# ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"

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

## La ciberseguridad y los riesgos de hacking en los cadetes de 4to año de La Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020

**PRESENTADO POR:**

**Dominguez Piñas Frank Richard**

**Cotera Cedano Renzo Marek**

**LIMA – PERÚ**

**2020**

**ASESORES Y MIEMBROS DEL JURADO**

**ASESOR**

**TEMÁTICO:**

**METODOLÓGICO:**

**PRESIDENTE DEL JURADO:**

**……..**

**MIEMBROS DEL JURADO:**

**……**

**……**

**…….....**

## DEDICATORIA

Dedicamos este trabajo a nuestros progenitores, hermanos y familiares que gracias a su apoyo y colaboración nos motivan a seguir esforzándonos en el camino duro pero satisfactorio de nuestra carrera militar como futuros oficiales del Ejército del Perú.

## RESUMEN

La presente investigación titulada: La Ciberseguridad y los riesgos de Hacking en 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 Ciberseguridad y los riesgos de Hacking en 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, con una población objetiva de 131 cadetes 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, en la actualidad la tecnología relacionada al espectro electromagnético predomina ante la tecnología física que tradicionalmente se utilizaba el siglo próximo pasado; esto nos lleva directamente a la Ciberseguridad, la cual está directamente relacionada con los delitos cibernéticos o los Hacking que generan un riego latente a la seguridad personal o institucional

Como parte final del estudio se exponen las recomendaciones de acuerdo a las conclusiones, las cuales son propuestas factibles para evitar y/o neutralizar el Hacking entre los Cadetes de Comunicaciones de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi

Palabras claves: *Ciberseguridad, hacking y comunicaciones.*

## ABSTRACT

The present investigation entitled Cybersecurity and the risks of Hacking in the 4th year Cadets of the Military School of Chorrillos Coronel Francisco Bolognesi, 2020; considers within its main objective, to determine what is the relationship that exists between Cybersecurity and the risks of Hacking in the 4th year Cadets of the Military School of Chorrillos Coronel Francisco Bolognesi, 2020

The study method has a quantitative approach, with a non-experimental design, with an objective population of 131 cadets from the Coronel Francisco Bolognesi Military School of Chorrillos involved in the subject, of the research; with the application of a questionnaire to determine the objectives of the investigation

During the development of this investigation, the following general conclusion was reached: We have been able to conclude through surveys that this hypothesis is valid; since, at present, the technology related to the electromagnetic spectrum predominates over the physical technology that was traditionally used in the next century; This leads us directly to Cybersecurity, which is directly related to cybercrimes or Hacking that generate a latent risk to personal or institutional security

As a final part of the study, the recommendations are presented according to the conclusions, which are feasible proposals to prevent and / or neutralize Hacking among the Cadets of Communications of the Military School of Chorrillos Coronel Francisco Bolognesi


Key words: *Cybersecurity, hacking and communications.*



## 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



## ÍNDICE DEL CONTENIDO

**Pág.**

## CAPÍTULO I

# PROBLEMA DE INVESTIGACIÓN

## 1.1 Planteamiento del problema

### 1.1.1 Situación problemática

"La ciencia de la informática hoy en día es un elemento esencial para cualquier país que desea el progreso y mejora de este, toda información virtual que esté presente en la red interna privada de una institución estatal o privada, militar o civil es considerada un activo. Este activo debería de ser considerada y resguardado como algo muy apreciado por una institución estatal o privada, militar o civil ya que esto puede hacer que surja adelante o fracase, es por ello por lo que debemos darle toda seguridad posible a la información virtual que existe en la red privada de una institución estatal o privada, militar o civil". (Pastor, O.; Pérez, J.; Arnáiz, D. & Taboso, P., 2009)

"La principal amenaza que afecta a la seguridad de la información 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 las institución estatal o privada, militar o civil 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". (Pastor, O.; Pérez, J.; Arnáiz, D. & Taboso, P., 2009)

"Hoy en día existen muchos factores que amenazan la seguridad de información de las instituciones estatales o privadas, militares o civiles y por lo general el presupuesto destinado para la proteger y resguardar la información de las redes de internet externas". "No es el suficientes, 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". (Pastor, O.; Pérez, J.; Arnáiz, D. & Taboso, P., 2009)

Con las ansias de lograr este objetivo el cual se basa en que las instituciones estatales o privadas, militares o civiles del Perú; especialmente los cadetes del arma de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, conozcan 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 las instituciones estatales o privadas, militares o civiles del Perú; especialmente los cadetes del arma de Comunicaciones 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” (Pastor, O.; Pérez, J.; Arnáiz, D. & Taboso, P., 2009).

Esta investigación es importante porque “los estudios realizados por empresas 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”. (Pastor, O.; Pérez, J.; Arnáiz, D. & Taboso, P., 2009)

Para ello con “el nuevo conocimiento acerca de la importancia de elaborar planes de acción y estrategias para minimizar los riesgos, las empresas tendrán el enfoque necesario para establecer una nueva gobernanza y directivas que garanticen la seguridad cibernética” (Pastor, O.; Pérez, J.; Arnáiz, D. & Taboso, P., 2009); garantizando la confidencialidad de la información que es compartida por parte de los cadetes del arma de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

### 1.1.3 Limitaciones y Viabilidad

***Limitaciones***

Dentro de las limitaciones encontradas en el presente trabajo de investigación, se encuentra la poca disponibilidad de tiempo del cadete EMCH para la investigación. Así mismo, en el presente trabajo de investigación, se encuentra la necesidad de asesoramiento especializado en el tema para el tratamiento científico de su aplicabilidad

***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 Ciberseguridad y los riesgos de Hacking en 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 Objetivos de la Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" 2020?

- ¿Cuál es la relación que existe entre las Amenazas a la Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" 2020?

- ¿Cuál es la relación que existe entre los Tipos de Ataques a la Ciberseguridad y los riesgos de Hacking en 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 Ciberseguridad y los riesgos de Hacking en 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 Objetivos de la Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020.

- Establecer cuál es la relación que existe entre las Amenazas a la Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2020.

- Establecer cuál es la relación que existe entre los Tipos de Ataques a la Ciberseguridad y los riesgos de Hacking en 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 Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2020.

### 2.1.2 Hipótesis Específicas

#### Hipótesis Específica 1

Los Objetivos de la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2020.

#### Hipótesis Específica 2

Las Amenazas a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2020.

#### Hipótesis Específica 3

Los Tipos de Ataques a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en 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): La Ciberseguridad
Variable (2): Los riesgos del Hacking

### 2.2.2 Variables Específicas intermedias o dimensiones

**La Ciberseguridad**

- Objetivos
- Amenazas
- Tipos de ataques

**La prevención del Hacking**

- Hacker ético
- Tipos de hacker
- Marco legal

## 2.3 Conceptualización de Variables

### 2.3.1 Definición conceptual

Variable (1): La Ciberseguridad

"Se conoce como ciberseguridad la práctica basada en proteger los sistemas informáticos, las redes y los programas de ataques digitales. En general, en una organización se trata de una estrategia que implica a las personas, los procesos y la tecnología para crear múltiples capas de protección ante los ciberataques". (Pastor, O.; Pérez, J.; Arnáiz, D. & Taboso, P., 2009)

Variable (2): Los riesgos del Hacking

"Llamamos ***hacking*** a un conjunto de técnicas para acceder a un sistema informático sin autorización. Existe autorización cuando se dispone de un control de acceso mediante el uso de identificadores de usuario y *passwords*. Es un término tradicionalmente ligado a la libertad de Información de Internet. En sus códigos está

el respetar la vida privada, pero eso después de aprender cómo funcionan los sistemas y dónde están los datos. Entre sus medios destacan los *Sniffers* o escaneadores de puertos, programas que buscan claves, *passwords* y puertos abiertos. Actúan juntamente con otras aplicaciones como reventadoras de claves y nukeadores". (De Miguel, M. y Oltra, J., 2007)

### 2.3.2 Operacionalizacion de las variables

**Tabla 1**

*Operacionalización de la Variable 1: La Ciberseguridad*

| Dimensión | Indicadores | Ítems |
|---|---|---|
| Objetivos | • Infraestructura | 1, 2, 3 |
| | • Usuario | 4, 5, 6 |
| | • Información | 7, 8, 9 |
| Amenazas | • Por el origen | 10, 11, 12 |
| | • Por el efecto | 13, 14, 15 |
| | • Por el medio utilizado | 16, 17, 18 |
| Tipos de Ataques | • Por repetición | 19, 20, 21 |
| | • De modificación de bits | 22, 23, 24 |
| | • De denegación de servicio | 25, 26, 27 |
| | • De diccionario | 28, 29, 30 |

**Tabla 2**

*Operacionalización de la Variable 2: Los riesgos del Hacking*

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

| | | |
|---|---|---|
| Hacker ético | • Eticidad | 31 |
| | • Elementos de seguridad | 32 |
| | • Facultades | 33 |
| Tipos de hacker | • Black hats | 34 |
| | • White hats | 35 |
| | • Gray hats | 36 |
| Marco legal | • Internacional | 37 |
| | • Nacional | 38 |

## 2.4 Antecedentes de la Investigación

### 2.4.1 Antecedentes internacionales

Aguirre, A. (2017). En su tesis para obtener su Maestría, titulada: *"Ciberseguridad en Infraestructuras Críticas de Información"*. Universidad de Buenos Aires. Buenos Aires. Argentina

**Resumen:** "El presente Trabajo Final de Maestría analiza la importancia de la ciberseguridad en las infraestructuras críticas de información, las actividades que se han desarrollado en este sentido de manera general en algunos países y el apoyo de las organizaciones internacionales que colaboran en el área de la ciberseguridad. Sobre esta base, propone un modelo para la identificación de los sectores y servicios críticos de una economía y una serie de controles mínimos para su protección. En efecto, las tecnologías de la información se han esparcido rápidamente en todos los sectores de la sociedad y prácticamente no existen servicios críticos que no dependan de aplicaciones, bases de datos, servidores, redes de comunicaciones,

centros de datos, etc".

**Conclusiones: "**La ciberseguridad en la mayoría de los países y especialmente en el Ecuador, se está desarrollando de manera aislada e independiente en cada sector de la economía. Tampoco existe una coordinación por parte del Estado que vele por la ciberseguridad a nivel nacional. Este escenario implica una duplicación de esfuerzos por parte de los diferentes sectores en la implementación de controles para la provisión de servicios confiables. Para que esto no suceda, es necesaria la creación de una estrategia nacional de ciberseguridad, documento a través del cual los países alinean sus objetivos a nivel nacional en la materia y que abarca también la identificación y protección de las infraestructuras críticas de información utilizadas para brindar servicios esenciales a la población. Cada Estado es responsable de establecer un plan para proteger sus infraestructuras críticas, el que debe ser auditado en cada sector y medido y mejorado continuamente. Esto se justifica en el hecho de que las amenazas son cada vez más sofisticadas y cambiantes y deben ser identificadas en forma oportuna".

**Comentario: "**El presente trabajo de investigación nos permite apreciar de qué forma los servicios esenciales tales como las telecomunicaciones o la energía, están utilizando masivamente tecnologías de la información debido a los grandes beneficios que esto acarrea; siendo la gestión de la ciberseguridad es una debilidad, a la que no se está prestando la seguridad requerida. Sirviendo de base teórica para nuestro trabajo la necesidad de profundizar el estudio de la ciberseguridad, enfocándose en la identificación de servicios críticos y en la protección de las infraestructuras de información que contribuyen a su provisión".

Mendaño, L. (2016). En su proyecto previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones, titulada: *"Implementación de Técnicas de Hacking Ético para el descubrimiento y evaluación de vulnerabilidades de la Red de una cartera de Estado"*. Escuela Politécnica Nacional. Quito. Ecuador

**Resumen:** "El objetivo del presente proyecto es la implementación de técnicas de hacking Ético para el descubrimiento y evaluación de vulnerabilidades, con el fin

de medir la estrategia de defensa de un sistema informático y realizar recomendaciones de mitigación ante las fallas encontradas".

**Conclusiones:** "El presente proyecto nos ha permitido desarrollar un hacking Ético perimetral, que es una parte de las funciones que realiza un profesional en seguridad para determinar brechas de seguridad y generar un plan de mitigación. Todo sistema informático es vulnerable y los sistemas de la organización evaluada en este proyecto no ha sido la excepción, es cuestión de tiempo para que personas comunes o expertos en hardware y software, con conocimientos en tecnología descubran errores y quieran vulnerar los sistemas tecnológicos. Es por esto que existe personas dedicadas a evaluar vulnerabilidades con el objetivo de evidenciar, corregir y mejorar la seguridad".

**Comentario:** "El presente trabajo nos muestra como al pasar de los tiempos ha surgido la necesidad de implementar procesos de seguridad más robustos y con ello efectuar técnicas de intrusiones bajo un ambiente controlado, lo cual simule un ataque real. Esta simulación permite encontrar brechas en la seguridad, las cuales un atacante podría aprovechar para infiltrarse en la red de una organización con propósitos malintencionados y de esta forma manipular información, suplantar identidades, colapsar servicios, u otras actividades propias de un delincuente informático. Lo cual se relaciona con la finalidad de nuestro trabajo de investigación y se constituye en base teórica".

Benítez, J. (2019). En su tesis titulada: *"Análisis de riesgo en redes wifi aplicando técnicas de hacking ético"*. Universidad de las Américas. Quito. Ecuador

**Resumen:** "El presente trabajo de titulación tiene como objetivo realizar un análisis de riesgos a nivel de redes inalámbricas en una empresa cuyo modelo de negocio es la venta y comercialización de productos en el área turística por lo que su especialidad es totalmente ajena al de la tecnología, por lo tanto, no están tan familiarizados con atacantes, métodos y técnicas que involucren la apropiación de información a través de dispositivos electrónicos o software por parte de usuarios no autorizados. Para este trabajo se utilizarán dos metodologías la primera de ellas

permitirá identificar los activos críticos, determinar si cuentan con procesos o una documentación robusta que les permita mitigar riesgos y amenazas de seguridad informática en sus activos, conocer si sus empleados saben cómo actuar frente alguna amenaza y sobre todo identificar si existen vulnerabilidades críticas en todas sus áreas".

**Conclusiones: "**El resultado de la aplicación de ambas metodologías de Octave e ISSAF permitieron identificar los principales activos críticos de la empresa, además se pudo crear sus correspondientes perfiles de amenazas y simular un ataque a la red con el objetivo de obtener una solución a las distintas vulnerabilidades presente en sus activos críticos. El uso del método cualitativo permitió manejar una mejor comunicación con todo el personal de la empresa, ya que se pudo establecer parámetros básicos que debían cumplir cada uno de los activos permitiendo clasificarlos y evaluarlos de mejor forma sin la necesidad de utilizar en su mayor parte términos técnicos que estén fuera de su comprensión".

**Comentario:** "El resultado obtenido le permitió a la empresa conocer sus vulnerabilidades, corregirlas, contar con una documentación que le permita actuar frente a posibles amenazas, reducir el nivel de riesgo, guiar a sus empleados y capacitarlos en función de las buenas prácticas de la seguridad informática. En conclusión, esta propuesta nos ayudara considerándola como ejemplo, a conocer, guiarnos y concienciar de que no están exentos a cualquier tipo de ataque informático que puede darse en cualquier momento".

### 2.4.2. Antecedentes nacionales

Berbeo, j. (2019). En su tesis para optar el grado académico de maestro en Ingeniería de Sistemas con mención en Tecnología de Información y Comunicación, titulada: *"Implementación de Hacking ético para la detección y evaluación de vulnerabilidades de red en la empresa Complex del Perú S.A.C.- Tumbes; 2017"*. Universidad Católica Los Ángeles de Chimbote. Tumbes. Perú

**Resumen:** "El presente informe de Tesis está desarrollado de acuerdo la línea de investigación en Implementación de las Tecnologías de la Información y

Comunicación, de la Escuela profesional de Ingeniería de Sistemas de la Universidad Los Ángeles de Chimbote (ULADECH CATÓLICA). El objetivo principal es realizar la Implementación de Hacking Ético, en la Empresa Complex del Perú S.A.C; para ayudar en la detección y evaluación de vulnerabilidades de Red, de acuerdo a las características, la investigación fue cuantitativa, de diseño no experimental, tipo descriptiva y de corte transversal; la cual tiene una población que está constituida por 24 trabajadores, donde se tomó una muestra similar a la cantidad de la población, es decir 24 trabajadores; convirtiéndose esta en una población muestral".

**Conclusiones: "**Se ha logrado realizar la Implementación de Hacking Ético, en la Empresa Complex del Perú S.A.C – Tumbes; 2017; como medio de ayuda en la detección y evaluación de vulnerabilidades de Red. Se ha realizado el análisis, utilizando herramientas tecnológicas de seguridad, de la actual red de datos en la empresa Complex del Perú S.A.C – Tumbes; por lo que se ha evaluado los problemas de vulnerabilidad a los que se encuentra expuesta la red. Así mismo, se ha formulado una propuesta tecnológica de seguridad, que permita establecer políticas de comunicación oportuna al detectarse posibles vulnerabilidades y/o penetraciones en la red de datos de la empresa Complex del Perú S.A.C – Tumbes".

**Comentarios:** "Podemos apreciar que, con la Implementación de Hacking Ético en la Empresa, aplicando el análisis con las herramientas tecnológicas de seguridad, de la actual red de datos en la empresa; se pudo establecer políticas de comunicación oportuna al detectarse posibles vulnerabilidades y/o penetraciones en la red de datos de la empresa Complex del Perú S.A.C – Tumbes. Lo cual nos sirve de base teórica para demostrar la validez de nuestras hipótesis".

Enríquez, U. y Mendoza, J. (2019). En su tesis para optar el Título Profesional de Ingeniero de Seguridad y Auditoría Informática, titulada: *"Aplicación de un hacking ético para mejorar la ciberseguridad de una entidad del Estado"*. Universidad Tecnológica del Perú. Lima. Perú

**Resumen:** “En el trabajo realizado se presenta como la aplicación de un hacking ético para mejorar la ciberseguridad de una entidad del estado, siendo la Biblioteca General del Ejército del Perú como entidad del estado a evaluar, el cual permitirá poner en evidencia las vulnerabilidades que puedan ocasionar un gran impacto a sus sistemas de información. En el primer capítulo se presenta la problemática que tiene la Biblioteca General del Ejército del Perú. Se presenta además los objetivos, alcance, limitaciones, justificación y estado del arte para la aplicación del hacking ético”.

**Conclusiones: “**Llegaron a la conclusión de que es necesario la implementación de un hacking ético que permita neutralizar los riesgos a la ciberseguridad que trae consigo el manejo del ciberespacio y que puede atentar contra la información de carácter confidencial y reservado de las entidades del Estado”.

**Comentario:** “El presente trabajo de investigación, con sus conclusiones se transforma en una herramienta de apoyo para consolidar nuestra tesis y así mismo, se constituye en base teórica del mismo”.

Maucaylle, A. (2019). En su tesis para optar el título profesional de Ingeniero de Sistemas, titulada*: “Construcción de un modelo de Red Virtual para aplicar técnicas de Hacking Ético y poder analizar los eventos relacionados a la Seguridad Informática sobre una Infraestructura Virtual”*. Universidad Nacional José María Arguedas. Andahuaylas. Apurímac. Perú

**Resumen:** “El objetivo del presente trabajo de investigación es construir un modelo de red virtual que permita aplicar técnicas de hacking ético y analizar los eventos relacionados a la seguridad informática. Para cumplir esta tarea se empleó la metodología PPDIOO (preparar, planificar, diseñar, implementar, operar) de Cisco para el diseño de redes, el enfoque principal de esta metodología es definir las actividades mínimas requeridas, por tecnología y complejidad de red, que permitan la instalación y operación exitosa de las tecnologías. Así mismo se logra optimizar el desempeño a través del ciclo de vida de la red”.

**Conclusiones:** “Para el análisis y monitoreo de los eventos generados en materia de seguridad informática en cada uno de los fases del hacking ético se empleó el software Wireshark; dicho análisis consistió entender el comportamiento de cada ataque generado y examinar los resultados obtenidos; producto de ello se pudo identificar el equipo que originó los ataques, los puertos y protocolos utilizados por las herramientas para lograr detectar las vulnerabilidades asociados a los elementos que conforman la red virtual, el nivel de concurrencia de los eventos que pudieron registrarse en contra de la seguridad de los servicios implementados”.

**Comentario:** “Podemos apreciar que a nivel de infraestructura tecnológica un factor decisivo a la hora de sufrir un ataque informático viene a ser una inadecuada gestión de configuración en los servicios implementados y una incorrecta administración y despliegue de actualizaciones en sistemas operativos y aplicaciones. Lo cual nos sirve de base teórica y apoyo para la determinación de nuestras conclusiones y recomendaciones”.

## 2.5 Sustento teórico de las variables

### 2.5.1 La Ciberseguridad

Según Information Systems Audit and Control (ISACA) da por definición a la Ciberseguridad como “Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, se almacena y se transporta mediante los sistemas de información que se encuentran interconectados”. (Llongueras, A., 2013)

Siendo ISACA es “el acrónimo de *Information Systems Audit and Control Association* (Asociación de Auditoría y Control de Sistemas de Información), una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información”. (Llongueras, A., 2013)

Una definición más amplia es dada por la Unión Internacional de Telecomunicaciones (UIT) como:

> “La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno”. “Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno”. “La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno”. (Llongueras, A., 2013)

**Objetivos**

“La Ciberseguridad debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores”. (Llongueras, A., 2013)

**a. Infraestructura**

> “Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar por que los equipos funcionen adecuadamente y anticiparse en caso de fallos, robos, incendios, sabotajes, desastres naturales, fallos en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática”. (Llongueras, A., 2013)

**b. Usuario**

"Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable". (Llongueras, A., 2013)

**c. Información**

"Este es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios". (Llongueras, A., 2013)

**Amenazas**

**a. Por el origen**

"El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo, el hecho de que la red no esté conectada un entorno externo, como Internet, no nos garantiza la seguridad de esta". (Llongueras, A., 2013)

"De acuerdo con el Computer Security Institute (CSI) de San Francisco aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma". (Llongueras, A., 2013)

"Basado en el origen del ataque podemos decir que existen dos tipos de amenazas":

- *Amenazas Internas*

Generalmente estas amenazas pueden ser más serias que las externas.

"Los usuarios o personal técnico conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc". "Además, tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos de movimientos". (Llongueras, A., 2013)

"Los sistemas de prevención de intrusos o IPS, y firewalls son mecanismos no efectivos en amenazas internas por, habitualmente, no estar orientados al tráfico interno". (Llongueras, A., 2013)

- *Amenazas externas*

  - "Se originan fuera de la red local".
  - "Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla".
  - "La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos".
  - "Para clasificarlo como externo debe ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red: rosetas, switches o Hubs accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etc".

**b. Por el efecto**

"El tipo de amenazas por el efecto que causan a quien recibe los ataques podría clasificarse en":

- "Robo de información".
- "Destrucción de información".
- "Anulación del funcionamiento de los sistemas o efectos que tiendan a ello".

- “Suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc”.
- “Robo de dinero, estafas, etc”.

**c. Por el medio utilizado**

“Amenazas por el medio utilizado Se pueden clasificar por el modus operandi del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque”. (Llongueras, A., 2013)

Aquí se clasifican acciones como:

- “Virus informático: malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos”. (Llongueras, A., 2013)
- “Worms”
- “BOTs”
- “Adware”
- “Cookies”
- “Phishing”
- “Ingeniería social”
- “Denegación de servicio”
- “Spoofing: de DNS, de IP, de DHCP, etc.”

**Tipos de ataques**

“Según Valdivia, 2014, los ataques informáticos más usuales son los siguientes”:

**a. Por repetición**

"Ocurre cuando un pirata informático copia una secuencia de mensajes entre dos usuarios y envía tal secuencia a uno o más usuarios". "A menos que esto sea minimizado, el sistema atacado procesa este comportamiento como mensajes legítimos y producen respuestas como pedidos redundantes". (Valdivia, 2014)

**b. De modificación de bits**

"Se basan en las respuestas predecibles de las estaciones receptoras. El pirata modifica bits de un mensaje para enviar un mensaje cifrado erróneo a la estación receptora, y este se puede comparar entonces contra la respuesta predecible para obtener la clave a través de múltiples repeticiones". (Valdivia, 2014)

**c. De denegación de servicio**

"Consiste en colapsar total o parcialmente a un servidor para que este no pueda dar respuesta a los comandos (no para sacar de la información). En la red internet, esto puede lograrse saturando un solo servidor con múltiples solicitudes desde múltiples ordenadores. Como el servidor es incapaz de responder a todas las solicitudes, colapsa". (Valdivia, 2014) "En las redes inalámbricas, esto se logra también provocando ruido: se coloca un teléfono a 2,4 GHz cerca del punto de acceso e iniciar una llamada. La energía de radiofrecuencia provocada es suficiente para bloquear de manera efectiva gran parte del tráfico de datos en el punto de acceso". (Valdivia, 2014)

**d. De diccionario**

"En algunos modelos de autenticación de datos, la contraseña para ingresar al sistema es secreta y el nombre de usuario es enviado en forma de texto simple y es fácilmente interceptable". "En este caso, el pirata informático obtiene distintos nombres de usuarios y con ellos, desde un ordenador, empieza a adivinar las contraseñas con base en palabras de diccionarios en distintos

idiomas. Este ataque es exitoso en gran medida porque muchos usuarios utilizan contraseñas poco creativas". (Valdivia, 2014)

### 2.5.2 Los riesgos del Hacking

**Hacker ético**

**a. Eticidad**

- "El nombre *hacker* es un neologismo utilizado para referirse a un experto (Gurú) en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes, sistemas operativos". (Dias, C., 2014)

- "El nombre *cracker* (criminal *hacker*, 1985) es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un *hacker*, sólo que, a diferencia de este último, el *cracker* realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo". (Dias, C., 2014)

- "El nombre *Hacker* ético hace referencia a profesionales de la seguridad que aplican sus conocimientos de *hacking* con fines defensivos (y legales)". (Dias, C., 2014)

- "Diremos *hacker* siempre, pero hay que fijarse en el contexto". (Dias, C., 2014)

- *Capacidades de un hacker ético*

  "Si conoces al enemigo y a ti mismo, no debes temer el resultado de cien batallas ". Sun Tzu, arte de la guerra

  - "Un *hacker* ético intenta responder a las siguientes preguntas":
    - "¿Qué puede saber un intruso de su objetivo? Fases 1 y 2"

  - “¿Qué puede hacer un intruso con esa información? Fases 3 y 4”
  - “¿Se podría detectar un intento de ataque? Fases 5 y 6”
- “¿Para que quisiera una empresa contratar a un *hacker* ético?”

- *Perfil de habilidades de un hacker ético*

  - “Experto en algún campo de la informática”.
  - “Conocimientos profundos de diversas plataformas (Windows, Unix, Linux)”.
  - “Conocimientos de redes”.
  - “Conocimientos de hardware y software”.

- *Deberes de un hacker ético*

  Fases de un proceso de evaluación de la seguridad:

  - Preparación: “Se debe tener un contrato firmado por escrito donde se exonere al *hacker* ético de toda responsabilidad como consecuencia de las pruebas que realice (siempre que sea dentro del marco acordado)”. (Dias, C., 2014)
  - Gestión: “Preparación de un informe donde se detallen las pruebas y posibles vulnerabilidades detectadas”. (Dias, C., 2014)
  - Conclusión: “Comunicación a la empresa del informe y de las posibles soluciones”. (Dias, C., 2014)

- *Modos de hacking ético*

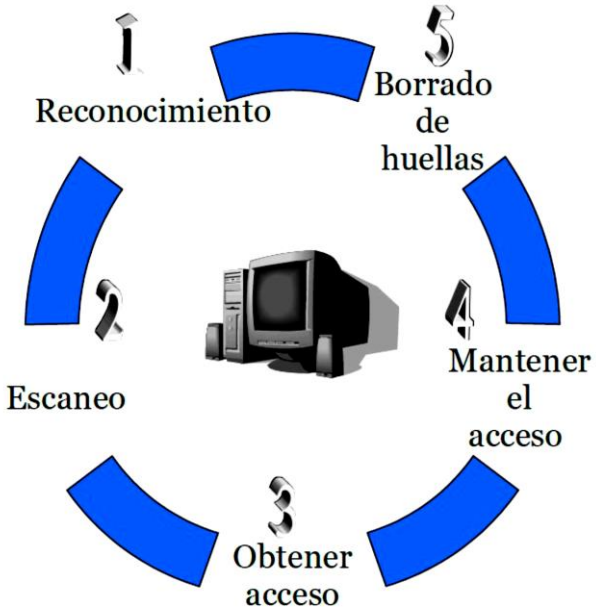
  - Redes remotas: “Simulación de un ataque desde Internet”.
  - Redes locales: “Simulación de un ataque desde dentro (empleados, *hacker* que ha obtenido privilegios en un sistema...)”
  - Ingeniería social: “Probar la confianza de los empleados”.
  - Seguridad física: “Accesos físicos (equipos, cintas de backup...)”

**b. Elementos de seguridad**

Elementos esenciales de la seguridad:

- *Confidencialidad: "*tiene que ver con la ocultación de información o recursos".
- *Autenticidad: "*es la identificación y garantía del origen de la información".
- *Integridad*: "se refiere a cambios no autorizados en los datos".
- *Disponibilidad*: "posibilidad de hacer uso de la información y recursos deseados".

**c. Facultades**




*1) Reconocimiento*

"Previo a cualquier ataque".

- "Información sobre el objetivo"
- "Reconocimiento pasivo":
  - "Google *Hacking"*

- “Ingeniería social”
- “Monitorización de redes de datos. Por ejemplo, sniffing, etc”.

2) *Escaneo*

“Escaneo es una fase de pre-ataque”.

- “Se escanea la red pero ya con información de la fase previa”.
- “Detección de vulnerabilidades y puntos de entrada”.
- “El escaneo puede incluir el uso de escaneadores de puertos y de vulnerabilidades”.
- Reconocimiento activo:
  - “Probar la red para detectar”.
  - “Hosts accesibles”
  - “Puertos abiertos”
  - “Localización de routers”
  - “Detalles de sistemas operativos y servicios”

3) *Obtener acceso*

“Obtención de acceso: Se refiere al ataque propiamente dicho”.

- Por ejemplo, hacer uso de un exploit o bug.
  - “Obtener una password, ataques man-inthe_middle (spoofing), exploits (buffer overflows), DoS (denial of service)”.

4) *Mantener acceso*

“Mantenimiento del acceso: Se trata de retener los privilegios obtenidos”.

- “A veces un *hacker* blinda el sistema contra otros posibles *hackers*, protegiendo sus puertas traseras, rootKits y Troyanos”.

*5) Borrado de huellas*

Borrado de huellas: Se intenta no ser descubierto.

- “Hay que tener claro que hay técnicas más intrusivas (y por lo tanto delatoras) que otras”.
- “Análisis forense”.

**Tipos de hacker**

**a. Black hats**

“Son individuos con habilidades extraordinarias en computación. Recurren a actividades maliciosas o destructivas. También se les conoce como *Crackers”*. (Dias, C., 2014)

**b. White hats**

“Son individuos con habilidades de *Hacker*. Utilizan sus habilidades con fines defensivos. También se les conoce como *Analistas de Seguridad”. (Dias, C., 2014)*

**c. Gray hats**

"Son individuos que trabajan tanto ofensivamente como defensivamente". (Dias, C., 2014)

## Marco legal

### a. Internacional

*Convenio sobre ciberdelincuencia*

"El convenio sobre ciberdelincuencia o convenio de Budapest se firma en Budapest en 2001 por parte de los miembros del Consejo Europeo. Podríamos considerarlo como el convenio más importante en el ámbito de la ciberdelincuencia. Hoy en día, ha sido firmado por más de 56 países y algunos más se encuentran a la espera de ser aceptados".

"El objetivo del convenio es crear una política penal común para los ciberdelitos y fomentar la cooperación internacional". "Para lograr este objetivo se establecen tres ejes centrales que se distribuyen a lo largo de los cuatro capítulos que posee el convenio y que son las siguientes":

- "Definir y clasificar los delitos informáticos: Esta clasificación se distribuye en las cuatro categorías que se muestran a continuación":
  - "Tecnología como fin": "Estos delitos dañan la confidencialidad, disponibilidad e integridad. Dentro de esta categoría se encuentran el acceso ilícito, la interceptación ilícita, ataques a la integridad de datos, ataques a la integridad del sistema y abuso de los dispositivos".
  - "Delitos informáticos o delitos" "que utilizan los sistemas informáticos como medio. Dentro de esta categoría se encuentran la falsificación y el fraude informáticos".
  - "Delitos relacionados con el contenido": "Se encuadran toda la tipología

de delitos de pornografía infantil".

- "Delitos relacionados con infracciones de la propiedad intelectual y derechos afines": "Se refiere a delitos vinculados con la vulneración de la propiedad intelectual y que utilizan como medio internet o sistemas informáticos".

• "Normas procesales": "En esta sección se instauran los procedimientos para proteger y salvaguardar la prueba o evidencia digital. Estos procedimientos son aplicables a cualquier delito en el que exista una evidencia digital o se haya cometido por algún medio o sistema electrónico. Establece la forma de recoger, asegurar, y conservar las evidencias digitales para que puedan utilizarse como pruebas en un proceso judicial".

• "Normas de cooperación internacional": "Facilitan unas directrices y reglas de cooperación para poder investigar internacionalmente delitos que incluyan evidencias digitales. Incluye disposiciones sobre los procesos de extradición, los envíos y recogidas de evidencias digitales para que se mantenga la cadena de custodia y la localización de sospechosos".

"Cuando un país es aceptado y ha firmado el convenio de Budapest ha de adecuar sus normas y legislaciones en materia de ciberseguridad a lo marcado en el convenio y además según el artículo 35 debe designar un punto de contacto para la red que este operativo 24 horas durante 7 días a la semana".

## b. Nacional

### 1) Política Nacional de Ciberseguridad

a) "Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el de la ciberseguridad, creando un entorno y las condiciones necesarias que permitan brindar protección en el ciberespacio".

b) "Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en materia de ciberseguridad dentro de la Administración Pública".

c) “Desarrollar un Plan de sensibilización y capacitación a todos los ciudadanos respecto a la Ciberseguridad”.

d) “Fortalecer la legislación en materia de ciberseguridad, la cooperación internacional y propiciar la adhesión del Perú a los diferentes organismos internacionales en esta temática”.

e) “Afianzar la integración y coordinación eficaz, entre las diversas Coordinadoras de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública y el sector privado”.

f) “Elaborar un Plan de Acción Nacional en Ciberseguridad”.

**g)** “Crear el Comité Nacional de Ciberseguridad”.

**2) Marco Normativo**

a) “Constitución Política del Perú”.
b) “Decreto Legislativo N° 604”.
c) “Ley N° 29158: Ley Orgánica del Poder Ejecutivo”.
d) “Ley Nº 27658: Ley Marco de Modernización de la Gestión del Estado”.
e) “Ley Nº 27806: Ley Transparencia y Acceso a la Información Pública”.
f) “Ley N° 27444: Ley de Procedimiento Administrativo General”.
g) “Ley N° 27269: Ley de Firmas y Certificados Digitales”.
h) “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”.
i) “Ley N° 28493: Ley que regula el uso del Correo Electrónico comercial no solicitado (SPAM)”.
j) “Ley N° 29733: Ley de Protección de Datos Personales”.
k) “Ley N° 28530: Ley de Promoción de Acceso a Internet para personas con discapacidad y adecuación del espacio físico en cabinas públicas

de internet".

l) "Ley N° 29904: Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica".

m) "Ley N° 30096 y su modificatoria Ley 30171: Ley de Delitos Informáticos".

n) "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".

o) "Decreto Supremo N° 022-2017-PCM, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros".

p) "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".

q) "Decreto Supremo N° 004-2013-PCM: Aprueba la Política Nacional de Modernización de la Gestión Pública".

r) "Decreto Supremo N° 081-2013-PCM: Aprueba la Política Nacional de Gobierno Electrónico 2013-2017".

s) "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".

t) "Resolución Ministerial N° 246-2007-PCM, que aprueba la Norma Técnica Peruana NTPISO/ 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".

u) "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".

v) “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”.

### 2.5.3 Definición de términos básicos

**2.5.3.1 Algoritmo RSA:** “Es un algoritmo para cifrar como para firmar digitalmente”.

**2.5.3.2 Ataque:** “Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera)”.

**2.5.3.3 Amenaza:** “Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información”.

**2.5.3.4 Autentificación:** “La autenticación es el acto o proceso para el establecimiento o confirmación de algo o alguien como real”.

**2.5.3.5 Auditoria:** “Es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes”.

**2.5.3.6 Bomba Lógica:** "Una bomba lógica es una parte de código insertada intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones pre programadas, en ese momento se ejecuta una acción maliciosa".

**2.5.3.7 Caballo de Troya:** "Es un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado".

**2.5.3.8 Ciberdefensa:** "Conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas".

**2.5.3.9 Ciberseguridad:** "Conjunto de acciones de carácter preventivo que tiene por objeto el uso de las redes propias y negarlo a terceros".

**2.5.3.10 Confiabilidad:** "La información disponible en la red presenta una serie de características que la hacen en extremo variable, por lo que su calidad no puede ser definida per segura. Entre los factores que determinan esta variabilidad".

**2.5.3.11 Congelación:** "Se produce cuando un programa de computadora, o todo el sistema dejan de responder a las entradas".

**2.5.3.12 Criptografía:** "Se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados".

**2.5.3.13 Cracker:** "Un hacker es alguien que descubre las debilidades de un computador o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas".

**2.5.3.14 Denegación:** "Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos".

**2.5.3.15** **Pulsos Electromagnéticos**: “Una emisión de energía electromagnética de alta intensidad en un breve período de tiempo”.

**2.5.3.16** **Guerra Electrónica:** “Consiste en una actividad tecnológica y electrónica con el fin de determinar, explotar, reducir o impedir el uso hostil de todos los espectros de energía”.

**2.5.3.17** **Gusano:** “Es un malware que tiene la propiedad de duplicarse a sí mismo”.

**2.5.3.18** **Hacker:** “Es todo individuo que se dedica a programar de forma entusiasta, o sea un experto entusiasta de cualquier tipo, que considera que poner la información al alcance de todos constituye un extraordinario bien”.

**2.5.3.19** **Malware:** “Código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario”.

**2.5.3.20** **Middleware:** “Es un software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones, o paquetes de programas, redes, hardware y/o sistemas operativos. Éste simplifica el trabajo de los programadores en la compleja tarea de generar las conexiones y sincronizaciones que son necesarias en los sistemas distribuidos”.

**2.5.3.21** **Modelo:** “Modelo informático Representación de la realidad por medio de abstracciones. Los modelos enfocan ciertas partes importantes de un sistema”.

**2.5.3.22** **Relación:** “Una relación o vínculo entre dos o más entidades describe alguna interacción entre las mismas”.

**2.5.3.23** **Set:** “Un comando para mostrar y asignar valor a las variables de entorno en sistemas operativos”.

**2.5.3.24** **Seguridad Informática:** “Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante”.

**2.5.3.25** **Servidor:** “Un servidor es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia”.

**2.5.3.26** **Sistema Distribuido:** “La computación distribuida o informática en malla es un modelo para resolver problemas de computación masiva utilizando un gran número de ordenadores organizados en clústeres incrustados en una infraestructura de telecomunicaciones distribuida”.

**2.5.3.27** **Variable:** “Una variable está formada por un espacio en el sistema de almacenaje (memoria principal de un ordenador) y un nombre simbólico (un identificador) que está asociado a dicho espacio”.

**2.5.3.28** **Virus:** “Es un malware que tiene por objetivo alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario”.

**2.5.3.29** **Vulnerabilidad:** “Las vulnerabilidades son puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad de este. Algunas de las vulnerabilidades más severas permiten que los atacantes ejecuten código arbitrario, denominadas vulnerabilidades de seguridad, en un sistema comprometido”.

**2.5.3.30** **Zombi:** “Es la denominación asignada a computadores personales que, tras haber sido infectados por algún tipo de malware, pueden ser usados por una tercera persona para ejecutar actividades hostiles”.

## CAPÍTULO III

# MARCO METODOLÓGICO

## 3.1 Método y Enfoque de la Investigación

"El método aplicado en el presente trabajo de investigación es el hipotético-deductivo. De hecho, el método hipotético deductivo consiste en elaborar una hipótesis que explicaría un fenómeno, para luego someterlo a prueba en un experimento". Argumenta, Guanipa (2010), el método hipotético deductivo, es el conjunto de teorías y conceptos básicos, elaborando en forma 60 deductiva las consecuencias empíricas de las hipótesis, y tratada de falsearla para reunir la información pertinente. Por tanto, busca la solución a los problemas planteados.

De la misma manera según Bernal (2006), "el método consiste en un procedimiento que parte de unas aseveraciones en calidad de hipótesis y busca reclutar o falsear tales hipótesis deduciendo de ellas con conclusiones las cuales deben confrontarse con los hechos. En tal sentido el enfoque hipotético deductivo llega a unas conclusiones a través de un procedimiento de inferencia o cálculo formal".

Según Sampieri R. et al (2004), "el enfoque cuantitativo se fundamenta en un esquema deductivo y lógico que busca formular preguntas de investigación e hipótesis para posteriormente probarlas. Por otro lado, el enfoque cualitativo se basa en un esquema inductivo y su método de investigación es interpretativo, contextual y etnográfico. Este método captura la experiencia de los individuos y estudia ambientes naturales". Ejemplos del enfoque cualitativo son las entrevistas y la observación no estructurada. Para el desarrollo del proyecto se adoptará el modelo de las dos etapas donde se aplica primero un enfoque y luego el otro de manera independiente. Al usar los dos enfoques, se enriquece la investigación con una perspectiva complementaria.

## 3.2 Tipo de Investigación

El tipo de investigación es básico-descriptivo-correlacional. Es descriptiva, ya que "Estos estudios describen la frecuencia y las características más importantes de un problema.

Arias (2006), “la investigación explicativa se encarga de buscar el porqué de los hechos mediante el establecimiento de relaciones causa efecto. En este sentido, los estudios explicativos pueden ocuparse tanto de la determinación de las causas (investigación post facto), como de los efectos 61 (investigación experimental), mediante la prueba de hipótesis sus resultados y conclusiones constituyen el nivel más profundo de conocimiento”.

## 3.3 Nivel y Diseño de la Investigación

La investigación será 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”.

En referencia, “a las acciones a utilizar por el investigador para obtener la información que dé respuesta a los objetivos de investigación, se abordó desde un diseño no experimental, donde se observó el comportamiento de las variables, sin manipular la información derivada del encuestado mediante la técnica del cuestionario; asimismo, se expresa como un diseño transversal, debido a los datos alcanzados mediante la planificación del investigador en tiempo y los recursos disponibles para su recolección”.

De esta manera, Hernández, Fernández y Baptista (2010), “refieren que las investigaciones no experimentales surgen cuando no se hacen variar intencionalmente las variables independientes, sino observan fenómenos tal y como se dan en su contexto natural, para después analizarlos. Por otra parte, de acuerdo con los autores, se identifica con el diseño transeccional o transversal, llevando a cabo la recolección de datos en un solo momento, en un tiempo único, teniendo como propósito de describir variables y analizar su incidencia e interpretación en un momento dado. En relación con los objetivos presentes en el estudio, se atribuyó a un diseño de campo, en los cuales la información de interés para dar respuesta a la situación investigada fue obtenida de la realidad, es decir se extrajo de la opinión poblacional que hace parte de las organizaciones académicas objeto de estudio”.

Para Arias (2006), “el diseño de campo consiste en la recolección de datos directamente en la realidad donde se generan los hechos, sin manipular o controlar variable alguna”. Por su parte, Tamayo y Tamayo (2009), “un diseño de campo recoge datos directamente de la realidad, por lo tanto, se le denomina primarios”.

Según Sabino (2008), “los diseños de campo son aquellos donde los datos de interés se recogen de manera directa de la realidad, bajo una experiencia empírica, en tal sentido son producto de la investigación en curso sin intermediación de alguna naturaleza”.

## 3.4 Técnicas e Instrumentos para la recolección de información

### 3.4.1 Elaboración de los instrumentos

#### a. Instrumento sobre la Ciberseguridad

**Variable 1 Ficha técnica:**

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

**Estructura:**

Las dimensiones que evalúan la Ciberseguridad son las siguientes:

1) Objetivos
2) Amenazas
3) Tipos de Ataques

Tabla 3

*Tabla de especificaciones para el cuestionario sobre la Ciberseguridad*

| Dimensiones | Estructura del cuestionario Ítems | Total | % |
|---|---|---|---|
| Objetivos | 1, 2, 3 | 3 | 30,0% |
| Amenazas | 4, 5, 6 | 3 | 30,0% |
| Tipos de Ataques | 7, 8, 9, 10 | 4 | 40,0% |
| Total, Ítems | | 10 | 100% |

*Fuente: Elaboración propia*

**b. Instrumento sobre los riesgos de Hacking en los Cadetes de 4to año de la EMCH**

**Variable 2 Ficha técnica**

- Nombre: Cuestionario para los riesgos de Hacking en los Cadetes de 4to año de la EMCH.
- Administración: Individual y colectiva
- Tiempo de administración: Entre 10 y 15 minutos, aproximadamente
- Ámbito de aplicación: Cadetes
- Significación: Conocimiento los riesgos de Hacking en los Cadetes de 4to año de la EMCH
- Tipo de respuesta: Los ítems son respondidos a través de escalamiento Likert con cinco valores categoriales.

**Estructura:**

Las dimensiones que evalúa los riesgos de Hacking en los Cadetes de 4to año de la EMCH son las siguientes:

1) Hacker ético
2) Tipos de hacker
3) Marco legal

Tabla 4

*Tabla de especificaciones para el cuestionario sobre los riesgos de Hacking en los Cadetes de 4to año de la EMCH*

| Dimensiones | Estructura del cuestionario Ítems | Total | % |
|---|---|---|---|
| Hacker ético | 11, 12, 13 | 3 | 37,50% |
| Tipos de hacker | 14, 15, 16 | 3 | 37,50% |
| Marco legal | 17, 18 | 2 | 25,00% |
| Total, Ítems | | 8 | 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 la Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la EMCH, 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 basada en elementos estandarizados | N de elementos |
|---|---|---|
| .893 | .893 | 18 |

*Fuente: Elaboración propia*

"El análisis nos reporta un resultado de 0,893 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 22", 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 56 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”.

Para Arias (2012) define como “…población un conjunto finito o infinito de elementos con características comunes para las cuales serán extensivas las conclusiones de la investigación…” (p.81).

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

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

$$n = 98 \ \ cadetes\ de\ 4to\ a\tilde{n}o\ de\ la\ EMCH$$

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:

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 x 0.35 = 14 |
| Artillería | 25 | 25 x 0.35 = 9 |
| Ingeniería | 33 | 33 x 0.35 = 12 |
| Comunicaciones | 30 | 30 x 0.35 = 11 |
| Inteligencia | 12 | 12 x 0.35 = 4 |
| Intendencia | 29 | 29 x 0.35 = 11 |
| Material de Guerra | 14 | 14 x 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 1: La Ciberseguridad

### Objetivos

1. ¿Considera usted que, la Infraestructura para cumplir los Objetivos de la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"?

Tabla 11. *La Infraestructura para cumplir los Objetivos de la Ciberseguridad*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 4 | 4,1 | 4,1 |
| | En desacuerdo | 12 | 12,2 | 16,3 |
| | De acuerdo | 4 | 4,1 | 20,4 |

| | | | | |
|---|---|---|---|---|
| | Totalmente de acuerdo | 78 | 79,6 | 100,0 |
| | Total | 98 | 100,0 | |

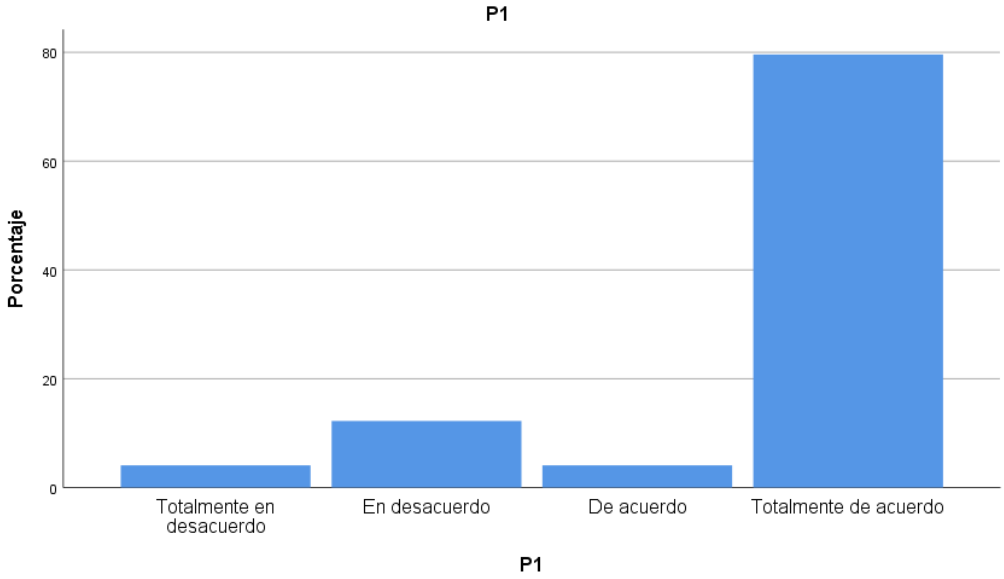



Figura 1. *La Infraestructura para cumplir los Objetivos de la Ciberseguridad*

**Análisis:** En cuanto a la interrogante si considera usted que la Infraestructura para cumplir los Objetivos de la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"; manifestaron que están totalmente de acuerdo 79,6%; por su parte dijeron que están de acuerdo el 4,1%; el 12,2% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 4,1%

2. ¿Considera usted que, el Usuario necesario para cumplir los Objetivos de la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"?

Tabla 12. *Usuario necesario para cumplir los Objetivos de la Ciberseguridad*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 8 | 8,2 | 8,2 |
| | En desacuerdo | 4 | 4,1 | 12,2 |
| | De acuerdo | 7 | 7,1 | 19,4 |
| | Totalmente de acuerdo | 79 | 80,6 | 100,0 |
| | Total | 98 | 100,0 | |

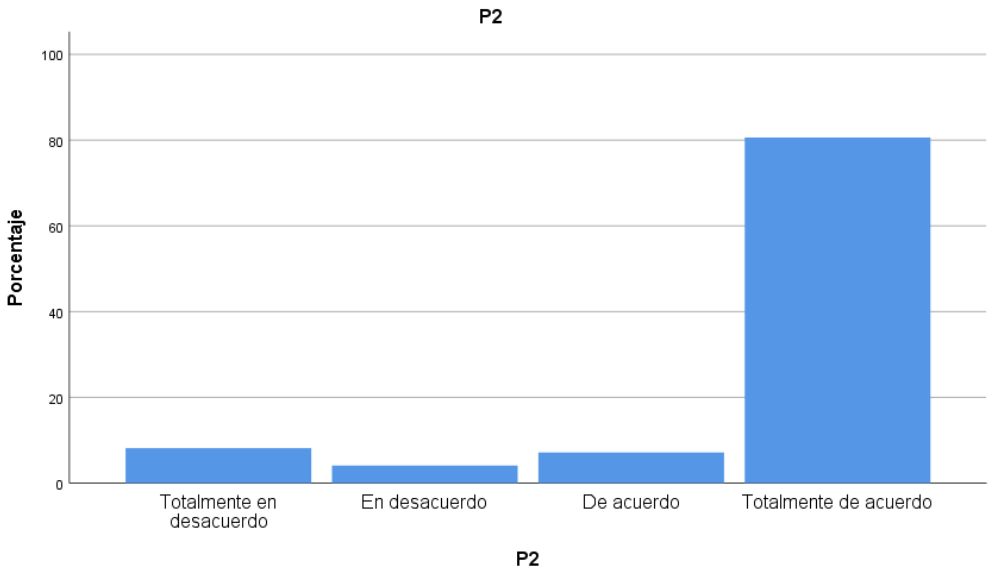



Figura 2. *Usuario necesario para cumplir los Objetivos de la Ciberseguridad*

**Análisis:** En cuanto a la interrogante si considera usted que el Usuario necesario para cumplir los Objetivos de la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"; manifestaron que están totalmente de acuerdo 80,6%; por su parte dijeron que están de acuerdo el 7,1%; el 4,1% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 8,2%

3. ¿Considera usted que, la Información necesaria para cumplir los Objetivos de la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"?

Tabla 13. *La Información necesaria para cumplir los Objetivos*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 12 | 12,2 | 12,2 |
| | En desacuerdo | 8 | 8,2 | 20,4 |
| | De acuerdo | 12 | 12,2 | 32,7 |
| | Totalmente de acuerdo | 66 | 67,3 | 100,0 |
| | Total | 98 | 100,0 | |

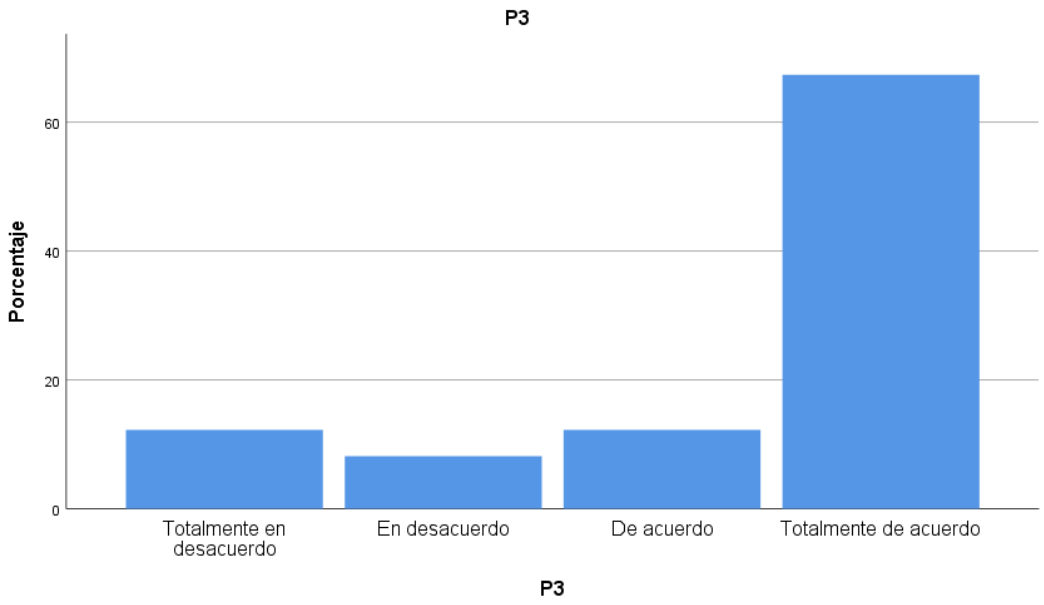



Figura 3. *La Información necesaria para cumplir los Objetivos*

**Análisis:** En cuanto a la interrogante si considera usted que la Información necesaria para cumplir los Objetivos de la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"; manifestaron que están totalmente de acuerdo 67,3%; por su parte dijeron que están de acuerdo el 12,2%; el 8,2% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 12,2%

## Amenazas

4. ¿Considera usted que las Amenazas a la Ciberseguridad, determinadas por su Origen se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"?

Tabla 14. *Las Amenazas a la Ciberseguridad determinadas por su Origen*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 4 | 4,1 | 4,1 |
| | En desacuerdo | 12 | 12,2 | 16,3 |
| | De acuerdo | 8 | 8,2 | 24,5 |
| | Totalmente de acuerdo | 74 | 75,5 | 100,0 |

| | | | | |
|---|---|---|---|---|
| | Total | 98 | 100,0 | |

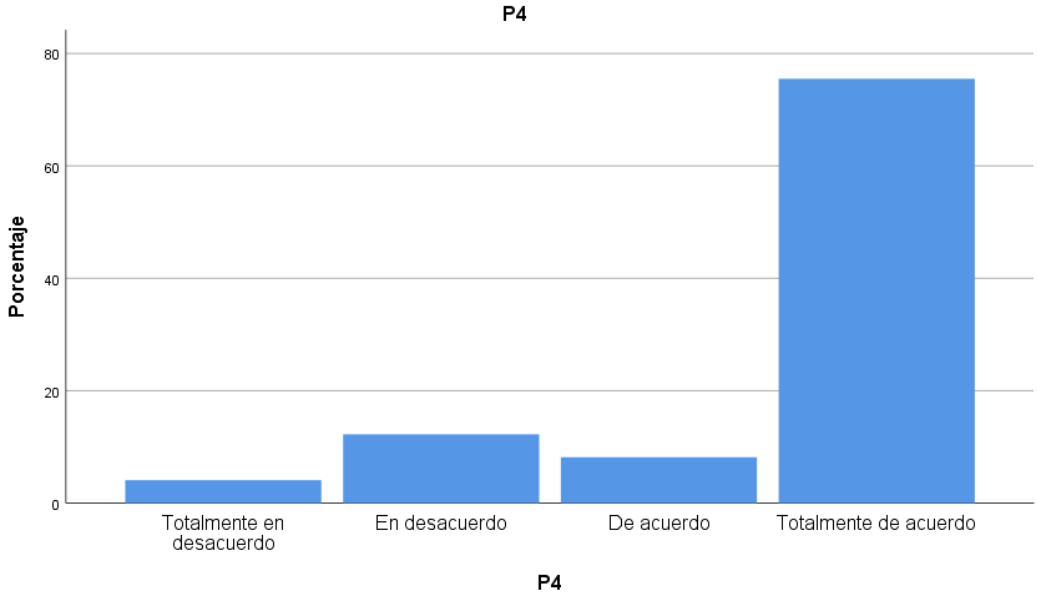



Figura 4. *Las Amenazas a la Ciberseguridad determinadas por su Origen*

**Análisis:** En cuanto a la interrogante si considera usted que las Amenazas a la Ciberseguridad, determinadas por su Origen se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"; manifestaron que están totalmente de acuerdo 75,5%; por su parte dijeron que están de acuerdo el 8,2%; el 12,2% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 4,1%

5. ¿Considera usted que las Amenazas a la Ciberseguridad, determinadas por su Efecto se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"?

Tabla 15. *Las Amenazas a la Ciberseguridad determinadas por su Efecto*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 7 | 7,1 | 7,1 |
| | En desacuerdo | 7 | 7,1 | 14,3 |
| | De acuerdo | 12 | 12,2 | 26,5 |
| | Totalmente de acuerdo | 72 | 73,5 | 100,0 |
| | Total | 98 | 100,0 | |

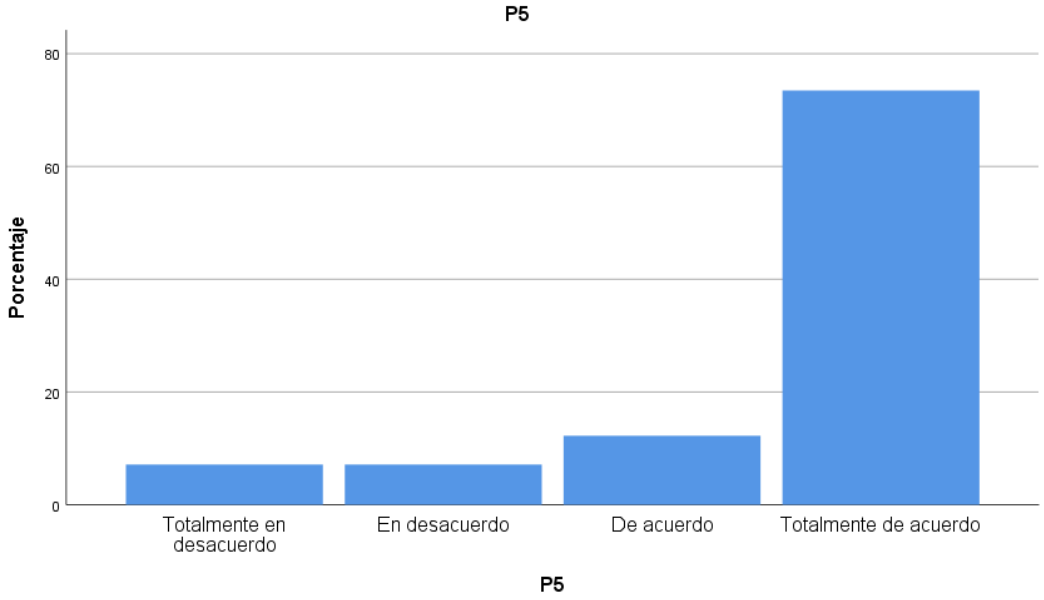



Figura 5. *Las Amenazas a la Ciberseguridad determinadas por su Efecto*

**Análisis:** En cuanto a la interrogante si considera usted que las Amenazas a la Ciberseguridad, determinadas por su Efecto se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"; manifestaron que están totalmente de acuerdo 73,5%; por su parte dijeron que están de acuerdo el 12,2%; el 7,1% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 7,1%

6. ¿Considera usted que las Amenazas a la Ciberseguridad, determinadas por el Medio Utilizado se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"?

Tabla 16. *Las Amenazas a la Ciberseguridad determinadas por el Medio*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 8 | 8,2 | 8,2 |
| | En desacuerdo | 8 | 8,2 | 16,3 |
| | De acuerdo | 11 | 11,2 | 27,6 |
| | Totalmente de acuerdo | 71 | 72,4 | 100,0 |
| | Total | 98 | 100,0 | |

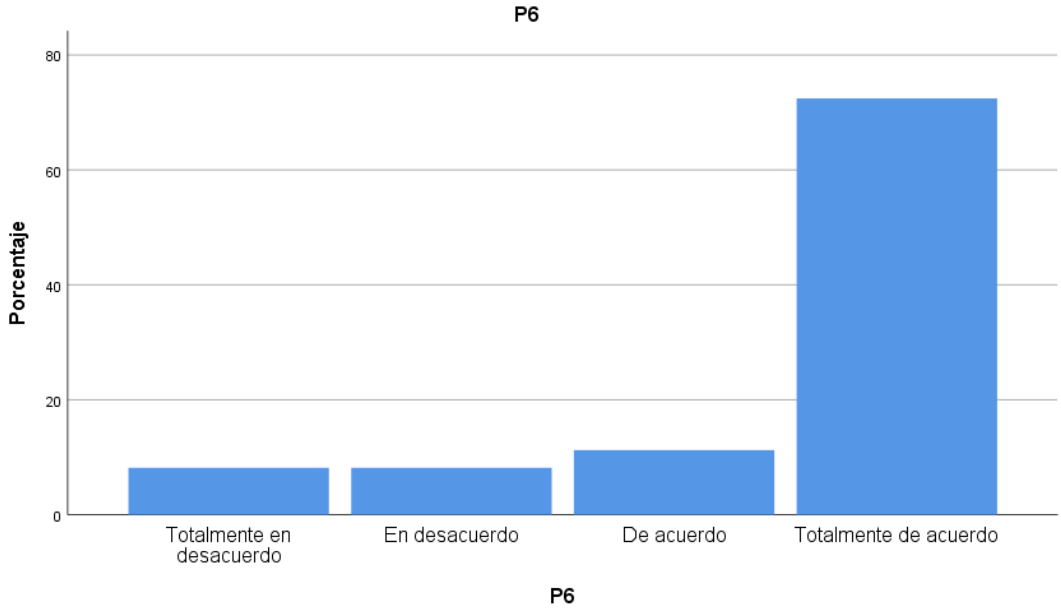



Figura 6. *Las Amenazas a la Ciberseguridad determinadas por el Medio*

**Análisis:** En cuanto a la interrogante si considera usted que las Amenazas a la Ciberseguridad, determinadas por el Medio Utilizado se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"; manifestaron que están totalmente de acuerdo 72,4%; por su parte dijeron que están de acuerdo el 11,2%; el 8,2% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 8,2%

## Tipos de Ataques

7. ¿Considera usted que los Tipos de Ataque por Repetición que atentan contra la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"?

Tabla 17. *Tipos de Ataque por Repetición*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 8 | 8,2 | 8,2 |
| | En desacuerdo | 8 | 8,2 | 16,3 |
| | De acuerdo | 8 | 8,2 | 24,5 |

| | | | | |
|---|---|---|---|---|
| | Totalmente de acuerdo | 74 | 75,5 | 100,0 |
| | Total | 98 | 100,0 | |

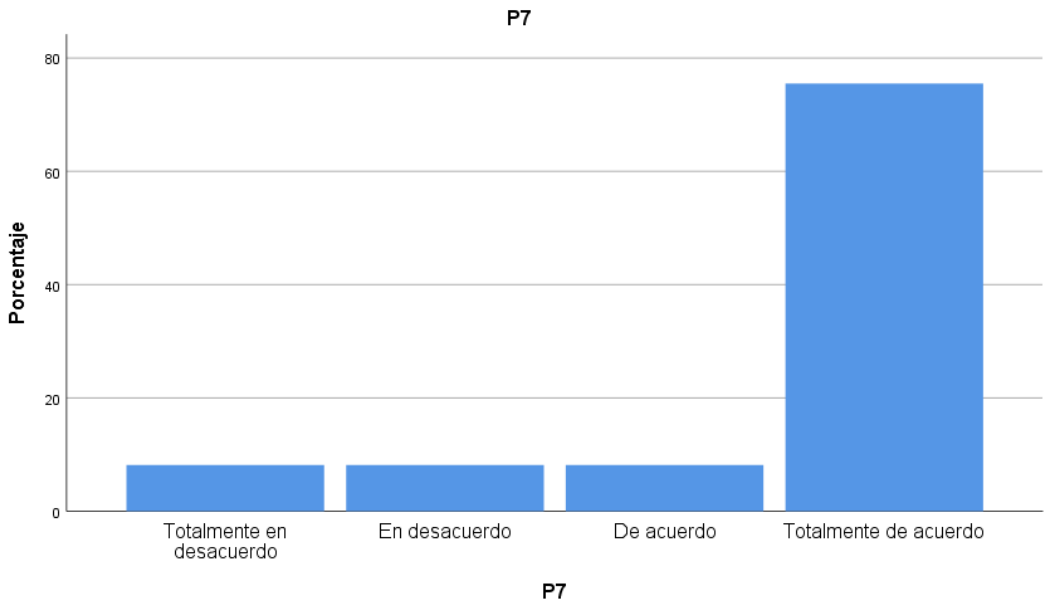



Figura 7. *Tipos de Ataque por Repetición*

**Análisis:** En cuanto a la interrogante si considera usted que los Tipos de Ataque por Repetición que atentan contra la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"; manifestaron que están totalmente de acuerdo 75,5%; por su parte dijeron que están de acuerdo el 8,2%; el 8,2% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 8,2%

8. ¿Considera usted que los Tipos de Ataque de Modificación de Bits que atentan contra la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"?

Tabla 18. *Tipos de Ataque de Modificación de Bits*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 7 | 7,1 | 7,1 |
| | En desacuerdo | 4 | 4,1 | 11,2 |
| | De acuerdo | 12 | 12,2 | 23,5 |
| | Totalmente de acuerdo | 75 | 76,5 | 100,0 |
| | Total | 98 | 100,0 | |

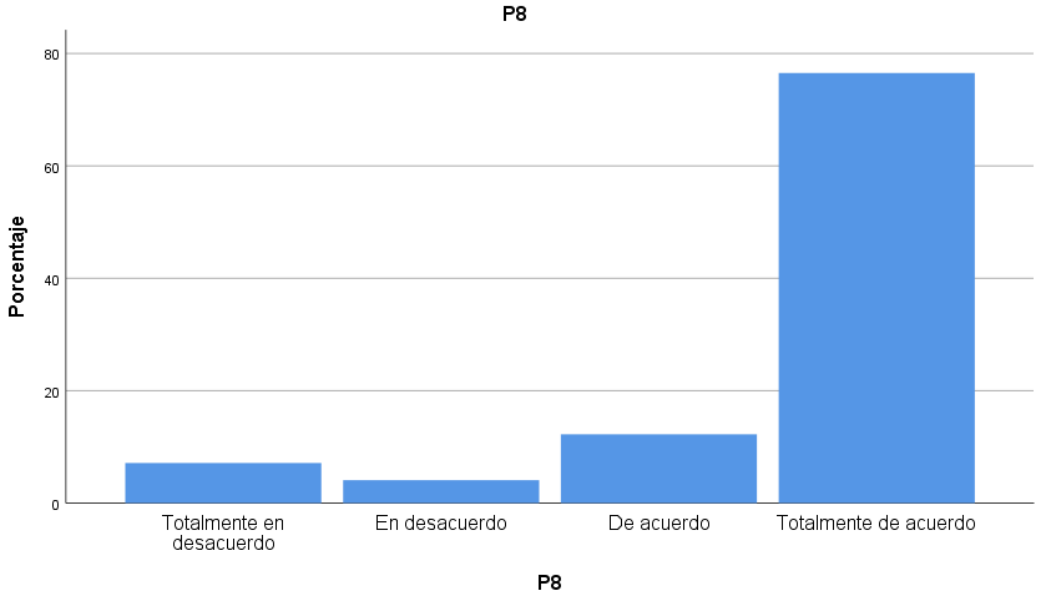



Figura 8. *Tipos de Ataque de Modificación de Bits*

**Análisis:** En cuanto a la interrogante si considera usted que los Tipos de Ataque de Modificación de Bits que atentan contra la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"; manifestaron que están totalmente de acuerdo 76,5%; por su parte dijeron que están de acuerdo el 12,2%; el 4,1% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 7,1%

9. ¿Considera usted que los Tipos de Ataque de Denegación de Servicio que atentan contra la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"?

Tabla 19. *Tipos de Ataque de Denegación de Servicio*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 7 | 7,1 | 7,1 |
| | En desacuerdo | 12 | 12,2 | 19,4 |
| | De acuerdo | 8 | 8,2 | 27,6 |
| | Totalmente de acuerdo | 71 | 72,4 | 100,0 |
| | Total | 98 | 100,0 | |

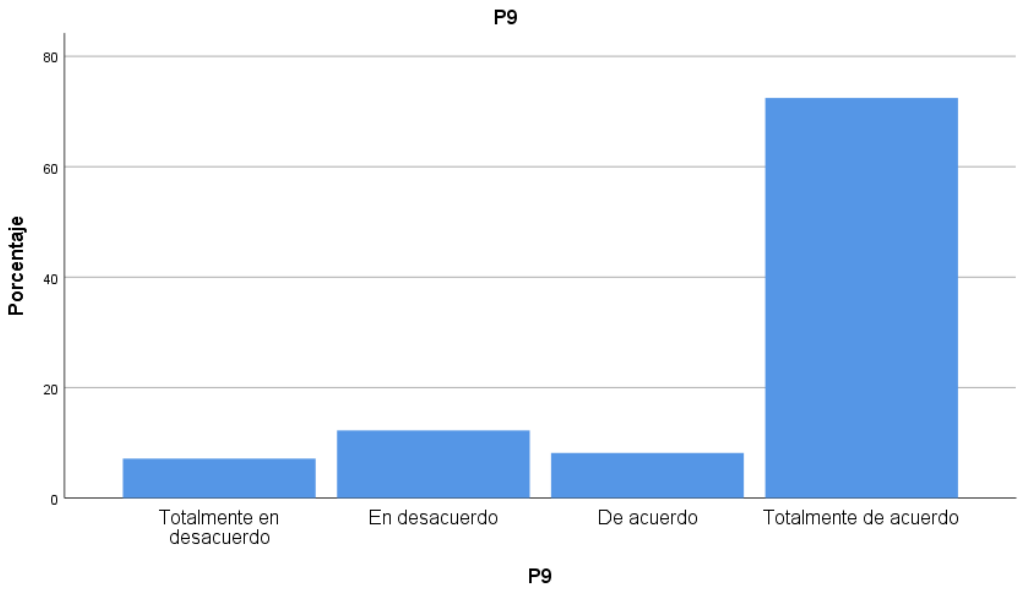



Figura 9. *Tipos de Ataque de Denegación de Servicio*

**Análisis:** En cuanto a la interrogante si considera usted que los Tipos de Ataque de Denegación de Servicio que atentan contra la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"; manifestaron que están totalmente de acuerdo 72,4%; por su parte dijeron que están de acuerdo el 8,2%; el 12,2% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 7,1%

10. ¿Considera usted que los Tipos de Ataque de Diccionario que atentan contra la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"?

Tabla 20. *Tipos de Ataque de Diccionario*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 8 | 8,2 | 8,2 |
| | En desacuerdo | 8 | 8,2 | 16,3 |
| | De acuerdo | 8 | 8,2 | 24,5 |
| | Totalmente de acuerdo | 74 | 75,5 | 100,0 |
| | Total | 98 | 100,0 | |

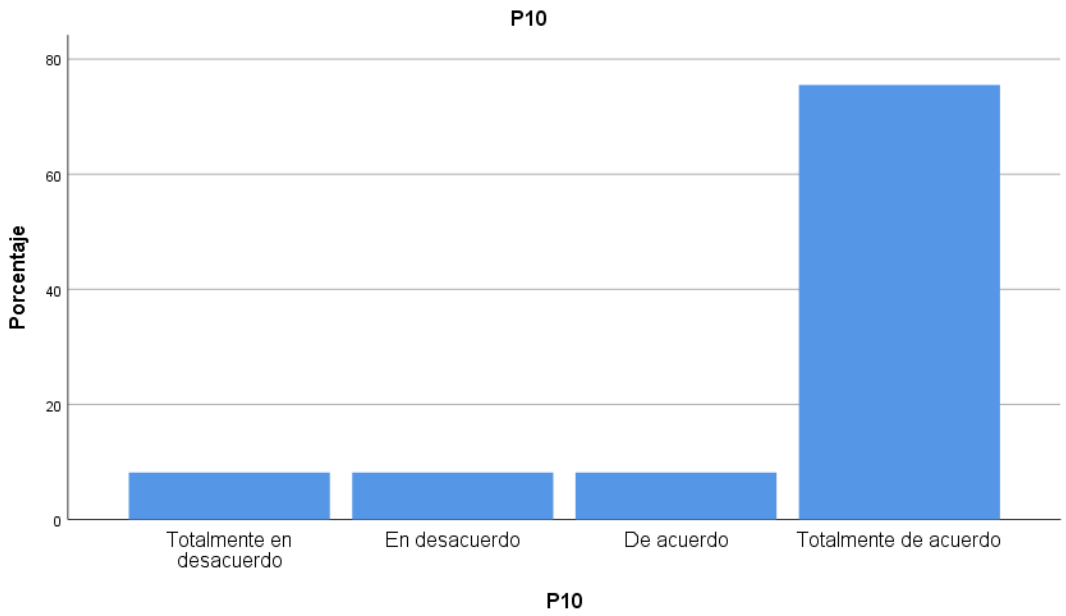



Figura 10. *Tipos de Ataque de Diccionario*

**Análisis:** En cuanto a la interrogante si considera usted que los Tipos de Ataque de Diccionario que atentan contra la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar "Coronel Francisco Bolognesi"; manifestaron que están totalmente de acuerdo 75,5%; por su parte dijeron que están de acuerdo el 8,2%; el 8,2% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 8,2%

**Para la Variable 1: Los Riesgos de Hacking en los Cadetes de 4to año de la EMCH Hacker Ético**

11. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, la Eticidad del Hacker puede ser influida por la Ciberseguridad?

Tabla 21. *La Eticidad del Hacker*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 8 | 8,2 | 8,2 |
| | En desacuerdo | 12 | 12,2 | 20,4 |
| | De acuerdo | 12 | 12,2 | 32,7 |
| | Totalmente de acuerdo | 66 | 67,3 | 100,0 |
| | Total | 98 | 100,0 | |

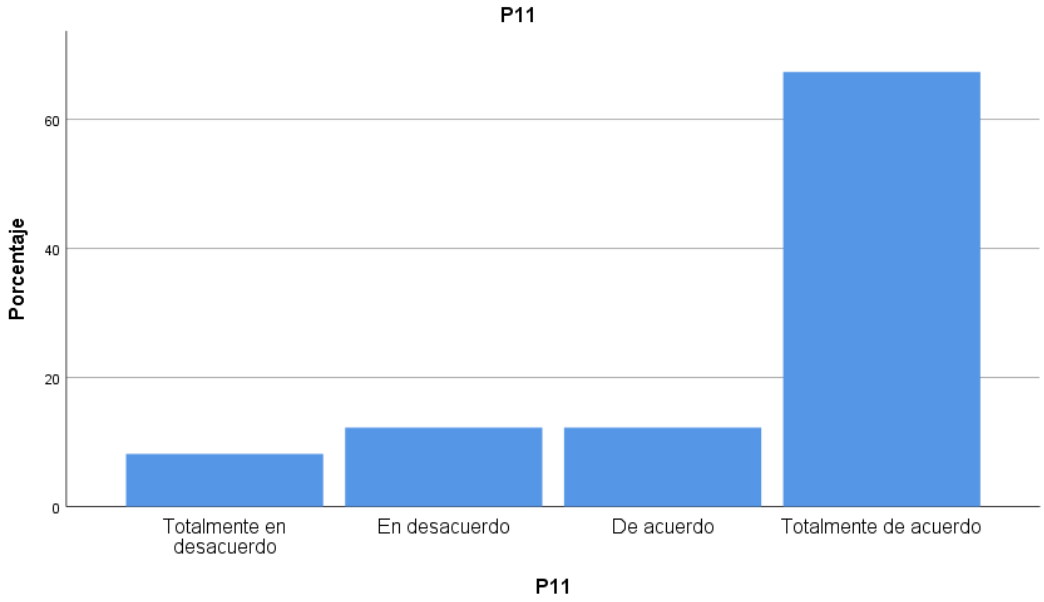



Figura 11. *La Eticidad del Hacker*

**Análisis:** En cuanto a la interrogante si considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, la Eticidad del Hacker puede ser influida por la Ciberseguridad; manifestaron que están totalmente de acuerdo 67,3%; por su parte dijeron que están de acuerdo el 12,2%; el 12,2% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 8,2%

12. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, los Elementos de Seguridad del Hacker pueden ser influidos por la Ciberseguridad?

Tabla 22. *Los Elementos de Seguridad del Hacker*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 4 | 4,1 | 4,1 |
| | En desacuerdo | 7 | 7,1 | 11,2 |
| | De acuerdo | 12 | 12,2 | 23,5 |
| | Totalmente de acuerdo | 75 | 76,5 | 100,0 |
| | Total | 98 | 100,0 | |

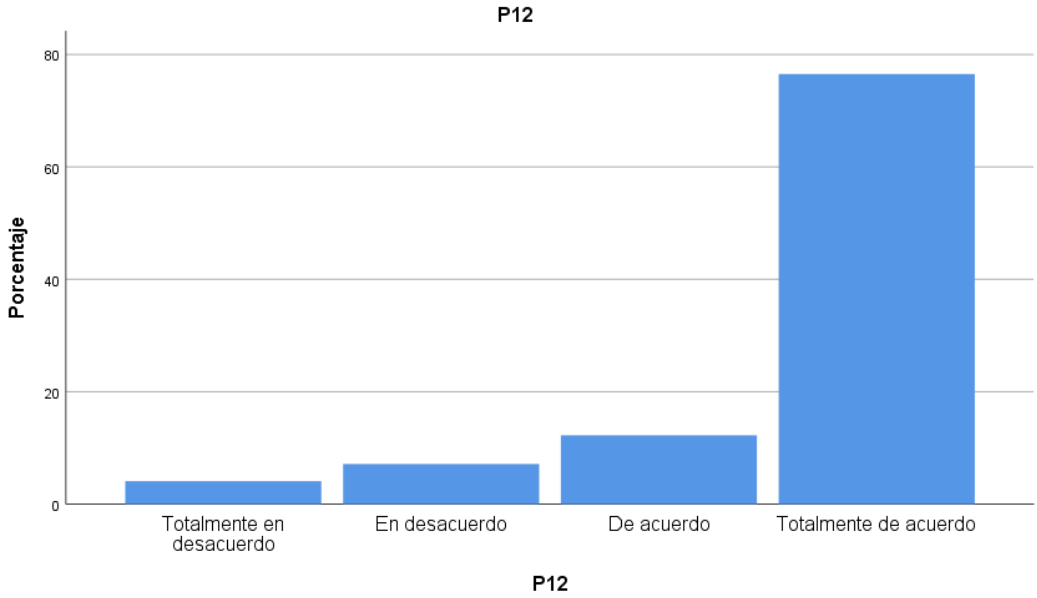



Figura 12. *Los Elementos de Seguridad del Hacker*

**Análisis:** En cuanto a la interrogante si considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, los Elementos de Seguridad del Hacker pueden ser influidos por la Ciberseguridad; manifestaron que están totalmente de acuerdo 76,5%; por su parte dijeron que están de acuerdo el 12,2%; el 7,1% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 4,1%

13. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, las facultades del Hacker pueden ser influidas por la Ciberseguridad?

Tabla 23. *Las facultades del Hacker*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 8 | 8,2 | 8,2 |
| | En desacuerdo | 11 | 11,2 | 19,4 |
| | De acuerdo | 12 | 12,2 | 31,6 |
| | Totalmente de acuerdo | 67 | 68,4 | 100,0 |
| | Total | 98 | 100,0 | |

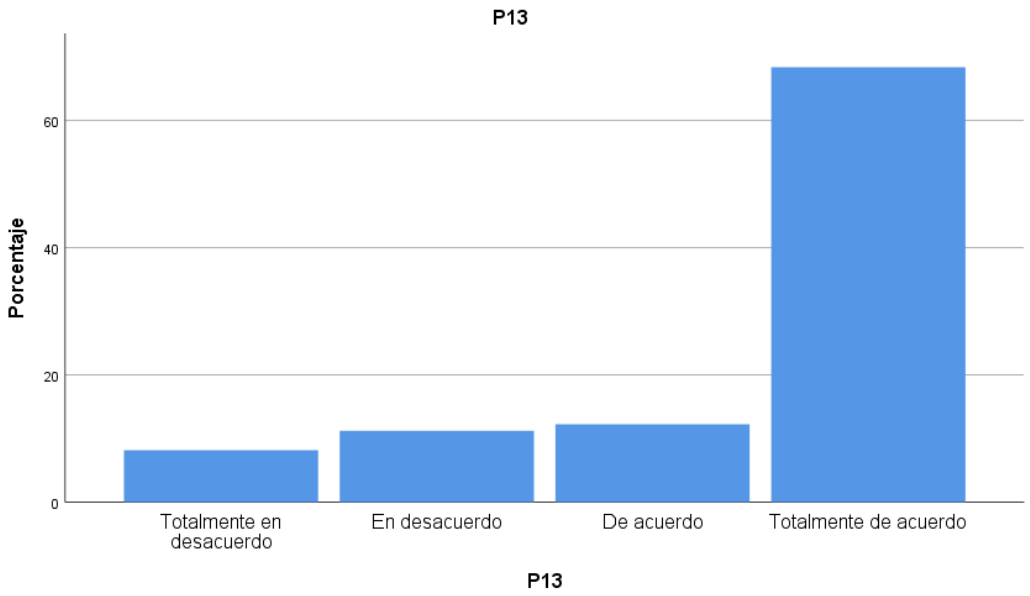



Figura 13. *Las facultades del Hacker*

**Análisis:** En cuanto a la interrogante si considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, las facultades del Hacker pueden ser influidas por la Ciberseguridad; manifestaron que están totalmente de acuerdo 68,4%; por su parte dijeron que están de acuerdo el 12,2%; el 11,2% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 8,2%

**Tipos de Hacker**

14. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Tipo de Hacker Black Hats puede ser influido por la Ciberseguridad?

Tabla 24. *Tipo de Hacker Black Hats*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 4 | 4,1 | 4,1 |
| | En desacuerdo | 12 | 12,2 | 16,3 |
| | De acuerdo | 16 | 16,3 | 32,7 |
| | Totalmente de acuerdo | 66 | 67,3 | 100,0 |
| | Total | 98 | 100,0 | |

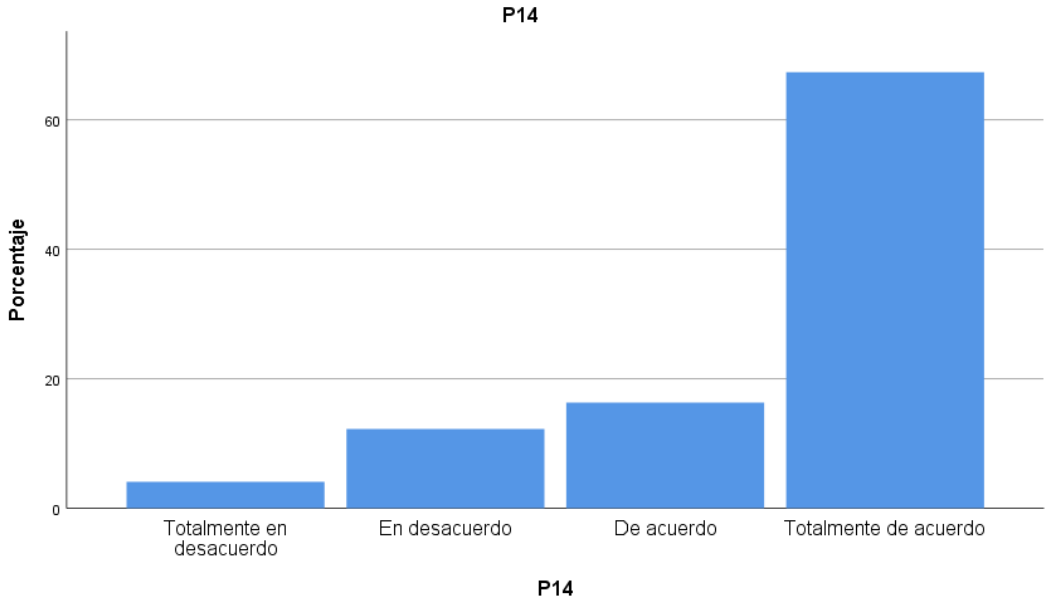



Figura 14. *Tipo de Hacker Black Hats*

**Análisis:** En cuanto a la interrogante si considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Tipo de Hacker Black Hats puede ser influido por la Ciberseguridad; manifestaron que están totalmente de acuerdo 67,3%; por su parte dijeron que están de acuerdo el 16,3%; el 12,2% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 4,1%

15. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Tipo de Hacker White Hats puede ser influido por la Ciberseguridad?

Tabla 25. *Tipo de Hacker White Hats*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 8 | 8,2 | 8,2 |
| | En desacuerdo | 8 | 8,2 | 16,3 |
| | De acuerdo | 20 | 20,4 | 36,7 |
| | Totalmente de acuerdo | 62 | 63,3 | 100,0 |
| | Total | 98 | 100,0 | |

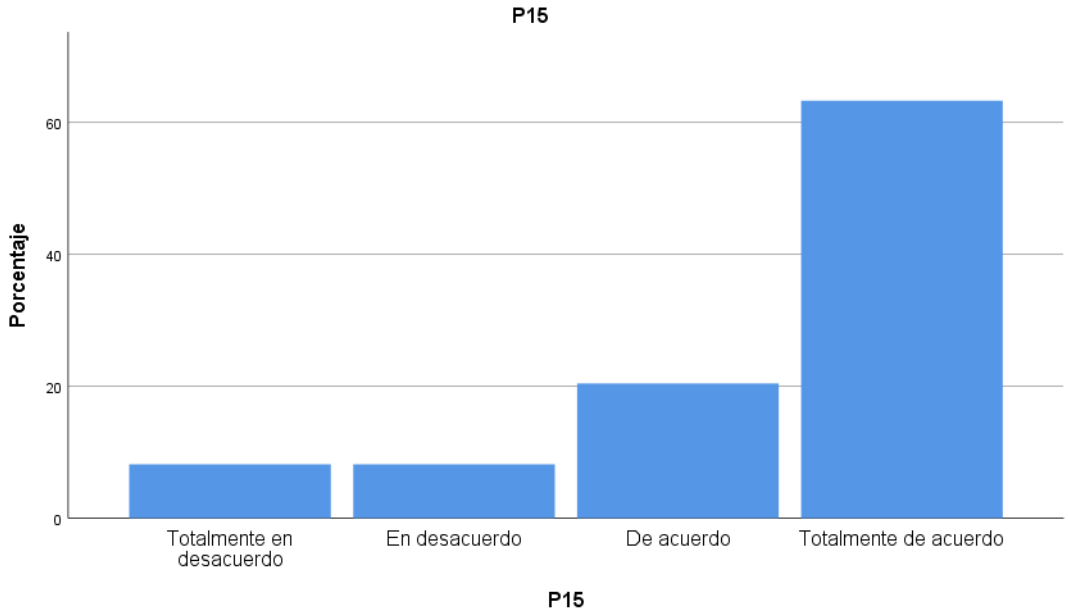



Figura 15. *Tipo de Hacker White Hats*

**Análisis:** En cuanto a la interrogante si considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Tipo de Hacker White Hats puede ser influido por la Ciberseguridad; manifestaron que están totalmente de acuerdo 63,3%; por su parte dijeron que están de acuerdo el 20,4%; el 8,2% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 8,2%

16. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Tipo de Hacker Gray Hats puede ser influido por la Ciberseguridad?

Tabla 26. *Tipo de Hacker Gray Hats*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 8 | 8,2 | 8,2 |
| | En desacuerdo | 8 | 8,2 | 16,3 |
| | De acuerdo | 12 | 12,2 | 28,6 |
| | Totalmente de acuerdo | 70 | 71,4 | 100,0 |
| | Total | 98 | 100,0 | |

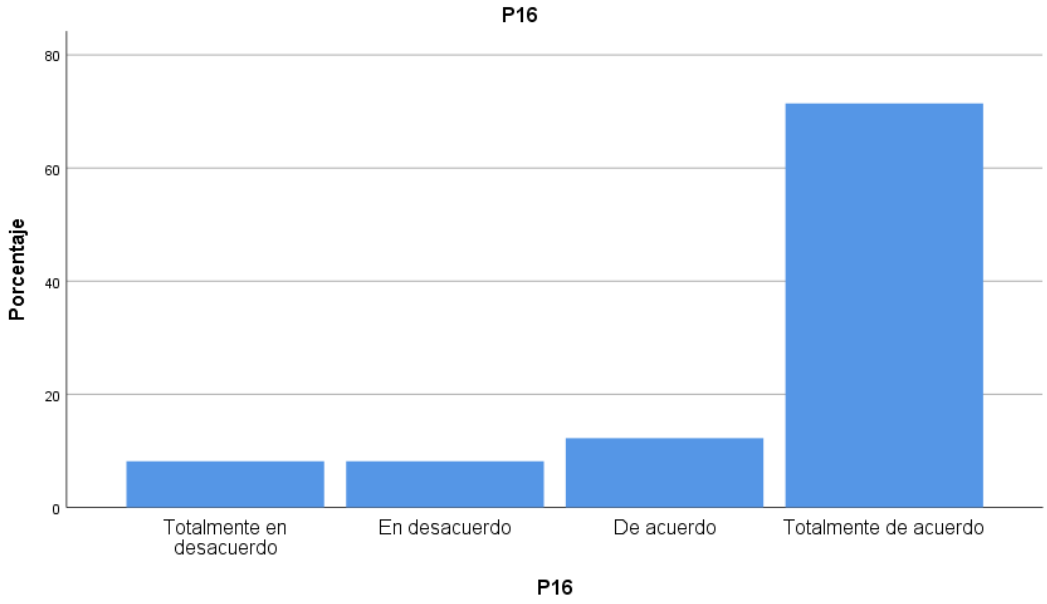



Figura 16. *Tipo de Hacker Gray Hats*

**Análisis:** En cuanto a la interrogante si considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Tipo de Hacker Gray Hats puede ser influido por la Ciberseguridad; manifestaron que están totalmente de acuerdo 71,4%; por su parte dijeron que están de acuerdo el 12,2%; el 8,2% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 8,2%

## Marco Legal

17. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Marco Legar Internacional puede ser influido por la Ciberseguridad?

Tabla 27. *Marco Legar Internacional*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 3 | 3,1 | 3,1 |
| | En desacuerdo | 16 | 16,3 | 19,4 |
| | De acuerdo | 16 | 16,3 | 35,7 |
| | Totalmente de acuerdo | 63 | 64,3 | 100,0 |
| | Total | 98 | 100,0 | |

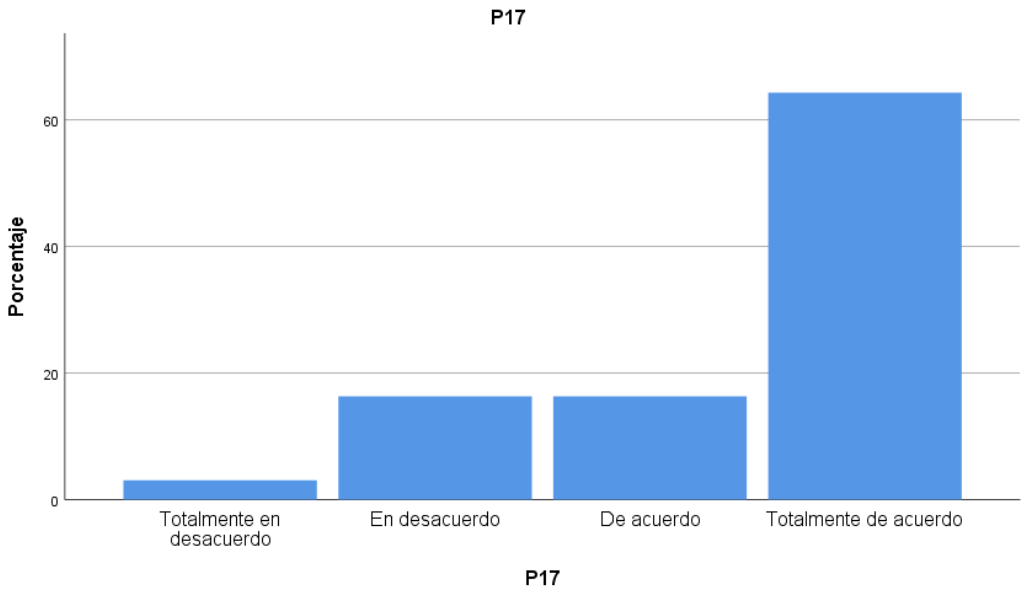



Figura 17. *Marco Legar Internacional*

**Análisis:** En cuanto a la interrogante si considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Marco Legar Internacional puede ser influido por la Ciberseguridad; manifestaron que están totalmente de acuerdo 64,3%; por su parte dijeron que están de acuerdo el 16,3%; el 16,3% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 3,1%

18. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Marco Legar Nacional puede ser influido por la Ciberseguridad?

Tabla 28. *Marco Legar Nacional*

| | | Frecuencia | Porcentaje | Porcentaje acumulado |
|---|---|---|---|---|
| Válido | Totalmente en desacuerdo | 3 | 3,1 | 3,1 |
| | En desacuerdo | 12 | 12,2 | 15,3 |
| | De acuerdo | 16 | 16,3 | 31,6 |
| | Totalmente de acuerdo | 67 | 68,4 | 100,0 |
| | Total | 98 | 100,0 | |

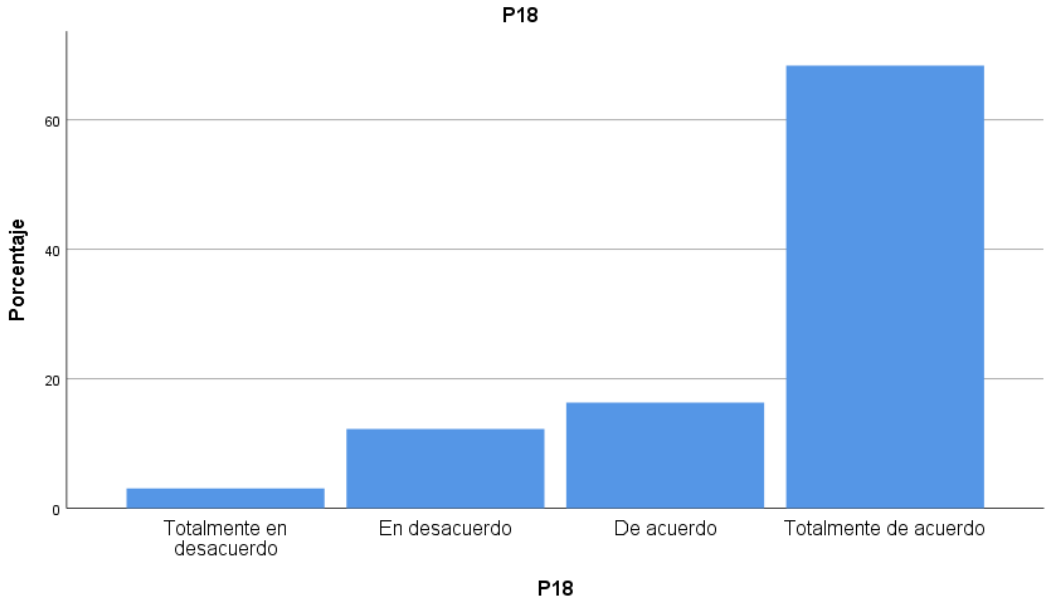



Figura 18. *Marco Legar Nacional*

**Análisis:** En cuanto a la interrogante si considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Marco Legar Internacional puede ser influido por la Ciberseguridad; manifestaron que están totalmente de acuerdo 68,4%; por su parte dijeron que están de acuerdo el 16,3%; el 12,2% dijeron que están en desacuerdo; y, manifestaron que están totalmente de acuerdo el 3,1%

## 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 Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020.

De los instrumentos de medición:

A su opinión ¿La Ciberseguridad se relaciona significativamente con los riesgos de Hacking en 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 29. *Pruebas de chi-cuadrado – hipótesis general*

| | Valor | gl | Sig. asintótica (2 caras) |
|---|---|---|---|
| Chi-cuadrado de Pearson | 50,313[a] | 561 | ,151 |
| Razón de verosimilitud | 31,957 | 561 | 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: 0.151

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

**Conclusión para la hipótesis general:**

El valor calculado para la Chi cuadrada (0.151) 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 Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020.

### 4.2.2. Prueba de hipótesis específica 1

Los Objetivos de la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020.

De los instrumentos de medición:

A su opinión ¿Los Objetivos de la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en 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 30. *Pruebas de chi-cuadrado – hipótesis especifica 1*

| | Valor | gl | Sig. asintótica (2 caras) |
|---|---|---|---|
| Chi-cuadrado de Pearson | 41,500[a] | 357 | ,198 |
| Razón de verosimilitud | 24,133 | 357 | 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 especifica 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 especifica 1 nula y se acepta la hipótesis general alterna.

Esto quiere decir los Objetivos de la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2020.

### 4.2.3. Prueba de hipótesis específica 2

Las Amenazas a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2020.

De los instrumentos de medición:

A su opinión ¿Las Amenazas a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en 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 31. *Pruebas de chi-cuadrado – hipótesis especifica 2*

| | Valor | gl | Sig. asintótica (2 caras) |
|---|---|---|---|
| Chi-cuadrado de Pearson | 35,513[a] | 323 | ,212 |
| Razón de verosimilitud | 27,090 | 323 | 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 especifica 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 especifica 2 nula y se acepta la hipótesis general alterna.

Esto quiere decir que las Amenazas a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2020.

### 4.2.4. Prueba de hipótesis específica 3

Los Tipos de Ataques a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en 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 a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en 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 especifica 3*

| | Valor | gl | Sig. asintótica (2 caras) |
|---|---|---|---|
| Chi-cuadrado de Pearson | 38,925[a] | 340 | ,105 |
| Razón de verosimilitud | 35,041 | 340 | 1,000 |
| Asociación lineal por lineal | 3,513 | 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: 0.105
Valor encontrado en el proceso: $X^2$ = 0.05

**Conclusión para la hipótesis especifica 3:**

El valor calculado para la Chi cuadrada (0.105) 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 especifica 3 nula y se acepta la hipótesis general alterna.

Esto quiere decir que los Tipos de Ataques a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en 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 Ciberseguridad se relaciona significativamente con los riesgos de Hacking en 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 Enríquez, U. y Mendoza, J. (2019). En su tesis para optar el Título Profesional de Ingeniero de Seguridad y Auditoría Informática, titulada: *“Aplicación de un hacking ético para mejorar la ciberseguridad de una entidad del Estado”*. Universidad Tecnológica del Perú. Lima. Perú. Concluyendo que: “En el trabajo realizado se presenta como la aplicación de un hacking ético para mejorar la ciberseguridad de una entidad del estado, siendo la Biblioteca General del Ejército del Perú como entidad del estado a evaluar, el cual permitirá poner en evidencia las vulnerabilidades que puedan ocasionar un gran impacto a sus sistemas de información. En el primer capítulo se presenta la problemática que tiene la Biblioteca General del Ejército del Perú. Se presenta además los objetivos, alcance, limitaciones, justificación y estado del arte para la aplicación del hacking ético. Llegaron a la conclusión de que es necesario la implementación de un hacking ético que permita neutralizar los riesgos a la ciberseguridad que trae consigo el manejo del ciberespacio y que puede atentar contra la información de carácter confidencial y reservado de las entidades del Estado”.

### 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 Objetivos de la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en 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 especifica 1, encontramos que tiene relación con la tesis de Maucaylle, A. (2019). En su tesis para optar el título profesional de Ingeniero de Sistemas, titulada*: “Construcción de un modelo de Red Virtual para aplicar técnicas de Hacking Ético y poder analizar los eventos relacionados a la Seguridad Informática sobre una*

*Infraestructura Virtual"*. Universidad Nacional José María Arguedas. Andahuaylas. Apurímac. Perú. Concluyendo lo siguiente: Para el análisis y monitoreo de los eventos generados en materia de seguridad informática en cada uno de los fases del hacking ético se empleó el software Wireshark; dicho análisis consistió entender el comportamiento de cada ataque generado y examinar los resultados obtenidos; producto de ello se pudo identificar el equipo que originó los ataques, los puertos y protocolos utilizados por las herramientas para lograr detectar las vulnerabilidades asociados a los elementos que conforman la red virtual, el nivel de concurrencia de los eventos que pudieron registrarse en contra de la seguridad de los servicios implementados.

### 4.3.3. Hipótesis Específica 2

Después del análisis de los datos que proporciono el trabajo estadístico respecto a la Hipótesis Especifica 2, que a la letra dice: Las Amenazas a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en 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 especifica 2, encontramos que tiene relación con la tesis de Benítez, J. (2019). En su tesis titulada: *"Análisis de riesgo en redes wifi aplicando técnicas de hacking ético"*. Universidad de las Américas. Quito. Ecuador. Llegando a la siguiente conclusión: El resultado de la aplicación de ambas metodologías de Octave e ISSAF permitieron identificar los principales activos críticos de la empresa, además se pudo crear sus correspondientes perfiles de amenazas y simular un ataque a la red con el objetivo de obtener una solución a las distintas vulnerabilidades presente en sus activos críticos. El uso del método cualitativo permitió manejar una mejor comunicación con todo el personal de la empresa, ya que se pudo establecer parámetros básicos que debían cumplir cada uno de los activos permitiendo clasificarlos y evaluarlos de mejor forma sin la necesidad de utilizar en su mayor parte términos técnicos que estén fuera de su comprensión.

### 4.3.4. Hipótesis Específica 3

Después del análisis de los datos que proporciono el trabajo estadístico respecto a la Hipótesis Especifica 3, que a la letra dice: Los Tipos de Ataques a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en 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 especifica 3, encontramos que tiene relación con la tesis de Mendaño, L. (2016). En su proyecto previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones, titulada: *"Implementación de Técnicas de Hacking Ético para el descubrimiento y evaluación de vulnerabilidades de la Red de una cartera de Estado"*. Escuela Politécnica Nacional. Quito. Ecuador. Concluyendo que: El presente proyecto nos ha permitido desarrollar un hacking Ético perimetral, que es una parte de las funciones que realiza un profesional en seguridad para determinar brechas de seguridad y generar un plan de mitigación. Todo sistema informático es vulnerable y los sistemas de la organización evaluada en este proyecto no ha sido la excepción, es cuestión de tiempo para que personas comunes o expertos en hardware y software, con conocimientos en tecnología descubran errores y quieran vulnerar los sistemas tecnológicos. Es por esto que existe personas dedicadas a evaluar vulnerabilidades con el objetivo de evidenciar, corregir y mejorar la seguridad.

## CONCLUSIONES

1. De acuerdo a la Hipótesis General que a la letra dice que, la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2020. El valor calculado para la Chi cuadrada 0.151 > 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, en la actualidad la tecnología relacionada al espectro electromagnético predomina ante la tecnología física que tradicionalmente se utilizaba el siglo próximo pasado; esto nos lleva a concluir que debe existir un Sistema de Ciberseguridad que permita neutralizar y/o minimizar todos los riesgos producidos por los Hacking a la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

2. De acuerdo a la Hipótesis Especifica 1 que a la letra dice que, los Objetivos de la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en 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, debemos tener en cuenta que los objetivos sobre los cuales se rige la Ciberseguridad tienen que generar sus medidas de seguridad a fin de evitar cualquier intromisión del hacking y los riesgos que este produce.

3. De acuerdo a la Hipótesis Especifica 2 que a la letra dice que, las Amenazas a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en 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, debemos tener en cuenta que las amenazas a la Ciberseguridad son múltiples por parte de los hacking y se deben adoptar las medidas adecuadas para anular y/o evitar dichas amenazas.

4. De acuerdo a la Hipótesis Especifica 3 que a la letra dice que, los Tipos de Ataques a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2020. El valor calculado para la Chi cuadrada 0.105 > 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, debemos tener en cuenta los tipos de ataques que se pueden gestar en el espacio electromagnético son diversos, por lo cual la Ciberseguridad debe adoptar las medidas adecuadas para anular y/o evitar las formas de actuar de los hacking.

## RECOMENDACIONES

1. Teniendo en consideración que la Ciberseguridad presenta objetivos, amenazas y tipos de ataques los cuales permiten analizar y estructurar los medios necesarios para prevenir y evitar los riesgos que de hacking en contra de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”; es recomendable que se implemente un Sistema de Ciberseguridad que asegure la neutralización y/o destrucción de todos los riesgos producidos por los Hacking a la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

2. Teniendo en consideración que los Objetivos de la Ciberseguridad incluyen la infraestructura, el usuario y la información, los cuales permiten focalizar y orientar de forma directa el esfuerzo para prevenir y evitar los riesgos que de hacking en contra de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”; es recomendable se implemente un sistema que permita tener en cuenta a los objetivos sobre los cuales se rige la Ciberseguridad, y de esta manera generar las medidas de seguridad adecuadas a fin de evitar cualquier intromisión del hacking y los riesgos que este produce.

3. Teniendo en consideración que las Amenazas a la Ciberseguridad incluyen el origen, el efecto y el medio utilizado por las mismas, las cuales permiten establecer de forma específica donde se debe combatir para prevenir y evitar los riesgos que de hacking en

contra de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”; es recomendable se implemente un sistema que permita tener en cuenta las amenazas a la Ciberseguridad, teniendo en consideración que estas son múltiples, a fin de evitar que se concrete cualquier amenaza proveniente de los hacking y los riesgos que estas pueden producir.

4. Teniendo en consideración que los Tipos de Ataque a la Ciberseguridad incluyen aquellos ataques por repetición, los de modificación de bits, los de denegación de servicio y los de diccionario, los cuales permiten establecer de forma específica como se debe prevenir los diferentes ataques y evitar los riesgos que de hacking en contra de los cadetes de 4to año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”; es recomendable se implemente un sistema que permita tener en cuenta los tipos de ataques que se pueden gestar en el espacio electromagnético, considerando que los mismos pueden ser diversos, a fin de evitar cualquier tipo de ataque proveniente de los hacking y los riesgos que estos pueden producir.

# PROPUESTA DE MEJORA
# "EVITANDO LOS RIESGOS QUE GENERA EL HACKING EN LA CIBERSEGURIDAD"

## 1. PRESENTACIÓN

Inicialmente debemos tener en cuenta que la ciencia de la informática en la actualidad es un elemento esencial y vía de acceso a cualquier país que desea el progreso y mejora de este; la totalidad de la información virtual que podemos encontrar en la red interna privada de una institución estatal o privada, militar o civil es considerada un activo. Por lo tanto, este activo deberá de ser considerad de vital importancia y resguardado. La principal amenaza que afecta a la seguridad de la información de una institución estatal o privada, militar o civil es el desconocimiento de los elementos que pueden generar riesgos para su seguridad. Por lo tanto, debe constituirse en un objetivo primordial el lograr una Ciberseguridad efectiva y acorde a las amenazas a las instituciones estatales o privadas, militares o civiles del Perú; en nuestro caso particular, a los cadetes del arma de Comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", los mismos que deben tener conocimiento de la importancia de salvaguardar la información virtual en sus redes privadas, y en las de interés institucional. Para la presente se ha utilizado los resultados de la investigación titulada "La Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020". Tras este análisis, se consideró necesaria

exposición de las razones son necesarias las medidas de ciberseguridad a fin de evitar los riegos que generan los hacking.

## 2. JUSTIFICACIÓN

Con la presente propuesta ayudaremos a fomentar una cultura de prevención y detección de riesgos cibernéticos entre los cadetes del arma de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”; teniendo pleno conocimiento del 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.

## 3. OBJETIVOS DE LA PROPUESTA

### 3.1. Objetivo general

Generar en los cadetes de 4to año del arma de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” una conciencia de seguridad cibernética que pueda anular y/o minimizar los riesgos producidos por los hacking a las informaciones privadas o institucionales.

### 3.2. Objetivos específicos

- Generar en los cadetes de 4to año del arma de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” una conciencia de seguridad cibernética orientada a los Objetivos que persigue la Ciberseguridad, que pueda anular y/o minimizar los riesgos producidos por los hacking a las informaciones privadas o institucionales.

- Generar en los cadetes de 4to año del arma de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” una conciencia de seguridad cibernética orientada a las Amenazas a las cuales debe hacer frente la Ciberseguridad, que pueda anular y/o minimizar los riesgos producidos por los hacking a las informaciones privadas o institucionales.

- Generar en los cadetes de 4to año del arma de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” una conciencia de seguridad cibernética orientada a los Tipos de Ataque a los cuales debe hacer frente la Ciberseguridad, que pueda anular y/o minimizar los riesgos producidos por los hacking a las informaciones privadas o institucionales.

## 4. META

Lograr que los Cadetes de 4to año del arma de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” puedan manejar los medios de Ciberseguridad necesarios para anular y/o minimizar los riesgos que producen los Hacking.

## 5. METODOLOGÍA

Los instrumentos, procedimientos y técnicas usadas en las actividades académicas y militares, tendrán una directriz procesual, porque ya no se trata de solo elaborar contenidos, sino conseguir procesos para el manejo, la interiorización y apropiación, tanto como el uso proactivo de los valores institucionales.

### 5.1. Plan de acción

Presentar una propuesta con medidas de Ciberseguridad ante la Sub Dirección Académica y el Departamento de Seguridad (S-2) de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, especificando las necesidades y las mejoras que estas pueden producir en la seguridad de las informaciones privadas de los Cadetes de Comunicaciones y el Batallón de Cadetes en General.

### 5.2. Actividades

- Elaborar las medidas de Ciberseguridad necesarias para proteger las informaciones.
- Exponer la propuesta.
- Realizar la complementación de las medidas de seguridad existentes.
- Presentar el trabajo terminado.

- Coordinar con la Sub Dirección Académica y el Departamento de Seguridad (S-2) para implementar las medidas de Ciberseguridad.

### 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 del arma de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, bajo la supervisión de su Jefe de Sección, Jefe de Área, Jefe del Departamento Académico y Jefe del Departamento de Seguridad (S-2) de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

## 7. VIABILIDAD

La propuesta es viable, toda vez que sean aprobados los aspectos que complementaran las medidas de seguridad existentes y estén de acuerdo a las circunstancias de las amenazas a la Ciberseguridad generadas por los Hacking; no siendo necesario recursos económicos ni materiales, solo el empleo de personal de Oficiales y Cadetes de 4to año de Comunicaciones.

## 8. SEGUIMIENTO Y EVALUACIÓN

El Plan de Mejora, es de interés de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”; 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 de los procesos (durante el desarrollo de las actuaciones) se llevará a cabo durante todo el proceso de implantación de las distintas

actuaciones previstas en el plan de mejora para comprobar, optimizar y mejorar su desarrollo.

- *Evaluación Final.* Para evaluar el grado de consecución de los objetivos propuestos, la evaluación final (reflexión y síntesis al final de la acción) considerará aspectos tanto cuantitativos como cualitativos.

## REFERENCIAS BIBLIOGRAFICAS

Aguirre, A. (2017). En su tesis para obtener su Maestría, titulada: *"Ciberseguridad en Infraestructuras Críticas de Información"*. Universidad de Buenos Aires. Buenos Aires. Argentina

Arias, F. (2006). *El proyecto de investigación: Introducción a la metodología científica* (5a ed.). Caracas: Episteme.

Arias, F. (2012). El Proyecto de Investigación. Introducción a la metodología científica. (6ª Edición). Caracas: Editorial Episteme.

Benítez, J. (2019). En su tesis titulada: *"Análisis de riesgo en redes wifi aplicando técnicas de hacking ético"*. Universidad de las Américas. Quito. Ecuador

Berbeo, j. (2019). En su tesis para optar el grado académico de maestro en Ingeniería de Sistemas con mención en Tecnología de Información y Comunicación, titulada: *"Implementación de Hacking ético para la detección y evaluación de vulnerabilidades de red en la empresa Complex del Perú S.A.C.-Tumbes; 2017"*. Universidad Católica Los Ángeles de Chimbote. Tumbes. Perú

Bernal, C. (2006). Metodología de la investigación para administración, economía, humanidades y ciencias sociales. (2da ed.). México: Pearson.

De Miguel, M. y Oltra, J. (2007). *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas*. Valencia: Ed. UPV. ISBN 978- 84-8363-112-6.

Dias, C. (2014). *Hacking ético*. Universitat Oberta de Catalunya. Madrid

Enríquez, U. y Mendoza, J. (2019). En su tesis para optar el Título Profesional de Ingeniero de Seguridad y Auditoría Informática, titulada: *"Aplicación de un hacking ético para mejorar la ciberseguridad de una entidad del Estado"*. Universidad Tecnológica del Perú. Lima. Perú

Guanipa, M. (2010). *Reflexiones básicas sobre investigación (Primera edición).* Fondo Editorial Universidad Rafael Belloso Chacín. Venezuela.

Hernández, R.; Baptista, P. y Fernández, C. (2004). Metodología de la investigación. México, editorial Mc Graw Hill, 3ª edición.

Hernández, R.; Baptista, P. y Fernández, C. (2010). *Metodología de la investigación*. (5.ta ed.). México: Mc Graw-Hill.

Llongueras, A. (2013). *La guerra inexistente, la ciberguerra*. Madrid (Esp.). Eae Editorial Acad MIA Espa Ola.

Maucaylle, A. (2019). En su tesis para optar el título profesional de Ingeniero de Sistemas, titulada*: "Construcción de un modelo de Red Virtual para aplicar técnicas de Hacking Ético y poder analizar los eventos relacionados a la Seguridad Informática sobre una Infraestructura Virtual"*. Universidad Nacional José María Arguedas. Andahuaylas. Apurímac. Perú

Mendaño, L. (2016). En su proyecto previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones, titulada: *"Implementación de Técnicas de Hacking Ético para el descubrimiento y evaluación de vulnerabilidades de la Red de una cartera de Estado"*. Escuela Politécnica Nacional. Quito. Ecuador

Palella, S. y Martins, F. (2008). Metodología de la Investigación Cuantitativa (2ª Edición). Caracas: FEDUPEL.

Pastor, O.; Pérez, J.; Arnáiz, D. & Taboso, P. (2009). *Seguridad Nacional y Ciberdefensa*. Madrid: Cátedra ISDEFE-UPM.

Pérez, C. (2005). Muestreo estadístico. Conceptos y problemas resueltos. Madrid: Pearson Educación s.a.

Sabino, C. (2008). *El proceso de investigación*. Caracas: Panapo

**ANEXOS**

**ANEXO 01** Matriz de consistencia

**ANEXO 02** Encuesta

**ANEXO 03** Base de datos

**ANEXO 04** Validación del instrumento

**ANEXO 05** Constancia donde se efectuó la investigación

**ANEXO 06** Compromiso de autenticidad

**ANEXO 07** Acta de sustentación de tesis

# Anexo 1


## Matriz de consistencia

# Anexo 1. Matriz de Consistencia

**Titulo:** La Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020

| PROBLEMAS | OBJETIVOS | HIPÓTESIS | VARIABLES | DIMENSIONES | INDICADORES | METODOLOGÍA |
|---|---|---|---|---|---|---|
| **Problema General**<br><br>¿Cuál es la relación que existe entre la Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" 2020?<br><br>**Problemas Específicos**<br><br>¿Cuál es la relación que existe entre los Objetivos de la Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" 2020?<br><br>¿Cuál es la relación que existe entre las Amenazas a la Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" 2020?<br><br>¿Cuál es la relación que existe entre los Tipos de Ataques a la Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" 2020? | **Objetivo General**<br><br>Determinar cuál es la relación que existe entre la Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020.<br><br>**Objetivos Específicos**<br><br>Establecer cuál es la relación que existe entre los Objetivos de la Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020.<br><br>Establecer cuál es la relación que existe entre las Amenazas a la Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020.<br><br>Establecer cuál es la relación que existe entre los Tipos de Ataques a la Ciberseguridad y los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020. | **Hipótesis General**<br><br>La Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020.<br><br>**Hipótesis Específicas**<br><br>Los Objetivos de la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020.<br><br>Las Amenazas a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020.<br><br>Los Tipos de Ataques a la Ciberseguridad se relaciona significativamente con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020. | **Variable Independiente**<br><br>**(X)**<br><br>**La Ciberseguridad** | $X_1$<br>Objetivos | • Infraestructura<br>• Usuario<br>• Información | **Tipo / Nivel investigación**<br>Descriptivo-Correlacional<br><br>**Diseño de investigación**<br>No Experimental<br><br>**Enfoque de investigación**<br>Cuantitativo<br><br>**Técnica**<br>Se ha aplicado:<br>• Investigación documental<br>• Investigación de campo<br><br>**Instrumentos**<br>Se utilizó:<br>• Cuestionarios<br>• Encuestas<br><br>**Población**<br>278 Cadetes del 4to año de la EMCH<br><br>**Muestra**<br>98 Cadetes del 4to año de la EMCH<br><br>**Métodos de Análisis de Datos**<br>Estadística SPSS22 |
| | | | | $X_2$<br>Amenazas | • Por el origen<br>• Por el efecto<br>• Por el medio utilizado | |
| | | | | $X_3$<br>Tipos de Ataques | • Por repetición<br>• De modificación de bits<br>• De denegación de servicio<br>• De diccionario | |
| | | | **Variable Dependiente**<br><br>**(Y)**<br><br>**Los riesgos de Hacking en los Cadetes de 4to año de la EMCH** | $Y_1$<br>Hacker ético | • Eticidad<br>• Elementos de seguridad<br>• Facultades | |
| | | | | $Y_2$<br>Tipos de hacker | • Black hats<br>• White hats<br>• Gray hats | |
| | | | | $Y_3$<br>Marco legal | • Internacional<br>• Nacional | |

# Anexo 2


## Encuesta

## Anexo 2. Encuesta

### Encuesta 1

### LA CIBERSEGURIDAD

La presente encuesta es para determinar cuál es la relación que existe entre la Ciberseguridad y los riesgos de Hacking en 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 |

| **Objetivos** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|
| 1. ¿Considera usted que, la Infraestructura para cumplir los Objetivos de la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar “Coronel Francisco Bolognesi”? | | | | |
| 2. ¿Considera usted que, el Usuario necesario para cumplir los Objetivos de la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar “Coronel Francisco Bolognesi”? | | | | |
| 3. ¿Considera usted que, la Información necesaria para cumplir los Objetivos de la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar “Coronel Francisco Bolognesi”? | | | | |
| **Amenazas** | **1** | **2** | **3** | **4** |
| 4. ¿Considera usted que las Amenazas a la Ciberseguridad, determinadas por su Origen se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar “Coronel Francisco Bolognesi”? | | | | |

| | | | | |
|---|---|---|---|---|
| 5. ¿Considera usted que las Amenazas a la Ciberseguridad, determinadas por su Efecto se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar “Coronel Francisco Bolognesi”? | | | | |
| 6. ¿Considera usted que las Amenazas a la Ciberseguridad, determinadas por el Medio Utilizado se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar “Coronel Francisco Bolognesi”? | | | | |
| **Tipos de Ataques** | **1** | **2** | **3** | **4** |
| 7. ¿Considera usted que los Tipos de Ataque por Repetición que atentan contra la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar “Coronel Francisco Bolognesi”? | | | | |
| 8. ¿Considera usted que los Tipos de Ataque de Modificación de Bits que atentan contra la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar “Coronel Francisco Bolognesi”? | | | | |
| 9. ¿Considera usted que los Tipos de Ataque de Denegación de Servicio que atentan contra la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar “Coronel Francisco Bolognesi”? | | | | |
| 10. ¿Considera usted que los Tipos de Ataque de Diccionario que atentan contra la Ciberseguridad se relaciona con los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar “Coronel Francisco Bolognesi”? | | | | |

**Encuesta 2**

**LOS RIESGOS DE HACKING EN LOS CADETES DE 4TO AÑO DE LA EMCH**

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

| **Hacker Ético** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|
| 11. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, la Eticidad del Hacker puede ser influida por la Ciberseguridad? | | | | |
| 12. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, los Elementos de Seguridad del Hacker pueden ser influidos por la Ciberseguridad? | | | | |
| 13. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, las facultades del Hacker pueden ser influidas por la Ciberseguridad? | | | | |
| **Tipos de Hacker** | **1** | **2** | **3** | **4** |
| 14. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Tipo de Hacker Black Hats puede ser influido por la Ciberseguridad? | | | | |
| 15. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Tipo de Hacker White Hats puede ser influido por la Ciberseguridad? | | | | |
| | | | | |

| | | | | |
|---|---|---|---|---|
| 16. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Tipo de Hacker Gray Hats puede ser influido por la Ciberseguridad? | | | | |
| **Marco Legal** | **1** | **2** | **3** | **4** |
| 17. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Marco Legar Internacional puede ser influido por la Ciberseguridad? | | | | |
| 18. ¿Considera usted que, dentro de los riesgos de Hacking en los Cadetes de 4to año de la Escuela Militar, el Marco Legar Nacional puede ser influido por la Ciberseguridad? | | | | |

# Anexo 3


## Base de datos

*Base de Datos CAD IV CON DOMINGUEZ.sav [ConjuntoDatos1] - IBM SPSS Statistics Editor de datos

Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

99 : P1

| | P1 | P2 | P3 | P4 | P5 | P6 | P7 | P8 | P9 | P10 | P11 | P12 | P13 | P14 | P15 | P16 | P17 | P18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 4 | 4 | 4 | 4 | 4 | 1 | 4 | 4 | 2 | 4 | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 4 |
| 2 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 2 | 4 | 1 | 4 | 3 | 2 | 2 | 2 |
| 3 | 2 | 4 | 1 | 4 | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 2 | 3 | 3 | 4 | 4 |
| 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 6 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 7 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 8 | 4 | 4 | 4 | 4 | 1 | 2 | 2 | 4 | 4 | 2 | 4 | 1 | 4 | 1 | 4 | 4 | 4 | 4 |
| 9 | 4 | 4 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 3 | 3 |
| 10 | 4 | 2 | 1 | 4 | 4 | 4 | 4 | 4 | 3 | 1 | 2 | 3 | 1 | 4 | 3 | 2 | 2 | 4 |
| 11 | 2 | 4 | 4 | 2 | 4 | 4 | 4 | 3 | 2 | 4 | 3 | 4 | 2 | 2 | 4 | 1 | 3 | 3 |
| 12 | 4 | 4 | 3 | 4 | 3 | 1 | 1 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 2 | 4 | 4 | 4 |
| 13 | 4 | 3 | 4 | 3 | 2 | 3 | 4 | 4 | 3 | 1 | 4 | 4 | 4 | 3 | 1 | 4 | 4 | 4 |
| 14 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 2 | 4 | 4 | 3 | 2 | 3 | 2 | 4 | 4 | 4 |
| 15 | 3 | 4 | 2 | 4 | 4 | 3 | 4 | 3 | 4 | 3 | 2 | 2 | 3 | 4 | 3 | 1 | 2 | 2 |
| 16 | 4 | 4 | 4 | 1 | 3 | 4 | 1 | 2 | 4 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 3 | 3 |
| 17 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 18 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 19 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 20 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 21 | 4 | 1 | 2 | 2 | 3 | 2 | 3 | 1 | 4 | 3 | 1 | 4 | 4 | 4 | 1 | 3 | 2 | 2 |
| 22 | 2 | 4 | 1 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 3 | 3 | 4 | 4 |
| 23 | 1 | 4 | 3 | 4 | 4 | 4 | 2 | 4 | 4 | 4 | 3 | 3 | 3 | 4 | 4 | 4 | 3 | 3 |
| 24 | 4 | 3 | 4 | 4 | 2 | 3 | 4 | 1 | 1 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 1 | 1 |
| 25 | 4 | 4 | 4 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 2 | 4 | 4 | 4 | 4 | 4 |
| 26 | 4 | 4 | 4 | 4 | 4 | 1 | 4 | 4 | 2 | 4 | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 4 |
| 27 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 2 | 4 | 1 | 4 | 3 | 2 | 2 | 2 |
| 28 | 2 | 4 | 1 | 4 | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 2 | 3 | 3 | 4 | 4 |
| 29 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 30 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 31 | 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 |
| 33 | 4 | 4 | 4 | 4 | 1 | 2 | 2 | 4 | 4 | 2 | 4 | 1 | 4 | 1 | 4 | 4 | 4 | 4 |
| 34 | 4 | 4 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 3 | 3 |
| 35 | 4 | 2 | 1 | 4 | 4 | 4 | 4 | 4 | 3 | 1 | 2 | 3 | 1 | 4 | 3 | 2 | 2 | 4 |

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 36 | 2 | 4 | 4 | 2 | 4 | 4 | 4 | 3 | 2 | 4 | 3 | 4 | 2 | 2 | 4 | 1 | 3 | 3 |
| 37 | 4 | 4 | 3 | 4 | 3 | 1 | 1 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 2 | 4 | 4 | 4 |
| 38 | 4 | 3 | 4 | 3 | 2 | 3 | 4 | 4 | 3 | 1 | 4 | 4 | 4 | 3 | 1 | 4 | 4 | 4 |
| 39 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 2 | 4 | 4 | 3 | 2 | 3 | 2 | 4 | 4 | 4 |
| 40 | 3 | 4 | 2 | 4 | 4 | 3 | 4 | 3 | 4 | 3 | 2 | 2 | 3 | 4 | 3 | 1 | 2 | 2 |
| 41 | 4 | 4 | 4 | 1 | 3 | 4 | 1 | 2 | 4 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 3 | 3 |
| 42 | 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 |
| 44 | 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 |
| 46 | 4 | 1 | 2 | 2 | 3 | 2 | 3 | 1 | 4 | 3 | 1 | 4 | 4 | 4 | 1 | 3 | 2 | 2 |
| 47 | 2 | 4 | 1 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 3 | 3 | 4 | 4 |
| 48 | 1 | 4 | 3 | 4 | 4 | 4 | 2 | 4 | 4 | 4 | 3 | 3 | 3 | 4 | 4 | 4 | 3 | 3 |
| 49 | 4 | 3 | 4 | 4 | 2 | 3 | 4 | 1 | 1 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 1 | 1 |
| 50 | 4 | 4 | 4 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 2 | 4 | 4 | 4 | 4 | 4 |
| 51 | 4 | 4 | 4 | 4 | 4 | 1 | 4 | 4 | 2 | 4 | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 4 |
| 52 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 2 | 4 | 1 | 4 | 3 | 2 | 2 | 2 |
| 53 | 2 | 4 | 1 | 4 | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 2 | 3 | 3 | 4 | 4 |
| 54 | 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 |
| 56 | 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 |
| 58 | 4 | 4 | 4 | 4 | 1 | 2 | 2 | 4 | 4 | 2 | 4 | 1 | 4 | 1 | 4 | 4 | 4 | 4 |
| 59 | 4 | 4 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 3 | 3 |
| 60 | 4 | 2 | 1 | 4 | 4 | 4 | 4 | 4 | 3 | 1 | 2 | 3 | 1 | 4 | 3 | 2 | 2 | 4 |
| 61 | 2 | 4 | 4 | 2 | 4 | 4 | 4 | 3 | 2 | 4 | 3 | 4 | 2 | 2 | 4 | 1 | 3 | 3 |
| 62 | 4 | 4 | 3 | 4 | 3 | 1 | 1 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 2 | 4 | 4 | 4 |
| 63 | 4 | 3 | 4 | 3 | 2 | 3 | 4 | 4 | 3 | 1 | 4 | 4 | 4 | 3 | 1 | 4 | 4 | 4 |
| 64 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 2 | 4 | 4 | 3 | 2 | 3 | 2 | 4 | 4 | 4 |
| 65 | 3 | 4 | 2 | 4 | 4 | 3 | 4 | 3 | 4 | 3 | 2 | 2 | 3 | 4 | 3 | 1 | 2 | 2 |
| 66 | 4 | 4 | 4 | 1 | 3 | 4 | 1 | 2 | 4 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 3 | 3 |
| 67 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 68 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 69 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 70 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 71 | 4 | 1 | 2 | 2 | 3 | 2 | 3 | 1 | 4 | 3 | 1 | 4 | 4 | 4 | 1 | 3 | 2 | 2 |
| 72 | 2 | 4 | 1 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 3 | 3 | 4 | 4 |
| 73 | 1 | 4 | 3 | 4 | 4 | 4 | 2 | 4 | 4 | 4 | 3 | 3 | 3 | 4 | 4 | 4 | 3 | 3 |
| 74 | 4 | 3 | 4 | 4 | 2 | 3 | 4 | 1 | 1 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 1 | 1 |
| 75 | 4 | 4 | 4 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 2 | 4 | 4 | 4 | 4 | 4 |
| 76 | 4 | 4 | 4 | 4 | 4 | 1 | 4 | 4 | 2 | 4 | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 4 |
| 77 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 2 | 4 | 1 | 4 | 3 | 2 | 2 | 2 |
| 78 | 2 | 4 | 1 | 4 | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 2 | 3 | 3 | 4 | 4 |
| 79 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 80 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 81 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 82 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 83 | 4 | 4 | 4 | 4 | 1 | 2 | 2 | 4 | 4 | 2 | 4 | 1 | 4 | 1 | 4 | 4 | 4 | 4 |
| 84 | 4 | 4 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 3 | 3 |
| 85 | 4 | 2 | 1 | 4 | 4 | 4 | 4 | 4 | 3 | 1 | 2 | 3 | 1 | 4 | 3 | 2 | 2 | 4 |
| 86 | 2 | 4 | 4 | 2 | 4 | 4 | 4 | 3 | 2 | 4 | 3 | 4 | 2 | 2 | 4 | 1 | 3 | 3 |
| 87 | 4 | 4 | 3 | 4 | 3 | 1 | 1 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 2 | 4 | 4 | 4 |
| 88 | 4 | 3 | 4 | 3 | 2 | 3 | 4 | 4 | 3 | 1 | 4 | 4 | 4 | 3 | 1 | 4 | 4 | 4 |
| 89 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 2 | 4 | 4 | 3 | 2 | 3 | 2 | 4 | 4 | 4 |
| 90 | 3 | 4 | 2 | 4 | 4 | 3 | 4 | 3 | 4 | 3 | 2 | 2 | 3 | 4 | 3 | 1 | 2 | 2 |
| 91 | 4 | 4 | 4 | 1 | 3 | 4 | 1 | 2 | 4 | 4 | 1 | 4 | 4 | 4 | 4 | 4 | 3 | 3 |
| 92 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 93 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 94 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 95 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 96 | 4 | 1 | 2 | 2 | 3 | 2 | 3 | 1 | 4 | 3 | 1 | 4 | 4 | 4 | 1 | 3 | 2 | 2 |
| 97 | 2 | 4 | 1 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 3 | 3 | 4 | 4 |
| 98 | 1 | 4 | 3 | 4 | 4 | 4 | 2 | 4 | 4 | 4 | 3 | 3 | 3 | 4 | 4 | 4 | 3 | 3 |

# Anexo 4


## Validación del instrumento

## Anexo 4.a. Validación De Instrumento Por Experto

**TÍTULO DEL TRABAJO DE INVESTIGACIÓN/TESIS**:
LA CIBERSEGURIDAD Y LOS RIESGOS DE HACKING EN LOS CADETES DE 4TO AÑO DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI", 2020

AUTORES:
DOMÍNGUEZ PIÑAS FRANK
COTERA CEDANO RENZO

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**:
LA CIBERSEGURIDAD Y LOS RIESGOS DE HACKING EN LOS CADETES DE 4TO AÑO DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI", 2020

AUTORES:
DOMÍNGUEZ PIÑAS FRANK
COTERA CEDANO RENZO

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**:
LA CIBERSEGURIDAD Y LOS RIESGOS DE HACKING EN LOS CADETES DE 4TO AÑO DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI", 2020

AUTORES:
DOMÍNGUEZ PIÑAS FRANK
COTERA CEDANO RENZO

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

## Anexo 5. 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: LA CIBERSEGURIDAD Y LOS RIESGOS DE HACKING EN LOS CADETES DE 4TO AÑO DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI", 2020

Investigadores:

DOMÍNGUEZ PIÑAS FRANK
COTERA CEDANO RENZO

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

Chorrillos,….. de…….. del 2020

# Anexo 6


## Compromiso de autenticidad

## Anexo 6. Compromiso de autenticidad del instrumento

Los Cadetes que suscriben líneas abajo, autores del trabajo de investigación titulado: LA CIBERSEGURIDAD Y LOS RIESGOS DE HACKING EN 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,….. de ……del 2020

…….…… ……

DOMÍNGUEZ PIÑAS FRANK COTERA CEDANO RENZO

# Anexo 7


## Acta de sustentación de tesis

# ESCUELA MILITAR DE CHORRILLOS
# "CORONEL FRANCISCO BOLOGNESI"

## ACTA DE SUSTENTACION DE TESIS – PROM CXXVII

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:

LA CIBERSEGURIDAD Y LOS RIESGOS DE HACKING EN LOS CADETES DE 4TO AÑO DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI", 2020

Presentada por:

- COTERA CEDANO RENZO MAREK
- DOMINGUEZ PIÑAS FRANK RICHARD

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 JESUS
- 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