

**ESCUELA MILITAR DE CHORRILLOS
“CORONEL FRANCISCO BOLOGNESI”**



**TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE LICENCIADO
EN CIENCIAS MILITARES CON MENCIÓN EN INGENIERÍA**

**Prevención de ataques cibernéticos y los procesos educativos en La
Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020**

PRESENTADO POR:

Huamani Caceres Renzo

Ubillus Del Castillo Axel

LIMA – PERÚ

2020

ASESORES Y MIEMBROS DEL JURADO

ASESOR

TEMÁTICO:

METODOLÓGICO:

PRESIDENTE DEL JURADO:

.....

MIEMBROS DEL JURADO:

.....

.....

.....

DEDICATORIA

Queremos dedicar este trabajo de investigación al creador por darnos la vida y acompañarnos en nuestro camino diario. A nuestros padres y hermanos a quienes amamos y han sido nuestro soporte y compañía durante todo este periodo de estudios. A nuestros instructores por habernos guiado en nuestra formación.

ÍNDICE DEL CONTENIDO

	Pág.
Título	
Asesores y miembros del jurado	ii
Dedicatoria	iii
Resumen	vi
Abstract	vii
Introducción	viii
CAPÍTULO I: PROBLEMA DE INVESTIGACIÓN	
1.1 Planteamiento del problema	15
1.1.1 Situación problemática	15
1.1.2 Justificación, trascendencia y relevancia de la investigación	16
1.1.3 Limitaciones y Viabilidad	17
1.2 Formulación del Problema	18
1.2.1 Problema General	18
1.2.2 Problemas Específicos	18
1.3 Objetivos de la investigación	18
1.3.1 Objetivo General	18
1.3.2 Objetivos Específicos	19
CAPÍTULO II: MARCO TEÓRICO	
2.1 Formulación de Hipótesis	20
2.1.1 Hipótesis General	20
2.1.2 Hipótesis Específicas	20
2.2 Sistema de Variables	21
2.2.1 Variables Generales	21
2.2.2 Variables Específicas intermedias o dimensiones	21
2.3 Conceptualización de Variables	21
2.3.1 Definición conceptual	21
2.3.2 Operacionalización de las variables	22
2.4 Antecedentes de la Investigación	23

2.4.1	Antecedentes internacionales	23
2.4.2	Antecedentes nacionales	25
2.5	Sustento teórico de las variables	28
2.5.1	Prevención de Ataques Cibernéticos	28
2.5.2	Procesos Educativos	41
2.5.3	Definición de términos básicos	57

CAPÍTULO III: MARCO METODOLÓGICO

3.1	Método y Enfoque de la Investigación	61
3.2	Tipo de Investigación	61
3.3	Nivel y Diseño de la Investigación	62
3.4	Técnicas e Instrumentos para la recolección de información	62
3.4.1	Elaboración de los instrumentos	62
3.4.2	Validez, confiabilidad y evaluación de instrumentos: juicio de Expertos	64
3.4.3	Aplicación de los instrumentos	66
3.5	Universo, Población y Muestra	66
3.6	Criterios de Selección de la muestra	67

CAPÍTULO IV: ANÁLISIS, INTERPRETACIÓN Y DISCUSIÓN DE LOS RESULTADOS

CONCLUSIONES	101	
RECOMENDACIONES	103	
PROPUESTA DE MEJORA	105	
BIBLIOGRAFIA	110	
ANEXOS	113	
Anexo 1	Matriz	114
Anexo 2	Encuesta	116
Anexo 3	Base de Datos	118
Anexo 4	Validación de Instrumento	125
Anexo 5	Constancia donde se efectuó la investigación	126
Anexo 6	Compromiso de autenticidad del instrumento	129
Anexo 7	Acta de sustentación de tesis	131

RESUMEN

La presente investigación titulada Prevención de Ataques Cibernéticos y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi 2020; considera dentro de su objetivo principal, determinar cuál es la relación que existe entre la Prevención de Ataques Cibernéticos y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi 2020”.

El método de estudio tiene un enfoque cuantitativo, con un diseño no experimental transversal, con una población objetiva de 98 cadetes 4to año de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi involucrados en el tema, de la investigación; con la aplicación de un cuestionario para determinar los objetivos de la investigación

Durante el desarrollo de la presente investigación se llegó a la conclusión general siguiente: Hemos podido concluir mediante las encuestas que dicha hipótesis es válida; ya que la Prevención de Ataques Cibernéticos que incluyen los tipos de ataque cibernético, las fases del ataque y los métodos de ataque; buscando proporcionar seguridad cibernética y potenciar los procesos educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi

Como parte final del estudio se exponen las recomendaciones de acuerdo a las conclusiones, las cuales son propuestas factibles para proteger el proceso educativo de los cadetes de 4to año de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi 2020

Palabras claves: *Prevención, ataques cibernéticos y procesos educativos.*

ABSTRACT

The present investigation titled Prevention of Cyber Attacks and the Educational Processes of the cadets of the 4th year of the Military School of Chorrillos “Coronel Francisco Bolognesi 2020; considers within its main objective, to determine what is the relationship that exists between the Prevention of Cyber Attacks and the Educational Processes of the cadets of the 4th year of the Military School of Chorrillos Coronel Francisco Bolognesi 2020

The study method has a quantitative approach, with a non-experimental cross-sectional design, with an objective population of 98 cadets 4th year of the Military School of Chorrillos Coronel Francisco Bolognesi involved in the research topic; with the application of a questionnaire to determine the objectives of the investigation

During the development of this research, the following general conclusion was reached: We have been able to conclude through the surveys that this hypothesis is valid; since the Prevention of Cyber Attacks which include the types of cyber attack, the phases of the attack and the attack methods; seeking to provide cyber security and enhance the educational processes of the 4th year cadets of Communications of the Military School of Chorrillos Coronel Francisco Bolognesi

As a final part of the study, the recommendations are presented according to the conclusions, which are feasible proposals to protect the educational process of the 4th year cadets of the Chorrillos Military School Coronel Francisco Bolognesi 2020

Keywords: Prevention, cyber attacks and educational processes.

INTRODUCCIÓN

El presente trabajo de investigación se ha estructurado en cuatro capítulos que desarrollados metodológicamente nos lleva hacia conclusiones y sugerencias importantes, tal es así que en el Capítulo I denominado Problema de Investigación se desarrolló el Planteamiento y Formulación del Problema, Justificación, Limitaciones, Antecedentes y Objetivos de la investigación

En lo concerniente al Capítulo II, titulado Marco Teórico, se recopiló valiosa información para sustentar la investigación respecto de las variables competitividad y calidad educativa, así como otros temas relacionados con las dimensiones planteadas en la matriz de consistencia

El Capítulo III comprende el Marco Metodológico, se estableció que el diseño de la presente investigación será descriptivo – correlacional, con diseño no experimental. Además, se determinó el tamaño de la muestra, las técnicas de recolección y análisis de datos así mismo se realizó la operacionalización de las variables

En lo concerniente al Capítulo IV Resultados, se interpretó los resultados estadísticos de cada uno de los ítems considerados en los instrumentos, adjuntándose los cuadros y gráficos correspondientes, Conclusiones y Sugerencias

CAPITULO I

PROBLEMA DE INVESTIGACION

1.1 Planeamiento del Problema

1.1.1 Situación Problemática

“Debemos empezar recordando que la seguridad cibernética implica proteger la infraestructura destinada a las plataformas cibernéticas previniendo, detectando y respondiendo a los incidentes en la red. A diferencia de las amenazas físicas que producen una acción inmediata como detenerse, agacharse y girar en caso de incendio, las amenazas cibernéticas son a menudo difíciles de identificar y de entender. Entre estos peligros se encuentran los virus que eliminan sistemas enteros, intrusos que entran a los sistemas y alteran archivos, quienes usan su computadora o dispositivo para atacar a otros o intrusos que roban información confidencial. La gama de riesgos cibernéticos es ilimitada: las amenazas, algunas más serias y elaboradas que otras, pueden tener un gran efecto en el individuo, la comunidad, las organizaciones y el país”.

“La principal amenaza que afecta a las plataformas cibernéticas de una institución estatal o privada, militar o civil es el desconocimiento del concepto de esta, la confidencialidad, la integridad y los niveles de disponibilidad de la información que se deben manejar no son los adecuados. Dejando así a la institución afectada con serios inconvenientes como el retraso de su continuidad operacional diaria la cual tiene como consecuencia una significativa pérdida de ingresos monetarios y contratiempos no pronosticados en la producción esperada”.

“Hoy en día existen muchos factores que amenazan la seguridad de información de las instituciones estatales o privadas, militares o civiles dentro de las cuales está incluida la Escuela Militar de Chorrillos Coronel Francisco Bolognesi y por lo general el presupuesto destinado para la proteger y resguardar la plataforma cibernética no es el suficiente; tener identificadas y controladas las vulnerabilidades de la información interna en la red se logra con un correcto plan de seguridad generado gracias a un análisis de riesgo previo”.

“Con las ansias de lograr como objetivo el minimizar los riesgos a la plataforma cibernética de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi y conocer la importancia de salvaguardar la información virtual en sus redes privadas, es que se presenta esta investigación”.

1.1.2 Justificación, Trascendencia y Relevancia de la Investigación

Con esta investigación ayudaremos a fomentar una cultura de prevención y detección de riesgos cibernéticos en los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, se dará a conocer sobre el peligro que representa no estar preparado para los diferentes ataques cibernéticos que existen actualmente y se brindará información de cómo elaborar los planes de acción y estrategias basadas en minimizar los riesgos.

Esta investigación es importante porque los estudios realizados por especialistas en ciberseguridad señalan que los ataques cibernéticos han evolucionado, los hackers están desarrollando softwares maliciosos cada vez más sofisticados con el fin de buscar vulnerabilidades en los sistemas interconectados para sustraer información digital con el fin de lograr su objetivo.

Para ello con el conocimiento adecuado de los aspectos formales y legales acerca de la importancia de la seguridad cibernética para minimizar los riesgos, la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” tendrá el enfoque necesario para establecer una nueva política de seguridad y por ende nuevas directivas que garanticen la seguridad cibernética; garantizando a la vez, la confidencialidad de la información que es compartida por parte de los cadetes de todos y cada uno de los años académicos dentro de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

1.1.3 Limitaciones y Viabilidad

Limitaciones

El presente trabajo de investigación presenta enfocadas en la mayor demanda de tiempo y dedicación.

- Se considera como limitación económica el hecho de que los investigadores en su condición de cadetes reciben propina, por lo que son apoyados económicamente con los aportes de sus padres y otros familiares para solventar los gastos que implica el desarrollo del presente trabajo de investigación.
- No se dispone con todo el tiempo necesario, debido a la apretada progresión de actividades académicas y administrativas que se cumplen, además se dispuso de los fines de semana y feriados para la búsqueda de información.

Viabilidad

Es viable la presente investigación porque se dispone de:

- “Los recursos humanos y materiales suficientes para realizar el estudio en el tiempo disponible previsto”.
- “Es factible lograr la participación de los sujetos u objetos necesarios para la investigación. La metodología por seguir conduce a dar respuesta al problema”.
- “Además de los aspectos mencionados la presente investigación es viable por se dispone de asesor, se dispone con el personal que desarrolla el método”.

1.2 Formulación del Problema

1.2.1 Problema General

¿Cuál es la relación que existe entre la Prevención de Ataques Cibernéticos y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

1.2.2 Problemas Específicos

- ¿Cuál es la relación que existe entre los Tipos de Ataques Cibernéticos según el Objetivo y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?
- ¿Cuál es la relación que existe entre las Fases del Ataque y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?
- ¿Cuál es la relación que existe entre las Medidas de Prevención y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

1.3 Objetivos de la Investigación

1.3.1 Objetivo General

Determinar cuál es la relación que existe entre la Prevención de Ataques Cibernéticos y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

1.3.2 Objetivos Específicos

- Establecer cuál es la relación que existe entre los Tipos de Ataques Cibernéticos según el Objetivo y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

- Establecer cuál es la relación que existe entre las Fases del Ataque y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.
- Establecer cuál es la relación que existe entre las Medidas de Prevención y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

CAPÍTULO II

MARCO TEÓRICO

2.1 Formulación de Hipótesis

2.1.1 Hipótesis General

La Prevención de Ataques Cibernéticos se relaciona significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

2.1.2 Hipótesis Específicas

Hipótesis Específica 1

Los Tipos de Ataques Cibernéticos según el Objetivo se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

Hipótesis Específica 2

Las Fases del Ataque se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

Hipótesis Específica 3

Las Medidas de Prevención se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

2.2 Sistema de Variables

2.2.1 Variables Generales

Variable (1): Prevención de Ataques Cibernéticos

Variable (2): Procesos Educativos

2.2.2 Variables Específicas intermedias o dimensiones

Prevención de Ataques Cibernéticos

- Tipos de Ataques Cibernéticos según el Objetivo
- Fases del Ataque
- Las Medidas de Prevención

Procesos Educativos

- Ciencias y Humanidades
- Ciencias Militares

2.3 Conceptualización de Variables

2.3.1 Definición conceptual

Variable (1): Prevención de Ataques Cibernéticos

Según Aguilera (2011), “se puede definir prevención de ataque cibernéticos a la disciplina encargada de evitar que se aprovechen de alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización”.

Variable (2): Procesos Educativos

“El proceso educativo se basa en la transmisión de conocimientos y valores. Si esquematizamos el proceso de la manera más simple, encontraremos a una persona (que puede ser un docente, una autoridad, un padre de familia,

etc.) que se encarga de transmitir dichos conocimientos a otra u otras. Hay, por lo tanto, un sujeto que enseña y otros que aprenden”. (Rivas, F., 1997)

2.3.2 Operacionalización de las variables

Tabla 1

Operacionalización de la Variable 1: Prevención de Ataques Cibernéticos

Dimensión	Indicadores	Ítems
X ₁ Tipos de Ataques Cibernéticos según el Objetivo	• Interrupción	1
	• Interceptación	2
	• Modificación	3
	• Generación	4
X ₂ Fases del Ataque	• Reconocimiento	5
	• Exploración	6
	• Obtener Acceso	7
	• Mantener el acceso	8
X ₃ Medidas de Prevención	• Borrar huellas	9
	• Modelo para prevenir ciberataques	10
	• Implementación de un portal cautivo para la gestión de acceso a la red	11
	• Monitoreo de la red a través de software de gestión	12
	• Políticas de seguridad en el servidor para la navegación	13
	• Métodos de encriptación y protección de la información	14

Tabla 2

Operacionalización de la Variable 2: Procesos Educativos

Dimensión	Indicadores	Ítems
-----------	-------------	-------

Y ₁	• Política Nacional de Seguridad	16
Ciencias y	• Convenio de Ginebra	17
Humanidades	• Tratados Internacionales	18
Y ₂	• Doctrina Militar de Comunicaciones	19
Ciencias Militares	• Planeamiento de Operaciones	20
	• Aplicación de la Guerra Ciberdefensa	21

2.4 Antecedentes de la Investigación

2.4.1 Antecedentes internacionales

Lara, E. (2019). Trabajo de titulación, previo a la obtención del título de Magister en Tecnologías de la Información, mención en Seguridad de Redes y Comunicación, titulada: *“Diseño de un modelo de Seguridad de la Información, basado en OSSTMMv3, NIST SP 800-30 E ISO 27001, para Centros de Educación: caso de estudio Universidad Regional Autónoma de los Andes, extensión Tulcán”*. Universidad Internacional SEK. Quito. Ecuador

La autora llegó a las siguientes conclusiones:

1. El modelo de seguridad propuesto, pone en evidencia serios factores de riesgo para la seguridad de la información y de la gestión de servicios en la Universidad, haciéndose necesario implementar los correctivos necesarios.
2. Se han determinado los procesos críticos de la gestión de información en la Universidad Regional Autónoma de los Andes, extensión Tulcán. El hallazgo más significativo está relacionado con la falta de políticas de seguridad y documentación de procesos internos.

3. Las políticas que se utilizaron en el modelo de seguridad están comprometidas con la privacidad y protección de los datos de los usuarios ante acciones ilegales o perjudiciales.
4. Para identificar las vulnerabilidades internas de la institución se aplicaron procesos técnicos como el mapeo de la red, revisión de puertos que están abiertos, acceso a la red wifi sin claves, no existen VPN's, no hay documentación de la red empresarial; adicionalmente se aplicaron encuestas a los usuarios de la red.
5. Es importante la utilización del presente modelo de seguridad con el fin de puntualizar el uso adecuado de los activos de la institución, en los que se debe incluir parámetros de seguridad acorde a las necesidades del establecimiento. Adicionalmente, estas deben ser difundidas con el fin de lograr una mayor eficiencia en la mitigación de riesgos dentro de la infraestructura de la red de información.
6. El aspecto más importante, y que afecta a cualquier modelo de seguridad, es que la Universidad no tiene interiorizado una cultura de seguridad de la información. El desarrollo de este tipo de cultura, es un proceso que se desarrollará de manera continua, aplicando rígidamente las políticas de seguridad propuestas.
7. Los incidentes de seguridad se pueden presentar, ya sea por desconocimiento o negligencia de los usuarios de la red, de manera accidental o incluso de forma deliberada (mediante un ataque cibernético), por lo que, el uso del modelo basado en OSSTMMv3, NIST 800-30 e ISO 27001 considera la aplicación de distintas perspectivas para aumentar y mejorar la seguridad de la información, a través de la utilización de estándares y mejores prácticas de los modelos utilizados.
8. La utilización de los modelos de seguridad OSSTMMv3 y NIST 800-30 son aconsejables por ser más flexibles y se pueden acoplar a las

necesidades de una institución, lo que no sucede con el estándar ISO 27001 que es más estricto debiendo llegar a la certificación de la misma, por ello se aconseja que esto se realice desde la matriz y no solo desde una extensión de la 85 universidad.

Comentario: El presente trabajo de investigación tiene como objetivo el determinar las mejores políticas de seguridad que serán utilizadas de acuerdo a la necesidad de la institución, tomando en cuenta que no todas tienen las mismas necesidades para el envío de la información dentro de su red de datos; lo cual nos sirve de referencia y antecedente ante las nuevas amenazas que debemos afrontar y las que deben generar las medidas de protección de información ante ataques cibernéticos al sistema educativo de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”

Cruz, E. y Rodríguez, D. (2010). En su tesis para obtener el título de Ingeniero en Informática, titulada: “*Modelo de Seguridad para la Medición de Vulnerabilidades y Reducción de Riesgos en Redes de Datos*”. Instituto Politécnico Nacional. Distrito Federal. México

Los autores llegaron a las siguientes conclusiones:

1. La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.
2. Estos riesgos que se enfrentan han llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas tecnologías y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar

serios problemas a los bienes, servicios y operaciones de la empresa. Pero no se encuentra documento alguno en el que se explique el qué preguntar o el qué analizar al desarrollar un análisis.

3. Para poder crear una metodología no solo se deben agregar cosas, sino que es necesario entregar un sentido lógico al procedimiento, para ello se debe conocer en primer lugar la existencia de metodologías o formas relacionadas con lo que se quiere hacer, también se deben conocer más a fondo los fundamentos de la seguridad y entenderlos. La seguridad en la información no es posible sin la cooperación del usuario.
4. Se puede tener la mejor tecnología para protegerlos y, aun así, sufrir una ruptura de seguridad. Se pudo apreciar que con el hecho de utilizar un conjunto de preguntas y procedimientos se logra concretar una excelente imagen de las vulnerabilidades a las que es susceptible la red.
5. Al desarrollar las herramientas del análisis se logró evidenciar que se cuenta con varias herramientas, como, por ejemplo, la utilización de ingeniería social, esta es una técnica bastante buena ya que no es tan rígida como llenar un cuestionario de preguntas, aquí las personas responden con mucha más franqueza y se sienten cómodas conversando y expresándose, esto se pudo comprobar con los usuarios entrevistados. Debido a las cambiantes condiciones y nuevas plataformas de computación disponibles, es vital el desarrollo de documentos y directrices que orienten a los usuarios en el uso adecuado de las tecnologías para aprovechar mejor sus ventajas.
6. En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva.

7. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.
8. Finalmente debe quedar claro que la Seguridad Informática es un aspecto muchas veces descuidado en nuestros sistemas, pero de vital importancia para el correcto funcionamiento de todos ellos. Seguridad es un proceso NO un producto. Elaborar este proyecto proporcionó mucha experiencia en el ámbito profesional, ya que en el mundo laboral es apreciado el profesional que posee conocimientos en el área de seguridad informática, puesto que las organizaciones se están dando cuenta cada vez más de la importancia de contar con un sistema con bajas vulnerabilidades, y los costos que esto implica.
9. En el ámbito personal las ganancias son invaluable, el trabajo en equipo, las relaciones con las personas, el desarrollo de la personalidad, al enfrentar gente que no conocemos.

Comentario: Siendo el objetivo principal del presente trabajo de investigación es crear un modelo de seguridad para medir las vulnerabilidades y reducir los riesgos de las redes de datos en las organizaciones, para facilitar al administrador de red conocer dichas vulnerabilidades y riesgos en donde a su vez pueda minimizarlos para la protección de la información así como también que se obtengan los datos necesarios para promover la planeación, el diseño y la implantación de dicho modelo de seguridad en la misma organización con el fin de establecer una cultura de seguridad en la institución; lo cual nos sirve de referencia para afrontar las amenazas cibernéticas y generar las medidas de protección de información ante ataques cibernéticos al sistema educativo de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

Arias, N. & Celis, J. (2015). En su trabajo de grado presentado como requisito para obtener el Título Profesional de Ingenieros de Sistemas, titulado: “*Modelo Experimental de Ciberseguridad y Ciberdefensa para Colombia*”. Universidad Libre. Bogotá. Colombia

Los autores llegaron a las siguientes conclusiones:

1. El programa de ingeniería de sistemas de la universidad libre gracias a la dirección de la línea de formación electiva en seguridad informática, proyecta su función como constructor de soluciones esquematizando descriptivamente un modelo de ínter nacional para Ciberseguridad y defensa
2. El MCCPC, establece los valoradores de acción logística, como resultado de la interpretación analítica de los ejes de referenciación organizacional para controlar y formular procedimientos para la Ciberseguridad y para la Ciberdefensa, fundamentados en la significancia de la administración moderna (P=planeación, O=organización, D=dirección, E=ejecución, R=revisión o control), significando que para implementar el modelo convencionalmente, el programa debe acercarse como consultor al MINTIC y MINDEFENSA
3. La Ciberseguridad y Ciberdefensa definen y categorizan tanto las acciones, servicios y mecanismos de seguridad que requiere Colombia para blindar su ciberespacio minimizando el riesgo destructivo de los piratas de la información.

Comentario: El presente trabajo de investigación pretende construir el modelo de referenciación que garantice al estado colombiano parametrizar las condiciones de protección en el ciberespacio como respuesta a los ataques producidos por guerra de la información; lo cual nos sirve de referencia para afrontar las amenazas cibernéticas y generar las medidas de protección de información ante ataques cibernéticos al sistema educativo de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

2.4.2. Antecedentes nacionales

Guillinta, O. y Merino, J. (2016). En su Proyecto Profesional para la obtención del Título Profesional de Ingeniero de Sistemas de Información, titulado: *“Modelo de Prevención y Defensa contra Ataques Cibernéticos basado en estándares de Seguridad Internacionales para It-Expert”*. Universidad Privada del Centro. Lima. Perú

Los autores llegaron a las siguientes conclusiones:

1. La empresa IT-Expert adoptó el modelo de seguridad propuesto en sus operaciones de TI, al considerar el análisis de vulnerabilidades en cada uno de sus despliegues, el monitoreo continuo de los niveles de riesgo, y la remediación de vulnerabilidades en cada uno de sus activos de TI
2. Los resultados de la implementación del modelo muestran una mejora notable con respecto a la protección contra ataques informáticos, remediación de vulnerabilidades críticas, y al establecimiento de niveles de riesgo óptimos en IT-Expert.
3. El análisis final de riesgos en la empresa IT-Expert revela que presenta 7 riesgos, destacando que ninguno se encuentra categorizado como “Alto” debido a los controles de TI implementados.
4. La administración del ciclo de vida de vulnerabilidades permitió remediar una cantidad significativa de vulnerabilidades de TI durante el ciclo 2015-2, categorizadas de forma principal como “Medias” y “Bajas”.
5. El equipo de TI de la empresa IT-Expert demostró un interés importante en el modelo propuesto, lo cual se evidenció en los notables resultados obtenidos en las evaluaciones aplicadas durante la etapa de capacitación.

Comentario: En el presente trabajo de investigación se hace referencia al Hacking Ético, que es un servicio que agrega valor a la seguridad corporativa, puesto que se basa en la aplicación de técnicas que utiliza un hacker para proteger la infraestructura de TI de una organización. Es por ello que el objetivo principal de este proyecto fue implementar un modelo de prevención y defensa que permita administrar riesgos tecnológicos, y disminuir la ventana de exposición ante nuevas vulnerabilidades de TI que son utilizadas por los delincuentes informáticos. Lo cual nos sirve como base teórica para implementar las medidas de prevención ante ataques cibernéticos al sistema educativo de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

Zúñiga, J. (2017). En su tesis para optar el grado académico de magister en Ingeniería de Sistema de Armas, titulada: “*Ciberdefensa y su incidencia en la Protección de la información del Ejército del Perú. caso: COPERE 2013 – 2014*”. Instituto Científico y Tecnológico del Ejército. Lima. Perú

El autor llego a las siguientes conclusiones:

1. Está probado que existen Deficiencias en los programas de capacitación relacionados a ciberdefensa para la protección de la Información del Ejército del Perú, porque no se cuenta con personal Militar o Civil que administra las infraestructuras de TI, que cuenten con un adecuado nivel de capacitación en temas relacionados a la ciberdefensa; o que este personal no posea el nivel de conocimiento adecuado de la Norma Técnica Peruana NTP/ISO/IEC 17799, para poner en práctica su aplicación y así de esta manera mejorar la protección de la Información del Ejército del Perú.
2. Está probado que existen Carencias de Recursos Disponibles relacionados a ciberdefensa para la protección de la Información del Ejército del Perú, porque no se cuenta con un adecuado nivel de asignación presupuestal destinado a ciberdefensa; o porque no se posea

un adecuado nivel de Funcionalidad de las infraestructuras estratégicas, que permitan mejorar la protección de la Información del Ejército del Perú.

3. Está probado que existen Desconocimiento o aplicación incorrecta de los procedimientos de seguridad informática relacionados a ciberdefensa para la protección de la Información del Ejército del Perú, porque no se cuenta con un adecuado nivel de conocimiento de los conceptos básicos relacionados con ciberdefensa; o porque no se posea un adecuado nivel de conocimiento de los principios básicos relacionados a ciberdefensa, que permitan mejorar la protección de la Información del Ejército del Perú.

4. Está probado que existen Incumplimientos Normativos relacionados a ciberdefensa para la protección de la Información del Ejército del Perú, debido a que no se da un adecuado grado de cumplimiento del plan de Desarrollo de la Sociedad de la Información en el Perú. La Agenda Digital 2.0; o porque no se da un adecuado grado de cumplimiento del plan de desarrollo Institucional “Bolognesi”; o porque no se da un adecuado grado de cumplimiento de la Directiva única para el funcionamiento del sistema de telemática y estadística del Ejército (DUF SITELE); o porque no se da un adecuado grado de cumplimiento de la Directiva N° 001/CGE/DITELE/SD SIDE (Lineamientos de seguridad de la información para la Ciberdefensa en el Ejército del Perú), que permitan mejorar la protección de la Información del Ejército del Perú

Comentario: El presente trabajo de investigación tuvo como objetivo principal, determinar las dificultades que impiden el mejoramiento de la Ciberdefensa que inciden en la protección de la información del Ejército del Perú. Caso: COPERE 2013 - 2014 con el propósito de identificar las causas que la generan y tener base para proponer el uso de nuevos conocimientos, que contribuyan a mejorar la protección de la información; lo cual nos sirve como base teórica para generar, establecer y/o implementar las medidas de

protección de información ante ataques cibernéticos al sistema educativo de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

Sánchez, J. (2017). En su tesis para optar el grado académico de magister en Ingeniería de Sistema de Armas, titulada: “*Adopción de Estrategias de Ciberseguridad en la Protección de la información en la Oficina De Economía del Ejército, San Borja- 2017*”. Instituto Científico y Tecnológico del Ejército. Lima. Perú

El autor llego a las siguientes conclusiones:

1. La Oficina de Economía del Ejército no cuenta con programas para concientizar al personal contra el cibercrimen.
2. La Oficina de Economía del Ejército no adopta medidas legales contra su personal que, manejando el sistema e información reservada, y que cometa negligencias que contribuyan directa o indirectamente con cibercriminales.
3. En las instalaciones de la Oficina de Economía del Ejército no se ha instalado un sistema de video cámaras para detectar intrusos con actitudes sospechosas para proteger la información contra el ciberespionaje.
4. En las salas de cómputo Oficina de Economía del Ejército no existen sistemas de control biométrico para proteger la información reservada contra el ciberespionaje.
5. En la Oficina de Economía del Ejército no existen planes de protección contra ciberterroristas y se ponen en ejecución.
6. La Oficina de seguridad Oficina de Economía del Ejército, no ejerce control con su personal en cuanto al manejo de los CPU, USB, discos

duros, etc. que puedan originar el robo de información; asimismo, no se efectúa un control estricto en el manejo de la información, tanto física como virtual, a fin de evitar el robo de información por descuido del personal que labora en dicha dependencia.

7. Los softwares que dispone la Oficina de Economía del Ejército no son de última generación, lo cual no garantiza la protección efectiva contra la alteración de la información.

Comentario: La presente investigación tiene en consideración que en el mundo actual ha surgido una nueva dimensión donde pueden materializarse las amenazas: el ciberespacio. Si antes en el ámbito de la defensa estaba claro que los escenarios estaban circunscritos en las tres dimensiones de tierra, mar y aire; ahora se cuenta con una dimensión adicional, y más intangible que las anteriores: el espectro electromagnético; lo cual se asemeja a las nuevas amenazas que debemos afrontar y las que deben generar las medidas de protección de información ante ataques cibernéticos al sistema educativo de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”

2.5 Sustento teórico de las variables

2.5.1 Prevención de Ataques Cibernéticos

a. Tipos de Ataques Cibernéticos según el Objetivo

“Se plantea el escenario de una comunicación entre dos o más equipos. Un ataque a un sistema concebido de esta forma se lleva a cabo generalmente por alguno de los siguientes métodos”:

1) Interrupción

Consiste en que un recurso del sistema es destruido o se vuelve no disponible. Es un ataque contra la disponibilidad de los recursos de sistema. Ejemplos de este tipo de ataque son: la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

2) Intercepción

En este caso, un usuario no autorizado consigue acceder a un recurso incluso antes del verdadero destinatario. Es un ataque contra la confidencialidad. Cuando hablamos de usuario entendemos que podría ser una Entidad, Organización, persona física, un programa o un ordenador. Ejemplos de este tipo de ataque son: Hacer click una línea para hacerse con datos que circulen por la red; hacer copia ilícita de ficheros o programas (intercepción de datos), o bien leer las cabeceras de paquetes, para desvelar la identidad de uno o más usuarios implicados en la comunicación ilegalmente intervenida (intercepción de identidad).

3) Modificación

“El intruso, que así llamaremos a la entidad no autorizada, no solo consigue el acceso a un recurso, sino que es capaz de manipularlo. Este es el caso de un ataque contra la integridad. Ejemplos de este ataque podrían ser: el cambio de valores en un archivo de datos, alteración de un programa para modificar su funcionamiento y corromper el contenido de mensajes que están siendo transferidos por la Red”.

4) Generación

Un usuario no autorizado introduce objetos, elementos, parámetros falsificados en el sistema, originando un ataque contra la autenticidad de los recursos. Ejemplos de este tipo de ataque son: insertar mensajes corruptos en una red, o añadir registros a un archivo.

b. Fases del Ataque

“Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque”.

1) Fase 1. Reconnaissance (Reconocimiento).

Esta etapa involucra la obtención de información (Information Gathering) con respecto a una potencial víctima que puede ser una persona u organización. Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el Dumpster Diving, el sniffing.

2) Fase 2. Scanning (Exploración)

En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros. Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el

networkmappers, portmappers, networkscanners, portscanners, y vulnerabilityscanners.

3) Fase 3. Gaining Access (Obtener acceso)

En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema (Flaw exploitation) descubiertos durante las fases de reconocimiento y exploración. Algunas de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow, de Denial of Service (DoS), Distributed Denial of Service (DDoS), Passwordfiltering y Session hijacking.

4) Fase 4. Maintaining Access (Mantener el acceso)

Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos.

5) Fase 5. CoveringTracks (Borrar huellas)

Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS).

c. Medidas de prevención

1) Modelo para prevenir ciberataques

En base a las amenazas existentes y las vulnerabilidades que tiene una empresa proponemos un modelo empresarial para prevenir ciberataques:

- a. Proteger la red con un Firewall. Es importante que la organización cuente con un firewall para monitorear el tráfico entrante y saliente de la red, creando reglas que permitan bloquear o autorizar el tráfico específico. (Erique, E., 2018)
- b. Proteger los Ordenadores. Se debe tomar en cuenta que, para prevenir un ataque, todas las computadoras o servidores cuenten con un antivirus actualizado. En caso de un ataque es recomendable la creación de copias de seguridad, además de contar con un protocolo de recuperación de datos. (Erique, E., 2018)
- c. Segmentar la Red. Es importante aislar todo el tráfico de la organización por segmentos para proteger de forma dinámica la infraestructura y los servicios de red. (Erique, E., 2018)
- d. Mantener al mínimo los privilegios de los usuarios. Se debe crear privilegios y controles en la navegación y descarga de archivos, la segmentación de red nos ayudara en esto creando VLAN para invitados, VLAN para usuarios y VLAN para súper usuarios estas se pueden autenticar en la red a través de la MAC. (Erique, E., 2018)
- e. Usar Protocolos de Seguridad. Para toda transferencia de archivos a un servidor se deben usar protocolos de seguridad (SFTP, FTPS, NFS). Además, es recomendable revisar las políticas de seguridad de los productos y monitorear frecuentemente las alertas y logs de incidencias. (Erique, E., 2018)

- f. Autenticidad de Enlaces. Se deben comprobar siempre los enlaces para no ser víctima del phishing, educando al personal para que filtren adecuadamente los correos electrónicos, tratando con precaución cualquier mensaje sospechoso, sin abrir enlaces que provengan de fuentes no confiables. (Erique, E., 2018)
- g. Realizar auditorías rutinarias y test de penetración. Es recomendable cada cierto tiempo realizar auditorías a la seguridad de la red y un test de penetración con la intención de encontrar debilidades de seguridad verificando si el sistema es vulnerable a los ataques. (Erique, E., 2018)
- h. Elegir prevención antes que detención. Con el fin de detectar y mitigar los daños causados a la brevedad, invirtiendo en tecnología y productos que pongan la prevención antes que la detección. (Erique, E., 2018)
- i. Cubrir todos los vectores de ataque. Los hackers usan todo tipo de truco para introducirse a la red de correo, búsquedas por la web, aplicaciones. Se debe encontrar una solución que puede cubrir todos los elementos y que ofrezca una protección en toda la superficie de ataque. (Erique, E., 2018)
- j. Crear una arquitectura de seguridad unificada. En muchas organizaciones se puede verificar que la arquitectura de seguridad está hecha con una variedad de productos de muchos proveedores, muchas ocasiones entre tecnologías que no colaboran entre sí, dando lugar a agujeros en la seguridad. (Erique, E., 2018)

En conclusión, el modelo descrito puede ayudar a evitar un ciberataque, pero se debe tomar en cuenta que no existe la bala de plata tecnológica que pueda 46 proteger a una organización ante

todas las amenazas de cualquier tipo. Hoy en día se cuenta con tecnologías excelentes que pueden ser muy efectivas frente a los ataques, pero no es la solución definitiva. (Erique, E., 2018)

Hay que estar preparados para cualquier tipo de ataque desde el más reciente hasta el que recién se acaba de inventar. El modelo propuesto permitirá a una organización tener una primera línea de respuesta para prevenir, detectar y bloquear estos ataques. (Erique, E., 2018)

2) Implementación de un portal cautivo para la gestión de acceso a la red

Una buena práctica de seguridad en la organización es la implementación de un portal cautivo en donde los usuarios que se conecten a una red inalámbrica se autenticuen en el portal para que puedan ejecutar políticas en la navegación, como, por ejemplo, controlar el ancho de banda, limitar el tiempo de conexión, permitir solo la conexión a ciertas páginas electrónicas, entre otras. (Erique, E., 2018)

En el aspecto comercial se puede usar el portal cautivo para llevar a cabo un marketing, ya que facilita la captación del cliente, haciendo que los usuarios llenen encuestas, visualicen publicidad patrocinada o presenten cualquier promoción activa en ese momento. (Erique, E., 2018)

Un portal cautivo se puede implementar a través de software con Linux, Windows, o por hardware, esto es, usar el portal nativo que viene instalado por defecto en los equipos sean estos Cisco, Ruckus, Fortinet, entre otros. (Erique, E., 2018)



Fig. 1. Diagrama esquemático de conexión del Portal Cautivo

Para el montaje del portal cautivo en una red Wifi pequeña lo mínimo que se necesita es:

- Un servidor (Ordenador) con 2 tarjetas de red donde se instalará el Portal Cautivo.
- Un ruteador (Punto de Acceso Wi-Fi)
- Acceso a Internet

Mediante la configuración de un portal cautivo se puede obtener un mejor control sobre el uso de la red, lo cual es de vital importancia, ya que puede mejorar la calidad de los servicios, asignar ancho de banda, restringir paginar, etc. En la figura 2 se muestran los principales software para la implementación de Portal Cautivo, unos propietarios y otros libres, dependiendo de las necesidades de la organización, si es conveniente comprar una licencia para portal cautivo o simplemente usar los software libre que hay hoy en día, como WifiDog, Easy Hotspot pfSense, etc. (Erique, E., 2018)



Fig. 2. Herramientas de Portal Cautivo

3) Monitoreo de la red a través de software de gestión

Para un nivel más avanzado de control de seguridad es recomendable el monitoreo de la red con software de gestión. Tener la red siempre monitoreada tiene sus ventajas, tales como:

- Minimiza el tiempo de caída de la red.
- Detectar fallas antes que ocurran.
- Con la ayuda de alertas se pueda brindar soluciones al momento que ocurra una caída del sistema.
- Elaborar un registro donde se pueda saber tiempo de conexión y desconexión de los dispositivos.
- Llevar un registro de las páginas más visitadas el tiempo y el ancho de banda que se consume. (Erique, E., 2018)

La gestión de redes no es solamente rastrear una dirección IP, asegurar que siempre haya conexión a la red o que el ancho de banda sea suficiente para transferencia de información. Se puede incluir el monitoreo del funcionamiento de ruteadores y conmutadores, incluso el mantenimiento de los servidores. Existen muchos gestores para el monitoreo de la red, al momento de escoger se debe validar primero cuales son las necesidades básicas de la empresa. (Erique, E., 2018) A continuación, se describen puntos importantes al momento de elegir un software para monitoreo de la red:

- a) *Principales componentes del software.* Es importante que al momento de seleccionar el software disponga de distintas características, ya que tiene que monitorear ancho de banda, tener alertas en caso de fallas y límites en niveles de capacidad. Es importante que se pueda rastrear las direcciones IP de los dispositivos conectados. Estas características son básicas al momento de escoger el software de gestión de redes, la misma debe ser mostrada de manera clara y precisa para poder tomar decisiones. (Erique, E., 2018)
- b) *Integración a la red.* En toda empresa es importante que el software de gestión se integre a los dispositivos de redes ya establecidos. Si es difícil integrar el software a la estructura ya existente se tornaría aún más complicado notar los beneficios del programa en su totalidad. Un buen software de gestión debe ser de sencilla instalación y fluidez al momento de configurar las características necesarias para poder vigilar los equipos. (Erique, E., 2018)
- c) *Sensores y alertas.* Un buen gestor de red debe vigilar todos los elementos que la componen y saber cuándo hay problemas. Mediante el uso de sensores y alertas es posible que se configure el software de gestión para que haya notificaciones cuando haya algún inconveniente en la red. (Erique, E., 2018)

En conclusión, es de vital importancia en las empresas monitorear la red, ya que da un control a los departamentos de TI. Con respecto al monitoreo de red, este debe ser continuo y no considerarse como una fase en la etapa de la implementación de la seguridad para evitar un ataque. Se debe recordar que la red de una organización debe tener un monitoreo permanente a cada uno de los componentes de la red. Sin un monitoreo de red, la caída de los servicios va a generar un malestar a los usuarios, provocando pérdida de productividad y creando una mala imagen a la empresa. En la actualidad existen varios softwares libres

para el monitoreo de red como se muestra en la figura 3 (Nagios, Munin, Zabbix).



Fig. 3. Herramientas de software de gestión

4) Políticas de seguridad en el servidor para la navegación

Es importante para toda empresa tener una política de seguridad en servidor de navegación, ya que en el servidor se aloja la página de la organización. En ella se muestra identidad, infraestructura, imagen desde la página electrónica más sencilla sin mucho contenido, hasta la más compleja que cuenta con capacidad de realizar operaciones como pagos, compras, transacciones. Con esto, los servidores donde se encuentran las páginas de las empresas son un blanco fácil y muy atractivo para cualquier atacante por tal motivo debe estar bien protegido. (Erique, E., 2018)

Los ataques a los servidores de las empresas son muy llamativos, debido a que es muy fácil divulgar el ataque en cuestión de segundos, haciendo que la mayor cantidad de usuarios se dé cuenta que se ha modificado algo en el servidor de la compañía. Hoy en día los servidores deben estar protegidos frente a cualquier amenaza, son el punto de entrada a la compañía por tal motivo tienen que estar bien resguardados. (Erique, E., 2018)

La gran mayoría de ataques a los servidores son la consecuencia de una muy mala configuración o un mal diseño en la infraestructura de red,

así como un fallo en la programación web. Las grandes corporaciones tienen sistemas más complejos y, por lo tanto, más difíciles de administrar. Las pequeñas empresas tienen servidores simples y con una configuración paupérrima, lo que hace que, en su gran mayoría, estos servidores sean susceptibles a ser atacados. (Erique, E., 2018)

Definir una política de seguridad en el servidor es importantísimo con el fin de evitar un ciberataque. Estas políticas se basan en la seguridad del servidor no de cliente. (Erique, E., 2018)

- a) *Autenticación*. Es importante que se usen contraseñas para acceder al servidor y estas se las cambien con frecuencia. (Erique, E., 2018)
- b) *Usuario y Grupos*. Eliminando usuarios y grupos que ya no estén en uso, manteniendo la lista actualizada, creando cuentas de usuario, cada una de ellas con privilegios. (Erique, E., 2018)
- c) *Servicios*. Aplicar en el servidor las mejores prácticas de seguridad de proveedores reconocidos como SQL Server, Apache, Plesk, entre otros. (Erique, E., 2018)
- d) *Firewall*. Asegurar el servidor con un firewall, a través hardware o de software. Es recomendable usar un sistema de detención de intrusos (IDS) y un sistema de prevención de intrusos (IPS) como el que se muestra en la figura 4, El firewall protege de los intrusos que traten de ingresar a la red desde ubicaciones externas a ella. (Erique, E., 2018)

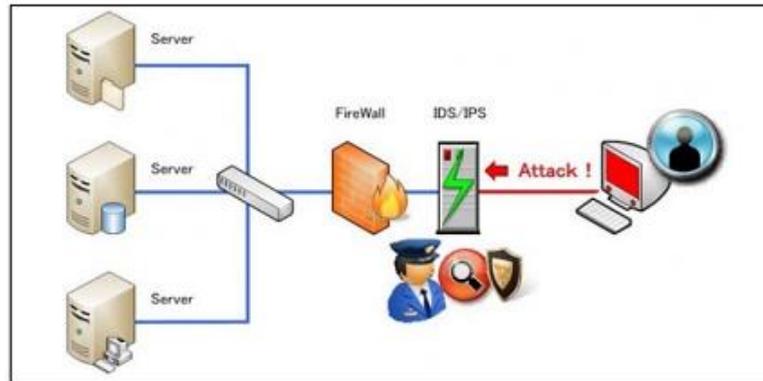


Fig. 4. Firewall Servidor

e) *Auditorias y Análisis*. Es de suma importancia realizar periódicamente auditorias. Esto ayuda a asegurarse que se están cumpliendo los requisitos de seguridad mínimos, también ayuda a identificar los problemas de seguridad, realizando análisis periódicos para identificar vulnerabilidades, recordando que los potenciales intrusos están siempre explorando la web en busca de servidores vulnerables. (Erique, E., 2018)

f) *Sistema Operativo*. Tener el sistema operativo actualizado es muy importante ya que evita problema de seguridad provocado por el uso de versiones antiguas. Se debe actualizar el software siempre de fuentes confiables, ya que de no ser así generan un gran riesgo al servidor a ser vulnerado. (Erique, E., 2018)

La mayoría de la empresa no tiene una política de seguridad en el servidor. Estas son esenciales orientaciones en la detención de ciberataques. Las políticas varían considerablemente según el tipo de compañía. (Erique, E., 2018)

5) Métodos de encriptación y protección de la información

La encriptación es un método de ocultar la información de forma que no se pueda interpretar, esto se lo hace por medio de una llave que es el método de encriptación; la información una vez se haya encriptado solo

puede leerse descriptándola de esta forma se asegura que la información sea auténtica, segura y confiable. En la figura 5 se muestra un ejemplo de esquema de encriptación. (Erique, E., 2018)

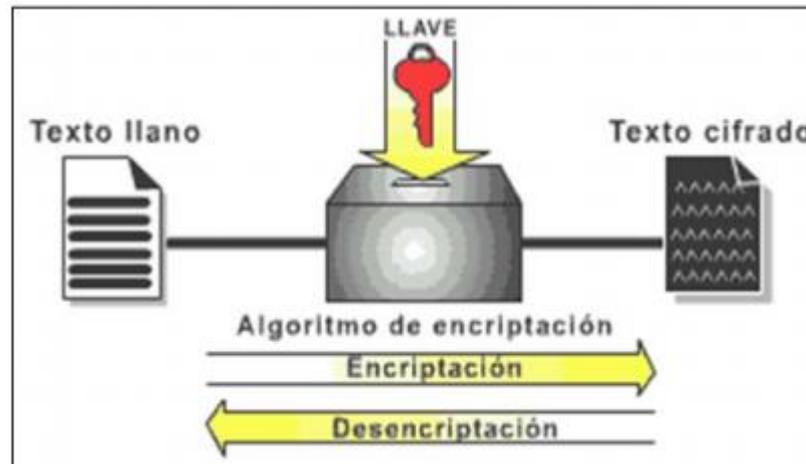


Fig. 5. Método de Encriptación y Desencriptación

Un esquema básico de encriptación implica la utilización de una llave o clave para encriptar el mensaje de tal forma que solo puedan descriptar aquellos que conocen la llave o la clave. El manejo de datos sensibles de los usuarios por parte de las aplicaciones y las webs, requiere que estas tengan técnicas y sistemas de seguridad para proteger dichos datos, ya que pueden ser muy relevantes y, por ello, es primordial el uso de técnicas de cifrado de datos. (Erique, E., 2018) Hay varios métodos de encriptación, listando los siguientes:

- a) *Algoritmo de HASH*. Este algoritmo se basa en el cálculo matemático sobre los datos del archivo el cual da como resultado un único número llamado MAC. Un mismo archivo siempre dará un mismo MAC. (Erique, E., 2018)
- b) *Criptografía de Clave secreta o Simétrica*. Este método utiliza una llave o clave en la cual se encripta y se descripta el archivo. Es importante mencionar que la llave viaja por los datos lo que hace que esta operación sea arriesgada, difícil de usar en sistemas full dúplex. Los sistemas de criptografía por clave secreta no son muy

robustos, ya que la clave del cifrado y del descifrado es la misma.

Sus principales funciones son:

- Fácil y rápidos de Implementar
- Cifrado y descifrado usan la misma clave
- Usuarios compartes la misma clave secreta
- Una comunicación full dúplex requieren muchas claves secretas (Erique, E., 2018)

En la actualidad existen dos métodos de cifrado para criptografía de clave secreta, el cifrado de flujo y el cifrado en bloques. (Erique, E., 2018)

- Cifrado de flujo. El emisor, con una clave secreta y un algoritmo, genera una secuencia binaria cuyos elementos se suman módulo 2 con los correspondientes bits de texto, dando lugar a los bits de texto cifrado, Esta secuencia es la que se envía a través del canal. En recepción, con la misma clave y el mismo algoritmo, genera la misma secuencia para descifrar, que se suma módulo 2 con la secuencia cifrada, dando lugar a los bits de texto claro. Los tamaños de las claves oscilan entre 120 y 250 bits. (Erique, E., 2018)
- Cifrado en bloque. Los cifrados en bloque se componen de cuatro elementos: a. Transformación inicial por permutación b. Transformación final para que las operaciones de encriptación y descifrado sean simétricas c. Uso de un algoritmo de expansión de claves que tiene como objeto convertir la clave de usuario, normalmente de longitud limitada entre 32 y 256 bits, en un conjunto de subclaves que puedan estar constituidas por varios cientos de bits en total. (Erique, E., 2018)

c) *Algoritmos Asimétricos (RSA)*. Se Requieren dos claves, una privada (propia y única, solo conocida por su dueño) y la otra

llamada pública, ambas vinculadas por una fórmula matemática compleja imposible de descifrar. El usuario, ingresando su PIN genera la clave pública y privada necesaria. La clave Pública podrá ser distribuida sin ningún inconveniente entre todos los interlocutores. La Privada deberá ser celosamente guardada. (Erique, E., 2018)

- d) *Message-Digest Algorithm, MD5*. Este algoritmo, ha sido en los últimos años el algoritmo Hash más usado, procesa mensajes de una longitud en bloques de 512 bits generando un resumen de 128 bits. Debido a su gran capacidad de procesamiento actual esos 128 bits son insuficientes para asegurar la integridad del algoritmo, además de que una serie de ataques criptoanalíticos han puesto en manifiesto algunas vulnerabilidades del algoritmo. (Erique, E., 2018)
- e) *Advanced Encryption Standard, (AES)*. En criptografía, Advanced Encryption Standard (AES), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. (Erique, E., 2018)

2.5.2 Procesos Educativos

a. Ciencias y Humanidades

1) Política Nacional de Ciberseguridad

➤ Objetivo

“Proteger la infraestructura de información, los datos e información del Estado y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y

confiabilidad de la información. Asegurar la implementación de las propuestas legislativas, y en general la normatividad relacionada con la seguridad de la información o Ciberseguridad comprendida en esta Política, identificando los recursos involucrados y las partidas presupuestales correspondientes. Mantener la Política Nacional de Ciberseguridad actualizada, a efectos de asegurar su vigencia y por ende su eficacia, promoviendo la participación de las entidades de sector público y privado, así como representantes de la sociedad civil y la academia”.

➤ **Alcance**

“La presente Política se aplica a todas las entidades de la Administración Pública a que hace referencia el Artículo I del Título Preliminar de la Ley N° 27444, así como a todos sus recursos y procesos sean estos internos o externos”.

➤ **Marco Normativo**

- “Constitución Política del Perú”.
- “Decreto Legislativo N° 604”.
- “Ley N° 29158: Ley Orgánica del Poder Ejecutivo”.
- “Ley N° 27658: Ley Marco de Modernización de la Gestión del Estado”.
- “Ley N° 27806: Ley Transparencia y Acceso a la Información Pública”.
- “Ley N° 27444: Ley de Procedimiento Administrativo General”.
- “Ley N° 27269: Ley de Firmas y Certificados Digitales”.
- “Ley N° 27291: Ley que modifica el código civil permitiendo la utilización de los medios electrónicos para

la comunicación de la manifestación de voluntad y la utilización de la firma electrónica”.

- “Ley N° 28493: Ley que regula el uso del Correo Electrónico comercial no solicitado (SPAM)”.
- “Ley N° 29733: Ley de Protección de Datos Personales”.
- “Ley N° 28530: Ley de Promoción de Acceso a Internet para personas con discapacidad y adecuación del espacio físico en cabinas públicas de internet”.
- “Ley N° 29904: Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica”.
- “Ley N° 30096 y su modificatoria Ley 30171: Ley de Delitos Informáticos”.
- “Decreto Legislativo N° 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses”.
- “Decreto Supremo N° 022-2017-PCM, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros”.
- “Decreto Supremo N° 066-2011-PCM: Aprueba el Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0”.
- “Decreto Supremo N° 004-2013-PCM: Aprueba la Política Nacional de Modernización de la Gestión Pública”.
- “Decreto Supremo N° 081-2013-PCM: Aprueba la Política Nacional de Gobierno Electrónico 2013-2017”.
- “Resolución Ministerial N° 179-2004-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 12207:2004 Tecnología de la Información. Procesos del Ciclo de Vida del Software, 1ª Edición” en entidades del Sistema Nacional de Informática”.
- “Resolución Ministerial N° 246-2007-PCM, que aprueba la Norma Técnica Peruana NTP-ISO/ IEC 17799:2007 EDI.

Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición en todas las entidades integrantes del Sistema Nacional de Informática”.

- “Resolución Ministerial N° 197-2011-PCM, que establece fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”.
- “Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición, en todas las entidades integrantes del Sistema Nacional de Informática”.
- “Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información”.

2) **Tratados Internacionales**

La presente Política cuenta con los siguientes marcos de referencia:

- “Resolución Ministerial N° 246-2007-PCM, que aprueba la Norma Técnica Peruana NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición en todas las entidades integrantes del Sistema Nacional de Informática, o la que haga sus veces”.

- “Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición, en todas las entidades integrantes del Sistema Nacional de Informática, o la que haga sus veces”.
- “Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información”.

b. Ciencias Militares

1) Doctrina Militar de Comunicaciones

“En cualquier Teatro de Operaciones el comando cuenta con un elemento de transmisión de información y de control que es el sistema de comunicaciones”.

“...Para ser transmitido un mensaje, se requiere de un sistema de comunicación que permita que la información sea transferida, a través del espacio y el tiempo, desde un punto llamado fuente hasta otro punto de destino, mediante un cable como en el caso de un teléfono o por ondas como en el caso de las radios...”

“Cualquier sistema de comunicación consta de tres componentes: emisor, canal de transmisión y el receptor. Sin embargo, no existen dos sistemas de comunicaciones iguales, incluso para un mismo tamaño y tipo de fuerzas. Es por esto que un comandante de una Fuerza Conjunta debe conocer cuáles son las capacidades y la arquitectura de las comunicaciones de la fuerza que va a comandar”.

“En el Teatro de Operaciones Conjunto conviven diversos sistemas de comunicaciones y al interactuar en forma conjunta surgen dificultades para la interoperabilidad”.

“Es por ello que en este capítulo se analiza en principio las características generales de los diferentes tipos de comunicaciones que utilizan las Fuerzas Armadas, que permita contar con una noción más clara sobre estas teniendo como premisa que el mando de las fuerzas conjuntas requiere una adecuada capacidad de comando y control”.

“Las redes pueden ser del tipo alámbricas o inalámbricas. Las redes de comunicaciones del tipo alámbrica son un conjunto de medios que permiten la comunicación a distancia entre equipos, los cuales se encuentran conectados por medio de cables (cable de cobre o fibra óptica) y que comparten información y recursos, por lo general para poder transmitir datos, audio o vídeo; mientras que las redes inalámbricas al no utilizar una línea física utilizan las ondas electromagnéticas, las cuales se transmiten o reciben por medio de antenas y de acuerdo al rango de frecuencia, se dividen en ondas de radio, microondas terrestres o satelitales”.

“Las ondas de radio son ondas electromagnéticas y omnidireccionales y se pueden dividir en UHF, VHF y HF”.

“La señal UHF (Ultra High Frequency, frecuencia ultra alta) es una banda del espectro electromagnético que ocupa el rango de frecuencias de 300 MHz a 3 GHz. En esta banda se produce la propagación por onda espacial troposférica”.

“La ventaja principal de este tipo de señal es la longitud de onda corta que se debe a la alta frecuencia y se puede decir que como desventaja es que la misma es a vista lineal teniendo que utilizar repetidores para realizar comunicaciones a mayores distancias”.

“La señal VHF (Very High Frequency) es la banda del espectro electromagnético que ocupa el rango de frecuencias de 30 MHz a 300 MHz”.

“...Las estaciones emisoras en esta banda tienen menor cobertura que las que se encuentran en las ondas cortas, sobre todo cuando su frecuencia se va alejando de los 30 MHz., adquiriendo cada vez más importancia la onda aérea y prácticamente perdiendo toda su importancia la onda terrestre o de superficie. Esto se debe a que las ondas de radio de VHF se propagan en línea recta, y en condiciones normales no se reflejan en la ionósfera, si no que la atraviesan, prolongándose en el espacio exterior hasta que en este medio se van debilitando y perdiendo...”

Estos dos tipos de transmisión UHF y VHF son afectados por muchas variables climáticas como por ejemplo la humedad atmosférica y el viento solar.

La señal HF (High Frequency, o altas frecuencias) son las siglas utilizadas para referirse a la banda del espectro electromagnético que ocupa el rango de frecuencias de 3 MHz a 30 MHz. Las comunicaciones realizadas en HF se utilizan principalmente para largas distancias, más allá del horizonte, pudiéndose incrementar la distancia de transmisión y recepción utilizando retransmisores.

Microondas terrestres: Opera en frecuencias de 1 hasta 300 GHz. Tiene cobertura de kilómetros con el inconveniente mayor de que el emisor y el receptor deben estar alineados. Este es el motivo por el cual a este tipo de comunicación se la denomina enlace punto a punto en distancias cortas. En este caso, la atenuación producida por la lluvia es más importante y debido a ello opera a una frecuencia más elevada.

Microondas por satélite: A diferencia de las microondas terrestres, las microondas satelitales lo que hacen básicamente, es retransmitir información. Se usan como enlace entre dos o más transmisores / receptores terrestres, denominados estaciones base. El satélite funciona como un espejo sobre el cual la señal rebota; su principal función es la de amplificar la señal, corregirla y retransmitirla a una o más antenas ubicadas en la tierra

Como se puede apreciar existen distintos tipos de comunicaciones y varias formas de poder realizar las mismas.

Las redes militares han evolucionado desde el siglo XIX, en el cual se montaban sobre las comunicaciones telefónicas y con la evolución de la tecnología en el siglo XX las comunicaciones militares se montaron sobre las comunicaciones radioeléctricas. A fines del mismo siglo la tecnología dio un nuevo salto en la informática y se conformaron nuevas arquitecturas en comunicaciones conformadas por fibra óptica al ser alámbricas, y electromagnéticas y satelitales en el caso de las inalámbricas, sumándose a ello el nuevo diseño en equipos de comunicaciones con saltos de frecuencia, encriptados que hacen que las comunicaciones sean más seguras y confiables.

Un ejemplo de cómo ha evolucionado la arquitectura en las comunicaciones y los resultados de tener redundancia de medios, pero sin el control conveniente de los mismos se dio en la primera guerra del Golfo, donde al finalizar el conflicto las Fuerzas Aliadas comprobaron que del otro lado existía tal redundancia de medios que si se hubiera utilizado correctamente por el enemigo pudo haber traído inconvenientes a las Fuerzas de la coalición.

“...La redundancia es un atributo que no solo poseen los países desarrollados: cuando finalizó la Guerra del Golfo donde el primer Plan de Operaciones consistía en destruir las instalaciones de

comando y control iraquíes, los aliados se dieron cuenta que quedaban más que los iniciales, a pesar del número que destruyeron. No obstante, parece ser que los iraquíes tenían muchos sistemas de comunicaciones, más aún de los que conocían, desde sistemas de radio hasta de contratistas de petróleo occidentales que habían dejado en el lugar líneas telefónicas rurales que unían a las principales ciudades...”

“Llevado lo acontecido en el ejemplo anterior a las Fuerzas Armadas de Argentina, nos vamos a encontrar que las mismas poseen una gran cantidad de medios de diferente tecnología, esto implica que a pesar de trabajar en iguales bandas de trabajo (HF – VHF – UHF) los mismos tienen diferentes alcances y rangos. Esto lleva que, al intentar armar la arquitectura de comunicaciones en la búsqueda de compatibilidad de medios, hace que las mismas entren en conflicto con los requisitos básicos de las comunicaciones”.

“Si bien no es competencia del Comandante conocer el detalle de cada uno de los sistemas, si es conveniente que este en claro con qué medios cuenta la fuerza a comandar y cuáles son sus capacidades.

“Aquí no solo se vio las características de los tipos de comunicaciones, sino que, además, como el avance tecnológico en este campo han afectado la forma no solo de hacer la guerra sino la necesidad de contar con un eficiente sistema de comunicaciones. En las siguientes líneas se intentará proponer las características de un sistema de comunicaciones que provea facilidades para ejercer la función de comando y en función de la orgánica vigente, se propondrá una orgánica dentro de la cual se contemple a esta compañía”.

“Las características de los sistemas de comunicaciones en un teatro de Operaciones no siempre van a ser las mismas. Estas varían de

acuerdo a la misión y al teatro propiamente dicho, permitiendo conducir las operaciones, ver los cambios y la evolución de la situación además de permitir la emisión de planes y ordenes, monitoreando las ejecuciones de las operaciones y finalmente evaluar los resultados”.

“Así se ayuda a reducir la incertidumbre propia de cualquier operación militar, recopilando información y transformándola, para luego utilizarla”.

“Independientemente de las características de los teatros de operaciones las características más relevantes de un sistema de comunicaciones conjunto están basadas en”:

- “Diseñado para la planificación, conducción y control de operaciones conjuntas”.
- “Despliegue de información en forma simple, completa y oportuna”.
- “Sistema integrable a cualquier red de comunicación”.
- “Puesto de Mando seguro, transportable y redundante”.
- “Asegurar la interoperabilidad, de acuerdo a su arquitectura flexible”.

Para el cumplimiento de estos requisitos sería conveniente que la compañía de comunicaciones contase con las siguientes facilidades:

- “Comunicaciones analógicas y digitales, con capacidad de integración de voz, datos y video”.
- “Comunicación en tiempo real entre esta y el Estado Mayor de las Fuerza Armadas y con los distintos componentes intervinientes en la operación”.

- “Comunicaciones satelitales, telefónicas y radioeléctricas del tipo alámbrica e inalámbrica de voz, datos y video con otras redes nacionales, provinciales e internacionales”.
- “Central meteorológica con capacidad para recibir emisiones meteorológicas, fax e imágenes”.
- “Debe brindar las instalaciones y medios necesarios para el trabajo del comandante y su estado mayor en el terreno, como así también debe estar integrado a los sistemas de comunicaciones instalados”.

2) **Planeamiento de Operaciones**

Comunicaciones no significa simplemente poder transmitir o recibir un mensaje. Las comunicaciones deben cumplir requisitos fundamentales tanto en la paz como en la guerra; ellos son confianza, seguridad y rapidez. Estos requisitos no han cambiado, pero si lo ha hecho la tecnología, ya que esta ha progresado de tal forma que ha hecho que estos requisitos estén más presentes que nunca en un teatro de operaciones. Es necesario tener presente de esta manera que no se debe sacrificar uno de estos requisitos en pos de cualquiera de los otros, ya que las comunicaciones quedarían expuestas.

En tiempo de paz, las comunicaciones no parecen jugar un rol fundamental, prueba de ello son que en la mayoría de los ejercicios en el nivel operacional las comunicaciones se dan por cumplidas. Sin embargo, en un conflicto las unidades a comunicarse se multiplican y con ello se multiplican los equipos de comunicaciones que tienen diferentes características, causa por la cual aumentan las necesidades de extremar la seguridad de las comunicaciones, ya sea con claves, códigos o silencios electrónicos.

“Es por ello que las comunicaciones facilitan el comando y al poseer deficientes comunicaciones, carecerán de la libertad de acción y flexibilidad que le son imprescindibles para ejercerlo; dicho en otras palabras: las comunicaciones hoy más que nunca son imprescindibles para el ejercicio del Comando”.

“La acción conjunta tiene dos niveles: planeamiento y conducción. La determinación de los objetivos de las fuerzas específicas debe ser convergentes para alcanzar el objetivo final; y la coordinación de los límites de las áreas de actuación, para facilitar el apoyo mutuo, debe evitar interferencias y bajas por fuego propio...”

3) Aplicación de la Guerra Cibernética

“La ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático que va desde”:

“La infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadores, pasando por la planificación de las operaciones, la gestión del abastecimiento, etc.”
(Colle, 2000).

“No obstante, para los que consideran que la cyberwar y la netwar son una misma cosa, hay que puntualizar, la ciberguerra es la utilización de todas las herramientas electrónicas e informáticas para derrumbar los sistemas electrónicos y de comunicación del

enemigo y mantener operativos los propios”. (Sánchez Medero, 2008: p. 15)

“En todo caso, si tuviéramos que enumerar las características de una guerra cibernética éstas serían: complejidad, asimetría, objetivos limitados, corta duración, menos daños físicos para los soldados, mayor espacio de combate y menor densidad de tropas, transparencia, lucha intensa por la superioridad de la información, aumenta la integración, mayores exigencias impuestas a los comandantes, nuevos aspectos de la concentración de fuerzas, reacción rápida, e igual de devastadora que una guerra convencional”. (Thomas, 2001). “Pero tal vez, de todas ellas, la más importante sea la de asimetría, porque la guerra cibernética proporciona los instrumentos necesarios para que los más pequeños puedan enfrentarse, incluso vencer y mostrarse superiores a los más grandes, con unos riesgos mínimos para ellos, sólo siendo necesario un ordenador y unos avanzados conocimientos informáticos”.

Más, cuando los objetivos de este tipo de guerra son:

- “Dañar un sistema o entidad hasta el punto en que ya no puede funcionar ni ser restaurado a una condición útil sin que lo reconstruyan por completo”.
- “Interrumpir o romper el flujo de la información”.
- “Destruir físicamente la información del adversario”.
- “Reducir la efectividad o eficiencia de los sistemas de comunicación del adversario y sus capacidades de recolección de información”.
- “Impedir al adversario acceder y utilizar los sistemas y servicios críticos”.
- “Engañar a los adversarios”.

- “Lograr acceder a los sistemas del enemigo y robarles información”.
- “Proteger sus sistemas y restaurar los sistemas atacados”.
- “Responder rápidamente a los ataques o invasiones del adversario”.

Por eso es necesario advertir que existen tres clases de ciberguerra:

- Clase I. Personal Information Warfare: “área relacionada con las cuestiones y la seguridad personal, así como la privacidad de los datos y del acceso a las redes de información#.
- Clase II. Corporate/Organizacional Level Information: “área del espionaje clásico entre organizaciones de diferente nivel (de la empresa al Estado) o al mismo nivel (de Estado a Estado)”.
- Clase III, Open/Global Scope Information Warfare: “área relacionada con las cuestiones de ciberterrorismo a todos los niveles, como pueden ser: los ataques realizados desde computadoras a centros tecnológicos; la propaganda como forma para enviar sus mensajes y para promover el daño ocasionado por sus ataques; y/o la planificación logística de atentados tradicionales, biológicos o tecnológicos”.

“Los guerreros del ciberespacio hoy son consultores e ingenieros equipados con arsenales informáticos ajenos a la imagen convencional de los armamentos, y los encargados de combatir a los «villanos» en el escenario bélico virtual llevarán micrófonos y audífonos, computadores portátiles, sensores, etc. Sus procedimientos se asemejan bastante al de los hackers, aunque sus fines, casi siempre, son completamente distintos. Lo primero que hace cualquier hacker es visitar o buscar algunos de los sitios donde hay scripts para escanear el sitio al cual se quiere violentar, con el fin de determinar cuál es su arquitectura tecnológica básica. Esos scripts indagan en el servidor del sitio para determinar qué sistema

operativo usa y que tipo de servidor de software emplean”. “Luego viene la parte más difícil: encontrar agujeros o fallas en la versión específica del software de ese este sitio, ya que éste puede proporcionar las entradas que nos permitan romper su código. Las informaciones sobre las fallas del software inmediatamente pasan a ser de conocimiento público dentro de la comunidad hacker, evidentemente cuando se trata de cibersoldados la información obtenida no se publicita. Así, una vez que un hacker encuentra un agujero, penetrar el sistema es sólo una cuestión de persistencia, aunque la enorme mayoría de los intentos terminan en fracaso”.

2.5.3 Definición de términos básicos

Amenaza: Causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Auditabilidad: Definir que todos los eventos de un sistema puedan ser registrados para su control posterior. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Autenticidad: Asegurar que la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Comité de Seguridad de la Información: Colegiado integrado por representantes de todas las áreas sustantivas de la entidad, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Confiability de la Información: Que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Confidencialidad: Garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Control: Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Disponibilidad: Garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Evaluación de Riesgos: Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma; la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Gestión de Riesgos: Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo. La gestión de riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Incidente de Seguridad: Evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la

confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de quebrar los mecanismos de seguridad existentes. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Información: Toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Integridad: Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Legalidad: Cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Propietario de la Información: Persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Responsable de Seguridad de la Información: Persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la entidad que así lo requieran. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Riesgo: Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Sistema de Información: Conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Tecnología de la Información: Hardware y software operados por la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Tratamiento de Riesgos: Proceso de selección e implementación de medidas para modificar el riesgo. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza. (www2.congreso.gob.pe/Política Nacional de Ciberseguridad)

CAPÍTULO III

MARCO METODOLÓGICO

3.1 Método y Enfoque de la Investigación

Según Popper, el método hipotético deductivo "consiste en ofrecer una explicación causal deductiva y en experimentar (por medio de predicciones). Este ha sido llamado a veces el método hipotético deductivo" (Popper, 1981, p. 146).

Popper señala que "una explicación causal de un cierto acontecimiento específico consiste en deducir una proposición que describa este acontecimiento, de dos clases de premisas: por una parte; de algunas leyes universales, y, por otra, de algunas proposiciones singulares o específicas que podríamos llamar condiciones iniciales específicas" (Popper, 1981, p. 137).

El enfoque del presente trabajo de investigación es cuantitativo. El enfoque cualitativo también se guía por áreas o temas significativos de investigación. Sin embargo, en lugar de que la claridad sobre las preguntas de investigación e hipótesis preceda a la recolección y el análisis de los datos (como en la mayoría de los estudios cuantitativos), los *estudios cualitativos* pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos. Con frecuencia, estas actividades sirven, primeramente, para descubrir cuáles son las preguntas de investigación más importantes; y después, para perfeccionarlas y responderlas. La acción indagatoria se mueve de manera dinámica en ambos sentidos: entre los hechos y su interpretación, y resulta un proceso más bien "circular" en el que la secuencia no siempre es la misma, pues varía con cada estudio. (Hernández, R. – Fernández, C. & Baptista, M., 2014)

3.2 Tipo de Investigación

"La Investigación Descriptiva busca especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis" (Danhke, (1989) cfr por Hernández, et al (2003) p. 117).

“La Investigación Correlacional.... es un tipo de estudio que tiene como propósito evaluar la relación que exista entre dos o más conceptos, categorías o variables (en un contexto en particular). Los estudios cuantitativos correlacionales miden el grado de relación entre esas dos o más variables (cuantifican relaciones). Es decir, miden cada variable presuntamente relacionada y después también miden y analizan la correlación. Tales correlaciones se expresan en hipótesis sometidas a prueba” (Hernández, et al (2003) p.121).

3.3 Nivel y Diseño de la Investigación

La investigación será de nivel básico. Ya que la misma se caracteriza porque parte de un marco teórico y permanece en él; la finalidad radica en formular nuevas teorías o modificar las existentes, en incrementar los conocimientos científicos o filosóficos, pero sin contrastarlos con ningún aspecto práctico.

El diseño de la presente investigación es de tipo *no experimental*; ya que se observaron las situaciones ya existentes dentro de las áreas de estudio; éstas no fueron provocadas intencionalmente. Este estudio a su vez fue de tipo *transeccional*, ya que la recolección de información se hizo en un solo momento y en un tiempo único; además de que, en este tipo de diseño no experimental, el propósito es describir las variables y analizar su incidencia e interrelación en un momento dado. (Hernández, et al (2003) p.187)

3.4 Técnicas e Instrumentos para la recolección de información

3.4.1 Elaboración de los instrumentos

a. Instrumento sobre Prevención de Ataques Cibernéticos

Variable 1 Ficha técnica:

- Nombre: Cuestionario para Prevención de Ataques Cibernéticos
- Administración: Individual y colectiva
- Tiempo de administración: Entre 10 y 15 minutos, aproximadamente

- **Ámbito de aplicación:** Cadetes
- **Significación:** Prevención de Ataques Cibernéticos.
- **Tipo de respuesta:** Los ítems son respondidos a través de escalamiento Likert con cinco valores categoriales.

Estructura:

Las dimensiones que evalúan la Prevención de Ataques Cibernéticos son las siguientes:

- 1) Tipos de Ataques Cibernéticos según el Objetivo
- 2) Fases del Ataque
- 3) Medidas de Prevención

Tabla 3

Tabla de especificaciones para el cuestionario sobre Prevención de Ataques Cibernéticos

Dimensiones	Ítems	Total	%
Tipos de Ataques	1, 2, 3, 4	4	28,57%
Fases del Ataque	5, 6, 7, 8, 9	5	35,71%
Medidas de Prevención	10, 11, 12, 13, 14	5	35,71%
Total, Ítems		14	100%

Fuente: Elaboración propia

b. Instrumento sobre Procesos Educativos

Variable 2 Ficha técnica

- **Nombre:** Cuestionario para Procesos Educativos.
- **Administración:** Individual y colectiva
- **Tiempo de administración:** Entre 10 y 15 minutos, aproximadamente
- **Ámbito de aplicación:** Cadetes
- **Significación:** Procesos Educativos
- **Tipo de respuesta:** Los ítems son respondidos a través de escalamiento Likert con cinco valores categoriales.

Estructura:

Las dimensiones que evalúa Procesos Educativos son las siguientes:

- 1) Ciencias y Humanidades
- 2) Ciencias Militares

Tabla 4

Tabla de especificaciones para Procesos Educativos

Dimensiones	Ítems	Total	%
Ciencias y Humanidades	15, 16	2	40,00%
Ciencias Militares	17, 18, 19	3	60,00%
Total, Ítems		5	100%

Fuente: Elaboración propia

3.4.2 Validez, confiabilidad y evaluación de instrumentos: juicio de expertos

Validez

Según Hernández (2014), “la validez es el grado en que un instrumento en verdad mide la variable que pretende medir” (p. 201).

Tabla 5

Juicio de expertos

Docente	Valoración
Mg. Carlos Oneto Mendoza	Aplicable
Dr. José Galindo Heredia	Aplicable
Mg. José Ravina Pévez	Aplicable

Fuente: Elaboración propia

Confiabilidad

Para la confiabilidad se realizaron un trabajo piloto con noventa y ocho (98) cadetes de características similares a quienes se les aplicó el

cuestionario de Prevención de Ataques Cibernéticos y los Procesos Educativos, para someterlo a un proceso de análisis estadístico mediante el coeficiente de Alfa de Cronbach, teniendo el siguiente resultado:

Tabla 6

Resumen de procesamiento de casos

		N	%
Casos	Valido	98	100%
	Excluido	0	0
	Total	98	100%

Fuente: Elaboración propia

Tabla 7

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach	N de elementos
.891	.891	19

Fuente: Elaboración propia

El análisis nos reporta un resultado de 0,891 por consecuente este resultado como nos menciona George y Mallery es una confiabilidad aceptable.

Tabla 8

Estadísticas de fiabilidad

Alfa de Cronbach	Confiabilidad
> ,9	Excelente
> ,8	Bueno
> ,7	Aceptable
> ,6	Cuestionable
> ,5	Pobre
< ,5	Inaceptable

Las variables de la presente investigación son confiables en un nivel bueno, con un puntaje de ,891.

3.4.3 Aplicación de los instrumentos

En el presente trabajo de investigación para el procesamiento de los datos se utilizará el software SPSS versión 25, así como lo define Hernández, L. (2017, p.53), SPSS es un programa estadístico informático muy usado en las ciencias sociales y las empresas de investigación de mercado. Dentro de las ciencias sociales, SPSS tiene especial interés en las ramas de la ingeniería, medicina, física, química, empresa, etc. Además, para la confiabilidad del instrumento se utilizará el Alpha de Cronbach; para la normalidad de los datos utilizaremos Kolmogorov Smirnov puesto que la muestra es mayor a 25 sujetos, nos ayudará a tomar una decisión estadística. Si son datos normales utilizaremos R –Pearson y si son datos no normales Rho Spearman.

3.5 Universo, Población y Muestra

El universo está constituido por la totalidad de individuos o elementos en los cuales puede presentarse determinada característica susceptible a ser estudiada. Debemos tener en consideración que no siempre es posible estudiarlo en su totalidad.

Esto implica que pueda ser finito o infinito, y en el caso de ser finito, puede ser muy grande y no poderse estudiar en su totalidad. Por eso es necesario escoger una parte de ese universo, para llevar a cabo el estudio.

Para el presente trabajo de investigación el Universo serán la totalidad de los cadetes de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

Según Tamayo (2012) señala que:

“La población es la totalidad de un fenómeno de estudio, incluye la totalidad de unidades de análisis que integran dicho fenómeno y que

debe cuantificarse para un determinado estudio integrando un conjunto N de entidades que participan de una determinada característica, y se le denomina la población por constituir la totalidad del fenómeno adscrito a una investigación”. (p.180)

La población estará conformada por noventa y ocho (98) Cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

3.6 Criterios de Selección de la muestra

En el caso de Palella y Martins (2008), definen la muestra como: "...una parte o el subconjunto de la población dentro de la cual deben poseer características reproducen de la manera más exacta posible” (p.93).

Tabla 9

Distribución de la población

Sección	Población
Infantería	97
Caballería	38
Artillería	25
Ingeniería	33
Comunicaciones	30
Inteligencia	12
Intendencia	29
Material de Guerra	14
Total	278

Muestra

En la determinación óptima de la muestra se utilizó la fórmula del muestreo aleatorio simple para estimar proporciones cuando la población es conocida, el tamaño muestral según Pérez (2005), el tamaño muestral para una población finita haciendo uso del muestreo aleatorio simple está dado por:

$$n = \frac{Z^2 * P * Q * N}{e^2 * (N - 1) + Z^2 * P * Q}$$

Dónde:

Z : Valor de la abscisa de la curva normal para una probabilidad del 95% de confianza.

P : P = 0.5, valor asumido debido al desconocimiento de P

Q : Q = 0.5, valor asumido debido al desconocimiento de P.

e : Margen de error 8%

N : Población.

n : Tamaño óptimo de muestra

Por lo tanto, aplicando la fórmula se obtuvo una muestra de

$$n = \frac{(1.96)^2 * 278 * (0.5) * (0.5)}{(0.08)^2 * (278 - 1) + (1.96)^2 * (0.5) * (0.5)}$$

$$n = 98 \text{ cadetes de 4to año de la EMCH}$$

Esta muestra será seleccionada de manera aleatoria

Al considerar la distribución de la población se va a llevar a cabo un muestreo estratificado y como tal los participantes de cada estrato se harán por fijación proporcional, cuya fórmula se precisa a continuación:

$$\text{Muestra proporcional } \frac{n}{N} = \frac{98}{278} = 0.35$$

Tabla 10

Muestra proporcional

Sección	Población	Muestra proporcional
Infantería	97	97 x 0.35 = 34

Caballería	38	$38 \times 0.35 = 14$
Artillería	25	$25 \times 0.35 = 9$
Ingeniería	33	$33 \times 0.35 = 12$
Comunicaciones	30	$30 \times 0.35 = 11$
Inteligencia	12	$12 \times 0.35 = 4$
Intendencia	29	$29 \times 0.35 = 11$
Material de Guerra	14	$14 \times 0.35 = 4$
Total	278	98

Fuente: Elaboración propia

3.7 Aspectos Éticos

Para la realización de la investigación se consideró diversos principios éticos, desde la etapa inicial, de recolección de datos, de cotejo de fuentes bibliográficas, hemerográficas, las fuentes electrónicas y demás soportes de interés utilizados.

Se ha hecho referencia a las fuentes de información, citando a los autores de cada obra. Este trabajo reunió la condición de originalidad, debido a que existen diversos estudios en este tipo de investigación de las ciencias militares.

La investigación considera los siguientes criterios éticos:

- La investigación tiene un valor social y científico.
- La investigación tiene validez científico-pedagógica.
- Para realizar la investigación ha existido un consentimiento informado y un respeto a los participantes.

CAPÍTULO IV ANÁLISIS, INTERPRETACIÓN Y DISCUSIÓN DE LOS RESULTADOS

4.1. Análisis de los resultados

Para la variable X: Prevención de Ataques Cibernéticos

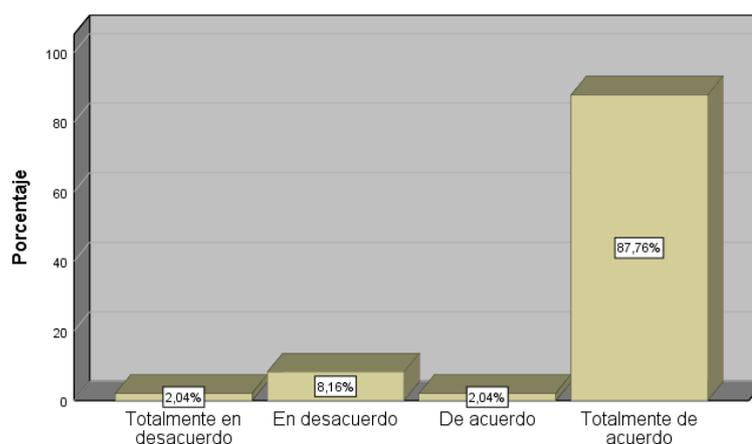
Tipos de Ataques Cibernéticos según el Objetivo

1. ¿Considera usted que la Interrupción dentro de los Tipos de Ataques Cibernéticos según el Objetivo se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 11. *La Interrupción*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	2,0	2,0
	En desacuerdo	8	8,2	10,2
	De acuerdo	2	2,0	12,2
	Totalmente de acuerdo	86	87,8	100,0
	Total	98	100,0	

P1



P1

Figura 6. *La Interrupción*

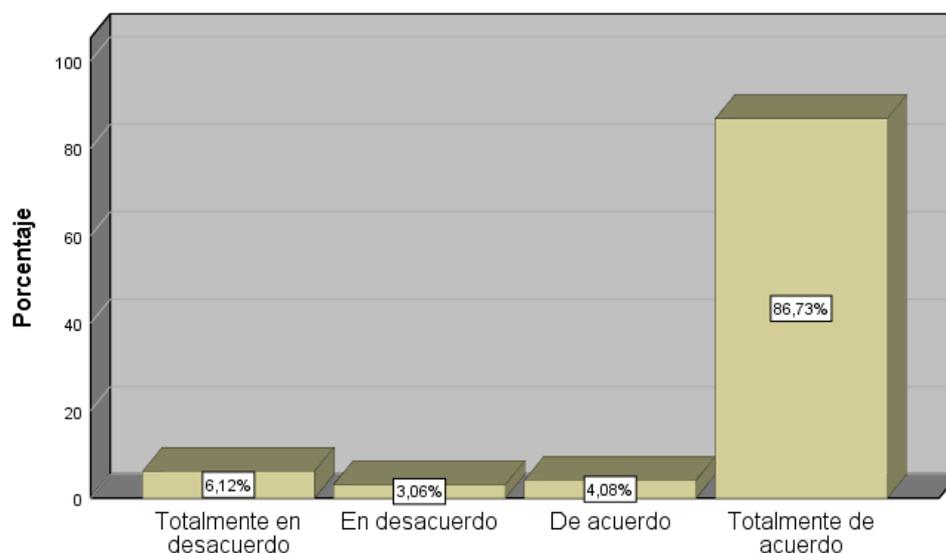
Análisis: En cuanto a si considera usted que la Interrupción dentro de los Tipos de Ataques Cibernéticos según el Objetivo se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 87,8%; que solo están de acuerdo un 2%; manifestaron que están en desacuerdo el 8,2%; y, manifestaron que están totalmente en desacuerdo un 2%.

2. ¿Considera usted que la Interpretación dentro de los Tipos de Ataques Cibernéticos según el Objetivo se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 12. *La Interpretación*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	6	6,1	6,1
	En desacuerdo	3	3,1	9,2
	De acuerdo	4	4,1	13,3
	Totalmente de acuerdo	85	86,7	100,0
	Total	98	100,0	

P2



P2

Figura 7. *La Interpretación*

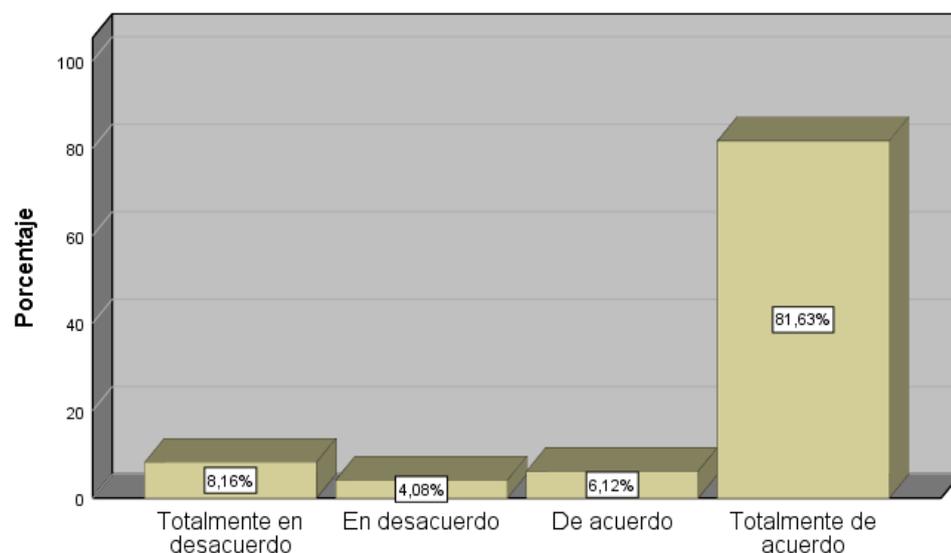
Análisis: En cuanto a si considera usted que la Interpretación dentro de los Tipos de Ataques Cibernéticos según el Objetivo se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 86,7%; que solo están de acuerdo un 4,1%; manifestaron que están en desacuerdo el 3,1%; y, manifestaron que están totalmente en desacuerdo un 6,1%.

3. ¿Considera usted que la Modificación dentro de los Tipos de Ataques Cibernéticos según el Objetivo se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 13. *La Modificación*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	8	8,2	8,2
	En desacuerdo	4	4,1	12,2
	De acuerdo	6	6,1	18,4
	Totalmente de acuerdo	80	81,6	100,0
	Total	98	100,0	

P3



P3

Figura 8. *La Modificación*

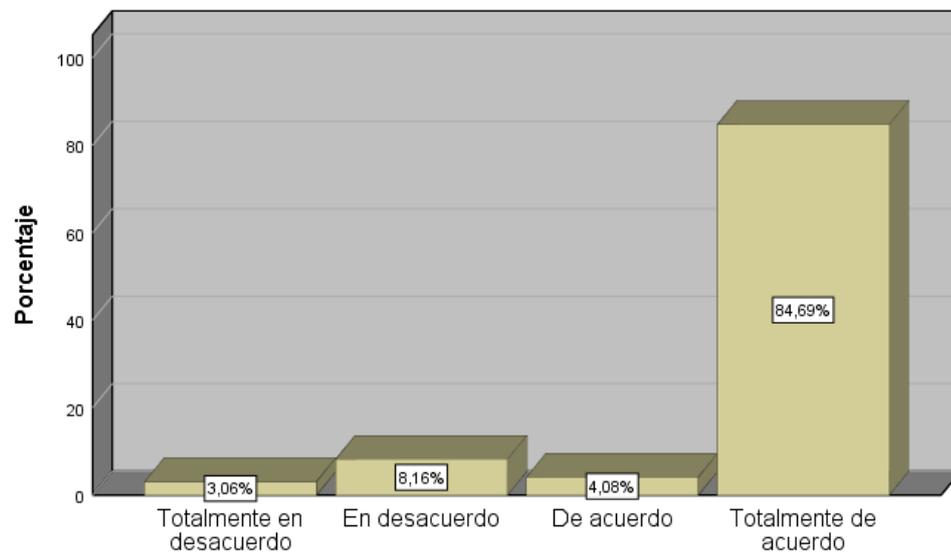
Análisis: En cuanto a si considera usted que la Modificación dentro de los Tipos de Ataques Cibernéticos según el Objetivo se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 81,6%; que solo están de acuerdo un 6,1%; manifestaron que están en desacuerdo el 4.1%; y, manifestaron que están totalmente en desacuerdo un 8,2%.

4. ¿Considera usted que la Generación dentro de los Tipos de Ataques Cibernéticos según el Objetivo se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 14. *La Generación*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	3	3,1	3,1
	En desacuerdo	8	8,2	11,2
	De acuerdo	4	4,1	15,3
	Totalmente de acuerdo	83	84,7	100,0
	Total	98	100,0	

P4



P4

Figura 9. *La Generación*

Análisis: En cuanto a si considera usted que la Generación dentro de los Tipos de Ataques Cibernéticos según el Objetivo se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 84,7%; que solo están de acuerdo un 4,1%; manifestaron que están en desacuerdo el 8,2%; y, manifestaron que están totalmente en desacuerdo un 3,1%.

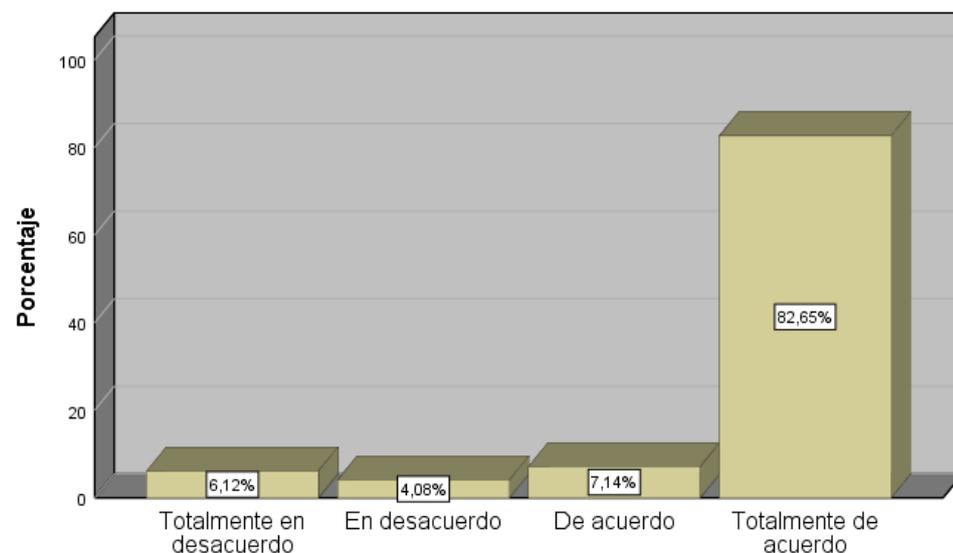
Fases del Ataque

5. ¿Considera usted que el Reconocimiento como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 15. *El Reconocimiento*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	6	6,1	6,1
	En desacuerdo	4	4,1	10,2
	De acuerdo	7	7,1	17,3
	Totalmente de acuerdo	81	82,7	100,0
	Total	98	100,0	

P5



P5

Figura 10. *El Reconocimiento*

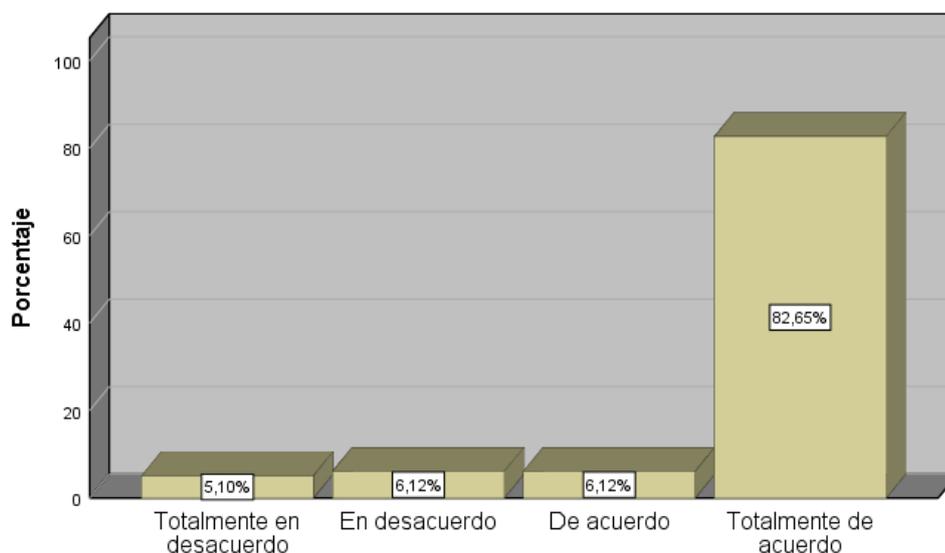
Análisis: En cuanto a si considera usted que el Reconocimiento como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 82,7%; que solo están de acuerdo un 7,1%; manifestaron que están en desacuerdo el 4,1%; y, manifestaron que están totalmente en desacuerdo un 6,1%.

6. ¿Considera usted que la Exploración como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 16. *La Exploración*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	5	5,1	5,1
	En desacuerdo	6	6,1	11,2
	De acuerdo	6	6,1	17,3
	Totalmente de acuerdo	81	82,7	100,0
	Total	98	100,0	

P6



P6

Figura 11. *La Exploración*

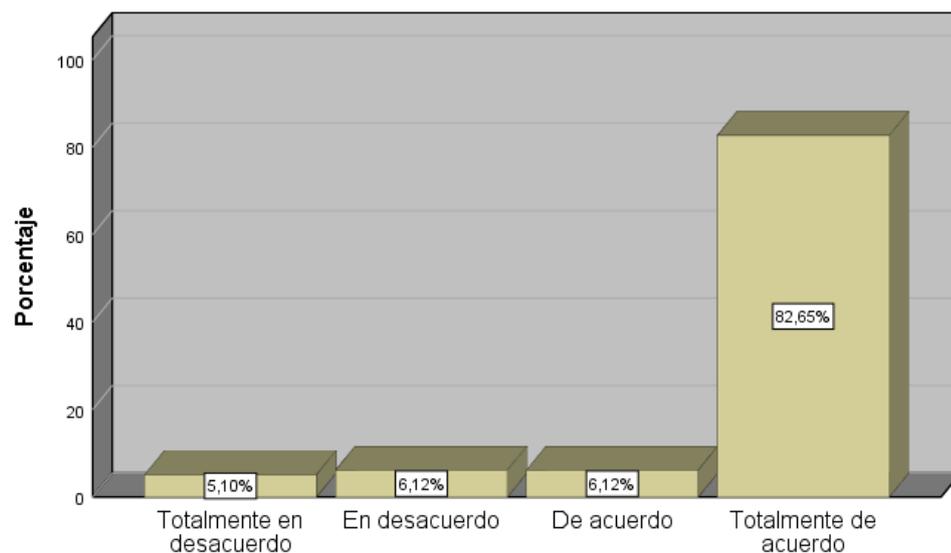
Análisis: En cuanto a si considera usted que la Exploración como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 82,7%; que solo están de acuerdo un 6,1%; manifestaron que están en desacuerdo el 6,1%; y, manifestaron que están totalmente en desacuerdo un 5,1%.

7. ¿Considera usted que el Obtener Acceso como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 17. *El Obtener Acceso*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	5	5,1	5,1
	En desacuerdo	6	6,1	11,2
	De acuerdo	6	6,1	17,3
	Totalmente de acuerdo	81	82,7	100,0
	Total	98	100,0	

P7



P7

Figura 12. *El Obtener Acceso*

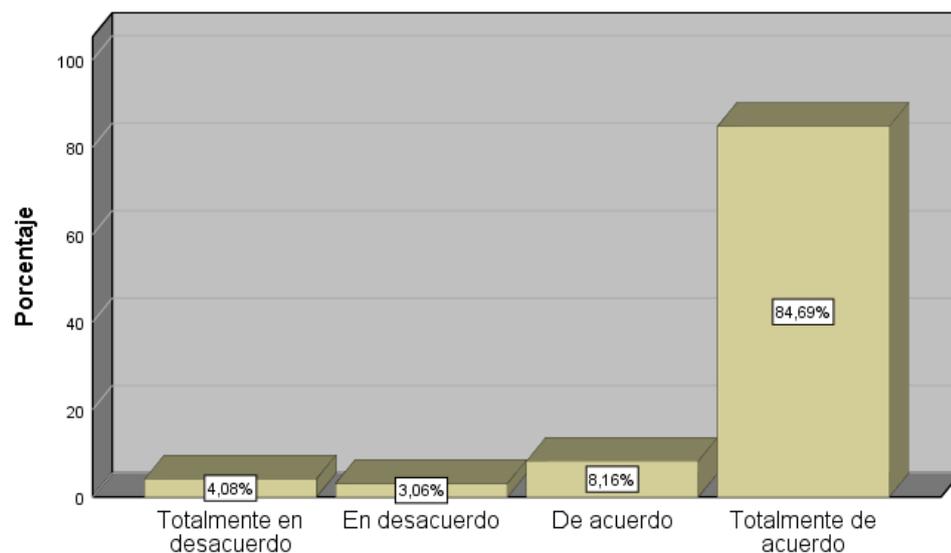
Análisis: En cuanto a si considera usted que el Obtener Acceso como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 82,7%; que solo están de acuerdo un 6,1%; manifestaron que están en desacuerdo el 6,1%; y, manifestaron que están totalmente en desacuerdo un 5,1%.

8. ¿Considera usted que el Mantener el Acceso como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 18. *El Mantener el Acceso*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	4	4,1	4,1
	En desacuerdo	3	3,1	7,1
	De acuerdo	8	8,2	15,3
	Totalmente de acuerdo	83	84,7	100,0
	Total	98	100,0	

P8



P8

Figura 13. *El Mantener el Acceso*

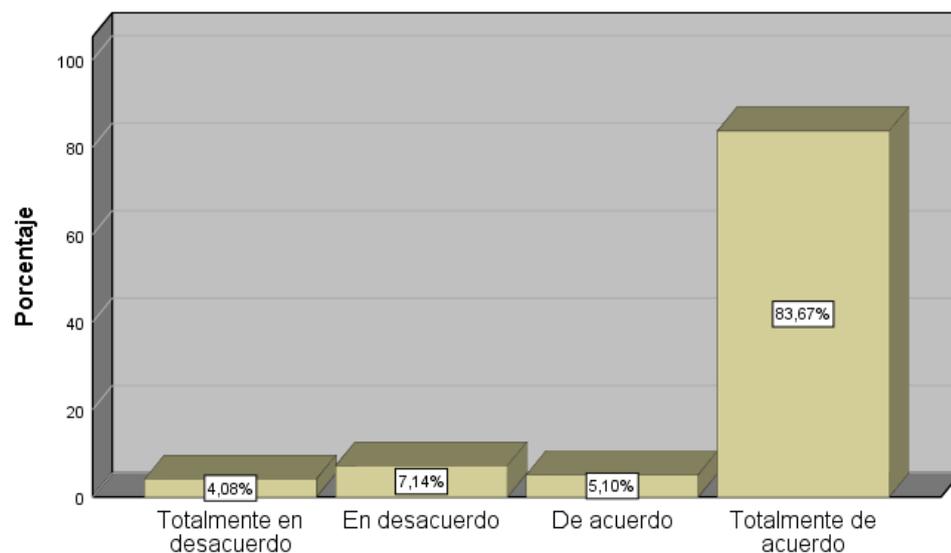
Análisis: En cuanto a si considera usted que el Mantener el Acceso como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 87,8%; que solo están de acuerdo un 2%; manifestaron que están en desacuerdo el 8,2%; y, manifestaron que están totalmente en desacuerdo un 2%.

9. ¿Considera usted que el Borrar Huellas como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 19. *El Borrar Huellas*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	4	4,1	4,1
	En desacuerdo	7	7,1	11,2
	De acuerdo	5	5,1	16,3
	Totalmente de acuerdo	82	83,7	100,0
	Total	98	100,0	

P9



P9

Figura 14. *El Borrar Huellas*

Análisis: En cuanto a si considera usted que el Borrar Huellas como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 83,7%; que solo están de acuerdo un 5,1%; manifestaron que están en desacuerdo el 7,1%; y, manifestaron que están totalmente en desacuerdo un 4,1%.

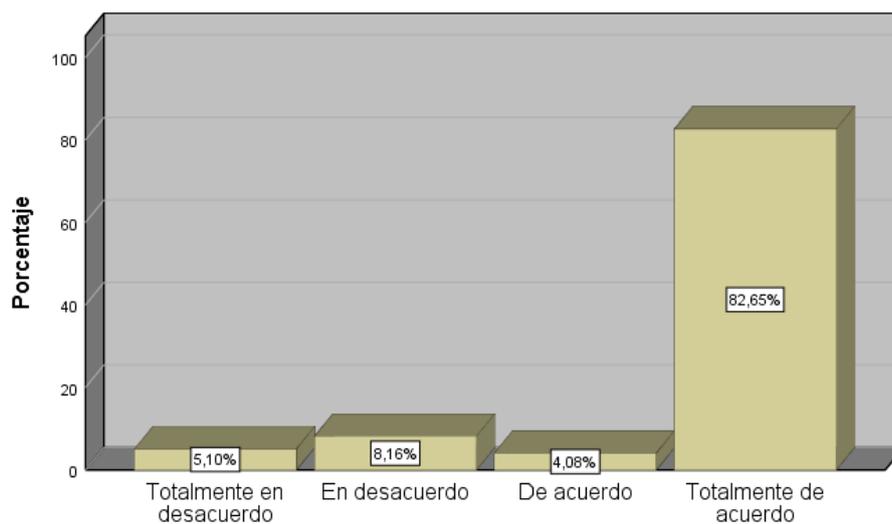
Medidas de Prevención

10. ¿Considera usted que el Modelo para prevenir ciberataques como uno de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 20. *Modelo para prevenir ciberataques*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	5	5,1	5,1
	En desacuerdo	8	8,2	13,3
	De acuerdo	4	4,1	17,3
	Totalmente de acuerdo	81	82,7	100,0
	Total	98	100,0	

P10



P10

Figura 15. *Modelo para prevenir ciberataques*

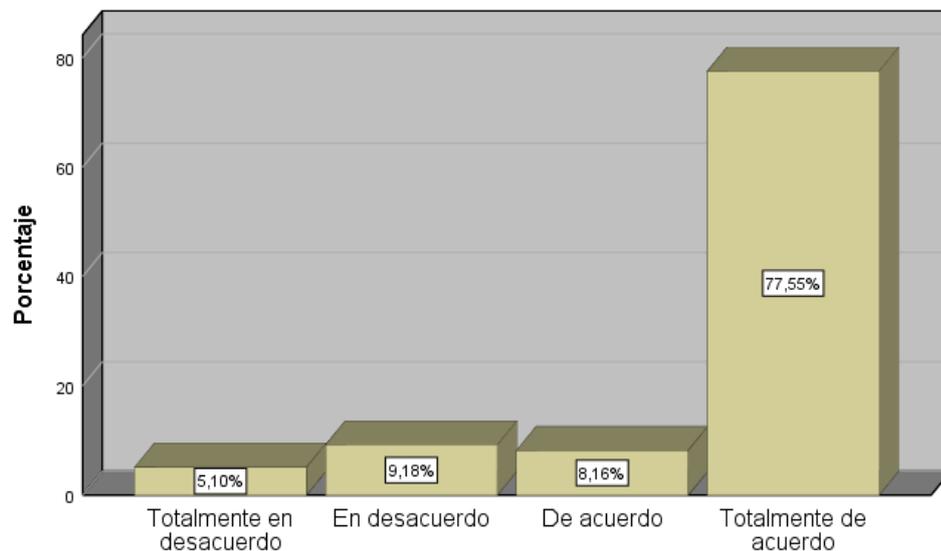
Análisis: En cuanto a si considera usted que el Modelo para prevenir ciberataques como uno de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 82,7%; que solo están de acuerdo un 4,1%; manifestaron que están en desacuerdo el 8,2%; y, manifestaron que están totalmente en desacuerdo un 5,1%.

11. ¿Considera usted que Implementación de un portal cautivo para la gestión de acceso a la red como una de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 21. *Implementación de un portal cautivo*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	5	5,1	5,1
	En desacuerdo	9	9,2	14,3
	De acuerdo	8	8,2	22,4
	Totalmente de acuerdo	76	77,6	100,0
	Total	98	100,0	

P11



P11

Figura 16. *Implementación de un portal cautivo*

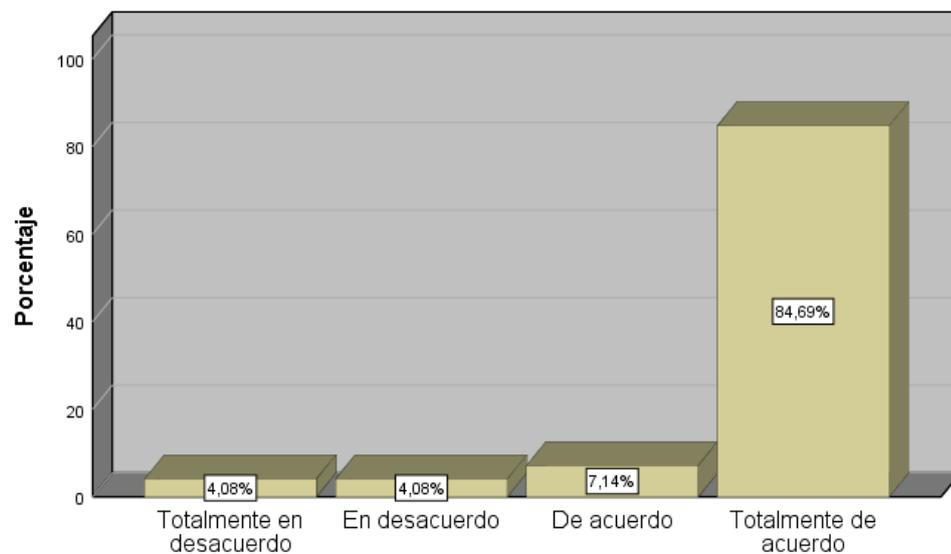
Análisis: En cuanto a si considera usted que Implementación de un portal cautivo para la gestión de acceso a la red como una de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 77,6%; que solo están de acuerdo un 8,2%; manifestaron que están en desacuerdo el 9,2%; y, manifestaron que están totalmente en desacuerdo un 5,1%.

12. ¿Considera usted que el Monitoreo de la red a través de software de gestión como una de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 22. *Monitoreo de la red a través de software de gestión*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	4	4,1	4,1
	En desacuerdo	4	4,1	8,2
	De acuerdo	7	7,1	15,3
	Totalmente de acuerdo	83	84,7	100,0
	Total	98	100,0	

P12



P12

Figura 17. *Monitoreo de la red a través de software de gestión*

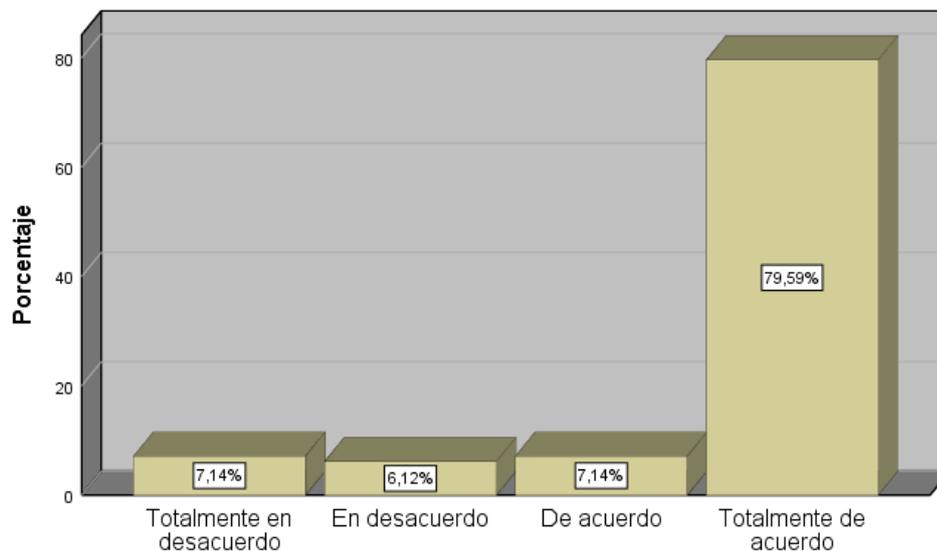
Análisis: En cuanto a si considera usted que el Monitoreo de la red a través de software de gestión como una de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 84,7; que solo están de acuerdo un 7,1%; manifestaron que están en desacuerdo el 4,1%; y, manifestaron que están totalmente en desacuerdo un 4,1%.

13. ¿Considera usted que las Políticas de seguridad en el servidor para la navegación como una de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 23. *Políticas de seguridad en el servidor para la navegación*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	7	7,1	7,1
	En desacuerdo	6	6,1	13,3
	De acuerdo	7	7,1	20,4
	Totalmente de acuerdo	78	79,6	100,0
	Total	98	100,0	

P13



P13

Figura 18. *Políticas de seguridad en el servidor para la navegación*

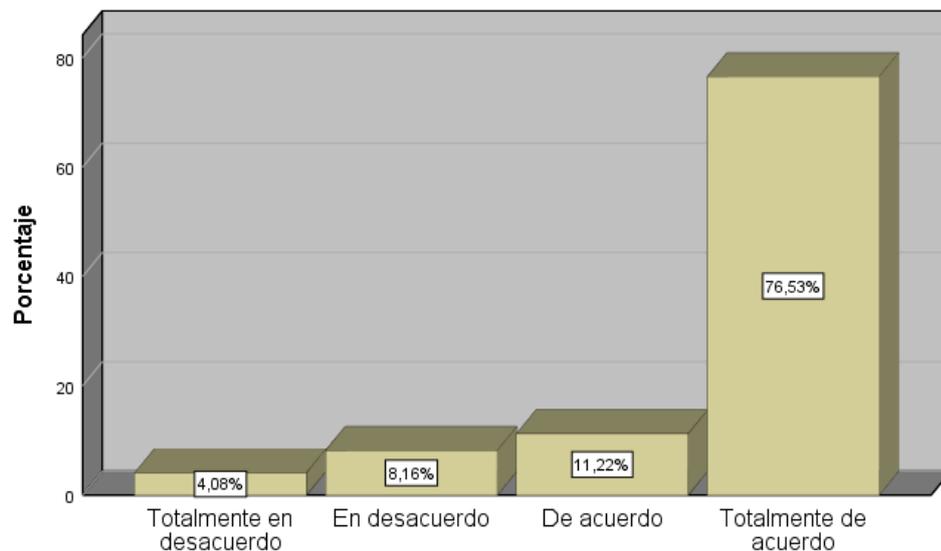
Análisis: En cuanto a si considera usted que las Políticas de seguridad en el servidor para la navegación como una de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 79,6%; que solo están de acuerdo un 7,1%; manifestaron que están en desacuerdo el 6,1%; y, manifestaron que están totalmente en desacuerdo un 7,1%.

14. ¿Considera usted que los Métodos de encriptación y protección de la información como una de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

Tabla 24. *Métodos de encriptación y protección de la información*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	4	4,1	4,1
	En desacuerdo	8	8,2	12,2
	De acuerdo	11	11,2	23,5
	Totalmente de acuerdo	75	76,5	100,0
	Total	98	100,0	

P14



P14

Figura 19. *Métodos de encriptación y protección de la información*

Análisis: En cuanto a si considera usted que los Métodos de encriptación y protección de la información como una de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020; manifestaron que están totalmente de acuerdo 76,58%; que solo están de acuerdo un 11,2%; manifestaron que están en desacuerdo el 8,2%; y, manifestaron que están totalmente en desacuerdo un 4,1%.

Para la Variable Y: Procesos Educativos

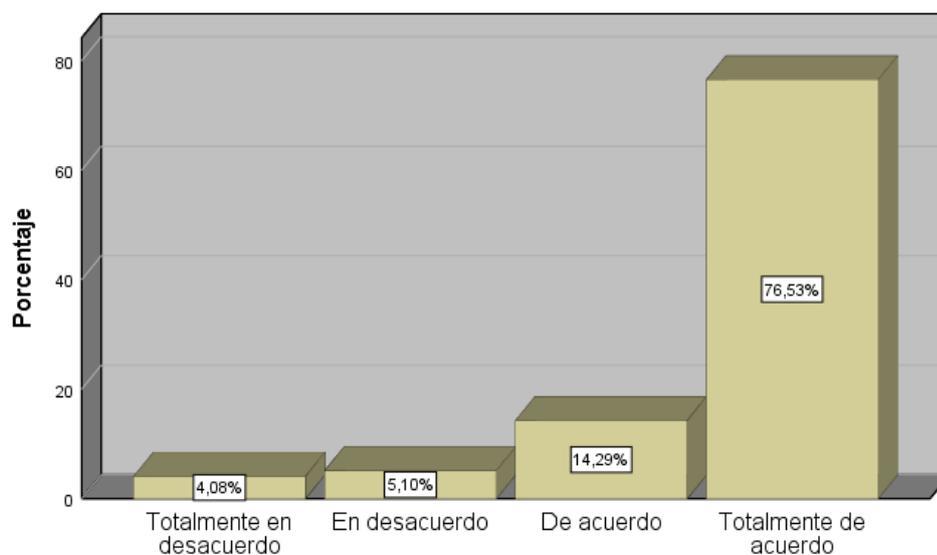
Ciencias y Humanidades

15. ¿Considera usted que el cumplimiento de los establecido por la Política Nacional de Seguridad dentro del área de Ciencias y Humanidades puede ser influido por los Ataques Cibernéticos?

Tabla 25. *La Política Nacional de Seguridad*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	4	4,1	4,1
	En desacuerdo	5	5,1	9,2
	De acuerdo	14	14,3	23,5
	Totalmente de acuerdo	75	76,5	100,0
	Total	98	100,0	

P15



P15

Figura 20. *La Política Nacional de Seguridad*

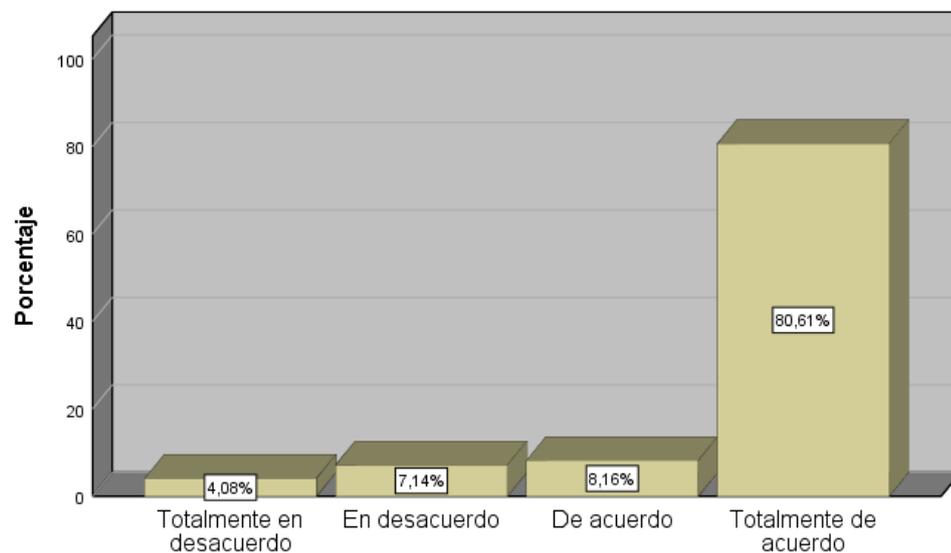
Análisis: En cuanto a si considera usted que el cumplimiento de los establecido por la Política Nacional de Seguridad dentro del área de Ciencias y Humanidades puede ser influido por los Ataques Cibernéticos; manifestaron que están totalmente de acuerdo 76,5%; que solo están de acuerdo un 14,3%; manifestaron que están en desacuerdo el 5,1%; y, manifestaron que están totalmente en desacuerdo un 4,1%.

16. ¿Considera usted que el cumplimiento de los establecido por los Tratados Internacionales dentro del área de Ciencias y Humanidades puede ser influidos por los Ataques Cibernéticos?

Tabla 26. *Los Tratados Internacionales*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	4	4,1	4,1
	En desacuerdo	7	7,1	11,2
	De acuerdo	8	8,2	19,4
	Totalmente de acuerdo	79	80,6	100,0
	Total	98	100,0	

P16



P16

Figura 21. *Los Tratados Internacionales*

Análisis: En cuanto a si considera usted que el cumplimiento de los establecido por los Tratados Internacionales dentro del área de Ciencias y Humanidades puede ser influidos por los Ataques Cibernéticos; manifestaron que están totalmente de acuerdo 80,6%; que solo están de acuerdo un 8,2%; manifestaron que están en desacuerdo el 7,1%; y, manifestaron que están totalmente en desacuerdo un 4,1%.

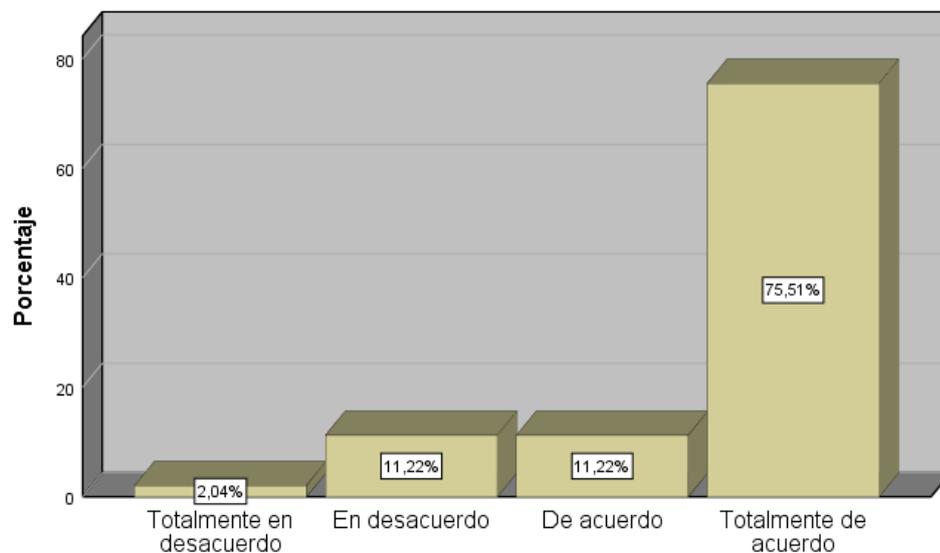
Ciencias Militares

17. ¿Considera usted que el cumplimiento de los establecido por la Doctrina Militar de Comunicaciones dentro del área de Ciencias Militares puede ser influido por los Ataques Cibernéticos?

Tabla 27. *La Doctrina Militar de Comunicaciones*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	2,0	2,0
	En desacuerdo	11	11,2	13,3
	De acuerdo	11	11,2	24,5
	Totalmente de acuerdo	74	75,5	100,0
	Total	98	100,0	

P17



P17

Figura 22. *La Doctrina Militar de Comunicaciones*

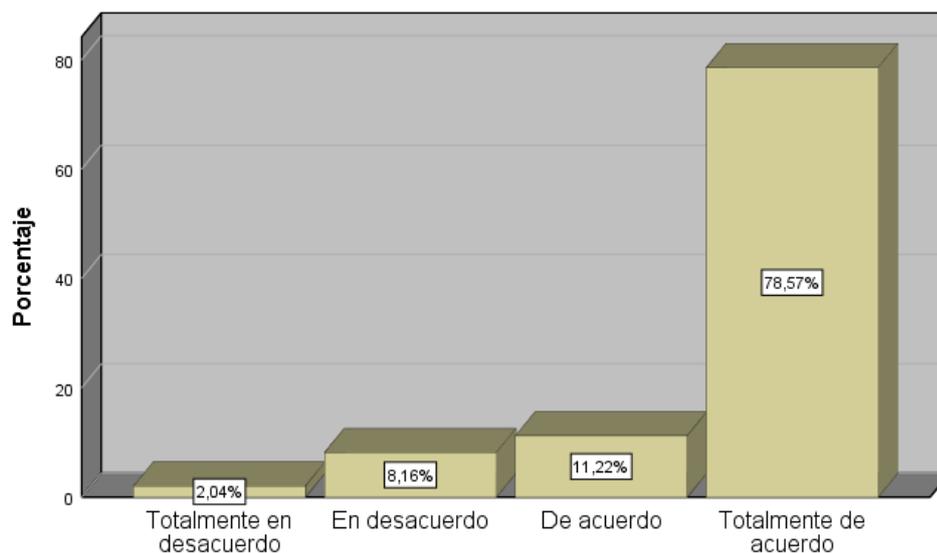
Análisis: En cuanto a si considera usted que el cumplimiento de los establecido por la Doctrina Militar de Comunicaciones dentro del área de Ciencias Militares puede ser influido por los Ataques Cibernéticos; manifestaron que están totalmente de acuerdo 75,5%; que solo están de acuerdo un 11,2%; manifestaron que están en desacuerdo el 11,2%; y, manifestaron que están totalmente en desacuerdo un 2%.

18. ¿Considera usted que el Planeamiento de Operaciones dentro del área de Ciencias Militares puede ser influido por los Ataques Cibernéticos?

Tabla 28. *El Planeamiento de Operaciones*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	2,0	2,0
	En desacuerdo	8	8,2	10,2
	De acuerdo	11	11,2	21,4
	Totalmente de acuerdo	77	78,6	100,0
	Total	98	100,0	

P18



P18

Figura 23. *El Planeamiento de Operaciones*

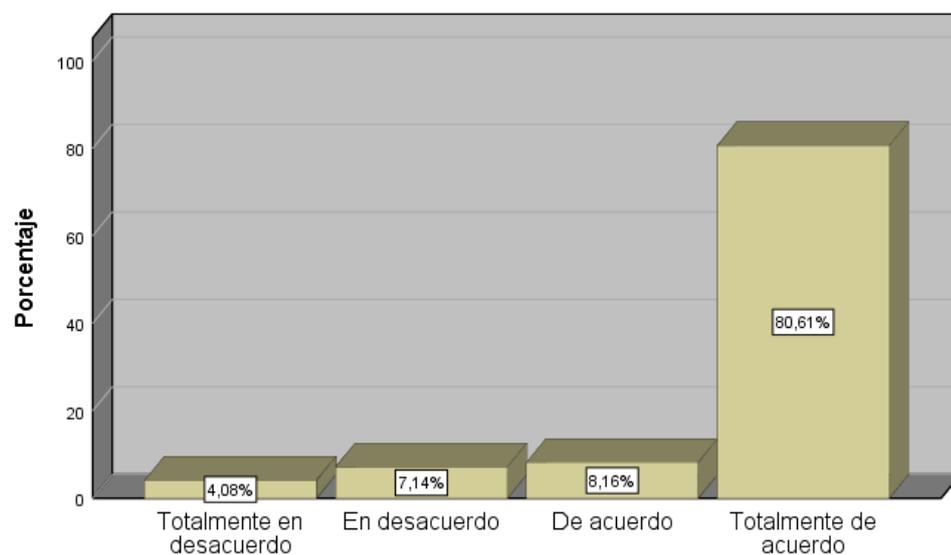
Análisis: En cuanto a si Considera usted que el Planeamiento de Operaciones dentro del área de Ciencias Militares puede ser influido por los Ataques Cibernéticos; manifestaron que están totalmente de acuerdo 78,6%; que solo están de acuerdo un 11,2%; manifestaron que están en desacuerdo el 8,2%; y, manifestaron que están totalmente en desacuerdo un 2%.

19. ¿Considera usted que la Aplicación de la Guerra Ciberdefensa dentro del área de Ciencias Militares puede ser influido por los Ataques Cibernéticos?

Tabla 29. *La Aplicación de la Guerra Ciberdefensa*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Totalmente en desacuerdo	4	4,1	4,1
	En desacuerdo	7	7,1	11,2
	De acuerdo	8	8,2	19,4
	Totalmente de acuerdo	79	80,6	100,0
	Total	98	100,0	

P19



P19

Figura 24. *La Aplicación de la Guerra Ciberdefensa*

Análisis: En cuanto a si considera usted que la Aplicación de la Guerra Ciberdefensa dentro del área de Ciencias Militares puede ser influido por los Ataques Cibernéticos; manifestaron que están totalmente de acuerdo 80,6%; que solo están de acuerdo un 8,2%; manifestaron que están en desacuerdo el 7,1%; y, manifestaron que están totalmente en desacuerdo un 4,1%.

4.2. Interpretación de resultados

Para la prueba de hipótesis se utilizó la Chi cuadrada para datos cuantitativos, estableciéndose en base a los resultados obtenidos, conclusiones para la hipótesis general y las hipótesis específicas.

4.2.1. Prueba de hipótesis general

La Prevención de Ataques Cibernéticos se relaciona significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

De los instrumentos de medición:

A su opinión ¿La Prevención de Ataques Cibernéticos se relaciona significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

- Se relaciona.
- No se relaciona.

Calculo de la CHI Cuadrada:

Tabla 32. *Pruebas de chi-cuadrado – hipótesis general*

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	5,313 ^a	131	,158
Razón de verosimilitud	3,127	131	1,000
Asociación lineal por lineal	3,936	1	,000
N de casos válidos	98		

a. 612 casillas (100.0%) han esperado un recuento menor que 5. El recuento mínimo esperado es .02.

$$X^2 = 0.05$$

G = Grados de libertad

(r) = Número de filas

(c) = Número de columnas

$$G = (r - 1) (c - 1)$$

$$G = (2 - 1) (2 - 1) = 1$$

Con un (1) grado de libertad entramos a la tabla y un nivel de confianza de 95% que para el valor de alfa es 0.05.

De la tabla Chi Cuadrada: 0.158

Valor encontrado en el proceso: $X^2 = 0.05$

Conclusión para la hipótesis general:

El valor calculado para la Chi cuadrada (0.158) es mayor que el valor que aparece en la tabla (0.05) para un nivel de confianza de 95% y un grado de libertad. Por lo que se adopta la decisión de no rechazar la hipótesis general nula y se acepta la hipótesis general alterna.

Esto quiere decir que la Prevención de Ataques Cibernéticos se relaciona significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

4.2.2. Prueba de hipótesis específica 1

Los Tipos de Ataques Cibernéticos según el Objetivo se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

De los instrumentos de medición:

A su opinión ¿Los Tipos de Ataques Cibernéticos según el Objetivo se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

- Se relaciona.
- No se relaciona.

Calculo de la CHI Cuadrada:

Tabla 33. Pruebas de chi-cuadrado – hipótesis específica 1

	Valor	gl	Sig. asintótica (2 carar)
Chi-cuadrado de Pearson	4,500 ^a	157	,198
Razón de verosimilitud	2,133	157	1,000
Asociación lineal por lineal	1,745	1	,000
N de casos válidos	98		

a. 396 casillas (100.0%) han esperado un recuento menor que 5. El recuento mínimo esperado es .02.

$$X^2 = 0.05$$

G = Grados de libertad

(r) = Número de filas

(c) = Número de columnas

$$G = (r - 1) (c - 1)$$

$$G = (2 - 1) (2 - 1) = 1$$

Con un (1) grado de libertad entramos a la tabla y un nivel de confianza de 95% que para el valor de alfa es 0.05.

De la tabla Chi Cuadrada: 0.198

Valor encontrado en el proceso: $X^2 = 0.05$

Conclusión para la hipótesis específica 1:

El valor calculado para la Chi cuadrada (0.198) es mayor que el valor que aparece en la tabla (0.05) para un nivel de confianza de 95% y un grado de libertad. Por lo que se adopta la decisión de no rechazar la hipótesis específica 1 nula y se acepta la hipótesis general alterna.

Esto quiere decir que los Tipos de Ataques Cibernéticos según el Objetivo se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

4.2.3. Prueba de hipótesis específica 2

Las Fases del Ataque se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

De los instrumentos de medición:

A su opinión ¿Las Fases del Ataque se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

- Se relaciona.
- No se relaciona.

Calculo de la CHI Cuadrada:

Tabla 34. Pruebas de chi-cuadrado – hipótesis específica 2

	Valor	Gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	3,513 ^a	113	,212
Razón de verosimilitud	2,090	113	1,000
Asociación lineal por lineal	3,297	1	,000
N de casos válidos	98		

a. 360 casillas (100.0%) han esperado un recuento menor que 5. El recuento mínimo esperado es .02.

$$X^2 = 0.05$$

G = Grados de libertad

(r) = Número de filas

(c) = Número de columnas

$$G = (r - 1) (c - 1)$$

$$G = (2 - 1) (2 - 1) = 1$$

Con un (1) grado de libertad entramos a la tabla y un nivel de confianza de 95% que para el valor de alfa es 0.05.

De la tabla Chi Cuadrada: 0.212

Valor encontrado en el proceso: $X^2 = 0.05$

Conclusión para la hipótesis específica 2:

El valor calculado para la Chi cuadrada (0.212) es mayor que el valor que aparece en la tabla (0.05) para un nivel de confianza de 95% y un grado de libertad. Por lo que se adopta la decisión de no rechazar la hipótesis específica 2 nula y se acepta la hipótesis general alterna.

Esto quiere decir que las Fases del Ataque se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

4.2.4. Prueba de hipótesis específica 3

Las Medidas de Prevención de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

De los instrumentos de medición:

A su opinión ¿Las Medidas de Prevención se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?

- Se relaciona.
- No se relaciona.

Calculo de la CHI Cuadrada:Tabla 35. *Pruebas de chi-cuadrado – hipótesis específica 3*

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	3,925 ^a	140	,115
Razón de verosimilitud	3,041	140	1,000
Asociación lineal por lineal	1,513	1	,000
N de casos válidos	98		

a. 378 casillas (100.0%) han esperado un recuento menor que 5. El recuento mínimo esperado es .02.

$$X^2 = 0.05$$

G = Grados de libertad

(r) = Número de filas

(c) = Número de columnas

$$G = (r - 1) (c - 1)$$

$$G = (2 - 1) (2 - 1) = 1$$

Con un (1) grado de libertad entramos a la tabla y un nivel de confianza de 95% que para el valor de alfa es 0.05.

De la tabla Chi Cuadrada: 0.115

Valor encontrado en el proceso: $X^2 = 0.05$

Conclusión para la hipótesis específica 3:

El valor calculado para la Chi cuadrada (0.115) es mayor que el valor que aparece en la tabla (0.05) para un nivel de confianza de 95% y un grado de libertad. Por lo que se adopta la decisión de no rechazar la hipótesis general nula y se acepta la hipótesis general alterna.

Esto quiere decir que las Medidas de Prevención se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

4.3. Discusión de resultados

4.3.1. Hipótesis General

Después del análisis de los datos que proporciono el trabajo estadístico respecto a la Hipótesis General, que a la letra dice: La Prevención de Ataques Cibernéticos se relaciona significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020. Podemos establecer que:

Una vez contrastado el resultado el resultado de la hipótesis general, encontramos que tiene relación con la tesis de Aguirre, A. (2017). En su tesis de Maestría, titulada: “*Ciberseguridad en Infraestructuras Críticas de Información*”. Universidad de Buenos Aires. Buenos Aires. Argentina. El cual concluyo que: La mayoría de los sectores que están utilizando tecnologías de información, proveen servicios importantes a la población. Sin embargo, debido a la falta de metodologías de clasificación de estos servicios, no se ha podido identificar cuáles son realmente críticos y que, por lo tanto, cuáles requieren una protección acorde por parte de los operadores que los proveen. Un aporte adicional del trabajo es el análisis del estado actual de la ciberseguridad en el Ecuador. En esta sección se analiza la situación de ese país, incluyendo las normativas y regulaciones que ha desarrollado para fortalecer la ciberseguridad en las empresas públicas y a nivel privado”.

4.3.2. Hipótesis Especifica 1

Después del análisis de los datos que proporciono el trabajo estadístico respecto a la Hipótesis Especifica 1, que a la letra dice: Los Tipos de Ataques Cibernéticos según el Objetivo se relacionan significativamente con los

Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020. Podemos establecer que:

Una vez contrastado el resultado el resultado de la hipótesis específica 1, encontramos que tiene relación con la tesis de Arias, N. & Celis, J. (2015). En su trabajo de grado presentado como requisito para obtener el Título Profesional de Ingenieros de Sistemas, titulado: “*Modelo Experimental de Ciberseguridad y Ciberdefensa para Colombia*”. Universidad Libre. Bogotá. Colombia. Llegaron a la siguiente conclusión: “el programa de ingeniería de sistemas de la universidad libre gracias a la dirección de la línea de formación electiva en seguridad informática proyecta su función como constructor de soluciones esquematizando descriptivamente un modelo de ínter nacional para Ciberseguridad y defensa”.

4.3.3. Hipótesis Específica 2

Después del análisis de los datos que proporciono el trabajo estadístico respecto a la Hipótesis Específica 2, que a la letra dice: Los Tipos de Ataques Cibernéticos según el Objetivo se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020. Podemos establecer que:

Una vez contrastado el resultado el resultado de la hipótesis específica 2, encontramos que tiene relación con la tesis de Vargas, E. (2014). En su trabajo de grado para optar al título de Especialista en Alta Gerencia de la Defensa Nacional, titulado: “*Ciberseguridad y Ciberdefensa: ¿Qué implicaciones tienen para la Seguridad Nacional?*”. Universidad Militar Nueva Granada. Bogotá. Colombia. El cual llevo a la siguiente conclusión: “las tecnologías de información y telecomunicaciones van avanzando a un ritmo más rápido al pasar de los días. Por ello, es importante estar a la vanguardia de los mecanismos para salvaguardar no solo la información sensible de los pobladores de un país o el ataque a una página oficial que se cataloga como un ataque de baja intensidad, sino también tener sistemas de

defensa que permitan proteger las infraestructuras críticas que con el paso del tiempo son más dependientes del ciberespacio y si no se protegen la sociedad estaría presenciando un ataque de alta intensidad”.

4.3.4. Hipótesis Específica 3

Después del análisis de los datos que proporciono el trabajo estadístico respecto a la Hipótesis Específica 3, que a la letra dice: Las Medidas de Prevención se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020. Podemos establecer que:

Una vez contrastado el resultado el resultado de la hipótesis específica 3, encontramos que tiene relación con la tesis de Inoguchi, A. & Macha, E. (2017). En su tesis para optar el grado de Bachiller en Ingeniería Empresarial y de Sistemas, titulado: *“Gestión de la Ciberseguridad y Prevención de los ataques Cibernéticos en las Pymes del Perú, 2016”*. Universidad San Ignacio de Loyola. Lima. Perú. Los cuales concluyeron que: “La Empresa Zavala Cargo S.A.C. tiene una falta del uso de planes contra ataques de Seguridad Cibernética, que resguarden su información cibernética permitiendo así una toma de decisiones más confiable”.

CONCLUSIONES

1. De acuerdo a la Hipótesis General que a la letra dice que, la Prevención de Ataques Cibernéticos se relaciona significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020. El valor calculado para la Chi cuadrada $0.158 > 0.05$ para un nivel de confianza de 95% y un grado de libertad. Hemos podido concluir mediante las encuestas que dicha hipótesis es válida; ya que la Prevención de Ataques Cibernéticos que incluyen los tipos de ataque cibernético, las fases del ataque y los métodos de ataque; buscando proporcionar seguridad cibernética y potenciar los procesos educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.
2. De acuerdo a la Hipótesis Especifica 1 que a la letra dice que, los Tipos de Ataques Cibernéticos según el Objetivo se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020. El valor calculado para la Chi cuadrada $0.198 > 0.05$ para un nivel de confianza de 95% y un grado de libertad. Hemos podido concluir mediante las encuestas que dicha hipótesis es válida; ya que los Tipos de Ataques Cibernéticos según el Objetivo incluye la interrupción, interceptación, la modificación y la generación; buscando proporcionar seguridad cibernética ante cada tipo de ataque y potenciar los procesos educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.
3. De acuerdo a la Hipótesis Especifica 2 que a la letra dice que, las Fases del Ataque se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020. El valor calculado para la Chi cuadrada $0.212 > 0.05$) para un nivel de confianza de 95% y un grado de libertad. Hemos podido concluir mediante las encuestas que dicha hipótesis es válida; ya que las Fases del Ataque incluyen el reconocimiento, la explotación, el obtener acceso, el mantener el acceso y el borrar las huellas; buscando proporcionar seguridad cibernética durante cada fase del ataque y

potenciar los procesos educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

4. De acuerdo a la Hipótesis Especifica 3 que a la letra dice que, las Medidas de Prevención se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020. El valor calculado para la Chi cuadrada $0.115 > 0.05$) para un nivel de confianza de 95% y un grado de libertad. Hemos podido concluir mediante las encuestas que dicha hipótesis es válida; ya que los Métodos de Ataque incluyen los códigos maliciosos, los virus informáticos, las bombas lógicas, las capturas de cuenta y contraseña, los fraudes, engaños y extorsiones y la inyección de SQL; buscando proporcionar seguridad cibernética durante cada método de ataque y potenciar los procesos educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

RECOMENDACIONES

1. Teniendo en consideración que la Prevención de los Ataques Cibernéticos que incluyen los tipos de ataque cibernético, las fases del ataque y los métodos de ataque son de mucha importancia para consolidar los Procesos Educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”; es recomendable se incremente y/o complemente la instrucción existente respecto a la Prevención de los Ataques Cibernéticos, orientada a la optimización de los Procesos Educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.
2. Teniendo en consideración que los Tipos de Ataques Cibernéticos según el Objetivo incluye la interrupción, interceptación, la modificación y la generación, son de mucha importancia para consolidar los Procesos Educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”; es recomendable se incremente y/o complemente la instrucción existente respecto a los Tipos de Ataques Cibernéticos, orientada a la optimización de los Procesos Educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.
3. Teniendo en consideración que las Fases del Ataque incluyen el reconocimiento, la explotación, el obtener acceso, el mantener el acceso y el borrar las huellas, son de mucha importancia para consolidar los Procesos Educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”; es recomendable se incremente y/o complemente la instrucción existente respecto a las Fases de los Ataques Cibernéticos, orientada a la optimización de los Procesos Educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.
4. Teniendo en consideración que las Medidas de Prevención incluyen los códigos maliciosos, los virus informáticos, las bombas lógicas, las capturas de cuenta y contraseña, los fraudes, engaños y extorsiones y la inyección de SQL, son de mucha

importancia para consolidar los Procesos Educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”; es recomendable se incremente y/o complemente la instrucción existente respecto a los Métodos de Ataque Cibernéticos, orientada a la optimización de los Procesos Educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

PROPUESTA DE MEJORA

“BLOQUEAR LOS ATAQUES CIBERNETICOS A LA ESCUELA MILITAR DE CHORRILLOS”

1. PRESENTACIÓN

Empezaremos recordando que la seguridad cibernética implica proteger la infraestructura destinada a las plataformas cibernéticas previniendo, detectando y respondiendo a los incidentes en la red. A diferencia de las amenazas físicas que producen una acción inmediata como “detenerse, agacharse y girar” en caso de incendio, las amenazas cibernéticas son a menudo difíciles de identificar y de entender. Entre estos peligros se encuentran los virus que eliminan sistemas enteros, intrusos que entran a los sistemas y alteran archivos, quienes usan su computadora o dispositivo para atacar a otros o intrusos que roban información confidencial. La gama de riesgos cibernéticos es ilimitada: las amenazas, algunas más serias y elaboradas que otras, pueden tener un gran efecto en el individuo, la comunidad, las organizaciones y el país. La principal amenaza que afecta a las plataformas cibernéticas de una institución estatal o privada, militar o civil es el desconocimiento del concepto de esta, la confidencialidad, la integridad y los niveles de disponibilidad de la información que se deben manejar no son los adecuados. Dejando así a la institución afectada con serios inconvenientes como el retraso de su continuidad operacional diaria la cual tiene como consecuencia una significativa pérdida de ingresos monetarios y contratiempos no pronosticados en la producción esperada. Hoy en día existen muchos factores que amenazan la seguridad de información de las instituciones estatales o privadas, militares o civiles dentro de las cuales está incluida la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” y por lo general el presupuesto destinado para la proteger y resguardar la plataforma cibernética no es el suficiente; tener identificadas y controladas las vulnerabilidades de la información interna en la red se logra con un correcto plan de seguridad generado gracias a un análisis de riesgo previo. Con la finalidad de minimizar los riesgos que traen consigo los Ataques Cibernéticos a la plataforma de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” y conocer la importancia de

salvaguardar la información virtual en sus redes privadas, es que se presenta esta investigación.

2. JUSTIFICACIÓN

Con esta investigación ayudaremos a fomentar una cultura de prevención y detección de riesgos cibernéticos en los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, se dará a conocer sobre el peligro que representa no estar preparado para los diferentes ataques cibernéticos que existen actualmente y se brindará información de cómo elaborar los planes de acción y estrategias basadas en minimizar los riesgos.

Esta investigación es importante porque los estudios realizados por especialistas en ciberseguridad señalan que los ataques cibernéticos han evolucionado, los hackers están desarrollando softwares maliciosos cada vez más sofisticados con el fin de buscar vulnerabilidades en los sistemas interconectados para sustraer información digital con el fin de lograr su objetivo.

Para ello con el conocimiento adecuado de los aspectos formales y legales acerca de la importancia de la seguridad cibernética para minimizar los riesgos, la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” tendrá el enfoque necesario para establecer una nueva política de seguridad y por ende nuevas directivas que garanticen la seguridad cibernética; garantizando a la vez, la confidencialidad de la información que es compartida por parte de los cadetes de todos y cada uno de los años académicos dentro de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

3. OBJETIVOS DE LA PROPUESTA

3.1. Objetivo general

Prevenir de forma activa los Ataques Cibernéticos, promoviendo la optimización del Proceso Educativo de los cadetes de 4to año de

Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

3.2. Objetivos específicos

- Detectar y prevenir los Tipos de Ataques Cibernéticos según el Objetivo que perjudiquen los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.
- Evitar el desarrollo de las Fases del Ataque que perjudiquen los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.
- Evitar el desarrollo de los Métodos de Ataque que perjudiquen los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

4. META

Lograr que los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, optimicen y consoliden sus Procesos Educativos que les permitirá obtener los conocimientos necesarios para prevenir los ataques cibernéticos como cadetes y como oficiales del arma de Comunicaciones.

5. METODOLOGÍA

Los procedimientos, técnicas e instrumentos utilizados en las actividades militares y académicas, tendrán una directriz procesual, pues ya no se trata simplemente de desarrollar contenidos, sino de lograr procesos donde se consiga la apropiación, manejo, interiorización y uso proactivo de los valores institucionales.

5.1. Plan de acción

Presentar una propuesta con medidas que incrementen y/o complementen las ya existentes, a fin de optimizar la Prevención de los Ataques Cibernéticos y

los Procesos Educativos de los cadetes de 4to año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

5.2. Actividades

- Elaborar propuesta especificando los aspectos por incorporar.
- Solicitar audiencia en el Sr General Director de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, el Sub Director Académico, el Comandante Jefe de Batallón de Cadetes, el S-3 (Instrucción y Operaciones) y el S-2 (Oficial de Inteligencia).
- Exponer la propuesta.
- Realizar la complementación de la currícula de estudio.
- Presentar el trabajo terminado.
- Coordinar con el Departamento Académico y el Batallón de Cadetes para materializar la propuesta.

5.3. Temporalización

La ejecución del proyecto debe estar enmarcado en el periodo de tiempo marzo 2020 a noviembre 2020.

6. RESPONSABLES

La ejecución de la propuesta estará a cargo de los cadetes de 4to año de Infantería de la Escuela Militar de Chorrillos, bajo la supervisión de sus Jefes de Sección, Jefes de Área, el S-2, el S-3, el Comandante del Batallón de Cadetes y Jefe del Departamento Académico de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

7. VIABILIDAD

La propuesta es viable, toda vez que la materialización de la propuesta no requiere de ningún recurso económico para su cristalización.

8. SEGUIMIENTO Y EVALUACIÓN

El Plan de Mejora, es de interés de la Escuela Militar de Chorrillos; por lo tanto, a este nivel el seguimiento y evaluación dependerá del estudio que haga el comando de la Escuela al respecto. Dicho seguimiento se dará especial relevancia a la evaluación en dos sentidos:

- *Evaluación de Procesos.* La evaluación procesual (durante el desarrollo de las actuaciones) se realizará a lo largo de todo el proceso de implementación de las distintas actuaciones contempladas dentro del Plan de Mejora, con el fin de comprobar, optimizar y mejorar el desarrollo del mismo.
- *Evaluación Final.* Con el fin de valorar el grado de consecución de los objetivos propuestos, la evaluación final (reflexión y síntesis al término de las actuaciones) tendrá en cuenta aspectos tanto cuantitativos como cualitativos.

REFERENCIAS BIBLIOGRAFICAS

- Aguilera, P. (2011). *Redes seguras (Seguridad informática)*. Madrid, España: Editex.
- Aguirre, A. (2017). En su tesis de Maestría, titulada: “*Ciberseguridad en Infraestructuras Críticas de Información*”. Universidad de Buenos Aires. Buenos Aires. Argentina
- Álvarez Marañón G. (2009). *Como protegernos de los peligros internet* España: Catarata
- Arias, N. & Celis, J. (2015). En su trabajo de grado presentado como requisito para obtener el Título Profesional de Ingenieros de Sistemas, titulado: “*Modelo Experimental de Ciberseguridad y Ciberdefensa para Colombia*”. Universidad Libre. Bogotá. Colombia
- Beekman, G. (2004). *Introducción a la Informática*. Madrid: Pearson Educación. 1ra Edición
- Bruderer, R. (2019). En su tesis para optar por el Título de Ingeniero Informático, titulada: “*Diseño de un modelo de ciberseguridad para dispositivos móviles en el sector empresarial*”. Pontificia Universidad Católica del Perú. Lima. Perú
- Colle, R. (2000). *Internet: un cuerpo enfermo y un campo de batalla*. Revista Latina de Comunicación Social
- Da Costa, C. (1992). *Fundamentos de Tecnología Documental*. Madrid: Complutense. 1ra Edición
- Erique, E. (2018). En su tesis previa a la obtención del Título de Magíster en Telecomunicaciones, titulada: “*Modelo de Prevención de Seguridad para un Sistema de Telecomunicaciones*”. Escuela Superior Politécnica del Litoral. Guayaquil. Ecuador
- Gris, M. (2010). *Clave Iniciación a Internet*. Barcelona: ENI. 1ra Edición

- Hernández, R.; Baptista, P. y Fernández, C. (2014). *Metodología de la investigación*. (6.ta ed.). México: Mc Graw-Hill.
- Inoguchi, A. & Macha, E. (2017). En su tesis para optar el grado de Bachiller en Ingeniería Empresarial y de Sistemas, titulado: “*Gestión de la Ciberseguridad y Prevención de los ataques Cibernéticos en las Pymes del Perú, 2016*”. Universidad San Ignacio de Loyola. Lima. Perú
- Marroqui, N. (2010). *Tras los pasos de un Hacker*. Estados Unidos de Norte América: 1ra Edición
- Mieres, J. (2009). *Ataques Informáticos*
- Pardo, C. (1993). *Microinformática de gestión*. Oviedo: McGraw-Hill. 1ra Edición
- Parsons J. (2008). *Conceptos de Computación: Nuevas Perspectivas*. México: Cengage Learning Editores, S.A. de C.V. 10 Edición
- Popper, K R., (1981) *La miseria del historicismo*, Madrid.
- RIVAS, F. (1997): *El proceso de enseñanza/Aprendizaje en la situación educativa*. Barcelona: Ariel.
- Rivera, A. (2019). En su tesis para optar el grado académico de maestro en Gestión Empresarial, titulado: “*Riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del Distrito de Yanacancha – Pasco 2016*”. Universidad Nacional Daniel Alcides Carrión. Cerro de Pasco. Perú
- Royer, J. (2004). *Seguridad en la Informática de Empresa: Riesgos, Amenazas, Prevención y Soluciones*. España: ENI. 1ra Edición
- Sánchez, G. (2008). *Ciberterrorismo: La guerra del siglo XXI*. El Viejo Topo, marzo, 242

Tamayo y Tamayo, M. (2006). Técnicas de Investigación. (2ª Edición). México: Editorial Mc Graw Hill.

Thomas, T. (2001). Las estrategias electrónicas de China. *Military Review*, julio-agosto, 72-79

Vargas, E. (2014). En su trabajo de grado para optar al título de Especialista en Alta Gerencia de la Defensa Nacional, titulado: “*Ciberseguridad y Ciberdefensa: ¿Qué implicaciones tienen para la Seguridad Nacional?*”. Universidad Militar Nueva Granada. Bogotá. Colombia

Anexo 1



Matriz de consistencia

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA
<p>Problema General</p> <p>¿Cuál es la relación que existe entre la Prevención de Ataques Cibernéticos y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?</p> <p>Problemas Específicos</p> <p>¿Cuál es la relación que existe entre los Tipos de Ataques Cibernéticos según el Objetivo y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?</p> <p>¿Cuál es la relación que existe entre las Fases del Ataque y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?</p> <p>¿Cuál es la relación que existe entre las Medidas de Prevención y los Procesos Educativos de los cadetes de 4to año de la Escuela</p>	<p>Objetivo General</p> <p>Determinar cuál es la relación que existe entre la Prevención de Ataques Cibernéticos y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.</p> <p>Objetivos Específicos</p> <p>Establecer cuál es la relación que existe entre los Tipos de Ataques Cibernéticos según el Objetivo y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.</p> <p>Establecer cuál es la relación que existe entre las Fases del Ataque y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.</p> <p>Establecer cuál es la relación que existe entre las Medidas de Prevención y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de</p>	<p>Hipótesis General</p> <p>La Prevención de Ataques Cibernéticos se relaciona significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.</p> <p>Hipótesis Específicas</p> <p>Los Tipos de Ataques Cibernéticos según el Objetivo se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.</p> <p>Las Fases del Ataque se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.</p> <p>Las Medidas de Prevención se relacionan significativamente con los Procesos Educativos de los cadetes de 4to año de la Escuela</p>	<p>Variable Independiente</p> <p>(X)</p> <p>Prevención de Ataques Cibernéticos</p>	<p>X₁ Tipos de Ataques Cibernéticos según el Objetivo</p> <p>X₂ Fases del Ataque</p> <p>X₃ Medidas de Prevención</p>	<ul style="list-style-type: none"> • Interrupción • Interceptación • Modificación • Generación <ul style="list-style-type: none"> • Reconocimiento • Exploración • Obtener Acceso • Mantener el acceso • Borrar huellas <ul style="list-style-type: none"> • Modelo para prevenir ciberataques • Implementación de un portal cautivo para la gestión de acceso a la red • Monitoreo de la red a través de software de gestión • Políticas de seguridad en el servidor para la navegación • Métodos de encriptación y protección de la información <ul style="list-style-type: none"> • Política Nacional de Seguridad • Convenio de Ginebra • Tratados Internacionales 	<p>Tipo / Nivel investigación</p> <p>Descriptivo-Correlacional</p> <p>Diseño de investigación</p> <p>No Experimental</p> <p>Enfoque de investigación</p> <p>Cuantitativo</p> <p>Técnica</p> <p>Se ha aplicado:</p> <ul style="list-style-type: none"> • Investigación documental • Investigación de campo <p>Instrumentos</p> <p>Se utilizó:</p> <ul style="list-style-type: none"> • Cuestionarios • Encuestas <p>Población</p> <p>278 Cadetes del 4to año de la EMCH</p> <p>Muestra</p> <p>98 Cadetes del 4to año de la EMCH</p> <p>Métodos de Análisis de Datos</p> <p>Estadística SPSS25</p>
			<p>Variable Dependiente</p>	<p>Y₁ Ciencias y Humanidades</p>		

Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?	Chorrillos “Coronel Francisco Bolognesi” 2020.	Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.	(Y) Procesos Educativos	Y ₂ Ciencias Militares	<ul style="list-style-type: none"> • Doctrina Militar de Comunicaciones • Planeamiento de Operaciones • Aplicación de la Guerra Ciberdefensa 	
---	--	---	--------------------------------	--------------------------------------	---	--

Anexo 2



Instrumentos de recolección

Instrumentos de Recolección de Datos

Encuesta 1

PREVENCIÓN DE ATAQUES CIBERNÉTICOS

La presente encuesta es para determinar cuál es la relación que existe entre la Prevención de Ataques Cibernéticos y los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020:

Escala de valoración	
Totalmente de acuerdo	4
De acuerdo	3
En desacuerdo	2
Totalmente en desacuerdo	1

Tipos de Ataques Cibernéticos según el Objetivo	1	2	3	4
1. ¿Considera usted que la Interrupción dentro de los Tipos de Ataques Cibernéticos según el Objetivo se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				
2. ¿Considera usted que la Interpretación dentro de los Tipos de Ataques Cibernéticos según el Objetivo se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				
3. ¿Considera usted que la Modificación dentro de los Tipos de Ataques Cibernéticos según el Objetivo se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				
4. ¿Considera usted que la Generación dentro de los Tipos de Ataques Cibernéticos según el Objetivo se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				
Fases del Ataque	1	2	3	4

5. ¿Considera usted que el Reconocimiento como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				
6. ¿Considera usted que la Exploración como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				
7. ¿Considera usted que el Obtener Acceso como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				
8. ¿Considera usted que el Mantener el Acceso como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				
9. ¿Considera usted que el Borrar Huellas como una de las Fases de Ataque Cibernético se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				
Medidas de Prevención	1	2	3	4
10. ¿Considera usted que el Modelo para prevenir ciberataques como uno de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				
11. ¿Considera usted que Implementación de un portal cautivo para la gestión de acceso a la red como una de las Medidas de Prevención se relacionan con los				

Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				
12. ¿Considera usted que el Monitoreo de la red a través de software de gestión como una de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				
13. ¿Considera usted que las Políticas de seguridad en el servidor para la navegación como una de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				
14. ¿Considera usted que los Métodos de encriptación y protección de la información como una de las Medidas de Prevención se relacionan con los Procesos Educativos de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020?				

Encuesta 2

PROCESOS EDUCATIVOS

Escala de valoración	
Totalmente de acuerdo	4
De acuerdo	3
En desacuerdo	2
Totalmente en desacuerdo	1

Ciencias y Humanidades	1	2	3	4
15. ¿Considera usted que el cumplimiento de los establecido por la Política Nacional de Seguridad dentro del área de Ciencias y Humanidades puede ser influido por los Ataques Cibernéticos?				

16. ¿Considera usted que el cumplimiento de los establecido por los Tratados Internacionales dentro del área de Ciencias y Humanidades puede ser influidos por los Ataques Cibernéticos?				
Ciencias Militares	1	2	3	4
17. ¿Considera usted que el cumplimiento de los establecido por la Doctrina Militar de Comunicaciones dentro del área de Ciencias Militares puede ser influido por los Ataques Cibernéticos?				
18. ¿Considera usted que el Planeamiento de Operaciones dentro del área de Ciencias Militares puede ser influido por los Ataques Cibernéticos?				
19. ¿Considera usted que la Aplicación de la Guerra Ciberdefensa dentro del área de Ciencias Militares puede ser influido por los Ataques Cibernéticos?				

Anexo 3



Base de datos

31	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
32	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
33	4	4	4	4	1	2	2	4	4	2	4	1	4	1	4	4	4	4	4
34	4	4	4	2	4	4	4	4	4	4	3	4	4	3	4	4	3	3	4
35	4	2	1	4	4	4	4	4	3	1	2	3	1	4	3	2	2	4	2
36	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
37	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
38	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
39	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
40	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
41	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
42	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
43	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
44	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
45	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
46	4	1	2	2	3	2	3	1	4	3	1	4	4	4	1	3	2	2	3
47	2	4	1	3	4	4	4	4	4	4	4	4	4	2	3	3	4	4	3
48	1	4	3	4	4	4	2	4	4	4	3	3	3	4	4	4	3	3	4
49	4	3	4	4	2	3	4	1	1	4	4	4	4	4	4	4	1	1	4
50	4	4	4	4	1	4	4	4	4	4	4	2	2	4	4	4	4	4	4
51	4	4	4	4	4	1	4	4	2	4	4	4	3	3	4	4	4	4	4
52	4	1	4	4	4	4	4	4	4	2	2	4	1	4	2	2	2	2	2
53	2	4	1	4	4	4	3	3	4	4	4	4	4	2	3	3	4	4	3
54	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
55	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
56	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
57	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
58	4	4	4	4	1	2	2	4	4	2	4	1	4	1	4	4	4	4	4
59	4	4	4	2	4	4	4	4	4	4	3	4	4	3	4	4	3	3	4
60	4	2	1	4	4	4	4	4	3	1	2	3	1	4	3	2	2	4	2
61	2	4	4	2	4	4	4	3	2	4	3	4	2	2	4	1	3	3	1
62	4	4	3	4	3	1	1	4	1	4	4	4	4	4	2	4	4	4	4
63	4	3	4	3	2	3	4	4	3	1	4	4	4	3	1	4	4	4	4
64	4	4	3	4	4	4	4	4	2	4	4	3	2	3	2	4	4	4	4
65	3	4	2	4	4	3	4	3	4	3	2	2	3	4	3	1	2	2	1

Anexo 4



**Validación del instrumento por
expertos**

Validación De Instrumento Por Experto

TÍTULO DEL TRABAJO DE INVESTIGACIÓN/TESIS:

PREVENCIÓN DE ATAQUES CIBERNÉTICOS Y LOS PROCESOS EDUCATIVOS DE LOS CADETES DE 4TO AÑO DE LA ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI” 2020

AUTORES:

Cad IV Com Huamaní Cáceres Renzo
Cad IV Com Ubillus Del Castillo Axel

INSTRUCCIONES: Coloque “x” en el casillero correspondiente la valoración que su experticia determine sobre las preguntas formuladas en el instrumento.

CRITERIOS	DESCRIPCIÓN	VALOR ASIGNADO POR EL EXPERTO									
		10	20	30	40	50	60	70	80	90	100
1. CLARIDAD	Está formado con el lenguaje adecuado.										
2. OBJETIVIDAD	Está expresado en conductas observables										
3. ACTUALIDAD	Adecuado de acuerdo al avance de la ciencia.										
4. ORGANIZACIÓN	Existe una cohesión lógica entre sus elementos.										
5. SUFICIENCIA	Comprende los aspectos requeridos en cantidad y calidad										
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de la investigación										
7. CONSISTENCIA	Basado en bases teóricas científicas.										
8. COHERENCIA	Hay correspondencia entre dimensiones, indicadores e índices.										
9. METODOLOGÍA	El diseño responde al propósito de la investigación										
10. PERTINENCIA	Es útil y adecuado para la investigación.										

PROMEDIO DE VALORACIÓN DEL EXPERTO: _____

OBSERVACIONES REALIZADAS POR EL EXPERTO:

GRADO ACADÉMICO DEL EXPERTO: _____

INSTITUCIÓN DONDE LABORA: _____

APELLIDOS Y NOMBRES DEL EXPERTO: _____

FIRMA:

POST FIRMA:

DNI:

Anexo 4.b. Validación De Instrumento Por Experto

TÍTULO DEL TRABAJO DE INVESTIGACIÓN/TESIS:

PREVENCIÓN DE ATAQUES CIBERNÉTICOS Y LOS PROCESOS EDUCATIVOS DE LOS CADETES DE 4TO AÑO DE LA ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI” 2020

AUTORES:

Cad IV Com Huamaní Cáceres Renzo

Cad IV Com Ubillus Del Castillo Axel

INSTRUCCIONES: Coloque “x” en el casillero correspondiente la valoración que su experticia determine sobre las preguntas formuladas en el instrumento.

CRITERIOS	DESCRIPCIÓN	VALOR ASIGNADO POR EL EXPERTO									
		10	20	30	40	50	60	70	80	90	100
1. CLARIDAD	Está formado con el lenguaje adecuado.										
2. OBJETIVIDAD	Está expresado en conductas observables										
3. ACTUALIDAD	Adecuado de acuerdo al avance de la ciencia.										
4. ORGANIZACIÓN	Existe una cohesión lógica entre sus elementos.										
5. SUFICIENCIA	Comprende los aspectos requeridos en cantidad y calidad										
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de la investigación										
7. CONSISTENCIA	Basado en bases teóricas científicas.										
8. COHERENCIA	Hay correspondencia entre dimensiones, indicadores e índices.										
9. METODOLOGÍA	El diseño responde al propósito de la investigación										
10. PERTINENCIA	Es útil y adecuado para la investigación.										

PROMEDIO DE VALORACIÓN DEL EXPERTO: _____

OBSERVACIONES REALIZADAS POR EL EXPERTO:

GRADO ACADÉMICO DEL EXPERTO: _____

INSTITUCIÓN DONDE LABORA: _____

APELLIDOS Y NOMBRES DEL EXPERTO: _____

FIRMA:

POST FIRMA:

DNI:

Anexo 4.c. Validación De Instrumento Por Experto

TÍTULO DEL TRABAJO DE INVESTIGACIÓN/TESIS:

PREVENCIÓN DE ATAQUES CIBERNÉTICOS Y LOS PROCESOS EDUCATIVOS DE LOS CADETES DE 4TO AÑO DE LA ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI” 2020

AUTORES:

Cad IV Com Huamaní Cáceres Renzo

Cad IV Com Ubillus Del Castillo Axel

INSTRUCCIONES: Coloque “x” en el casillero correspondiente la valoración que su experticia determine sobre las preguntas formuladas en el instrumento.

CRITERIOS	DESCRIPCIÓN	VALOR ASIGNADO POR EL EXPERTO									
		10	20	30	40	50	60	70	80	90	100
1. CLARIDAD	Está formado con el lenguaje adecuado.										
2. OBJETIVIDAD	Está expresado en conductas observables										
3. ACTUALIDAD	Adecuado de acuerdo al avance de la ciencia.										
4. ORGANIZACIÓN	Existe una cohesión lógica entre sus elementos.										
5. SUFICIENCIA	Comprende los aspectos requeridos en cantidad y calidad										
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de la investigación										
7. CONSISTENCIA	Basado en bases teóricas científicas.										
8. COHERENCIA	Hay correspondencia entre dimensiones, indicadores e índices.										
9. METODOLOGÍA	El diseño responde al propósito de la investigación										
10. PERTINENCIA	Es útil y adecuado para la investigación.										

PROMEDIO DE VALORACIÓN DEL EXPERTO: _____

OBSERVACIONES REALIZADAS POR EL EXPERTO:

GRADO ACADÉMICO DEL EXPERTO: _____

INSTITUCIÓN DONDE LABORA: _____

APELLIDOS Y NOMBRES DEL EXPERTO: _____

FIRMA:

POST FIRMA:

DNI:

Anexo 5



**Constancia donde se efectuó la
investigación**

Constancia de entidad donde se efectuó la investigación**ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO
BOLOGNESI”**

CONSTANCIA

El que suscribe Sub Director Académico de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”

HACE CONSTAR

Que los Cadetes que se mencionan han realizado la investigación en esta dependencia militar sobre el tema titulado: PREVENCIÓN DE ATAQUES CIBERNÉTICOS Y LOS PROCESOS EDUCATIVOS DE LOS CADETES DE 4TO AÑO DE LA ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI” 2020

Investigadores:

Bach Huamaní Cáceres Renzo

Bach Ubillus Del Castillo Axel

Se le expide la presente Constancia a efectos de emplearla como anexo en su investigación.

Chorrillos,..... de..... del 2020

Anexo 6



**Compromiso de autenticidad del
instrumento**

Compromiso de autenticidad del instrumento

Los Cadetes que suscriben líneas abajo, autores del trabajo de investigación titulado: PREVENCIÓN DE ATAQUES CIBERNÉTICOS Y LOS PROCESOS EDUCATIVOS DE LOS CADETES DE 4TO AÑO DE LA ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI” 2020.

HACEN CONSTAR:

Que el presente trabajo ha sido íntegramente elaborado por los suscritos y que no existe plagio alguno, ni temas presentados por otra persona, grupo o institución, comprometiéndonos a poner a disposición del COEDE (EMCH “CFB”) los documentos que acrediten la autenticidad de la información proporcionada si esto lo fuera solicitado por la entidad.

En tal sentido asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión, tanto en los documentos como en la información aportada.

Nos afirmamos y ratificamos en lo expresado, en fe de lo cual firmamos el presente documento.

Chorrillos,..... dedel 2020

.....
Bach Huamaní Cáceres Renzo

.....
Bach Ubillus Del Castillo Axel

Anexo 7



Asesor y miembro del jurado



ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"

ACTA DE SUSTENTACION DE TESIS

En el distrito de Chorrillos de la ciudad de Lima, siendo las horas del día de del 2020, se dio inicio a la sustentación de la tesis titulada:

PREVENCIÓN DE ATAQUES CIBERNÉTICOS Y LOS PROCESOS EDUCATIVOS EN LA ESCUELA MILITAR DE CHORRILLOS "CRL. FRANCISCO BOLOGNESI." 2020

Presentada por:

- HUAMANI CACERES RENZO
- UBILLUS DEL CASTILLO ERIQUE AXEL

Ante el Jurado de Sustentación de Tesis nombrado por la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" y conformada por:

- Presidente : TC MEDINA DIAZ RONALD
- Secretario : TC ANDRADE ZAMORA CHRISTOPHER PAUL
- Vocal : DR MACAZANA FERNÁNDEZ DANTE

Concluida la sustentación, los miembros del Jurado dictaminaron:

.....

APROBADA POR UNANIMIDAD () APROBADA POR MAYORIA () OBSERVADA ()
DESAPROBADA ()

Siendo las horas del día de se dio por concluido el presente acto académico, firmando los miembros del Jurado

VOCAL

SECRETARIO

PRESIDENTE