52
Tabla 7	Distribución de frecuencias y los porcentajes de la variable Ciberdefensa y sus dimensiones.....	52
Tabla 8	Distribución del nivel de la Ciberseguridad	53
Tabla 9	Distribución del nivel de la Ciberdefensa	54
Tabla 10	Frecuencias de media y mediana de la ciberseguridad.....	55
Tabla 11	Frecuencias de la autenticación del multifactor	56
Tabla 12	Frecuencias de la encriptación.....	57
Tabla 13	Frecuencias de las auditorias de seguridad	58
Tabla 14	Frecuencias de análisis de riesgo del nivel de ciberseguridad.....	59
Tabla 15	Frecuencias de los sistemas críticos tienen verificación de datos.....	60
Tabla 16	Frecuencias de los sistemas críticos tienen controles de cambio.....	61
Tabla 17	Frecuencias de los sistemas críticos tienen validación de datos.....	62
Tabla 18	Frecuencias de los sistemas críticos tienen copia de seguridad y recuperación	63
Tabla 19	Frecuencias de los sistemas críticos tienen redundancia para la gobernanza	64
Tabla 20	Frecuencias del plan de continuidad del negocio.....	65
Tabla 21	Frecuencias de un plan de recuperación de desastres.....	66
Tabla 22	Frecuencias de monitoreo y gobernanza de datos que se actualizan constantemente	67
Tabla 23	Frecuencias de la planeación de una operación de ciberdefensa....	68
Tabla 24	Frecuencias de la organización de una operación de ciberdefensa..	69
Tabla 25	Frecuencias de la dirección de una operación de ciberdefensa.....	70

Tabla 26 Frecuencias en el control de una organización de una operación de ciberdefensa	71
Tabla 27 Frecuencias en auditoria de una operación de ciberdefensa	72
Tabla 28 Frecuencias en la previsión de una operación de ciberdefensa	73
Tabla 29 Frecuencias del análisis forense de una operación de ciberdefensa	74
Tabla 30 Frecuencias en el ataque de una operación de ciberdefensa	75
Tabla 31 Frecuencias en los protocolos de una operación de ciberdefensa.....	76
Tabla 32 Frecuencias en la protección de una operación de ciberdefensa.....	77
Tabla 33 Frecuencias en la coordinación de una operación de ciberdefensa..	78
Tabla 34 Frecuencias del I+D+i de una operación de ciberdefensa.....	79
Tabla 35 Correlación Spearman entre la ciberseguridad y la ciberdefensa.....	80
Tabla 36 Interpretación del coeficiente de correlación de Spearman.....	81
Tabla 37 Correlación entre la confidencialidad y el planeamiento.....	82
Tabla 38 Correlación entre servicios avanzados de ciberseguridad y la respuesta.....	83
Tabla 39 Correlación entre gobernanza y los resultados.....	84

LISTA DE FIGURAS

Figura	1 Hackeado del Sistema SCADA de la planta de agua Tipton.....	xiii
Figura	2 Hackeado del Sistema SCADA de la planta de agua Hale Center Lockney, Muleschoe y Abernathy.....	2
Figura	3 Causas comunes de las infracciones empresariales año 2024.....	5
Figura	4 Desvelando las dimensiones de la investigación de ciberseguridad...	29
Figura	5 Tipos de operaciones de respuesta en ciberdefensa.....	35
Figura	6 Distribución de los niveles de ciberseguridad.....	53
Figura	7 Distribución de los niveles de ciberdefensa.....	54
Figura	8 Porcentaje de autenticación del multifactor.....	56
Figura	9 Frecuencia de la encriptación.....	57
Figura	10 Porcentaje de auditoria de seguridad.....	58
Figura	11 Porcentaje del análisis del riesgo.....	59
Figura	12 Porcentaje de los sistemas críticos tienen verificación de datos.....	60
Figura	13 Porcentaje de los sistemas críticos tienen controles de cambio	61
Figura	14 Porcentaje de los sistemas críticos hacen validación de datos	62
Figura	15 Porcentaje de los sistemas críticos tienen una copia de seguridad para la validación de datos.....	63
Figura	16 Porcentaje de los sistemas críticos tienen redundancia para gobernanza	64
Figura	17 Porcentaje de un plan de continuidad.....	65
Figura	18 Porcentaje de un plan de recuperación de desastre.....	66
Figura	19 Porcentaje del monitoreo y gobernanza de datos.....	67
Figura	20 Porcentaje de la planeación de una operación de ciberdefensa.....	68
Figura	21 Porcentaje de la organización de una operación de ciberdefensa.....	69
Figura	22 Porcentaje de la dirección de una operación de ciberdefensa.....	70
Figura	23 Porcentaje del control de una operación de ciberdefensa.....	71
Figura	24 Porcentaje de la auditoría de una operación de ciberdefensa.....	72
Figura	25 Porcentaje de la previsión de una operación de ciberdefensa.....	73
Figura	26 Porcentaje del análisis forense de una operación de ciberdefensa.....	74
Figura	27 Porcentaje de ataque de una operación de ciberdefensa	75
Figura	28 Porcentaje en los protocolos de una operación de ciberdefensa	76

Figura 29 Porcentaje en la protección de una operación de ciberdefensa.....	77
Figura 30 Porcentaje de la coordinación de una operación de ciberdefensa.....	78
Figura 31 Porcentaje de I+D+i de una operación de ciberdefensa.....	79
Figura 32 Correlación positiva perfecta entre la ciberseguridad y ciberdefensa...	85

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 teórico, 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.