ESCUELA MILITAR DE CHORRILLOS
“CORONEL FRANCISCO BOLOGNESI”

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

LA ASIGNATURA DE GUERRA CIBERNÉTICA Y LA FORMACIÓN ACADÉMICA ESPECIALIZADA DE LOS CADETES DE COMUNICACIONES DE LA ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI” 2019

PRESENTADO POR

GONZALES CONCHA LUIS ANGEL

RAMOS CASTILLO GUSTAVO ADOLFO

LIMA – PERÚ

2019

COMANDO DE EDUCACIÓN Y DOCTRINA DEL EJÉRCITO

ESCUELA MILITAR DE CHORRILLOS

LA ASIGNATURA DE GUERRA CIBERNÉTICA Y LA FORMACIÓN ACADÉMICA ESPECIALIZADA DE LOS CADETES DE COMUNICACIONES DE LA ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI” 2019

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

PRESENTADA POR:

GONZALES CONCHA LUIS ANGEL

RAMOS CASTILLO GUSTAVO ADOLFO

LIMA – PERÚ

2019

ASESOR Y MIEMBROS DEL JURADO

ASESOR

ASESOR TEMÁTICO: Dr. GIOVANNI CASTAÑADA ALVAREZ

ASESOR METODOLÓGICO: Dr. CASIMIRO DAVILA

ECHEVARRIA PRESIDENTE DEL JURADO

Dr……

MIEMBROS DEL JURADO

Dr……

Dr……

DEDICATORIA

A nuestros padres por su permanente apoyo y nuestro instructor que supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

AGRADECIMIENTO

Agradecemos a Dios por bendecirnos la vida, por guiarnos a lo largo de nuestra existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Gracias a todas las personas que ayudaron directa e indirectamente en la realización de este proyecto.

PRESENTACIÓN

Señores miembros del Jurado

Dando cumplimento a las normas establecidas en el Reglamento de Grados y Títulos de la Escuela Militar de Chorrillos para optar la Licenciatura en Ciencias Militares, presentamos la tesis titulada**:**

"LA ASIGNATURA DE GUERRA CIBERNETICA Y LA FORMACIÓN ACADÉMICA ESPECIALIZADA DEL CADETE DE CUARTO AÑO DE COMUNICACIONES DE LA ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI" 2019

Las responsabilidades del trabajo son las siguientes:

Aspecto Metodológico: Bach. Gonzales Concha Luis Angel
Aspecto Temático: Bach. Ramos Castillo Gustavo Adolfo

La investigación tiene por finalidad determinar la relación que existe entre La Asignatura de Guerra Cibernetica con La Formación Académica Especializada.

Por lo expuesto Señores Miembros del Jurado ponemos a vuestra consideración la presente investigación para ser evaluada con su alto criterio, esperando sea aprobada.

Los Autores

ÍNDICE DE CONTENIDO

CAPÍTULO I: PROBLEMA DE INVESTIGACIÓN

CAPÍTULO II: MARCO TEÓRICO

CAPÍTULO III: MARCO METODOLÓGICO

CAPÍTULO IV: RESULTADOS

CONCLUSIONES

RECOMENDACIONES

REFERENCIAS BIBLIOGRÁFICAS

ANEXOS

ÍNDICE DE TABLAS

Tablas **Página**

ÍNDICE DE FIGURAS

Figuras **Página**

RESUMEN

El objetivo general del presente estudio se circunscribió en determinar la relación que existe entre La Asignatura de Guerra Cibernética con La Formación Académica Especializada de los Cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi, 2019

La población alcanza a sesenta Cadetes de Comunicaciones, tomando como muestra la población en su totalidad.

Los datos fueron recogidos mediante una encuesta que contó con doce ítems los cuales se construyeron en base a las variables de estudio, dimensiones e indicadores motivo del estudio; los datos fueron procesados con el paquete estadístico SPSS para obtener resultados consistentes en tablas y figuras procedentes de la encuesta aplicada a la muestra.

Como producto de este trabajo se obtuvo importantes conclusiones y sugerencias respecto de La Asignatura de Guerra Cibernética y La Formación Académica de los Cadetes de Comunicaciones de la Escuela Militar. Palabras claves: *Guerra, cibernética y comunicaciones.*

ABSTRACT

The general objective of the present study is circumscribed in the relationship that exists in the Cybernetic War Subject with the Specialized Academic Training in the Fourth Year Cadets of the Military School of "Coronel Francisco Bolognesi, 2019

The population reaches a nineteen Fourth Year Communications Cadets.

The data were recognized by means of a survey that included twelve elements that were constructed based on the study variables, dimensions and indicators of the study; The data were processed with the statistical package SPSS to obtain consistent results in tables and figures of the survey applied to the sample.

News related to the Cybernetic War Subject and the Academic Training of the Fourth Year Communications Cadets of the Military School.

Keywords: War, cybernetics and communications.

INTRODUCCIÓN

Ante la situación que se presenta en el arma de Comunicaciones de la EMCH “CFB”, la asignatura de Guerra Cibernética juega un papel preponderante en la formación de los cadetes de Comunicaciones; el presente trabajo de investigación se desarrolló con la finalidad de presentar las recomendaciones factibles y pragmáticas para optimizar y mejorar esta situación en relación a la asignatura de Guerra Cibernética por parte de los Cadetes de Comunicaciones de la EMCH.

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.

CAPÍTULO I: PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema

Desde el inicio de los tiempos el hombre lucha por diversas razones; estas pueden ser religiosas, políticas, militares u otras. Suarez (2015) manifiesta que:

> Los conflictos armados nacen desde que los seres humanos tienen diferentes intereses dentro de una misma sociedad, los pueblos se enfrentan y luchan por lograr una mejora económica, jurídica, política y/o social. Los Estados necesitan responder a las necesidades de la población civil y sus Fuerzas Armadas ya que la nueva tecnología ha ingresado al campo de batalla actual, el ciberespacio, los sistemas de control de armas a distancia, como las aeronaves no tripuladas, los sistemas autónomos, como los robots de combate, serían parte de un nuevo escenario bélico. (p. 13)

En la actualidad la situación no es muy diferente a la que se generaba al inicio de los tiempos en cuanto a las razones para que se generen los conflictos; lo único que difiere son los ámbitos en los que se desarrollan los mismos.

Uno de los objetivos principales y primarios de la guerra es la captura y eliminación de la información que proporciona o que requiere el enemigo. Gordon R. Sullivan y James M. Dubik (1995) manifiestan que:

En las nuevas formas de guerra, basada intensivamente en las fuentes y recursos informáticos, la victoria se dirime en la capacidad de destrucción y dominio de los sistemas de información. Las nuevas tecnologías constituyen un aporte a la esfera militar integradas en las diversas

instituciones de seguridad pública, asumida por principio la intencionada confusión entre estrategias de televigilancia y operaciones bélicas. (p.35)

El desarrollo de la tecnología ha transformado la forma como se percibe la información y como se utiliza en las actividades bélicas.

La política de uso del espacio radioeléctrico y las tecnologías de telecomunicaciones al servicio de la doctrina de Seguridad Nacional no es nueva. Constituye, de hecho, históricamente uno de los ejes centrales de expansión del poder internacional de los Estados Unidos en el mundo, mediante la coordinación de las redes telemáticas militares con el sector civil y comercial (Teledesic, Global Star, Orbicom, . . .) en función de las actividades de inteligencia, básicamente las operaciones de inteligencia sobre las comunicaciones. Gordon R. Sullivan y James M. Dubik (1995)

El Perú, inmerso en la política global de la región sudamericana no está exento de poder recibir algún ataque a las comunicaciones, ya que es de nuestro conocimiento que a pesar que de acuerdo al Código Penal vigente es ilícita la intervención de comunicaciones telefónicas e interceptación de comunicación escrita, cuando no se haya respetado las disposiciones normativas establecidas para tales casos y que constituyan los resultados de las mismas como prueba. Lo cual es los últimos tiempos viene siendo pan de cada día y herramienta preferida para manipular políticamente situaciones propias de las altas esferas del gobierno.

Si trasladamos esta situación al ambiente militar, podemos hablar de Operaciones de Inteligencia de las Comunicaciones, las mismas que se realizan para obtener información del enemigo y/o negarle nuestra información al enemigo; para ello en la actualidad juega un papel preponderante el ciberespacio, el espectro electromagnético; que, al ser usado para el arte de la guerra acompañado de los avances tecnológicos de nuestra generación, nos permite hablar de guerra cibernética.

Atendiendo a la definición de Guerra Cibernética, debemos considerar de acuerdo a MD31-M-07 (2014). DOUTRINA MILITAR DE DEFESA CIBERNÉTICA: es el conjunto de acciones ejecutadas en el espacio cibernético, librado a nivel esencialmente militar y normalmente, como parte complementaria y de apoyo a otro tipo de operaciones, aunque como se verá más adelante, su papel es cada día mayor.

Es por ello la necesidad de que dicho aspecto de la seguridad global de las comunicaciones sea incluido como asignatura que complemente la carga académica en cuanto a la instrucción especializada de los cadetes de comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, proyectándolos a un futuro en el que el obtener el predominio sobre el ciberespacio será crucial para obtener la victoria en tiempo de paz y más aún en tiempo de guerra.

Esta asignatura, es de imperiosa necesidad para la Formación Académica Especializada de los cadetes del arma de Comunicaciones como futuros oficiales que serán encargados de realizar las modificaciones que tenga que realizarse en un futuro no muy lejano para estar a la par de los avances tecnológicos como oficiales recién egresados, potenciando su rendimiento y desempeño en la Guerra Cibernetica y las Operaciones de Comunicaciones.

1.2. Formulación del problema

1.2.1. Problema General

¿Cuál es la relación que existe entre la asignatura de Guerra Cibernética y la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

1.2.2. Problemas Específicos

1.2.2.1. Problema Específico

¿Cuál es la relación que existe entre los Fundamentos de la asignatura de Guerra Cibernética y la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

1.2.2.2. Problema Específico

¿Cuál es la relación que existe entre la Estructura y Responsabilidades de la asignatura de Guerra Cibernética y la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

1.2.2.3. Problema Específico

¿Cuál es la relación que existe entre la Aplicación en Operaciones Terrestres de la asignatura de Guerra Cibernética y la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

1.3. Objetivos

1.3.1. Objetivo General

Determinar cuál es la relación que existe entre la asignatura de Guerra Cibernética y la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

1.3.2. Objetivos Específicos

1.3.2.1. Objetivo Específico

Establecer cuál es la relación que existe entre los Fundamentos de la asignatura de Guerra Cibernética y la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

1.3.2.2. Objetivo Específico

Establecer cuál es la relación que existe entre la Estructura y Responsabilidades de la asignatura de Guerra Cibernética y la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

1.3.2.3. Objetivo Específico

Establecer cuál es la relación que existe entre la Aplicación en Operaciones Terrestres de la asignatura de Guerra Cibernética y la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

1.4. Justificación

Debemos recordar que hace poco más de 20 años el mundo entero participaba del prometedor y vertiginoso desarrollo de la red global: la información podía ser conocida, gestionada y compartida instantáneamente desde cualquier punto del planeta gracias a un simple terminal, de una manera libre y gratuita.

Las tecnologías de la información se convertían entonces en una herramienta imprescindible para las actividades económicas, sociales, empresariales, militares o de prestación de servicios, que comprobaban simultáneamente cómo estas actividades se convertían en objetivos de la influencia maliciosa de virus, troyanos o gusanos que boicoteaban su seguridad.

Ello nos lleva a determinar la importancia de la Guerra Cibernética en diferentes campos:

1.4.1. Justificación teórica

La aparición de un espacio virtual de interacción, al que se accede de manera inmediata y por un bajo coste, ha difuminado las fronteras existentes hasta el momento, modificando el comportamiento de defensa de los actores implicados ante el fantasma de un ataque de graves consecuencias cuya autoría, a pesar de las pruebas existentes, es difícilmente imputable.

Actualizaremos los datos relativos a la relación que existe entre la asignatura de Guerra Cibernética y la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” y unificar criterios, tanto en el diseño como en los métodos de análisis de los resultados obtenidos teniendo en cuenta las particularidades de este problema en nuestro entorno.

Toda la vertiginosa avalancha de conocimientos y cambios sustanciales en el uso del ciberespacio tienen que ser plasmadas en la instrucción especializada de los cadetes de Comunicaciones de la escuela Militar de Chorrillos “Coronel Francisco Bolognesi”; ya que ellos son los llamados a utilizar de forma sustancial los elementos

necesarios para poder estar a la par de la tecnología que circunda el uso del ciberespacio.

1.4.2. Justificación practica

Si se dictara de forma regular la asignatura de Guerra Cibernética, nos proporcionaría herramientas que nos permitirían desarrollarnos como elementos de comunicaciones preparados para afrontar la necesidad de dominar el espectro electromagnético y con ello contribuirían a nuestra Formación Académica Especializada como cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

1.4.3. Justificación metodológica

La justificación metodológica de este estudio propone generar un nuevo conocimiento valido y confiable buscando nuevos métodos o técnicas que generen nuevos conocimientos y sirva de modelo para futuros trabajos de investigación.

1.4.4. Justificación social

Para conocer, de acuerdo a los resultados de la Investigación, el verdadero perfil de la relación que existe entre la asignatura de Guerra Cibernética y la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”. Esperamos que esta investigación sea el inicio de otros estudios similares y en un futuro cercano y estudios similares, ayuden a mejorar la calidad de vida.

1.4.5. Justificación normativa

Para desarrollar este trabajo se cuenta con la autorización de las autoridades de la institución con el permiso correspondiente de todo el escalón superior de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” y esto permite que los oficiales superiores tengan conocimiento de la investigación que se desarrolla con la finalidad de propiciar otras investigaciones similares.

1.5. Limitaciones

- El uso de la biblioteca puede considerarse como limitación en determinadas circunstancias, ya que con la combinación de tiempo el acceso a material bibliográfico se hace complicado.

  Pero en nuestra condición de cadete de la “EMCH-CFB” se hace complicado el proceso de recolección de información y el procesamiento de los datos obtenidos; los obstáculos más comunes que se presentan son: el servicio de guardia, comisiones, formaciones, ensayos y las diferentes actividades extracurriculares que lleva la escuela.
- El tiempo si bien es cierto se transforma en una limitación cuando lo consideramos de forma específica en ciertos aspectos, este si es suficiente para realizar el trabajo de investigación completo; el cual será terminado dentro de los plazos establecidos.

  Siendo el tiempo empleado en cada una de ellas o en su conjunto de vital importancia en el proceso de investigación y de desarrollo de nuestro informe de tesis.
- El aspecto económico se presenta como una limitación para el financiamiento del trabajo de investigación,

1.6. Viabilidad

- Si es posible realizar la investigación con los medios disponibles.

- Es factible lograr la participación de los sujetos u objetos necesarios para la investigación. La metodología a seguir conduce a dar respuesta al problema.
- Los recursos humanos y materiales suficientes para realizar el estudio en el tiempo disponible previsto.
- El tiempo que tomará realizar el trabajo de investigación será el adecuado, no excediendo los plazos previstos.

CAPÍTULO II: MARCO TEÓRICO.

2.1. Antecedentes

2.1.1. Antecedentes Internacionales

Sánchez (2009). En su artículo publicado en la Revista Política y Estrategia N° 114: *"Internet: Una Herramienta Para Las Guerras En El Siglo XXI"*. Academia Nacional de Estudios Políticos y Estratégicos. Madrid. España.

- **Resumen:**

La enorme dependencia de las sociedades occidentales respecto de los sistemas informáticos y electrónicos está haciendo que estas sean más vulnerables a los posibles ataques cibernéticos. Es más, en un mundo tan hiperconectado, un impacto en el corazón de los Networks de información y tecnología podría generar pérdidas millonarias a cualquier país o institución, por no hablar de las fuertes consecuencias psicológicas que podría ocasionar un ataque de estas características. De ahí que un gran número de países estén desarrollando herramientas para atacar los sistemas gubernamentales de otros Estados al mismo tiempo que intentan reforzar sus medidas de seguridad. Pero no solo los Estados han descubierto las ventajas que les proporciona la red, sino también lo están haciendo los grupos terroristas. Y es precisamente en estos puntos donde hemos centrado todo nuestro artículo, es decir, en averiguar qué usos están realizando unos y otros en función de una estrategia defensiva y ofensiva.

- **Conclusiones:**

  1º. El ciberespacio se está convirtiendo en un nuevo escenario de conflicto.

  2º. La ciberguerra es una forma de guerra asimétrica, en la que el ordenador es el arma, la red, el campo de batalla y la información, las balas.

  3º. De momento, tanto Estados como grupos terroristas están haciendo un uso pasivo de la red que les está proporcionando enormes ventajas y beneficios.

  4º. Los medios que se están empleando para intentar contrarrestar la posibilidad de un ciberataque aún no están dando los resultados esperados.

  5º. La ciberguerra parece estar abocada, por todo lo que ello implica y por el mundo en el que nos encontramos viviendo, a ser la guerra del siglo XXI.

- **Comentarios:**

  Teniendo en consideración que nos encontramos en un mundo tan hiperconectado algunos han empezado a preguntarse qué sucedería si el centro de control del Metro sufriera un ataque, si los periódicos online, cadenas de TV y radio, así como las agencias de noticias, se hicieran eco de una noticia falsa; si se accedieran ilegalmente al tablero de control de una presa hidroeléctrica y se realizara una apertura descontrolada de sus compuertas; si se hiciera un *blinds* de radar, generando un bloqueo de tráfico aéreo por 12 horas, etc. Más aún cuando resulta imposible garantizar la seguridad total de los sistemas informáticos y cuando solo es necesario disponer de un ordenador y de ciertos conocimientos informáticos para llevar a cabo este tipo de acciones.

[1] Blinds, es el punto ciego que se puede encontrar en el radar oculto detrás de algún objeto y/o obstáculo natural que bloquee la señal

Díaz del Rio (2010). En su artículo titulado: *"La Ciberseguridad en el Ámbito Militar"*. Ministerio de Defensa. España.

- **Resumen:**

  El presente trabajo de investigación estudia la Ciberseguridad en el ámbito militar. Para ello, se comienza dando un enfoque general de estrategia, referido a los nuevos retos y amenazas del comienzo del siglo XXI, para pasar a continuación a analizar los riesgos en el ciberespacio y el estado del arte de la defensa, explotación y ataque en esta nueva dimensión, considerada un nuevo «global common». Se repasa, asimismo, la necesidad de introducir nuevas perspectivas en el concepto estratégico de la OTAN ante el papel cada vez más relevante de esta dimensión y se describen las actuaciones y medidas tomadas, tanto por otros países de nuestro entorno como por nuestro Ministerio de Defensa para afrontar este desafío y la estructura y organización adoptada. Se finaliza examinando el importante esfuerzo de colaboración internacional en este campo del Ministerio de Defensa, así como las numerosas actividades de formación, concienciación y adiestramiento desarrolladas en el ámbito del EMAD, concluyendo con un análisis de la cifra y su industria en España.

- **Conclusiones:**

  - Las tecnologías de la información hacen posible casi todo lo que nuestras FAS necesitan: apoyo logístico, mando y control de sus fuerzas, información de inteligencia en tiempo real y un largo etcétera.
  - Los ataques cibernéticos ya no solamente tienen motivación intelectual económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus

fuerzas, además de en las dimensiones de tierra, mar y aire, a través del ciberespacio.

- La amenaza a las tecnologías de la información nunca ha sido mayor y los usuarios necesitan y demandan seguridad como nunca antes había ocurrido.
- En el ámbito de las operaciones militares, los ciberataques también tienen que ser considerados como una amenaza.
- La ciberguerra es asimétrica.
- Los sistemas en red no son los únicos susceptibles de presentar vulnerabilidades y ser atacados.
- Ejércitos de diversos países han reconocido formalmente al ciberespacio como un nuevo dominio de enfrentamiento («Global Commons»).
- La convergencia a NEC exigirá una mayor interconexión con otros sistemas (Federación de Redes), incluso con ONGs, lo que exigirá un considerable esfuerzo en seguridad de la información.
- A nivel nacional, el Ministerio de Defensa ha llevado a cabo numerosas iniciativas, publicando la Política de Seguridad de la Información, sus normas de aplicación y tomando un buen número de medidas para incrementar la seguridad de su información, tanto en el ámbito.

- **Comentarios:**

El presente artículo nos presenta un escenario estratégico del comienzo de este siglo XXI, el mismo que se caracteriza porque junto a los tradicionales riesgos y amenazas para la paz, el equilibrio, la estabilidad y la seguridad internacionales, han surgido nuevos riesgos, como el del terrorismo de carácter transnacional y alcance global, con gran capacidad de ocasionar daño indiscriminadamente, así como las diferentes modalidades de ataques que se pueden producir a través del ciberespacio.

Espinosa (2012). En su tesis titulada: *"Guerra Cibernética: Un problema estratégico con envolvimiento de las Fuerzas Armadas"*. Escuela Superior de Guerra. Rio de Janeiro. Brasil

- **Resumen:**

  Esta tesis explora la guerra cibernética y estudia el papel de las fuerzas armadas en la Seguridad Nacional y Defensa. El ciberespacio es un ambiente relativamente nuevo y complejo, aún no asignado, y totalmente desconocido. Los desafíos que los países se enfrentan a proteger sus infraestructuras esenciales, de información estratégica, sistemas bancarios, operaciones gubernamentales, industrias privadas de investigación y desarrollo, y las universidades representan una tarea titánica cuyas las fronteras son desconocidas. Es en este estudio que se busca determinar la magnitud del problema de instigar el pensamiento sobre la forma de resolverlo para evitar que salga del control.

- **Conclusiones:**

  - La generación X que está envejeciendo y la nueva generación Y tendrán que vivir con este nuevo deber cívico, y van a tener que buscar la forma de protección general en el camino de la información (information highway).

  - El futuro de las economías está en juego.

  - El papel de los militares será mejor definido con el paso del tiempo, en la forma en que se define el ciberespacio.

  - Tal vez el viejo Verde (Ejército), Blanco (Marina de Guerra) y Azul (Fuerza Aérea) no sean las respuestas más correctas a la Ciberdefensa.

- Tal vez la "fuerza gris (Ciber)", debe ser la responsable de defender economías y países.

- Si los Estados o naciones optan por el contraataque a los ciberataques, como han hecho hasta ahora, el camino hacia el éxito va a ser de largo.

- **Comentario:**

  Debemos considerar que el ciberespacio es actualmente reconocido como el quinto dominio de guerra y debe incorporarse a las estrategias de Seguridad Nacional de cualquier Estado. Es por ello que el campo de batalla está siendo redefinido y, aunque la vida directamente no puede ser perdida directamente a través de este dominio; las economías de los países y las infraestructuras críticas pueden paralizarse por un ataque cibernético bien estructurado, afectando el día a día de las sociedades.

  Por lo tanto, los presupuestos para la Seguridad y la Defensa Nacional, que deben preparar las diferentes naciones, debe considerar las inversiones en ciber-mandos (civiles y militares) con el fin de enfrentarse a los retos aquí citados; que, comparados a una guerra convencional, en la cual los enemigos y las fronteras se encuentran bien definidos en el campo de batalla, en la guerra cibernética el ciberespacio es impredecible.

Zambrano E. (2014). En su tesis para a la obtención del Grado Académico de Magister en Docencia y Currículo para la Educación Superior, titulada: *"Capacitación continua del Personal Militar y su relación con el proceso de Aprendizaje en la Escuela de Perfeccionamiento de Aerotécnicos".* Universidad Técnica de Ambato. Ambato. Ecuador

- **Resumen:**

La presente investigación que tiene como tema: “Capacitación Continua del personal militar y su relación con el proceso de aprendizaje en la Escuela de Perfeccionamiento de Aerotécnicos”, se planteó como objetivo general: Determinar los factores por los cuales no se da una relación total entre la capacitación continua con respecto al proceso de aprendizaje en la Escuela de Perfeccionamiento de Aerotécnicos. La Fuerza Aérea Ecuatoriana crea el Instituto Tecnológico Superior Aeronáutico (ITSA), presta sus servicios educativos con cursos de perfeccionamiento que el personal militar que en los diferentes grados y jerarquía deben realizar para cumplir los requisitos de ascenso establecidos en la ley de Personal de las Fuerzas Armadas y el Reglamento de Educación de la Fuerza Aérea estipulado por el CEDE (Comando de educación y Doctrina del Ejercito)p, para realzar cursos de ascenso a Suboficiales Mayores en el CEC (Centro de Educación Continua) con diferentes materias administrativas y militares para su aplicación y perfil. Desde que la Fuerza Aérea Ecuatoriana ha centrado sus esfuerzos en el ámbito académico con la creación del GAM (Gerencia Administrativa Militar) el 31 de agosto de 1994 que se desarrolló en dos fases presencial y a distancia por los diferentes destacamentos y bases donde cumplen su objetivo militar, pero muy poco se ha hecho por optimizar el proceso de aprendizaje, por lo que se vuelve indispensable tomar acciones al respecto.

- **Conclusiones:**

1. Un alto porcentaje desde su óptica consideran que la participación en una capacitación es el medio más utilizado para socializar los contenidos de algún módulo o asignatura por tanto es evidente como una estrategia metodológica que el

proceso de aprendizaje se ubica en la dialéctica tradicional dentro la institución militar.

2. Erróneamente los instructores y facilitadores de capacitación creen que para socializar su curso es menester dotarle de comprensión, mediante la construcción de operaciones mentales como análisis síntesis, interpretación y argumentación, herramientas básicas para el aprendizaje y no crear conciencia de una armonía colectiva en el grupo en cuestión con igualdad de conocimientos con carácter académico y humanista.

3. Analizados holísticamente las categorías Capacitación Continua del personal militar y Proceso de Aprendizaje es determinante pensar que el instructor, a pesar de conocer el uso de técnicas docentes fomentan el desarrollo del pensamiento mediante la reflexión, espíritu competitivo y creatividad versus el tiempo estimado para los eventos programados que en muchos de los casos se improvisa su cumplimiento por órdenes superiores.

4. El desconocimiento de los sistemas y programas de capacitación actuales como trainer, practitoner, y coach presentados en esta investigación para fortalecer la base del pensamiento y desarrollo del intelecto que en la mayoría del análisis determinan errores de interpretación entre el ejercicio de actividades cotidianas y la capacitación netamente pura.

5. Un aspecto preocupante es No considerar el lado humano a nivel institucional como resultado de una Planificación Curricular experimental es deficiente con un precario compromiso personal y la evolución de exigencias superiores de las órdenes directas del Comando de Educación y Doctrina del Ejército y catedráticos por un objetivo dual ósea finalizar el

módulo y cargar de trabajos al personal para suponer que se aprendió.

- **Comentarios:**

Podemos apreciar que las aportaciones del presente estudio al aprendizaje, en cuanto a los cursos de actualización militar desarrolladas desde diversas perspectivas, para develar su probable incidencia en la capacitación continua, se debe ver a partir de aportaciones y teorías, se trata de evidenciar un esquema educativo estandarizado de aprendizaje por disposiciones del Comando de Educación y Doctrina del Ejercito que regula a todas las instituciones de educación básico, medio y superior que es mediado por las contribuciones de una educación parcializada al nuevo modelo de aprendizaje moderno que utiliza técnicas no convencionales para su aplicación.

2.1.2. Antecedentes Nacionales

Chamaya, R. & Olaya, J. (2018). En su Tesis para obtener el Título de Bachiller en Ciencias Militares, titulada: *"La Capacitación Universitaria y El Rendimiento Académico de los cadete de Artillería de la Escuela Militar de Chorrillos – 2018".* Escuela Militar de Chorrillos "Coronel Francisco Bolognesi". Chorrillos. Lima. Perú

- **Resumen:**

La presente investigación titulada "La Capacitación Universitaria y el Rendimiento Académico de los cadetes de Artillería de la Escuela Militar de Chorrillos – 2018"; considera dentro de su objetivo principal, determinar qué relación existe entre la Capacitación Universitaria y el Rendimiento Académico de los cadetes de Artillería de la EMCH, 2018. El método de estudio tiene un enfoque cuantitativo, con un alcance descriptivo y diseño no

experimental, con una población de 42 personas, conformadas por cadetes del arma de Artillería; con la aplicación de un cuestionario para determinar los objetivos de la investigación, y utilizándose la prueba Chi Cuadrado para la demostración de las hipótesis general siguiente: “Existe una relación significativa entre la Capacitación Universitaria y el Rendimiento Académico de los cadetes de Artillería de la EMCH, 2018” Se llegó a la conclusión general siguiente: En la actualidad en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” desde hace más de una década se implementó la segunda profesión en post de la profesionalización para los cadetes, lo cual implica la intervención de las universidades en la EMCH “CFB”; para tal efecto se incrementó la cantidad de conocimientos requeridos para lograr los fines propuestos; es por ello, que debemos considerar como un aspecto muy importante la Capacitación Universitaria para generar un óptimo rendimiento académico entre los cadetes de Artillería de la EMCH “CFB”. Como parte final se recomienda se continúe la Capacitación Universitaria de los cadetes de del arma de Artillería, a fin de lograr Oficiales mejor preparados y capacitados para los retos futuros como profesionales.

- **Conclusiones:**

1. En la actualidad en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” desde hace más de una década se implementó la segunda profesión en post de la profesionalización para los cadetes, lo cual implica la intervención de las universidades en la EMCH “CFB”; para tal efecto se incrementó la cantidad de conocimientos requeridos para lograr los fines propuestos; es por ello, que debemos considerar como un aspecto muy importante la Capacitación Universitaria para generar un óptimo rendimiento académico entre los cadetes de Artillería de la EMCH “CFB”.

2. De acuerdo a la Hipótesis General que a la letra dice que, existe una relación significativa entre la Capacitación Universitaria y el Rendimiento Académico de los cadetes de Artillería de la EMCH, 2018. Hemos podido concluir mediante las encuestas que dicha hipótesis es válida; ya que como en cualquier profesión a mayor Capacitación teórico-práctico y exigencia académica se generara un Rendimiento Académico óptimo.

3. De acuerdo a la Hipótesis Especifica 1 que a la letra dice que, existe una relación significativa entre la Profesionalización de las FFAA y el Rendimiento Académico de los cadetes de Artillería de la EMCH, 2018. Hemos podido concluir mediante las encuestas que dicha hipótesis es válida; ya que dentro de la planificación del Ejército se encuentra la Profesionalización de su personal, y siendo los cadetes el producto de su Alma Mater merece atención especial para que los resultados sean óptimos.

4. De acuerdo a la Hipótesis Especifica 2 que a la letra dice que, existe una relación significativa entre los Fundamentos del Proyecto Educativo y el Rendimiento Académico de los cadetes de Artillería de la EMCH, 2018. Hemos podido concluir mediante las encuestas que dicha hipótesis es válida; ya que los fundamentos filosóficos, antropológicos, culturales, sociales, psicológicos y pedagógicos permitirán la cimentación de los 140 conocimientos adquiridos y por consecuente el mejoramiento en el Rendimiento Académicos de los cadetes de Artillería de la EMCH.

5. De acuerdo a la Hipótesis Especifica 3 que a la letra dice que, existe una relación significativa entre los Modelos Educativos y el Rendimiento Académico de los cadetes de Artillería de la EMCH, 2018. Hemos podido concluir mediante las encuestas que dicha hipótesis es válida; ya que los modelos educativos

que existen aplicados de forma adecuada de acuerdo a las necesidades de las asignaturas y de las necesidades académicas de los cadetes permitirán la cimentación de los conocimientos adquiridos y por consecuente el mejoramiento en el Rendimiento Académicos de los cadetes de Artillería de la EMCH.

6. De acuerdo a la Hipótesis Especifica 4 que a la letra dice que, existe una relación significativa entre el Plan Bicentenario y el Rendimiento Académico de los cadetes de Artillería de la EMCH, 2018. Hemos podido concluir mediante las encuestas que dicha hipótesis es válida; ya que los objetivos y lineamientos del plan están orientados a potenciar las necesidades académicas de los cadetes, permitiendo la cimentación de los conocimientos adquiridos y por consecuente el mejoramiento en el Rendimiento Académicos de los cadetes de Artillería de la EMCH.

- **Comentarios:**

Debemos considerar que en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, los cadetes que conforman el arma de Artillería vienen desarrollando dentro de su curricula de estudio un proceso educativo orientado de potenciar las habilidades necesarias para enfrentarse a la vida, en donde el conocimiento es la base para pensar, juzgar, describir, crear y actuar; centrada en el cadete, para valorar su diversidad, sus estilos de aprendizaje, las formas de ser, actuar y pensar; en el proceso de descubrimiento y en el método científico de resolución de problemas, donde el conocimiento se construye en conjunto entre los cadetes e instructores como facilitadores del proceso de enseñanza y aprendizaje.

Suarez (2015). Tesis para optar el Título Profesional de Abogado: *"La Ciberguerra y la aplicación de los Principios del Derecho Internacional Humanitario"*. Universidad San Martin de Porres. Lima. Perú (tipo de estudio, diseño, población muestra)

- **Resumen:**

La guerra cibernética o ciberguerra es un tema nuevo para la Comunidad Internacional y se refiere a los medios y métodos bélicos que consisten en operaciones cibernéticas que alcanzan el nivel de un conflicto armado sea de carácter internacional o no internacional.

El problema principal de esta tesis es ¿En qué medida la creación de un Departamento Especializado en ciberguerra dentro del Ministerio de Defensa del Perú podría garantizar los principios del Derecho Internacional Humanitario?

El objeto materia de análisis son los ataques cibernéticos dentro de los conflictos armados. En ese sentido la hipótesis principal estima que la creación del Departamento Especializado en Ciberguerra garantizaría los principios del Derecho Internacional Humanitario ya que se encargaría de prevenir, planear, coordinar, ejecutar y conducir operaciones cibernéticas defendiendo las redes de información en la ciberguerra.

Para comprobar la hipótesis en el Primer Capítulo se establece los problemas, objetivos y las hipótesis que serán resueltas al concluir la investigación; posteriormente en los demás capítulos se desarrollarán temas como la soberanía internacional en la ciberguerra, la responsabilidad internacional dentro de la ciberguerra, los principios del Derecho Internacional Humanitario, la diferencia entre ataques cibernéticos y la ciberguerra, entre otros.

Todo ello nos permitirá elaborar conclusiones y recomendaciones pertinentes.

- **Conclusiones:**

a) Los ataques informáticos son regulados a nivel interno siempre y cuando no se desarrollen dentro de un conflicto armado.

b) Los ataques dentro de la ciberguerra deben ser dirigidos a la infraestructura estatal y debe generar un daño determinable.

c) Los principios del Derecho Internacional Humanitario o Derecho Internacional de los Conflictos Armados muchas veces son vulnerados por los ciberataques, ya que sus efectos pueden ocasionar daños colaterales y males superfluos.

d) Al no existir normativa internacional que regule específicamente los ataques cibernéticos dentro de un conflicto armado, es necesario que cada uno de los Estados realicen un análisis jurídico para determinar la licitud o ilicitud de los ataques cibernéticos: esto es conforme al artículo 36 del Protocolo Adicional I.

e) En el Perú, la normativa cibernética se encuentra en constante evolución.

- **Comentarios:**

En la presente investigación el autor desarrolla temas relacionados al Derecho Internacional Humanitario relacionados directamente con la ciberguerra; de la misma forma analiza si los ciberataques dentro de un conflicto armado amenazan o no los principios del DIH; de la misma forma, sustenta la necesidad que tiene el Estado

Peruano para crear un “Plan estratégico de Ciberseguridad” y el “Comité Especializado en Ciberguerra.”

Sánchez, J. (2017). En su tesis para optar el grado académico de magister en ingeniería de sistemas de armas, titulada: *“Adopción de Estrategias de Ciberseguridad en la protección de la información en la oficina de Economía del Ejército, San Borja- 2017”.* Instituto Científico Tecnológico del Ejército. Lima. Perú

- **Resumen:**

El presente estudio trata de la “Adopción de Estrategias de Ciberseguridad en la Protección de la Información en la Oficina de Economía del Ejército. San Borja 2017”, estudio que se efectuó teniendo en consideración la información digitalizada que tiene a cargo esta importante Dependencia del Ejército, cual es el manejo presupuestal y el control del gasto de toda la Institución, lo que la hace objetivo remunerativo para el accionar de los ciberdelincuentes muy de moda en los últimos tiempos para lograr sus objetivos malévolos.

Por tal motivo, el investigador formuló el siguiente problema: ¿De qué manera la adopción de estrategias de ciberseguridad incide en la protección de la información en la Oficina de la Economía del Ejército? San Borja – 2017

De igual modo, se planteó el siguiente Objetivo: Determinar de qué manera la adopción de estrategias de ciberseguridad incide en la protección de la información en la Oficina de Economía del Ejército.

La presente investigación se justifica teniendo en consideración que en el mundo actual ha surgido una nueva dimensión donde pueden materializarse las amenazas: el ciberespacio. Si antes en el ámbito de la defensa estaba claro que los escenarios estaban

circunscritos en las tres dimensiones de tierra, mar y aire; ahora se cuenta con una dimensión adicional, y más intangible que las anteriores: el espectro electromagnético.

Además tiene una importancia táctica y estratégica porque este estudio permitió determinar algunas falencias que podrían poner en riesgo la seguridad de la información reservada que se maneja en la Oficina de Economía del Ejército, cayendo en manos de ciberdelincuentes y lograr sus objetivos criminales y delincuenciales, arribando el investigador a conclusiones y plantear las recomendaciones que se estima conveniente mencionarlas, como producto de todo un trabajo investigativo, aplicando el Método de Investigación Científica y adecuándose las exigencias universitarias existentes.

La hipótesis planteada fue: La adopción de estrategias de ciberseguridad incidiría significativamente en la protección de la información en la Oficina de Economía del Ejército.

El tipo de investigación es No experimental, de enfoque cuantitativo, siendo una investigación aplicada y sustantiva, porque tiene propósitos prácticos inmediatos. De un Nivel Descriptivo y Explicativo; de un diseño transaccional, porque indagó la incidencia y los valores en que se manifiestan las variables que se investigan en un tiempo determinado.

La principal conclusión a la que arribó el investigador, luego de un análisis exhaustivo y resultados estadísticos aplicados fue que La adopción de estrategias de ciberseguridad incide significativamente en la protección de la información en la Oficina de Economía del Ejército, desprendiéndose conclusiones particulares de acuerdo a las hipótesis específicas planteadas.

- **Conclusiones:**

1. La Oficina de Economía del Ejército no cuenta con programas para concientizar al personal contra el cibercrimen.

2. La Oficina de Economía del Ejército no adopta medidas legales contra su personal que, manejando el sistema e información reservada, y que cometa negligencias que contribuyan directa o indirectamente con cibercriminales.

3. En las instalaciones de la Oficina de Economía del Ejército no se ha instalado un sistema de video cámaras para detectar intrusos con actitudes sospechosas para proteger la información contra el ciberespionaje.

4. En las salas de cómputo Oficina de Economía del Ejército no existen sistemas de control biométrico para proteger la información reservada contra el ciberespionaje.

5. En la Oficina de Economía del Ejército no existen planes de protección contra ciberterrortistas y se ponen en ejecución.

6. La Oficina de seguridad Oficina de Economía del Ejército, no ejerce control con su personal en cuanto al manejo de los CPU, USB, discos duros, etc. que puedan originar el robo de información; asimismo, no se efectúa un control estricto en el manejo de la información, tanto física como virtual, a fin de evitar el robo de información por descuido del personal que labora en dicha dependencia.

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

- **Comentarios:**

  El presente trabajo de investigación nos hace reflexionar sobre la necesidad de que los líderes y autoridades de las empresas e instituciones, respectivamente, adopten estrategias de ciberseguridad para neutralizar y/o minimizar cualquier riesgo que pueda poner en riesgo el robo de la información, la pérdida y/o la alteración de la misma. Es por ello que como responsable del manejo presupuestal y financiero del Ejército, la Oficina de Economía del Ejército no está exenta a este tipo de amenazas, pues es consciente de que individuos u organizaciones delictivas, busquen y aprovechen de las vulnerabilidades que pudieran presentarse en los Sistemas Informáticos de las Redes que dispone esta importante Dependencia de nuestro Ejército, por lo tiene que estar alerta a través del Departamento de Telemática de la OEE, y adoptar estrategias de ciberseguridad para garantizar la inviolabilidad e intangibilidad de la información reservada bajo su responsabilidad.

2.2. Bases teóricas

2.2.1. VARIABLE 1: Asignatura de Guerra Cibernética

Definición de Guerra Cibernética

La ciberguerra es un área dentro de las agencias militares de los países que tiene como objetivo encontrar las vulnerabilidades técnicas de los sistemas o redes informáticas del enemigo para penetrarlas y atacarlas, tanto, así como para extraer datos e información sensible. En este caso el ciberespacio es el campo de batalla y las armas son programas o aplicaciones informáticas. (Sain, 2016)

Ciberguerra se refiere al desplazamiento de un conflicto, en principio de carácter bélico, que toma el ciberespacio y las tecnologías de la

información como escenario principal, para producir alteraciones en datos y sistemas del enemigo, a la vez que se protege la información y sistemas del atacante. Para llevar a cabo estas actividades, se conocen distintos métodos para vulnerar la estructura informática del objetivo. Desde la inteligencia social hasta la aplicación de procedimientos requerientes de conocimiento técnico avanzado. Las armas de la guerra informática son los virus informáticos y programas especiales para penetrar la seguridad de los sistemas informáticos y los luchadores son los expertos en informática y telecomunicaciones. Generalmente, los blancos de los ataques son los sistemas financieros, bancarios y militares, aunque se han visto numerosos casos donde se ven afectados los sistemas de comunicación. (Pantano, 2014)

El ciberespacio se define como “un dominio global dentro del entorno de la información, cuyo carácter distintivo y único está enmarcado por el uso del espectro electrónico y electromagnético para crear, almacenar, modificar, intercambiar y explotar la información a través de redes interdependientes e interconectadas” (Kuehl, 2009, pág. 27); por lo que presenta particularidades que lo diferencian de otros dominios, y algunas de esas características hacen que este entorno sea muy llamativo para la guerra en él.

La ciberguerra, desde una conceptualización teórica, puede ser definida por una gran cantidad de autores que se han apropiado de los asuntos cibernéticos. Maness y Valeriano (2012) definen la ciberguerra como “las capacidades y acciones ofensivas en el ciberespacio de un Estado (…) El uso de las tecnologías computacionales en el campo de batalla militar y diplomática de los asuntos y la interacción internacional” (pág. 142). Para Schreir (2012) la guerra cibernética “se refiere a un asalto digital coordinado de forma masiva de un gobierno a otro. Es la acción de un Estado-nación para penetrar las redes y los ordenadores de otra nación con el fin de causar daños o molestias” (pág. 16). La noción política se incluye, al afirmar que: 41 La guerra cibernética es una extensión de la política a través de las acciones tomadas en el

ciberespacio por parte de actores estatales que o bien constituyen una grave amenaza para la seguridad de una nación o se llevan a cabo en respuesta a una amenaza percibida contra la seguridad de una nación (Ruef, Shakaraian & Shakarian, 2013, p. 2).

Importancia de la Asignatura de Guerra Cibernética

La importancia de la Asignatura de Guerra Cibernética radica en la necesidad de que los cadetes del arma de Comunicaciones, en su calidad de futuros oficial del arma, tengan los conocimientos suficientes para contribuir con el Ejercito del Perú a minimizar y/o eliminar la amenaza de una guerra cibernética; la misma que nunca ha tenido tanta importancia como ahora, ya que hoy en día, los adelantos tecnológicos y la creciente infraestructura digital han hecho que poblaciones enteras dependan de sistemas entrelazados y complejos. Por su parte la demanda de Internet y de conectividad digital exige una integración cada vez mayor de las TIC en productos que anteriormente funcionaban sin estas tecnologías, por ejemplo, automóviles, edificios e incluso sistemas de control para las redes de distribución eléctrica y de transporte. Prácticamente todos los servicios modernos dependen de la utilización de las TIC y de la estabilidad del ciberespacio, ya se trate del suministro eléctrico, los sistemas de transporte, los servicios militares, la logística, etc. El "ciberespacio" es un ámbito físico y conceptual en el que existen todos estos sistemas. Por consiguiente, el significado general de "guerra cibernética" es una guerra que se lucha en el ciberespacio y donde las TIC son a su vez las armas y los objetivos. (Steven, E. 2010)

Así mismo debemos atender al rápido aumento de la dependencia respecto de las redes inteligentes y otros sistemas de control y supervisión basados en Internet, hace que los recursos de energía, transporte y defensa hayan quedado expuestos a los ataques de quienes desean causar estragos a los gobiernos y la población civil. (Messmer, E. 2010) Es por ello que cada día es más importante la

ciberseguridad y la protección de la infraestructura esencial de la información son dos aspectos fundamentales para la seguridad y la economía de cualquier país.

Fundamentos

Antes de proceder a la descripción de los fundamentos de la Guerra Cibernética, debemos mencionar que no existe doctrina del Ejercito del Perú al respecto; por lo tanto estamos tomando como base teórica la doctrina del Ejército Brasileño, mediante el Manual de Campaña de Guerra Cibernética (EB70-MC-10.232, 2017, 1ª Edición). Sin embargo la Asignatura de Guerra Cibernetica si se esta dando en la Escuela de Comunicaciones.

- **Principios de empleo**

  Los principios tradicionales de guerra se aplican a todo tipo de operaciones militares, incluidas las acciones cibernéticas. Las peculiaridades de la guerra cibernética, sin embargo, impone que otros principios sean considerados. (EB70-MC-10.232, 2017, 1ª Edición)

  Son principios de empleo de la guerra cibernética:
  a) principio del efecto;
  b) principio de la disimulación;
  c) principio de trazabilidad; y
  d) principio de adaptabilidad.

  - Principio del Efecto: las acciones cibernéticas deben producir efectos que se traduzcan en una ventaja estratégica, operacional o táctica que afecte al mundo real, aunque estos efectos no sean cinéticos.

- Principio de la disimulación: medidas activas deben ser adoptadas para disimular en el espacio cibernético, dificultando la rastreabilidad de las acciones cibernéticas ofensivas y exploratorias llevadas a cabo contra los sistemas de información oponentes. Se pretende, así, enmascarar la autoría y el punto de origen de esas acciones.

- Principio de la trazabilidad: se deben adoptar medidas efectivas para detectar acciones cibernéticas ofensivas y exploratorias contra los sistemas de TIC amigos. Casi siempre, las acciones cibernéticas involucran el movimiento o la manipulación de datos, las cuales pueden ser registradas en los sistemas de TIC.

- Principio de la Adaptabilidad: consiste en la capacidad de la guerra cibernética de adaptarse a la característica de mutabilidad del espacio cibernético, manteniendo la proactividad incluso ante cambios súbitos e imprevisibles.

• **Características de la guerra cibernética**

La guerra cibernética posee las mismas características de la defensa cibernética, adaptándose a los niveles operativo y táctico (EB70-MC-10.232, 2017, 1ª Edición). Y estas son:

- Inseguridad Latente: ningún sistema computacional es totalmente seguro, teniendo en cuenta que las vulnerabilidades en los activos de información serán siempre objeto de explotación por amenazas cibernéticas.

- Alcance Global: la guerra cibernética posibilita la conducción de acciones a escala global, simultáneamente, en diferentes frentes. Las limitaciones físicas de distancia y espacio no se aplican al espacio cibernético.

- Vulnerabilidad de las Fronteras Geográficas: las acciones de guerra cibernética no se limitan a fronteras geográficamente definidas, pues los agentes pueden actuar desde cualquier lugar y provocar efecto en cualquier lugar.

- Mutabilidad: no existen leyes de comportamiento inmutables en el espacio cibernético, pues pueden adaptarse a las condiciones ambientales y de la creatividad del ser humano.

- Incerteza: las acciones cibernéticas pueden o no generar los efectos deseados como consecuencia de las diversas variables que afectan el comportamiento de los sistemas informatizados.

- Dualidad: en la guerra cibernética, las mismas herramientas pueden ser usadas por atacantes y administradores de sistemas con finalidades distintas: una herramienta que busque las vulnerabilidades del sistema, por ejemplo, puede es usado por atacantes para encontrar puntos que representen oportunidades de ataque en sus sistemas objetivo y por administradores para descubrir las vulnerabilidades de equipos y redes.

- Función de Apoyo: las acciones cibernéticas no son un fin en sí mismas, siendo empleadas para apoyar la conducción de las operaciones militares.

- Asimetría: basada en el desbalanceamiento de fuerzas, causado por la introducción de uno o más elementos de ruptura tecnológicos, metodológicos o procedimentales que pueden causar daños tan perjudiciales como aquellos perpetrados por estados u organizaciones con mayores condiciones económicas, por ejemplo.

- **Posibilidades de la guerra cibernética**

Son posibilidades de la guerra cibernética (EB70-MC-10.232, 2017, 1ª Edición):

a) Actuar en el espacio cibernético, por medio de acciones ofensivas, defensivas y exploratorias;
b) Cooperar en la producción del conocimiento de inteligencia por medio de los datos obtenidos de la fuente cibernética;
c) Alcanzar sistemas de información de un oponente sin limitación de alcance físico y exposición de tropa;
d) Cooperar con la seguridad cibernética, incluso de órganos externos al MD, a solicitud o en el contexto de una operación;
e) Cooperar con el esfuerzo de movilización para asegurar la capacidad disuasoria de la guerra cibernética;
f) Facilitar la obtención de la sorpresa, sobre la base de la explotación de las vulnerabilidades de los sistemas de información del oponente;
g) Realizar acciones contra oponentes con poder de combate superior; y
h) Realizar acciones con costos significativamente menores que aquellos involucrados en las operaciones militares en los demás dominios.

- **Limitaciones de la guerra cibernética**

Son limitaciones de la guerra cibernética (EB70-MC-10.232, 2017, 1ª Edición):

a) Restringida capacidad de identificación del origen y atribución de responsabilidades por ataques cibernéticos;
b) Restringida eficacia de las acciones cibernéticas defensivas, debido a la existencia de vulnerabilidades en los sistemas computacionales;

c) Restringida capacidad de gestión de personas, particularmente en lo que concierne a la identificación, selección, capacitación y retención de talentos;
d) Dificultad de seguimiento de la evolución tecnológica en el área cibernética; y
e) Posibilidad de ser sorprendido sobre la base de las vulnerabilidades de los propios sistemas de información.

Estructura y Responsabilidades (EB70-MC-10.232, 2017, 1ª Edición)

- **Visión Sistémica**

  - A fin de que se tenga la mejor comprensión de la inserción del Sistema de Guerra Cibernética del Ejercito de Brasil (SGCEB) en un contexto más amplio, en la Figura presenta la concepción del Sistema Militar de Defensa Cibernética (SMDC), del que forma el SGCE.
  - En el nivel táctico, cuando se activa la Estructura Militar de Defensa (Etta Mi D), la Fuerza Terrestre Componente (FTC) será apoyada por una Etta G Ciber. La Batalla de las Comunicaciones y la Guerra Electrónica (B), el Batallón de Comunicaciones y la Guerra Electrónica (BIM), el Batallón de Comunicaciones y la Guerra Electrónica (BIM), el Batallón de Comunicaciones y la Guerra Electrónica (BIM) y Control (Cia C2) y las Compañías de Comunicaciones (Cia Com.
  - Los elementos de las OM arriba enumeradas integran la estructura del estado mayor de la FTC. En un momento determinado, de acuerdo con la misión de la FTC, el comando podrá variar la Estructura de Guerra Cibernética.
    - En una situación de conflicto, dependiendo de la misión y de acuerdo con los factores de la decisión, la capacidad militar terrestre cibernética de la FTC será operativa por el empleo de las estructuras operativas presentadas en la Figura, cada

una con sus respectivas acciones cibernéticas.

- La planificación y el asesoramiento relacionado con las acciones cibernéticas en favor de la FTC pueden ser realizadas por el comandante del BGE, de un B Com, de un B con GE, de la Cia C2 o de las Cia Com, dependiendo de la composición de la FTC. El comandante del BIM es responsable de la planificación y asesoramiento relacionados con las acciones de explotación cibernética. Estas acciones son de interés para las operaciones de inteligencia conducidas en provecho de la maniobra de la FTC y para la producción del conocimiento de inteligencia.

- **Capacidades del Sistema de Guerra Cibernética del Ejército de Brasil**

La capacidad es la aptitud requerida a una fuerza u organización militar, para que pueda cumplir determinada misión o tarea. Se obtiene a partir del desarrollo de un conjunto de siete factores determinantes, interrelacionados e indisociables: doctrina, organización (y procesos), adiestramiento, material (y sistemas), educación, personal e infraestructura (EB70-MC-10.232, 2017, 1ª Edición). Las capacidades operativas de SGCEB se describen en la siguiente tabla:

Capacidades Operativas

Capacidad Operativa	Descripción
Protección Cibernética	Ser capaz de conducir acciones para neutralizar ataques y exploración cibernética contra nuestros dispositivos computacionales, redes de ordenadores y de comunicaciones, incrementando las acciones de guerra cibernética frente a una situación de crisis o conflicto. Es una actividad de carácter permanente.
Ataque Cibernético	Ser capaz de conducir acciones para interrumpir, negar, degradar, corromper o destruir información o sistemas computacionales almacenados en dispositivos y redes de ordenadores y de comunicaciones del oponente.
Exploración Cibernética	Ser capaz de conducir acciones de búsqueda o recolección en los Sistemas de Tecnología de la Información de interés, a fin de obtener datos. Se debe preferentemente evitar que esas acciones sean rastreadas y sirvan para la producción de conocimiento o para la identificación de las vulnerabilidades de esos sistemas.

Aplicación en Operaciones Terrestres (EB70-MC-10.232, 2017, 1ª Edición)

- **Operaciones Combinadas**
  - Elementos especializados en G Ciber pueden componer tropas de F Ter que integran arreglos internacionales de defensa colectiva, de acuerdo con los intereses nacionales.

Estos acuerdos consisten en la formación de coaliciones de fuerzas multinacionales para el restablecimiento del ordenamiento jurídico internacional.

- El uso del espacio cibernético de una nación requiere coordinación y negociación formal, buscando desarrollar la capacidad de interoperabilidad. Las acciones cibernéticas desarrolladas en misiones multinacionales requieren un gran esfuerzo de integración. Estos esfuerzos mitigar las posibles complicaciones causadas por diferencias de políticas o en cuanto a los dispositivos y sistemas de integración y de intercambio de información.
- Diferencias entre patrones y entre legislaciones referentes a la soberanía del ciberespacio pueden afectar la disposición y la legalidad de participación de un país en una operación. Por lo tanto, algunos países pueden negarse a participar, mientras que otros pueden realizar sus propias acciones por separado.
- La conectividad y la integración son esenciales cuando las fuerzas multinacionales trabajan en apoyo mutuo en las operaciones. Algunas incompatibilidades o disparidades de equipos y programas, además de políticas de garantía y seguridad de la información, pueden causar brechas de seguridad o de capacidad operativa.
- Con el objetivo de minimizar una probable lentitud para alcanzar los objetivos, se debe realizar la planificación anticipada sobre los requisitos técnicos de integración, para evitar las disparidades o incompatibilidades.
- En el espacio cibernético, el intercambio de información con aliados y socios multinacionales es muy importante durante la operación combinada. Al conducir acciones cibernéticas, todas las tropas participantes deben adoptar los procedimientos y las políticas establecidos para la garantía del funcionamiento y de la protección de sistemas de información y de redes de computadoras.

- Cada país tiene soberanía sobre el espacio cibernético en su delimitación geográfica. Por lo tanto, el uso del ciberespacio de una nación requiere coordinación y negociación formales. Esta coordinación busca desarrollar la capacidad de interoperabilidad en el ciberespacio.

- **Operaciones Ofensivas**

  - La complejidad de las redes y su rápida adaptación al desarrollo de las acciones exigen una minuciosa planificación. Para las acciones cibernéticas, se emplearán todos los recursos, con el objetivo de crear soluciones alternativas para el cumplimiento de la misión.
  - En las operaciones ofensivas, crecen de importancia las acciones de ataque y de explotación cibernética.

  - En coordinación con los fuegos y con la guerra electrónica, se debe elaborar una lista de blancos cibernéticos (LIA Ciber) y una lista priorizada de blancos cibernéticos (LIPA Ciber).
  - Las diferentes tareas de ataque descritas en el capítulo 4 se pueden realizar a nivel táctico en apoyo a las operaciones de la FTC, observándose la integración con las diversas funciones de combate.
  - La estructura de guerra Cibernética de la FTC puede, también, realizar tareas ofensivas para negar servicio o perjudicar el funcionamiento de las infraestructuras críticas del oponente localizadas dentro de su zona de acción.
  - Esta estructura puede, además, realizar acciones de exploración cibernética, para identificar vulnerabilidades en las redes de computadoras de los sistemas militares y de las infraestructuras críticas del enemigo. Esto facilitará la planificación de las acciones de ataque cibernético y la producción de datos para la inteligencia de fuente cibernética.

- Las acciones de protección cibernética tienen carácter permanente en todas las fases de la operación. La protección cibernética de los sistemas de información es esencial para su eficaz ejercicio durante el ataque. Redundancias y otros mecanismos contra fallas de seguridad de los sistemas de información deben proporcionar la continuidad de la misión.

- **Operaciones Defensivas**

  - En las operaciones defensivas prevalecen las acciones de protección cibernética. El mantenimiento de estas acciones en relación con los sistemas de información en una operación suele ser crítico. G Ciber es fundamental en una defensa móvil debido a los siguientes factores:
    a) un intenso flujo de información;
    b) rapidez en la toma de decisiones y en la difusión de las órdenes; y
    c) coordinación de todas las funciones de combate en tiempo y espacio.

  - Las acciones de explotación cibernética y de ataque cibernético pueden ser conducidas, siempre que no denuncien la posición, la dirección lógica y las intenciones de las tropas amigas.
  - Establecido el contacto con el enemigo, las acciones cibernéticas realizadas vía radio tendrán mayor libertad de uso, pero siempre con el empleo de medidas preventivas de protección cibernética.

- **Operaciones de Información**

  - La guerra cibernética contribuye con las operaciones de información como una capacidad relacionada a la información (CRI). Así, posee áreas de superposición con las OP Info, pero

sin vínculo de subordinación. Las CRI son aptitudes requeridas para afectar la capacidad de oponentes o potenciales adversarios de orientar, obtener, producir y / o difundir informaciones, en cualquiera de las tres perspectivas de la dimensión informacional (física, cognitiva o lógica).

- Para G Ciber, los principios fundamentales de la Op Info de mayor interés se presentan a continuación:
  a) Dirección e implicación personal del comandante - por ese principio, el comandante tiene conocimiento de todas las acciones cibernéticas desencadenadas y puede emplear a G Ciber con técnicas adecuadas para alcanzar el estado final deseado (EFD).
  b) Estrecha coordinación - las tareas deben coordinarse y sincronizarse con otras actividades operativas, de forma sinérgica, para evitar los efectos colaterales por el empleo de acciones cibernéticas.
  c) Aguzada actividad de inteligencia - las acciones cibernéticas, cuando se alimentan de informaciones confiables, tienen resultados más eficaces en favor de la EFD.
  d) Planificación basada en efectos - las acciones cibernéticas emplearán la técnica operacional de acuerdo con el efecto deseado: destrucción, neutralización, inutilización, influencia, disimulación y negación de la información.
  e) Participación precoz y preparación anticipada - la planificación de las OP Info debe comenzar lo antes posible. Para contribuir a esta planificación, las acciones cibernéticas deben realizarse con la antelación necesaria, ya que sus resultados no son inmediatos.
  f) Las acciones cibernéticas a ser conducidas en determinada operación deben ser mencionadas en el apéndice de guerra cibernética al anexo de operaciones de información al Pl / O Operaciones de la FTC.

2.2.2. VARIABLE 2: Formación Académica especializada

La formación académica en las instituciones de educación superior en las últimas décadas atraviesa por cambios acelerados y grandes transformaciones. Algunos de estos cambios han elevado la tensión de la profesionalización y el acreditar las instituciones ante los organismos educativos, en particular en los enfoques de formación académica y profesionales por competencias.

La formación universitaria no puede entenderse o justificarse, en cuanto a educación superior solamente, sino como resultado de un proceso educativo que presupone una educación primaria y secundaria con sus propias especificidades que la docencia universitaria completa, y que la persona culmina en su educación a lo largo de su vida. La formación del nivel superior sería inútil o limitada sin la educación primaria y secundaria orientadas al desarrollo cognitivo de los jóvenes, ya que la formación universitaria no se caracteriza tanto por los contenidos de conocimientos, sino por el nivel de desarrollo intelectual de los estudiantes (Sanchez-Parga, 2003).

Por ello el perfil adecuado que reúna las competencias necesarias dentro de la formación académica especializada se podría resumir de acuerdo a lo estipulado por: Aponte, E. (2004)

1. Visión prospectiva – cómo prever para aprender nuevas habilidades y conocimiento para anticipar y manejar lo que aún no se puede considerar.

2. Inclusión/equidad – autogestionar conocimiento y adquisición de habilidades de la ciudadanía, que les permitan hacerse cargo de su aprendizaje para construirse, transformarse, insertarse, participar y actuar en el trabajo y la sociedad.

3. Temporalidad y espacios – cómo aprender a manejar el tiempo, los espacios y las localidades de otros y con otros.

4. Creatividad/inventiva – cómo aprender a desarrollar la creatividad para la acción emprendedora y así enfrentar los cambios, la incertidumbre y la inseguridad.

5. Diversidad/convivencia y trabajo con otros – cómo aprender a relacionarnos con diferentes culturas y personas con otras ideas, valores, creencias y formas de ver el mundo y hacer las cosas.

6. Innovación orientada a elevar la capacidad de autogestión para el desarrollo endógeno local para interactuar con lo global.

7. Autorrealización/existencia – cómo aprender y desarrollar las actitudes, percepciones y habilidades de autoconocimiento para llegar a "ser" una persona que pueda vivir una vida ética, estética y en harmonía con los otros y con la naturaleza.

La educación en general deberá proporcionar a las personas modos flexibles de organización de conocimiento integral y de desarrollo de la solidaridad, tolerancia y capacidad para hacer ajustes y auto transformación ante la diversidad, compartiendo valores que constituyen el núcleo no negociable de identificación individual y de grupo que suponen las necesidades de la convivencia intercultural en la era del conocimiento del siglo XXI.

Por su parte la curricula académica nos muestra detalladamente como se desarrolla la preparación de los futuros Oficiales de Comunicaciones.

a. EMPLEO DE COMUNICACIONES PARA TODAS LAS ARMAS

1) ORGANIZACIÓN DE COMUNICACIONES

- Consideraciones básicas
- Unidades de comunicaciones.
- Organización de la sección comunicaciones en UU tipo Batallón

2) FUNDAMENTOS DE EMPLEO

- Normas de comunicaciones y necesidades de enlace.
- Informaciones de los OO de comunicaciones.
- Consideraciones para el funcionamiento del sistema de comunicaciones.
- Medios de comunicaciones.
- Comando y comunicaciones

3) PERSONAL DE COMUNICACIONES DE LAS UU TIPO BATALLÓN

- Generalidades
- Actividades y responsabilidades del oficial de comunicaciones.
- Actividades del personal de la sección de comunicaciones.

4) PROCEDIMIENTOS DE EXPLOTACIÓN Y CONSTITUCIÓN DE EQUIPOS BÁSICOS DE COMUNICACIONES

- Conceptos y definiciones.
- Denominación Genérica y Nomenclatura.
- Empleo de la denominación genérica.
- Estaciones de radio, equipos de construcción, explotación alámbrica y CM en campaña.

b. SISTEMA DE COMUNICACIONES SATELITAL VSAT

1) GENERALIDADES

- Sistemas satelitales.
- Necesidades de comunicaciones satelitales para un ejército.
- Arquitectura de un sistema de comunicaciones satelitales de un ejército.
- Comando y control en movimiento.
- El sistema de comunicaciones satelital VSAT del Ejercito del Perú.

2) ESTACIÓN BASE

- Fundamentos de la tecnología.
- Efectos de la naturaleza en el sistema.

- Segmento terrestre.

3) ESTACIONES FIJAS

- El padrón DVB-RCS.
- Equipos, instalación y montaje.
- Apuntamiento de la antena.
- Configuración del sistema vía web.
- Line up (alineación).
- Configuración vía comandos y ayuda.

4) UNIDADES MÓVILES

- Generalidades.
- Descripción de las unidades móviles.
- Problemas comunes y práctica.

c. MEDIOS DE COMUNICACIÓN EN CAMPAÑA

1) EQUIPO DE RADIO PRC – 6020 HF

- Características básicas.
- Características operacionales.
- Programación del equipo.

2) EQUIPO DE RADIO PRC – 730 VHF

- Características.
- Componentes.
- Operación del equipo de radio.

3) EQUIPO DE RADIO PRC – 710 VHF/UHF

- Características básicas.
- Características operacionales.
- Programación del equipo.

4) EQUIPO DE RADIO SELEX UHF

- Características básicas.
- Características operacionales.
- Programación del equipo.

d. FUNDAMENTOS DE COMANDO Y CONTROL

1) GENERALIDADES

- Consideraciones generales.
- Siglas y conceptos relacionados a C4I.

2) DEFINICIONES, PRINCIPIOS Y FUNCIONES DEL C2

- Definición de comando.
- Definición de control.
- Definición de comando y control.
- Principios de C2.
- Funciones de C2.

3) COMPONENTES DE UN SISTEMA DE COMANDO Y CONTROL

- Definiciones de sistema de C2.
- Componentes de un sistema de C2.
- Tipos de sistemas de C2.

4) SOFTWARE DE COMANDO Y CONTROL WIRACOCHA

- Conceptos del software de C2 WIRACOCHA
- Instalación y Configuración del software de C2 WIRACOCHA.
- Composición de las Redes Operacionales
- Operación del software de C2 WIRACOCHA

2.3. Definición de términos básicos

2.3.1 Activos de Información

Medios de almacenamiento, transmisión y procesamiento de datos e información, los equipos necesarios para ello (ordenadores, equipos de comunicaciones y de interconexión), los sistemas utilizados para ello, los sistemas de información de un modo general, así como los lugares donde se encuentren esos medios y las personas a las que tienen acceso (EB70-MC-10.232, 2017).

2.3.2 Amenaza Cibernética

Causa potencial de un incidente indeseado, que puede resultar en daño al espacio cibernético de interés (EB70-MC-10.232, 2017).

2.3.3. Antivirus

Programa diseñado para detectar, detener y eliminar códigos maliciosos. (ISDEFE-6:2009)

2.3.4 Artefacto Cibernético

Equipo o sistema empleado en el espacio cibernético para ejecución de acciones de protección, explotación y ataque cibernético (EB70-MC-10.232, 2017).

2.3.5. Ataque de “Agujero De Agua”

Tipo de ataque informático que consiste en la creación de un sitio web falso o en la “infección” de uno real con el objetivo de estafar a los usuarios visitantes. (ISDEFE-6:2009)

2.3.6. Autenticación

Procedimiento para comprobar que alguien es realmente quien dice ser cuando accede a un ordenador o a un servicio online. (ISDEFE-6:2009)

2.3.7. Botnet

Red de equipos infectados por un atacante remoto. Los equipos quedan a su merced cuando desee lanzar un ataque masivo, tal como envío de spam o denegación (distribuida) de servicio. (ISDEFE-6:2009)

2.3.8. Ciberamenaza

Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste. (ISDEFE-6:2009)

2.3.9. Ciberataque

1. Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan. O.M. 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. (ISDEFE-6:2009)

2. Uso del ciberespacio para atacar a los sistemas y servicios presentes en el mismo o alcanzables a través suyo. El atacante busca acceder sin autorización a información, o alterar o impedir el funcionamiento de los servicios. (ISDEFE-6:2009)

3. Intentos maliciosos de daño, interrupción y acceso no autorizado a sistemas computacionales, redes o dispositivos por medio de la red. (ISDEFE-6:2009)

2.3.10. Ciberdefensa

Concepto que engloba todas las actividades ofensivas y defensivas en las que se utilizan como medio aquellos relacionados con las infraestructuras TIC (Ej. Redes de ordenadores, ordenadores, programas informáticos, etc.), y cuyo “campo de batalla” es el Ciberespacio. Las actividades de desarrollo de la ciberdefensa van encaminadas hacia la capacitación de los gobiernos y naciones en la denominada “Ciberguerra”. (ISDEFE-6:2009)

2.3.11. Cibernética

Término que se refiere a la comunicación y control, actualmente relacionado al uso de computadoras, sistemas computacionales, redes de computadoras y de comunicaciones y su interacción.
En el marco de una planificación nacional de nivel estratégico, coordinado e integrado por el MD, con las finalidades de proteger los sistemas de información (Sistemas de Información) el interés de la defensa nacional, obtener datos para la producción de conocimiento de inteligencia y comprometer los sistemas de información del oponente (EB70-MC-10.232, 2017).

2.3.12. Ciberguerra

1. Lucha armada (en este caso las armas son las TIC) entre dos o más naciones o entre bandos de una misma nación, en la que se utiliza el Ciberespacio como campo de batalla. (ISDEFE-6:2009)

2. Término se utiliza para designar ataques, represalias o intrusión ilícita en un ordenador o en una red. (ISDEFE-6:2009)

2.3.13. Ciberseguridad

Protección de dispositivos, servicios o redes, así como la protección de datos frente a intentos de robo o daño. (ISDEFE-6:2009)

2.3.14. Códigos Maliciosos

Programas diseñados para infiltrarse en los sistemas y ocasionar daños en los dispositivos electrónicos como ordenadores, tablets, smartphones, etc., alterando su funcionamiento y poniendo en riesgo la información de los usuarios. (ISDEFE-6:2009)

2.3.15. Contraseña Segura

Clave de identificación virtual que permite acceder a la información privada que se almacena en dispositivos electrónicos o servicios en línea como el correo electrónico, las redes sociales, la banca en línea, etc. En términos generales, para que esta sea segura se recomienda que está compuesta por una combinación de ocho caracteres intercalando mayúsculas, minúsculas, números y símbolos. (ISDEFE-6:2009)

2.3.16. Cortafuegos o Firewall

1. Hardware o software que utiliza un conjunto de reglas definidas para restringir el tráfico de la red e impedir accesos no autorizados. (ISDEFE-6:2009)

2. Tecnología de hardware y/o software que protege los recursos de red contra el acceso no autorizado. Un firewall autoriza o bloquea el tráfico de computadoras entre redes con diferentes niveles de seguridad basándose en un conjunto de reglas y otros criterios. http://es.pcisecuritystandards.org

2.3.17. Desfigurar

Ataque sobre un servidor web como consecuencia del cual se cambia su apariencia. El cambio de imagen puede ser a beneficio del atacante, o por mera propaganda (a beneficio del atacante o para causar una situación embarazosa al propietario de las páginas). (ISDEFE-6:2009)

2.3.18. Encriptación

Función matemática que protege la información haciéndola ilegible excepto para quienes tengan la clave. (ISDEFE-6:2009)

2.3.19. Espacio Cibernético

Espacio virtual compuesto por dispositivos computacionales conectados en redes o no, donde las informaciones digitales transitan y son procesadas y / o almacenadas (EB70-MC-10.232, 2017).

2.3.20. Guerra Cibernética

Corresponde al uso ofensivo y defensivo de información y sistemas de información para negar capacidades de C2 al adversario, explotarlas, corromperlas, degradarlas o destruirlas, en el contexto de una planificación militar de nivel operativo o táctico o de una operación militar. Comprende acciones que involucran las herramientas de TIC para desestabilizar o sacar provecho de los sistemas de información del oponente y defender los propios Sistemas de Información. Abarca, esencialmente, las acciones cibernéticas. La oportunidad para el empleo de esas acciones o su efectiva utilización será proporcional a la dependencia del oponente en relación a las TIC (EB70-MC-10.232, 2017).

2.3.21. Identidad Digital

Es lo que somos para otros en la red; un perfil que se crea de cada usuario a partir de la información que se almacena en la red. (ISDEFE-6:2009)

2.3.22. Infraestructura Crítica de la Información

Subconjunto de los activos de información que afecta directamente la consecución y la continuidad de la misión del estado y la seguridad de la sociedad (EB70-MC-10.232, 2017).

2.3.23. Fuente Cibernética

Recurso que posibilita la obtención de datos en el espacio cibernético, utilizando acciones de búsqueda o recolección, normalmente realizadas con ayuda de herramientas computacionales. La fuente cibernética puede ser integrada a otras fuentes (humanas, imágenes y señales) para producir conocimiento de inteligencia (EB70-MC-10.232, 2017).

2.3.24. Ingeniería Social

Técnicas utilizadas para manipular a la gente a fin de que realice acciones específicas o se sume a la difusión de información que es útil para un atacante. (ISDEFE-6:2009)

2.3.25. Malware

Abreviatura de Malicious Software que hace referencia a todos los programas o códigos informáticos cuya función es dañar o causar el mal funcionamiento de un sistema. (ISDEFE-6:2009)

2.3.26. Parche

Actualizaciones de seguridad que permiten mejorar la misma y el funcionamiento de un software. (ISDEFE-6:2009)

2.3.27. Pharming

Ataque informático que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a otra dirección IP donde se aloja una web falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad. http://www.inteco.es/glossary/Formacion/Glosario

2.3.28. Phishing

1. Método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio. (ISDEFE-6:2009)

2. Envío masivo de mensajes de correo electrónico con el objetivo de apropiarse de información confidencial de los usuarios o incitarlos a visitar sitios web falsos. (ISDEFE-6:2009)

2.3.29 Poder Cibernético

Capacidad de utilizar el espacio cibernético para crear ventajas y eventos de influencia en este y otros ámbitos operativos y en instrumentos de poder (EB70-MC-10.232, 2017).

2.3.30. Ransomware

Códigos maliciosos creados por ciberdelincuentes que bloquean el acceso a los dispositivos de los usuarios para después pedirles un pago a las víctimas para recuperar su información. (ISDEFE-6:2009)

2.3.31 Resiliencia Cibernética

Capacidad de mantener las infraestructuras críticas de la información operando bajo condiciones de ataque cibernético o de restablecerlas después de una acción adversa (EB70-MC-10.232, 2017).

2.3.32 Riesgo Cibernético

Probabilidad de ocurrencia de un incidente cibernético asociado a la magnitud del daño provocado por él (EB70-MC-10.232, 2017).

2.3.33. Rootkit

Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo. Está disponible para una amplia gama de sistemas operativos. (http://www.alerta-antivirus.es /seguridad/ ver_pag.html?tema=S.)

2.3.34. Seguridad Cibernética

Arte de asegurar la existencia y la continuidad de la sociedad de la información de una nación, garantizando y protegiendo, en el espacio cibernético, sus activos de información y sus infraestructuras críticas (EB70-MC-10.232, 2017).

2.3.35. Seguridad de la Información y Comunicaciones (SIC)

Acciones que objetivan viabilizar y asegurar la disponibilidad, la integridad, la confidencialidad y la autenticidad de datos e informaciones (EB70-MC-10.232, 2017).

2.3.35.1. Disponibilidad

Propiedad según la cual la información debe ser accesible y utilizable bajo demanda por una persona física o por determinado sistema, órgano o entidad (EB70-MC-10.232, 2017).

2.3.35.2. Integridad

Propiedad según la cual la información no debe ser modificada o destruida de manera no autorizada o accidental (EB70-MC-10.232, 2017).

2.3.35.3. Confidencialidad

Propiedad según la cual la información no debe estar disponible o ser revelada a la persona física, sistema, órgano o entidad no autorizados o no acreditados (EB70-MC-10.232, 2017).

2.3.35.4. Autenticidad

Propiedad según la cual la información fue producida, expedida, modificada o destruida por una determinada persona física o por un determinado sistema, órgano o entidad (EB70-MC-10.232, 2017).

2.3.36. Sector cibernético

Uno de los tres sectores de importancia estratégica para la defensa nacional, de acuerdo con la Estrategia Nacional de Defensa, abarcando a las personas, instalaciones, infraestructuras y recursos tecnológicos, de nivel estratégico, necesarios para que las FA puedan actuar en red con seguridad, tales como el Sistema Militar de Control y Control (SISMC2), sistemas de armas / vigilancia y sistemas administrativos que puedan afectar a las actividades operativas (EB70-MC-10.232, 2017).

2.3.37. Software Malicioso o Malware

Software o firmware desarrollado para infiltrarse en una computadora o dañarla sin conocimiento ni consentimiento del propietario, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema operativo del propietario. Por lo general, esta clase de software se infiltra en una red durante diversas actividades aprobadas por el negocio, lo que permite explotar las vulnerabilidades del sistema. Algunos ejemplos son los virus, gusanos, troyanos (o caballos de Troya), spyware, adware y rootkits. http://es.pcisecuritystandards.org(ISDEFE-6:2009)

2.3.38. Spear-Phishing

Ataque dirigido de phishing, que se lleva a cabo una vez que el delincuente ha estudiado a su posible víctima a través de mensajes de correo electrónico muy específicos. (ISDEFE-6:2009)

2.3.39. Troyano

Código malicioso con apariencia de software fiable que se oculta en el sistema para infectarlo. (ISDEFE-6:2009)

2.4. Hipótesis

2.4.1. Hipótesis General

La asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

2.4.2. Hipótesis Específicas

2.4.2.1. Hipótesis Especifica 1

Los Fundamentos de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

2.4.2.2. Hipótesis Especifica 2

La Estructura y Responsabilidades de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

2.4.2.3. Hipótesis Especifica 3

La Aplicación en Operaciones Terrestres de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

2.5. Variables

Es un componente o fenómeno en estudio que representa cierto interés dentro de una investigación. Se conoce como variable porque el componente estudiado puede obtener distintos valores entre una observación y otra.

2.5.1. Definición Conceptual

2.5.1.1 Variable 1: La Asignatura de Guerra Cibernética

La guerra cibernética se define como "las acciones de un estado nación para penetrar en los ordenadores o redes de otra nación con el fin de causar daños o trastornos". Muchas personas sugerirían que el Ciberterrorismo se refiere a la voluntad de un grupo terrorista de causar muerte o lesiones graves utilizando herramientas de ataque basadas en Internet. Si bien, por desgracia, estos ataques son posibles, afortunadamente hasta la fecha no tenemos ninguna constancia de que grupos terroristas empleen estas tácticas. Eso no quiere decir que no estén dispuestos a hacerlo y, en consecuencia, existen estrategias de Ciberseguridad nacional que intentan hacer frente a estas vulnerabilidades.

Lyons, J. (2017)

2.5.1.2 Variable 2: Formación Académica especializada

La formación académica es un conjunto de conocimientos adquiridos, los cuales son una herramienta que te ayudarán a consolidar las competencias que posees. ... “Los profesionales deben saber que hoy en día tienen que diversificarse y hacer que su capital humano sea flexible.

2.5.2. Definición Operacional

VARIABLES	DEFINICION CONCEPTUAL	DIMENSIONES	INDICADORES	ITEM
La Asignatura de Guerra Cibernética	La guerra cibernética se define como "las acciones de un estado nación para penetrar en los ordenadores o redes de otra nación con el fin de causar daños o trastornos". Muchas personas sugerirían que el Ciberterrorismo se refiere a la voluntad de un grupo terrorista de causar muerte o lesiones graves utilizando herramientas de ataque basadas en Internet. Si bien, por desgracia, estos ataques son posibles, afortunadamente hasta la fecha no tenemos ninguna constancia de que grupos terroristas empleen estas tácticas. Eso no quiere decir que no estén dispuestos a hacerlo y, en consecuencia, existen estrategias de Ciberseguridad nacional que intentan hacer frente a estas vulnerabilidades.	Fundamentos	• Características de la guerra cibernética • Posibilidades de la guerra cibernética	¿Cree usted que las características de empleo de la Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH "CFB"? ¿Cree usted que las posibilidades de empleo de la Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH "CFB"?
		Estructura y Responsabilidades	• Visión Sistémica • Capacidades del Sistema de Guerra Cibernética del Ejército	¿Considera usted que la Visión Sistemática de la Estructura y Responsabilidades de la Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH "CFB"? ¿Considera usted que las Capacidades del Sistema de Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH "CFB"?
		Aplicación en Operaciones Terrestres	• Operaciones Ofensivas • Operaciones Defensivas	¿Cree usted que la aplicación de las operaciones ofensivas de la Guerra Cibernética se relaciona con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH "CFB"? ¿Cree usted que la aplicación de las operaciones defensivas de la Guerra Cibernética se relaciona con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH "CFB"?
	La formación académica es un conjunto de conocimientos adquiridos, los cuales son una herramienta que te ayudarán a consolidar las competencias que posees. ... "Los profesionales deben saber que hoy en día tienen que diversificarse y hacer que su capital humano sea flexible.	Empleo de comunicaciones para todas las armas	• Organización de comunicaciones • Fundamentos de empleo • Personal de comunicaciones de las UU tipo batallón • Procedimientos de explotación y constitución de equipos básicos de comunicaciones.	¿Considera usted que, atendiendo a la formación especializada, el empleo de las comunicaciones para todas las armas es influido por la asignatura de Guerra Cibernética?

Formación Académica especializada				
		Sistema de comunicaciones satelital VSAT	• Estación base • Estaciones fijas	¿Considera usted que, atendiendo a la formación especializada, el Sistema de Comunicaciones Satelital VSAT es influido por los fundamentos de la asignatura de Guerra Cibernética?
		Medios de comunicación en campaña	• Equipo de radio PRC – 6020 HF • Equipo de radio PRC – 710 VHF/UHF • Equipo de radio SELEX UHF	¿Considera usted que, atendiendo a la formación especializada, los medios de comunicación en campaña son influidos por los fundamentos de la asignatura de Guerra Cibernética? ¿Cree usted que la aplicación de las operaciones defensivas de la Guerra Cibernética se relaciona con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?
		Fundamentos de comando y control	• Definiciones, principios y funciones del C2 • Componentes de un sistema de comando y control • Software de comando y control Wiracocha	¿Considera usted que, atendiendo a la formación especializada, los fundamentos de comando y control son influidos por los fundamentos de la asignatura de Guerra Cibernética?

CAPÍTULO III: MARCO METODOLÓGICO

3.1. Enfoque

La presente investigación se ha realizado mediante un enfoque cuantitativo ya que, se centra fundamentalmente en los aspectos observables y susceptibles de cuantificación de los fenómenos, utiliza la metodología empírico analítico y se sirve de pruebas estadísticas para el análisis de datos.

Por otro lado, Hernández, Fernández y Baptista (2006, p. 5) refiere que “el enfoque cuantitativo usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías”.

3.2. Tipo de estudio.

Básico, Investigación Básica o Fundamental busca el conocimiento de la realidad o de los fines nuevos de la naturaleza para contribuir a una sociedad cada vez mas avanzada y que responda mejor a los retos de la humanidad.
Este tipo de Investigación no busca la aplicación práctica de sus descubrimientos sino el aumento del conocimiento para responder a preguntas.

3.3. Diseño

No experimental, de corte transversal

Tafur (2009)

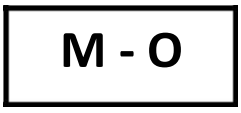
El diseño de investigación será no experimental de corte transversal. Es aquella que se realiza sin manipular deliberadamente variables. ... “La investigación no experimental o expost-facto es cualquier investigación en la

que resulta imposible manipular variables o asignar aleatoriamente a los sujetos o a las condiciones".

Según el autor (Santa Palella y Feliberto Martins (2010)), define: El diseño no experimental es el que se realiza sin manipular en forma deliberada ninguna variable. El investigador no sustituye intencionalmente las variables independientes. Se observan los hechos tal y como se presentan en su contexto real y en un tiempo determinado o no, para luego analizarlos. Por lo tanto, en este diseño no se construye una situación especifica si no que se observa las que existen (pag.87).

Kerlinger (2002) Sostiene que generalmente se llama diseño de investigación al plan y a la estructura de un estudio. Es el plan y estructura de una investigación concebidas para obtener respuestas a las preguntas de un estudio.

Esquema:



Dónde:

M: Muestra con quien(es) vamos a realizar el estudio.

O: Información (observaciones) relevante o de interés que recogemos de la muestra.

3.4 Método de Investigación.

Los Métodos de Investigación son encuestas para recolección de datos, formulan y responder preguntas para llegar a conclusiones a través de una análisis sistemático y teórica aplicado

El Método de Investigación será el método científico con el Propósito Hipotético deductivo que es un modelo del Método Científico compuesto por

los siguientes pasos esenciales: Observación del fevocirco a estudiar, creación de una Hipotesis para explicar dicho fevocurco. Deducción de consecuencias.

3.5 Población y muestra

3.5.1 Población

La población se refiere al universo, conjunto o totalidad de elementos sobre los que si investigan o hacen estudios.

La Población es el conjunto total de individuos, o medidas que poseen algunas características comunes observables en un lugar y momento determinado y solo considerar a los cadetes de comunicaciones.

La población a delimitar la investigación, estará conformada por los 62 cadetes del arma de Comunicaciones que estudian en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

AÑO	N° DE CADETES
4to Año	19
3er Año	23
2do Año	20
TOTAL	**62**

3.5.2 Muestra

Sierra (2003) considera a la muestra como una parte representativa de un conjunto o población debidamente elegida que se somete a observación científica en representación del conjunto, con el propósito de obtener resultados válidos para el universo total investigado.

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::

$$! = \frac{\$^{\%} * ' * (*)}{*^{\%} * () - 1) + \$^{\%} * ' * (}$$

Dónde:

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

e : Margen de error 8%

N : Población.

n : Tamaño óptimo de muestra

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

$$! = \frac{(1.96)^{\%} * (62) * (0.5) * (0.5)}{(0.08)^{\%} * (62 - 1) + (1.96)^{\%} * (0.5) * (0.5)}$$

$$! = 42\ 89{:}*;*{<}{:}* =>?@!A898A>!*<$$

Esta muestra será seleccionada de manera aleatoria

3.6. Técnicas e instrumentos de la recolección de datos.

Se ha empleado como técnicas la encuesta y como instrumento el cuestionario, conformado por 16 ítems para recoger los datos.

3.6.1. Técnicas

La Encuesta. Una encuesta es un conjunto de preguntas normalizadas dirigidas a una muestra representativa de la población o instituciones, con el fin de conocer estados de opinión o hechos específicos. La intención de la encuesta no es describir los individuos particulares

quienes, por azar, son parte de la muestra sino obtener un perfil compuesto de la población. Una "encuesta" recoge información de una "muestra." Una "muestra" es usualmente sólo una porción de la población bajo estudio.

La Observación. La observación es otra técnica útil para el analista en su proceso de investigación, consiste en observar a las personas cuando efectúan su trabajo. La observación es una técnica de observación de hechos durante la cual el analista participa activamente actúa como espectador de las actividades llevadas a cabo por una persona para conocer mejor su sistema. El propósito de la observación es múltiple, permite al analista determinar que se está haciendo, como se está haciendo, quien lo hace, cuando se lleva a cabo, cuánto tiempo toma, donde se hace y porque se hace.

3.6.2. Instrumentos

Los instrumentos son medios auxiliares para recoger y registrar los datos obtenidos a través de las técnicas y pueden ser: Guía de Observación, Ficha de Observación; Cuestionario, Guía de Análisis de Documentos; Escalas Tipo Likert, Diferencial Semántico; Test; Cuestionario.
Se realizará una encuesta de preguntas cerradas.

Instrumentos:

El instrumento empleado en el presente trabajo fue el cuestionario que es un conjunto de preguntas formuladas por escrito a ciertas personas para que opinen sobre un asunto. Es un instrumento de investigación que se utiliza para recabar, cuantificar, universalizar y finalmente, comparar la información recolectada. Como herramienta, el cuestionario es muy común en todas las áreas de estudio porque resulta ser una forma no costosa de investigación, que permite llegar a un mayor número de participantes y facilita el análisis de la información.

Por ello, este género textual es uno de los más utilizados por los investigadores a la hora de recolectar información.

Martínez (2013) manifiesta que las técnicas más comunes que se utilizan en la investigación social son la observación, la encuesta y la entrevista, y como instrumentos tenemos la recopilación documental, la recopilación de datos a través de cuestionarios que asumen el nombre de encuestas o entrevistas y el análisis estadístico de los datos.

3.7. Validación y Confiabilidad del Instrumento.

Ñaupas (2008), plantea que el análisis de datos se realiza con el concurso de la ciencia estadística descriptiva, cuyo objeto fundamental es determinar un conjunto de medidas estadísticas o estadígrafos como las medidas de tendencia central y las medidas de dispersión.

Se decidió utilizar el software Word, Excel y el software estadístico SPSS 22.

En el análisis propiamente dicho se procederá a determinar medidas y parámetros:

3.7.1 Validez

Esta escala de Actitudes hacia la Implementación de la Asignatura de Guerra Cibernética para los cadetes del arma de Comunicaciones de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, quienes informaron acerca de la pertinencia, relevancia, claridad y aplicabilidad del cuestionario de la presente investigación.

En lo concerniente a la validez de contenido, se puede indicar que según Hernández (ibid), es la que consiste en el grado en que un determinado instrumento expresa concisamente, lo que se pretende medir. Así pues, para determinarla, se debe en primera instancia, revisar

cómo ha sido utilizada previamente la variable en otras investigaciones. Para luego, sobre la base de base de la anterior revisión, elaborar otro instrumento, en el cual, sea posible medir la variable.

Como paso siguiente, se procede a consultar con los investigadores especializados en el tema de estudio, con el fin de evaluar la veracidad del instrumento. Posteriormente, se hace una selección de los ítems, consecuentemente extrayéndose una muestra probabilística de ítems. Luego, se aplican los ítems y se hace una correlación de los resultados entre ellos, haciéndose estimaciones estadísticas, con la finalidad de comprobar si la muestra es representativa o no.

- **Validez de criterio:** Según Hernández (ibid), para obtener la validez de criterio, es necesario comparar dicha validez con algún criterio externo. En tal sentido, se debe correlacionar su medición con el criterio que se va a utilizar como patrón de medida, para obtener un coeficiente que consecuentemente será tomado como coeficiente de validez.

- **Validez de constructo**: Con respecto a la validez de constructo, se puede mencionar lo expresado por Hernández (ob cit), quien señala que la validez en cuestión, es el grado en que una medición se encuentra relacionada de forma consistente con otras mediciones, en concordancia con hipótesis derivadas teóricamente y que conciernen a los constructos o conceptos que son objeto de una determinada medición. En ese mismo orden, para obtener la validez de constructo, se utiliza el procedimiento de Análisis de Factores, el cual, amerita, el uso de un cúmulo de fórmulas estadísticas.

3.7.2 Confiabilidad

Para establecer la confiabilidad del cuestionario, se utilizó la prueba estadística de fiabilidad alfa de Cronbach, con una prueba piloto de 20. Luego se procesarán los datos, haciendo uso del Programa Estadístico SPSS versión 22.0.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,995	16

3.8. Procedimientos para el proceso de Datos

Se procede a realizar el contacto con los oficiales encargados del área respectiva. En los referentes a los procesos de acceso se solicita a través de una constancia de la entidad donde se efectúa la investigación invertido este creció respaldado ante cada una de las personas encuestadas.

3.9 Aspectos Éticos

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: RESULTADOS

4.1. Descripción:

Para la variable independiente: LA GUERRA CIBERNETICA

1. ¿Cree usted que las características de empleo de la Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de comunicaciones de la EMCH “CFB”?

Tabla 1. *Características – Sistemas VSAT*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	3	7,1	7,1	7,1
	Casi Nunca	1	2,4	2,4	9,5
	A veces	7	16,7	16,7	26,2
	Casi Siempre	11	26,2	26,2	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

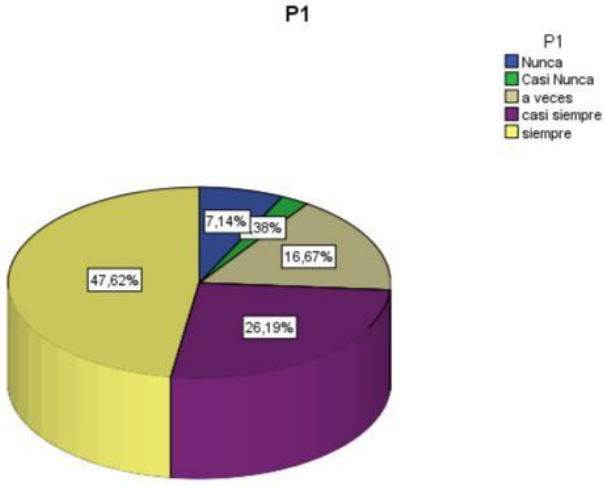


Figura 1. *Características – Sistemas VSAT*

Descripción: En cuanto a si cree usted que las características de empleo de la Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 26,2%; manifestaron que muy poco un 16,7%; un 2,4% dijeron que casi nada; y, un 7,1% manifestaron que nunca.

2. ¿Cree usted que las posibilidades de empleo de la Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

Tabla 2. *Posibilidades – Sistemas VSAT*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	3	7,1	7,1	7,1
	Casi Nunca	4	9,5	9,5	16,7
	A veces	4	9,5	9,5	26,2
	Casi Siempre	11	26,2	26,2	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

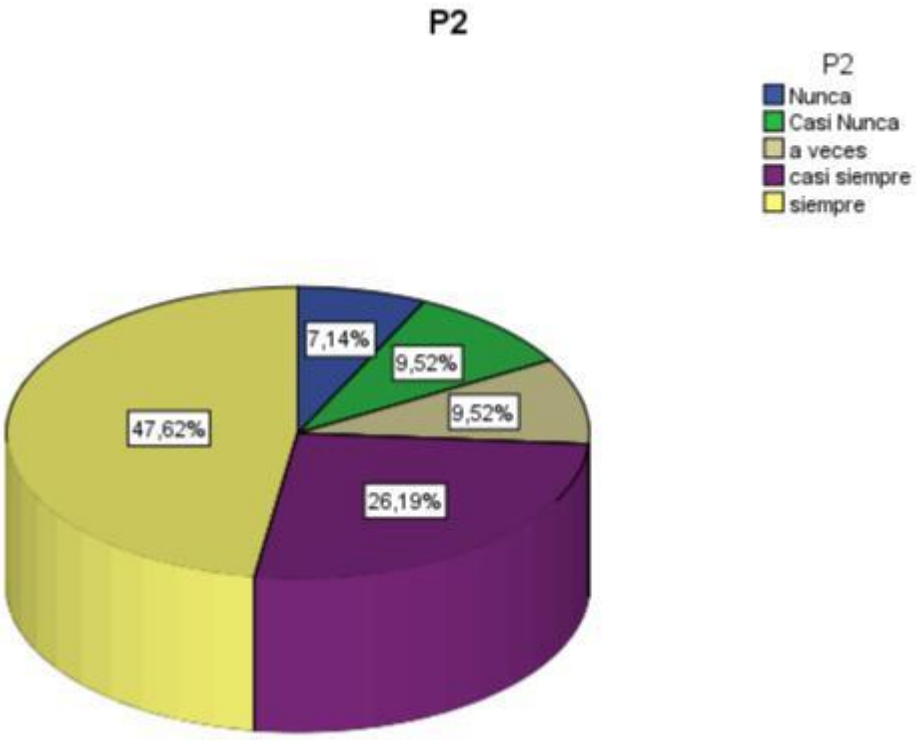


Figura 2. *Posibilidades – Sistemas VSAT*

Descripción: En cuanto a si cree usted que las posibilidades de empleo de la Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 26,2%; manifestaron que muy poco un 9,5%; un 9,5% dijeron que casi nada; y, un 7,1% manifestaron que nunca.

3. ¿Cree usted que las características de empleo de la Guerra Cibernética se relacionan con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

Tabla 3. *Características – Medios de Campaña*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	2	4,8	4,8	4,8
	Casi Nunca	2	4,8	4,8	9,5
	A veces	1	2,4	2,4	11,9
	Casi Siempre	17	40,5	40,5	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

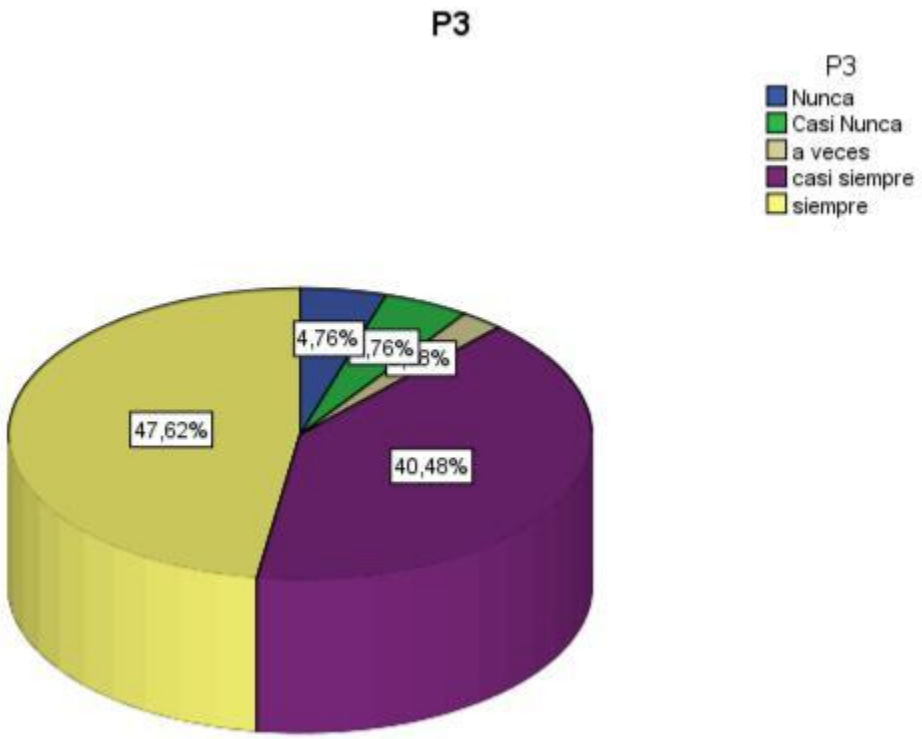


Figura 3. *Características – Medios de Campaña*

Descripción: En cuanto a si Cree usted que las características de empleo de la Guerra Cibernética se relacionan con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 40,5%; manifestaron que muy poco un 2,4%; un 4,8% dijeron que casi nada; y, un 4,8% manifestaron que nunca.

4. ¿Cree usted que las posibilidades de empleo de la Guerra Cibernética se relacionan con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

Tabla 4. *Posibilidades – Medios de Campaña*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	2	4,8	4,8	4,8
	Casi Nunca	2	4,8	4,8	9,5
	A veces	3	7,1	7,1	16,7
	Casi Siempre	15	35,7	35,7	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

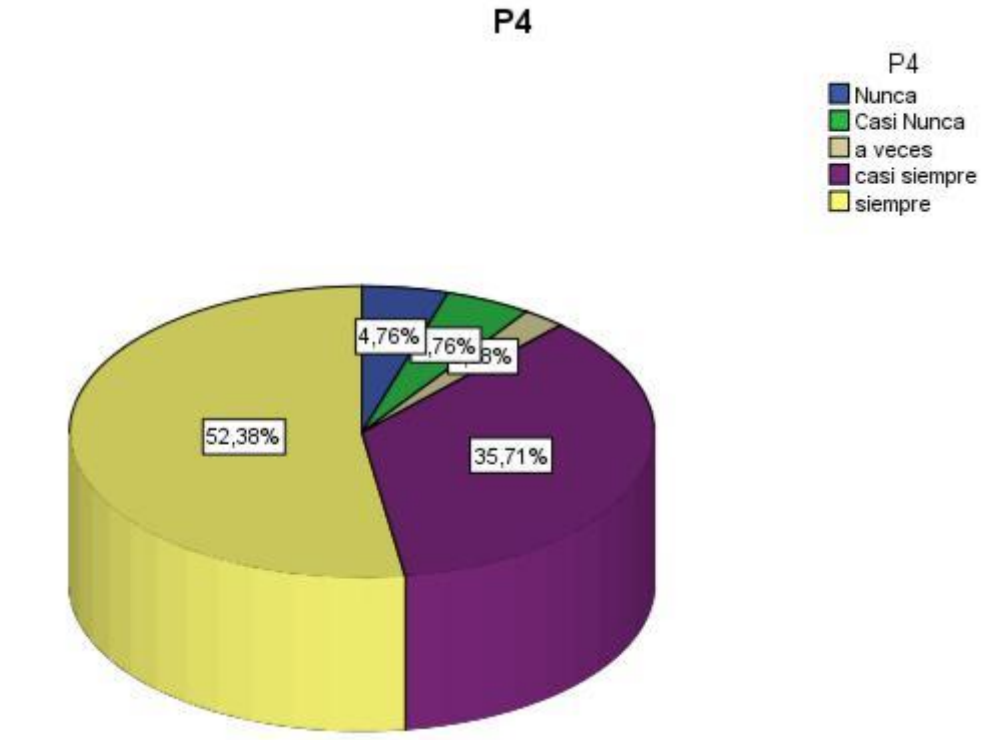


Figura 4. *Posibilidades – Medios de Campaña*

Descripción: En cuanto a si cree usted que las posibilidades de empleo de la Guerra Cibernética se relacionan con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 35,7%; manifestaron que muy poco un 7,1%; un 4,8% dijeron que casi nada; y, un 4,8% manifestaron que nunca.

5. ¿Considera usted que la Visión Sistemática de la Estructura y Responsabilidades de la Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

Tabla 5. *Visión Sistemática – Sistemas VSAT*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	1	2,4	2,4	2,4
	Casi Nunca	3	7,1	7,1	9,5
	A veces	1	2,4	2,4	11,9
	Casi Siempre	18	42,9	42,9	54,8
	Siempre	19	45,2	45,2	100,0
	Total	42	100,0	100,0	

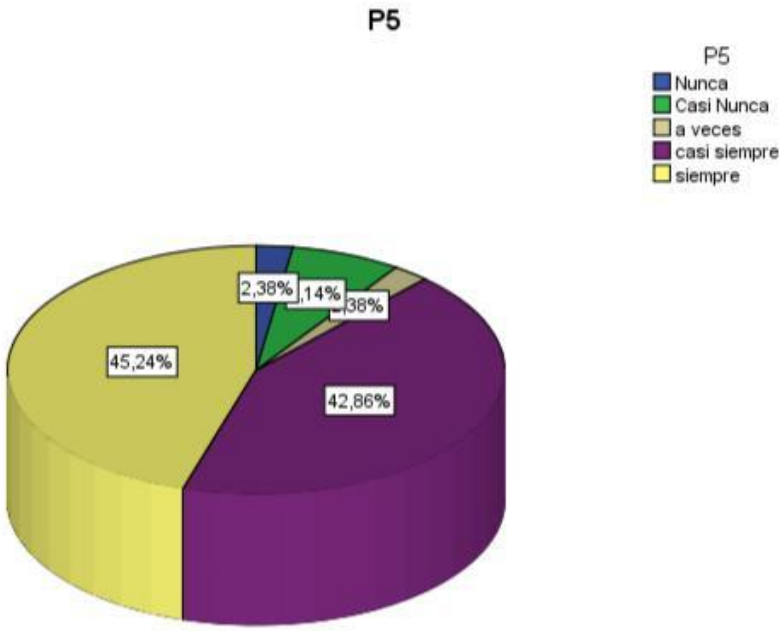


Figura 5. *Visión Sistemática – Sistemas VSAT*

Descripción: En cuanto a si considera usted que la Visión Sistemática de la Estructura y Responsabilidades de la Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”; manifestaron que totalmente un 45,2%; así mismo dijeron que solo en parte un 42,9%; manifestaron que muy poco un 2,4%; un 7,1% dijeron que casi nada; y, un 2,4% manifestaron que nunca.

6. ¿Considera usted que las Capacidades del Sistema de Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH "CFB"? Tabla 6. *Capacidades del Sistema – Sistemas VSAT*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	1	2,4	2,4	2,4
	Casi Nunca	2	4,8	4,8	7,1
	A veces	4	9,5	9,5	16,7
	Casi Siempre	15	35,7	35,7	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

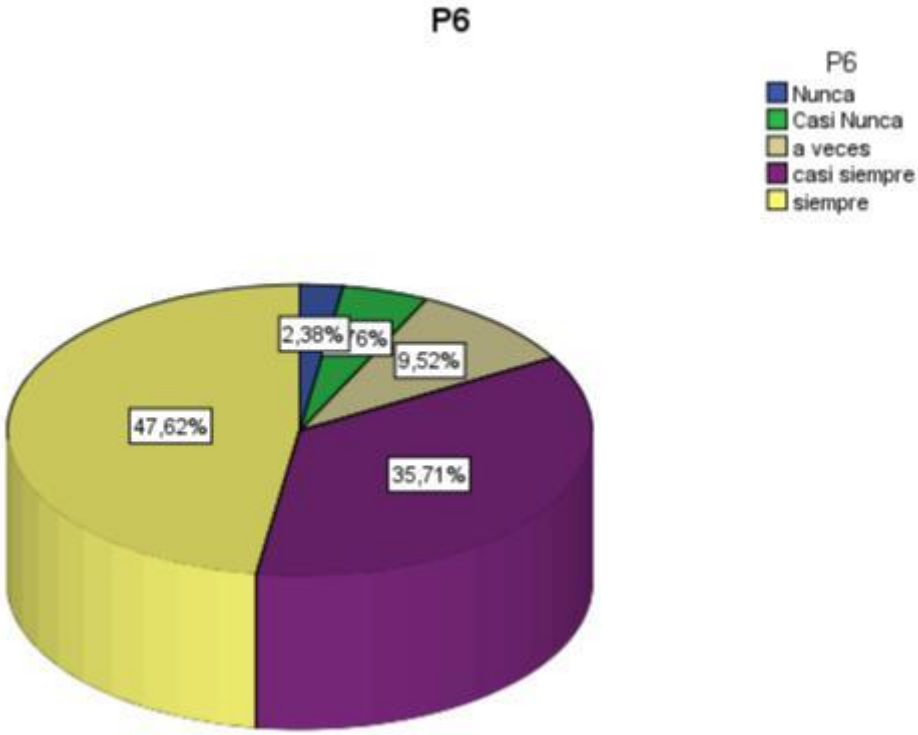


Figura 6. *Capacidades del Sistema – Sistemas VSAT*

Descripción: En cuanto a si considera usted que las Capacidades del Sistema de Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH "CFB"; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 35,7%; manifestaron que muy poco un 9,5%; un 4,8% dijeron que casi nada; y, un 2,4% manifestaron que nunca.

7. ¿Considera usted que la Visión Sistemática de la Estructura y Responsabilidades de la Guerra Cibernética se relacionan con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

Tabla 7. *Visión Sistemática – Medios de Campaña*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	2	4,8	4,8	4,8
	Casi Nada	2	4,8	4,8	9,5
	Muy Poco	6	14,3	14,3	23,8
	Solo en parte	12	28,6	28,6	52,4
	Totalmente	20	47,6	47,6	100,0
	Total	62	100,0	100,0	

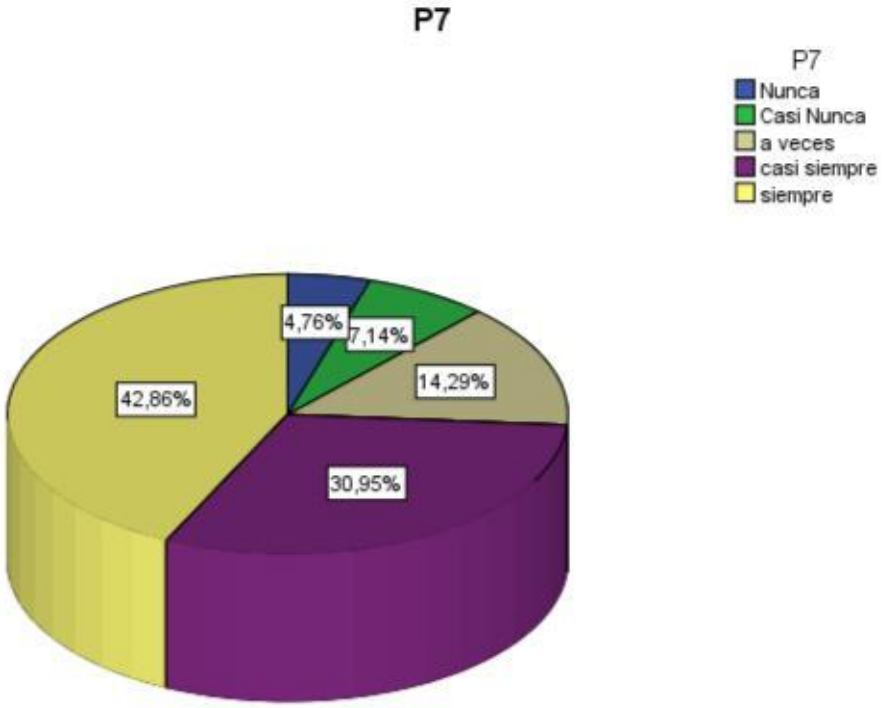


Figura 7. *Visión Sistemática – Medios de Campaña*

Descripción: En cuanto a si Considera usted que la Visión Sistemática de la Estructura y Responsabilidades de la Guerra Cibernética se relacionan con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 28,6%; manifestaron que muy poco un 14,3%; un 4,8% dijeron que casi nada; y, un 4,8% manifestaron que nunca.

8. ¿Considera usted que las Capacidades del Sistema de Guerra Cibernética se relacionan con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

Tabla 8. *Capacidades del Sistema – Medios de Campaña*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	1	2,4	2,4	2,4
	Casi Nunca	3	7,1	7,1	9,5
	A veces	1	2,4	2,4	11,9
	Casi Siempre	17	40,5	40,5	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

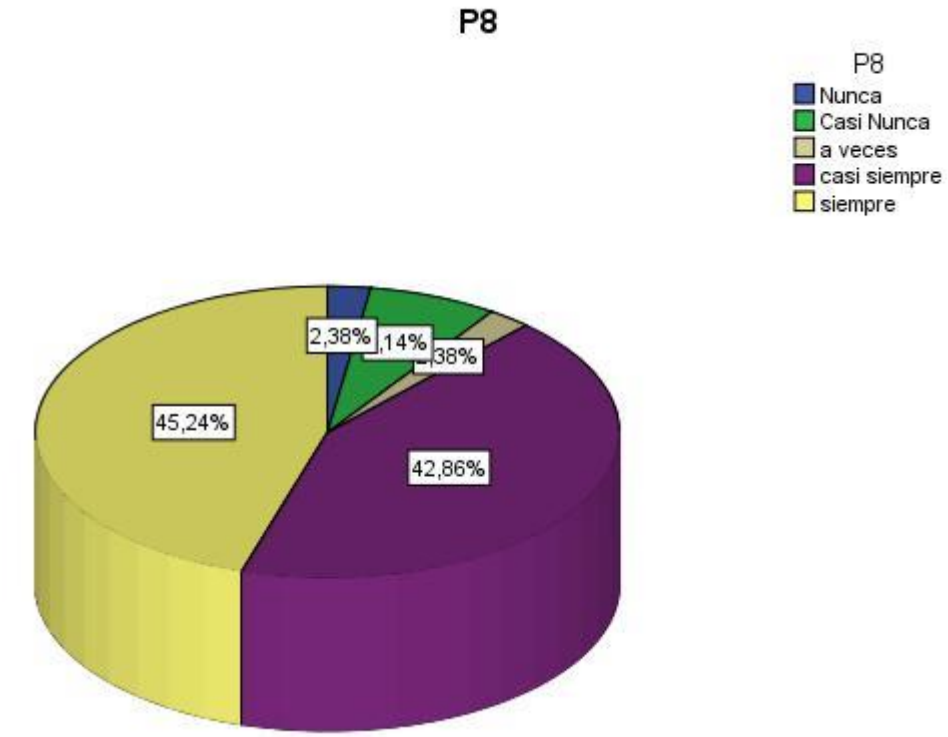


Figura 8. *Capacidades del Sistema – Medios de Campaña*

Descripción: En cuanto a si considera usted que las Capacidades del Sistema de Guerra Cibernética se relacionan con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 40,5%; manifestaron que muy poco un 2,4%; un 7,1% dijeron que casi nada; y, un 2,4% manifestaron que nunca.

9. ¿Cree usted que la aplicación de las operaciones ofensivas de la Guerra Cibernética se relaciona con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

Tabla 9. *Operaciones Ofensivas – Sistemas VSAT*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	2	4,8	4,8	4,8
	Casi Nunca	2	4,8	4,8	9,5
	A veces	1	2,4	2,4	11,9
	Casi Siempre	17	40,5	40,5	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

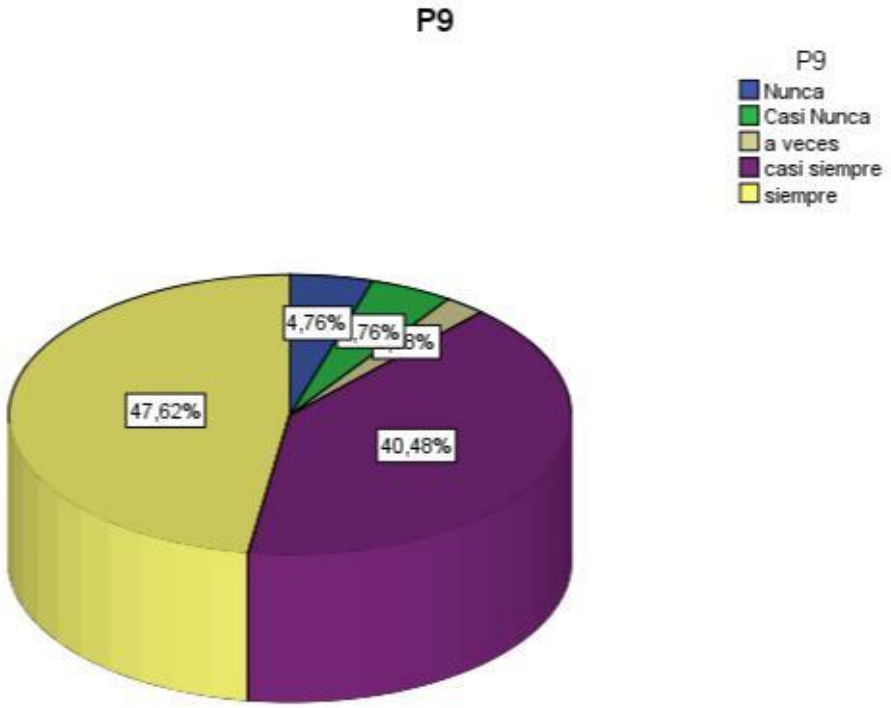


Figura 9. *Operaciones Ofensivas – Sistemas VSAT*

Descripción: En cuanto a si Cree usted que la aplicación de las operaciones ofensivas de la Guerra Cibernética se relaciona con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 40,5%; manifestaron que muy poco un 2,4%; un 4,8% dijeron que casi nada; y, un 4,8% manifestaron que nunca.

10. ¿Cree usted que la aplicación de las operaciones defensivas de la Guerra Cibernética se relaciona con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

Tabla 10. *Operaciones Defensivas – Sistemas VSAT*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	1	2,4	2,4	2,4
	Casi Nunca	2	4,8	4,8	7,1
	A veces	6	14,3	14,3	21,4
	Casi Siempre	13	31,0	31,0	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

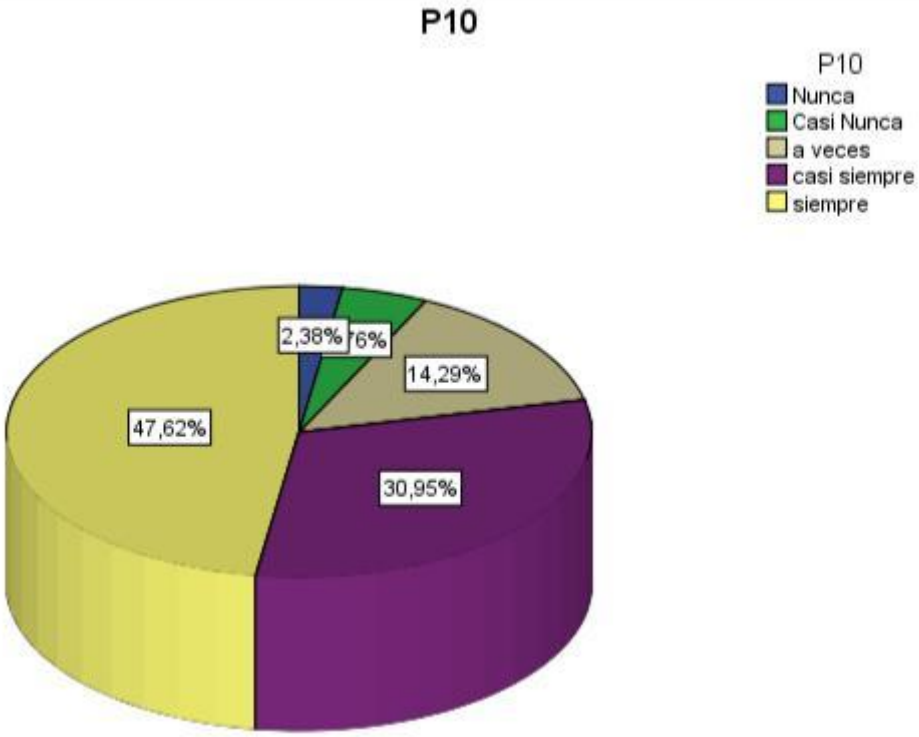


Figura 10. *Operaciones Defensivas – Sistemas VSAT*

Descripción: En cuanto a si Cree usted que la aplicación de las operaciones defensivas de la Guerra Cibernética se relaciona con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 31%; manifestaron que muy poco un 14,3%; un 4,8% dijeron que casi nada; y, un 2,4% manifestaron que nunca.

11. ¿Cree usted que la aplicación de las operaciones ofensivas de la Guerra Cibernética se relaciona con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

Tabla 11. *Operaciones Ofensivas - Medios de Campaña*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	2	4,8	4,8	4,8
	Casi Nunca	1	2,4	2,4	7,1
	A veces	4	9,5	9,5	16,7
	Casi Siempre	15	35,7	35,7	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

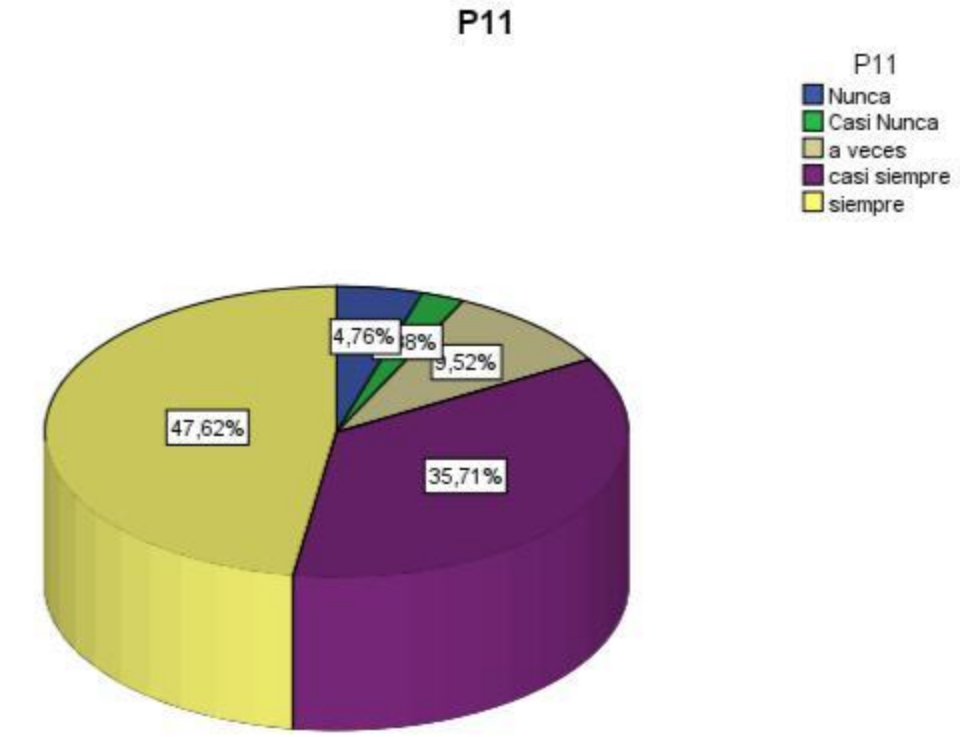


Figura 11. *Operaciones Ofensivas - Medios de Campaña*

Descripción: En cuanto a si cree usted que la aplicación de las operaciones ofensivas de la Guerra Cibernética se relaciona con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 35,7%; manifestaron que muy poco un 9,5%; un 2,4% dijeron que casi nada; y, un 4,8% manifestaron que nunca.

12. ¿Cree usted que la aplicación de las operaciones defensivas de la Guerra Cibernética se relaciona con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

Tabla 12. *Operaciones Defensivas – Medios de Campaña*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	2	4,8	4,8	4,8
	Casi Nunca	1	2,4	2,4	7,1
	A veces	6	14,3	14,3	21,4
	Casi Siempre	13	31,0	31,0	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

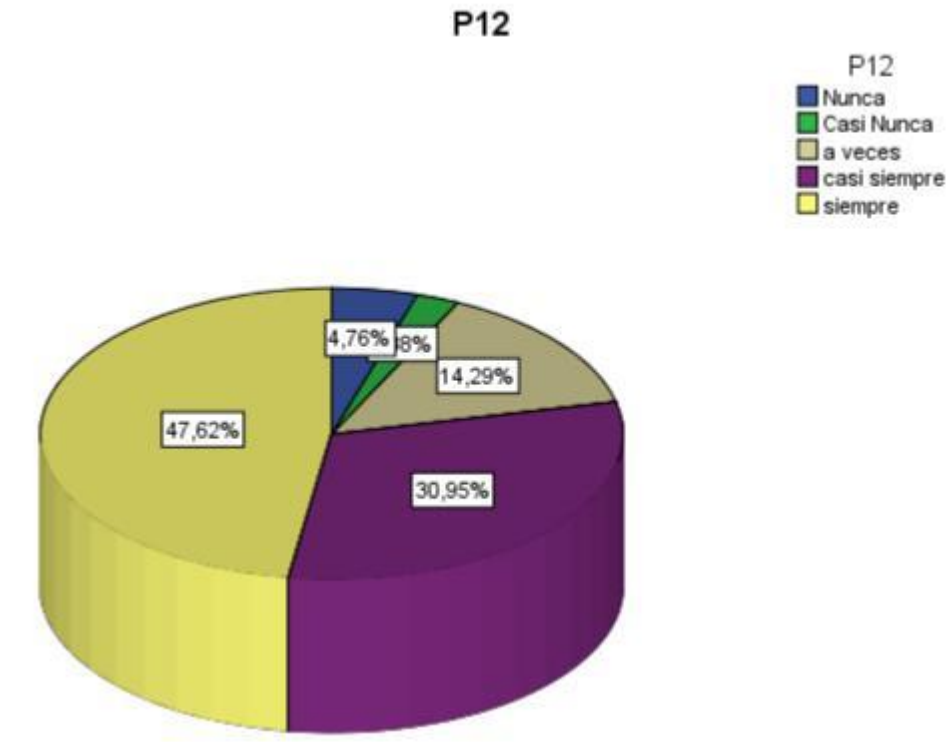


Figura 12. *Operaciones Defensivas – Medios de Campaña*

Descripción: En cuanto a si cree usted que la aplicación de las operaciones defensivas de la Guerra Cibernética se relaciona con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 31%; manifestaron que muy poco un 14,3%; un 2,4% dijeron que casi nada; y, un 4,8% manifestaron que nunca.

Para la variable dependiente: FORMACIÓN ACADÉMICA ESPECIALIZADA

Empleo de las Comunicaciones para todas las armas

13. ¿Considera usted que, atendiendo a la Formación Especializada, el Empleo de las Comunicaciones para todas las Armas es influido por la asignatura de Guerra Cibernética?

Tabla 13. *Empleo de las Comunicaciones – Guerra Cibernética*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	1	2,4	2,4	2,4
	Casi Nunca	3	7,1	7,1	9,5
	A veces	1	2,4	2,4	11,9
	Casi Siempre	17	40,5	40,5	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

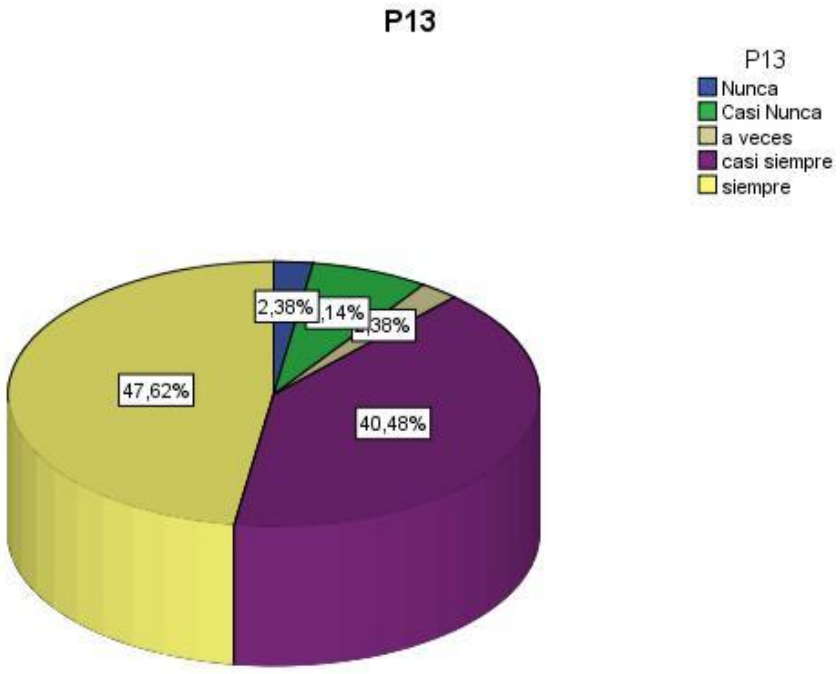


Figura 13. *Empleo de las Comunicaciones – Guerra Cibernética*

Descripción: En cuanto a si considera usted que, atendiendo a la formación especializada, el empleo de las comunicaciones para todas las armas es influido por la asignatura de Guerra Cibernética; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 40,5%; manifestaron que muy poco un 2,4%; un 7,1% dijeron que casi nada; y, un 2,4% manifestaron que nunca.

Sistema de Comunicaciones Satelital VSAT

14. ¿Considera usted que, atendiendo a la Formación Especializada, el Sistema de Comunicaciones Satelital VSAT es influido por la asignatura de Guerra Cibernética?

Tabla 14. *Sistema VSAT – Guerra Cibernética*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	1	2,4	2,4	2,4
	Casi Nunca	3	7,1	7,1	9,5
	A veces	1	2,4	2,4	11,9
	Casi Siempre	17	40,5	40,5	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

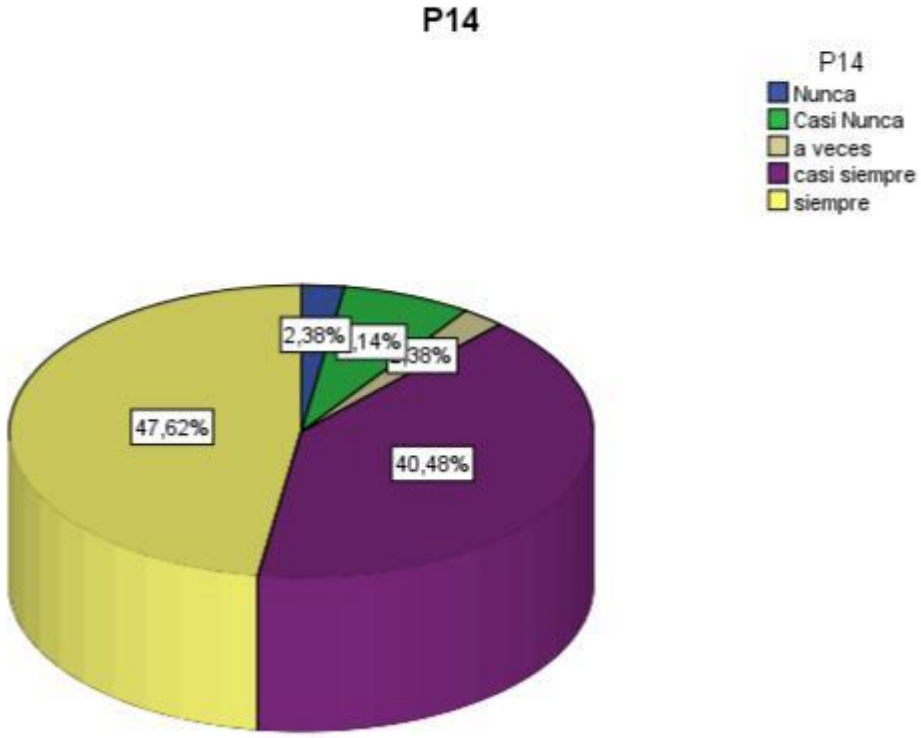


Figura 14. *Sistema VSAT – Guerra Cibernética*

Descripción: En cuanto a si considera usted que, atendiendo a la formación especializada, el Sistema de Comunicaciones Satelital VSAT es influido por la asignatura de Guerra Cibernética; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 40,5%; manifestaron que muy poco un 2,4%; un 7,1% dijeron que casi nada; y, un 2,4% manifestaron que nunca.

Medios de Comunicación en Campaña

15. ¿Considera usted que, atendiendo a la Formación Especializada, los Medios de Comunicación en Campaña son influidos por la asignatura de Guerra Cibernética?

Tabla 15. *Medios de Campaña – Guerra Cibernética*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	3	7,1	7,1	7,1
	Casi Nunca	1	2,4	2,4	9,5
	A veces	2	4,8	4,8	14,3
	Casi Siempre	16	38,1	38,1	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

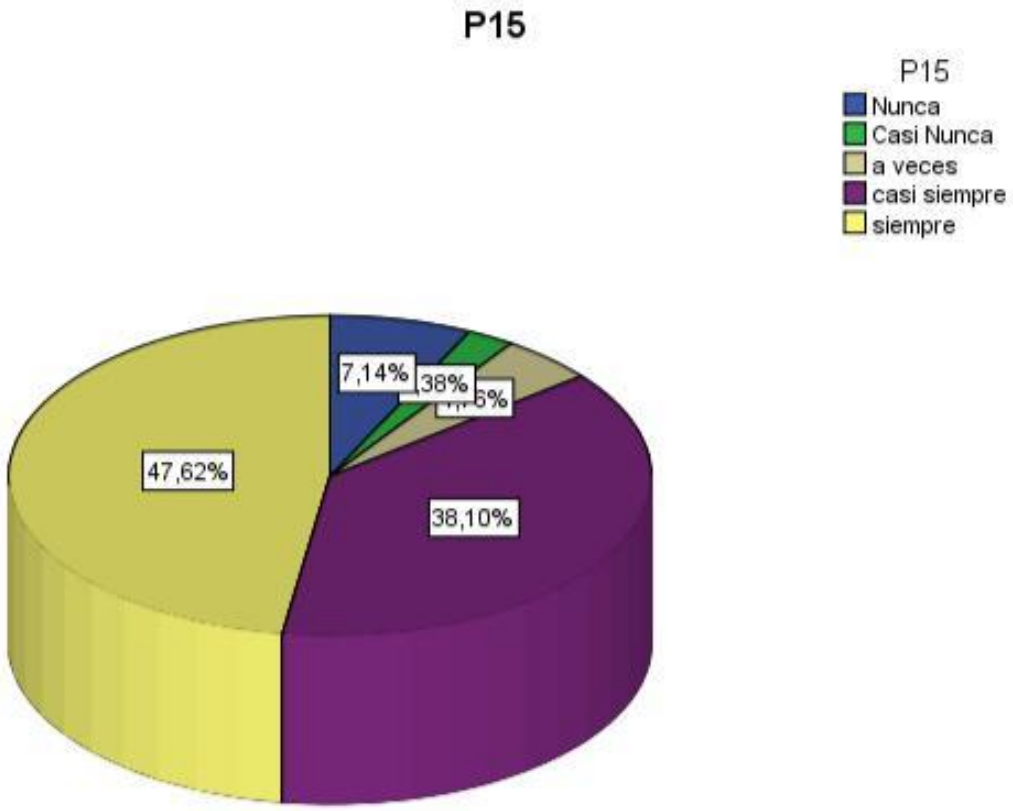


Figura 15. *Medios de Campaña – Guerra Cibernética*

Descripción: En cuanto a si considera usted que, atendiendo a la formación especializada, los medios de comunicación en campaña son influidos por la asignatura de Guerra Cibernética; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 38,1%; manifestaron que muy poco un 4,8%; un 2,4% dijeron que casi nada; y, un 7,1% manifestaron que nunca.

Fundamentos de Comando y Control

16. ¿Considera usted que, atendiendo a la Formación Especializada, los Fundamentos de Comando y Control son influidos por la asignatura de Guerra Cibernética?

Tabla 16. *Fundamentos de Comando y Control – Guerra Cibernética*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	1	2,4	2,4	2,4
	Casi Nunca	3	7,1	7,1	9,5
	A veces	3	7,1	7,1	16,7
	Casi Siempre	15	35,7	35,7	52,4
	Siempre	20	47,6	47,6	100,0
	Total	42	100,0	100,0	

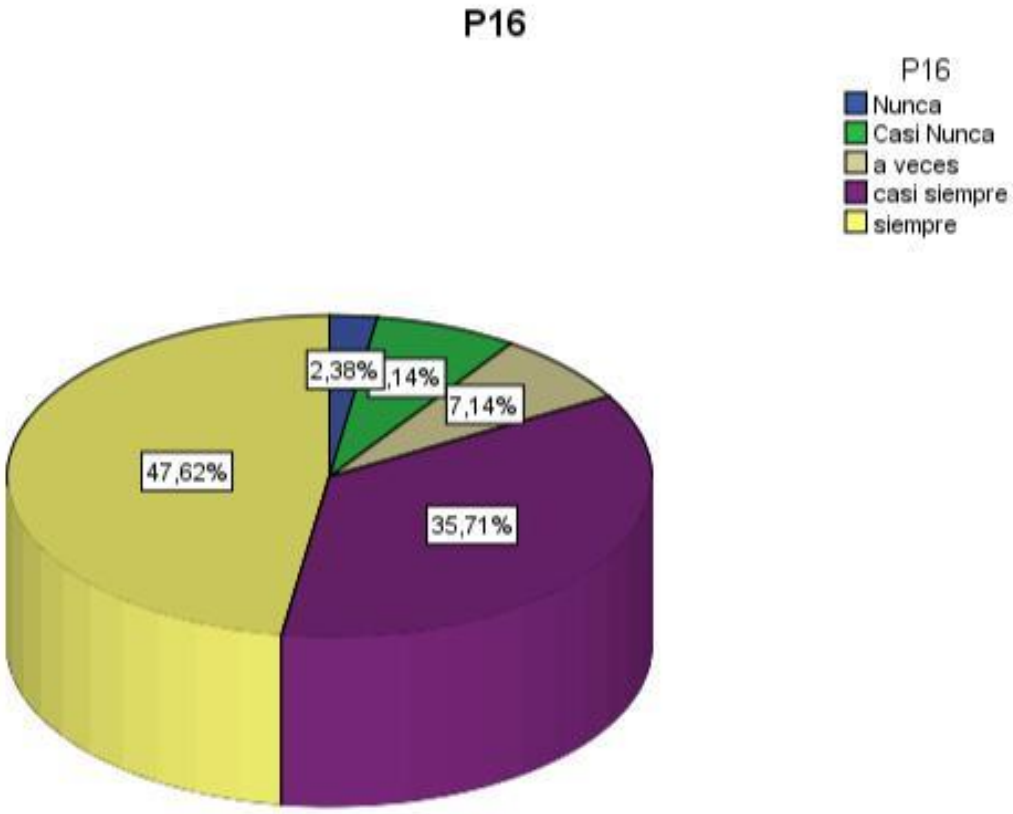


Figura 16. *Fundamentos de Comando y Control – Guerra Cibernética*

Descripción: En cuanto a si considera usted que, atendiendo a la formación especializada, los fundamentos de comando y control son influidos por la asignatura de Guerra Cibernética; manifestaron que totalmente un 47,6%; así mismo dijeron que solo en parte un 35,7%; manifestaron que muy poco un 7,1%; un 7,1% dijeron que casi nada; y, un 2,4% manifestaron que nunca.

4.2 Interpretación

Tabla 17. *Resumen de procesamiento de casos*

	N	%
Casos Válido	42	100,0
Excluido[a]	0	,0
Total	42	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Tabla 18. *Estadísticas de fiabilidad*

Alfa de Cronbach	N de elementos
,996	16

Tabla 19. *ANOVA con prueba de Cochran*

		Suma de cuadrados	gl	Media cuadrática	Q de Cochran	Sig
Inter sujetos		12,560	18	4,909		
Intra sujetos	Entre elementos	,184	16	,116	1,841	,201
	Residuo	1,600	1764	,097		
	Total	5,784	1800	,098		
Total		19,344	1849	,755		

Media global = 3,51

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

4.2.1 PRUEBA DE HIPÓTESIS GENERAL

La asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

De los instrumentos de medición:

A su opinión ¿La asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

- Se relaciona.
- No se relaciona.

Cálculo de la CHI Cuadrada:

Tabla 20. *Pruebas de chi-cuadrado – hipótesis general*

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	580,313[a]	561	,358
Razón de verosimilitud	311,957	561	1,000
Asociación lineal por lineal	35,936	1	,000
N de casos válidos	42		

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: 0.358

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

Conclusión para la hipótesis General:

El valor calculado para la Chi cuadrada (0.358) 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 asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

4.2.2 PRUEBA DE HIPÓTESIS ESPECÍFICA 1

Los Fundamentos de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

De los instrumentos de medición:

A su opinión ¿Los Fundamentos de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

- Se relaciona.
- No se relaciona.

Cálculo de la CHI Cuadrada:

Tabla 21. *Pruebas de chi-cuadrado – hipótesis especifica 1*

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	43,500[a]	357	,198
Razón de verosimilitud	24,133	357	1,000
Asociación lineal por lineal	4,745	1	,000
N de casos válidos	42		

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 general nula y se acepta la hipótesis especifica 1 alterna.

Esto quiere decir que los Fundamentos de la asignatura de Guerra Cibernética se relacionan significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

4.2.3 PRUEBA DE HIPÓTESIS ESPECÍFICA 2

La Estructura y Responsabilidades de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

De los instrumentos de medición:

A su opinión ¿La Estructura y Responsabilidades de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

- Se relaciona.
- No se relaciona.

Cálculo de la CHI Cuadrada:

Tabla 22. *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	42		

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 general nula y se acepta la hipótesis especifica 2 alterna.

Esto quiere decir que la Estructura y Responsabilidades de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

4.2.4 PRUEBA DE HIPÓTESIS ESPECÍFICA 3

La Aplicación en Operaciones Terrestres de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

De los instrumentos de medición:

A su opinión ¿La Aplicación en Operaciones Terrestres de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

- Se relaciona.
- No se relaciona.

Cálculo de la CHI Cuadrada:

Tabla 23. *Pruebas de chi-cuadrado – hipótesis especifica 3*

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	38,925[a]	340	,315
Razón de verosimilitud	37,041	340	1,000
Asociación lineal por lineal	3,513	1	,000
N de casos válidos	42		

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: 0.315

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

Conclusión para la hipótesis específica 3:

El valor calculado para la Chi cuadrada (0.315) 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 especifica 3 alterna.

Esto quiere decir que la Aplicación en Operaciones Terrestres de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

4.3. Discusión

4.3.1. Hipótesis General

De acuerdo con los resultados obtenidos en la prueba estadística de Person para la hipótesis que han orientado la investigación se ha podido observar que en cuanto a la Hipótesis General si existen relaciones significativas entre la Guerra Cibernética y la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”; hallándose que el valor calculado para la Chi cuadrada (0.358) 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.

Y estos resultados coinciden con la tesis de Suarez, M. (2015). Tesis para optar el Título Profesional de Abogado: *“La Ciberguerra y la aplicación de los Principios del Derecho Internacional Humanitario”*. Universidad San Martin de Porres. Lima. Perú; cuyas conclusiones son las siguientes:

a. Los ataques informáticos son regulados a nivel interno siempre y cuando no se desarrollen dentro de un conflicto armado.

b. Los ataques dentro de la ciberguerra deben ser dirigidos a la infraestructura estatal y debe generar un daño determinable.

c. Los principios del Derecho Internacional Humanitario o Derecho Internacional de los Conflictos Armados muchas veces son vulnerados por los ciberataques, ya que sus efectos pueden ocasionar daños colaterales y males superfluos.

d. Al no existir normativa internacional que regule específicamente los ataques cibernéticos dentro de un conflicto armado, es necesario

que cada uno de los Estados realicen un análisis jurídico para determinar la licitud o ilicitud de los ataques cibernéticos: esto es conforme al artículo 36 del Protocolo Adicional I.

e. En el Perú, la normativa cibernética se encuentra en constante evolución.

4.3.2. Hipótesis Especifica 1

De acuerdo con los resultados obtenidos en la prueba estadística de Person para la hipótesis que han orientado la investigación se ha podido observar que en cuanto a la Hipótesis Especifica 1 si existen relaciones significativas entre los Fundamentos de la asignatura de Guerra Cibernética y la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"; hallándose que 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 general nula y se acepta la hipótesis especifica 1 alterna.

Y estos resultados coinciden con la tesis de Febres, J. – Libuy, D. & Tapia, P. (2014). En su tesis para optar al Título Profesional de Ingeniero Comercial mención Administración, titulada: *"Análisis del uso de las Tecnologías de la Información y la Comunicación en los establecimientos educacionales de Chile: Caso del Colegio Santo Tomás de la Comuna de Ñuñoa".* Universidad de Chile. Santiago de Chile. Chile; cuyas conclusiones son las siguientes:

- La instalación de hardware no es suficiente, más necesaria, para establecer un uso de TICs como tal. Los investigadores de este trabajo consideran que se deben dar muchos pasos más para que la TIC sea un real apoyo en el proceso de aprendizaje de los estudiantes, partiendo por el hardware, después por un software adecuado, una

capacitación hacia un encargado, una segunda capacitación a docentes, para dar paso finalmente a una entrega final hacia los alumnos.

- El uso de TIC no es lo mismo que usar TICs dedicadas a la educación. Si bien el uso de las primeras permite facilitar el flujo de información de esfera a esfera, estas no son capaces por sí mismas de ser instrumentos de aprendizaje efectivo en la esfera de estudiantes.

- Los mecanismos de medición de impacto son escasos y no permiten establecer un cambio de paradigma con respecto a los TICs. Hoy en día las pocas (sino las únicas) herramientas de medición son los resultados que los mismos establecimientos exigen, estos radican en aumentos de los puntajes SIMCE y PSU, particularmente.

- Las TICs dedicadas a la educación deben entregar más que un reforzamiento de las áreas que los colegios ya estudian, pudiendo entregar un valor agregado tal y como lo hacen dos TICs chilenas dedicadas citadas en este trabajo.

- La reforma plantea la creación de zonas o regiones educacionales, en base a esto los investigadores creen que se debería reforzar el uso de TICs en establecimientos de zonas aledañas con el objetivo de compartir los métodos que puedan ser replicados por otros.

4.3.3. Hipótesis Específica 2

De acuerdo con los resultados obtenidos en la prueba estadística de Person para la hipótesis que han orientado la investigación se ha podido observar que en cuanto a la Hipótesis Especifica 2 si existen relaciones significativas entre la Estructura y Responsabilidades de la asignatura de Guerra Cibernética y la Formación Académica Especializada de los cadete de Comunicaciones de la Escuela Militar

de Chorrillos “Coronel Francisco Bolognesi”; hallándose 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 general nula y se acepta la hipótesis especifica 2 alterna.

Y estos resultados coinciden con la tesis de Díaz del Rio, J. (2010). En su artículo titulado: *“La Ciberseguridad en el Ámbito Militar”*. Ministerio de Defensa. España; cuyas conclusiones son las siguientes:

a. Las tecnologías de la información hacen posible casi todo lo que nuestras FAS necesitan: apoyo logístico, mando y control de sus fuerzas, información de inteligencia en tiempo real y un largo etcétera.

b. Los ataques cibernéticos ya no solamente tienen motivación intelectual económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus fuerzas, además de en las dimensiones de tierra, mar y aire, a través del ciberespacio.

c. La amenaza a las tecnologías de la información nunca ha sido mayor y los usuarios necesitan y demandan seguridad como nunca antes había ocurrido.

d. En el ámbito de las operaciones militares, los ciberataques también tienen que ser considerados como una amenaza.

e. La ciberguerra es asimétrica.

f. Los sistemas en red no son los únicos susceptibles de presentar vulnerabilidades y ser atacados.

g. Ejércitos de diversos países han reconocido formalmente al ciberespacio como un nuevo dominio de enfrentamiento («Global Commons»).

h. La convergencia a NEC exigirá una mayor interconexión con otros sistemas (Federación de Redes), incluso con ONGs, lo que exigirá un considerable esfuerzo en seguridad de la información.

i. A nivel nacional, el Ministerio de Defensa ha llevado a cabo numerosas iniciativas, publicando la Política de Seguridad de la Información, sus normas de aplicación y tomando un buen número de medidas para incrementar la seguridad de su información, tanto en el ámbito.

4.3.4. Hipótesis Específica 3

De acuerdo con los resultados obtenidos en la prueba estadística de Person para la hipótesis que han orientado la investigación se ha podido observar que en cuanto a la Hipótesis Especifica 3 si existen relaciones significativas entre la Aplicación en Operaciones Terrestres de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada de los cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”; hallándose el valor calculado para la Chi cuadrada (0.315) 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 especifica 3 alterna.

Y estos resultados coinciden con la tesis de Espinosa, J. (2012). En su tesis titulada: *“Guerra Cibernética: Un problema estratégico con envolvimiento de las Fuerzas Armadas”*. Escuela Superior de Guerra. Rio de Janeiro. Brasil; cuyas conclusiones son las siguientes:

a. La generación X que está envejeciendo y la nueva generación Y tendrán que vivir con este nuevo deber cívico, y van a tener que buscar la forma de protección general en el camino de la información (information highway).

b. El futuro de las economías está en juego.

c. El papel de los militares será mejor definido con el paso del tiempo, en la forma en que se define el ciberespacio.

d. Tal vez el viejo Verde (Ejército), Blanco (Marina de Guerra) y Azul (Fuerza Aérea) no sean las respuestas más correctas a la Ciberdefesa.

e. Tal vez la "fuerza gris (Ciber)", debe ser la responsable de defender economías y países.

f. Si los Estados o naciones optan por el contraataque a los ciberataques, como han hecho hasta ahora, el camino hacia el éxito va a ser de largo.

CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Después de hallar en la Hipótesis General que el valor calculado para la Chi cuadrada (0.358) es mayor que el valor que aparece en la tabla (0.05) para un nivel de confianza de 95% y un grado de libertad. Se llegó a la conclusión de que la ausencia de la asignatura de Guerra Cibernética en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, no contribuye positivamente a la Formación Académica Especializada ni a interiorizar en los cadetes de Comunicaciones la doctrina respectiva. Tomando en consideración que la Ciberguerra se refiere al desplazamiento de un conflicto, en principio de carácter bélico, que toma el ciberespacio y las tecnologías de la información como escenario principal, para producir alteraciones en datos y sistemas del enemigo, a la vez que se protege la información y sistemas del atacante; aspectos que como militares y de la especialidad de Comunicaciones debemos manejar con la destreza que proporciona su conocimiento contribuyendo directamente a nuestra Formación Militar.

2. Después de hallar en la Hipótesis Específica 1 que 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. Se llegó a la conclusión de que la falta de conocimiento de los fundamentos de la asignatura de Guerra Cibernética no nos proporciona los elementos necesarios para poder aplicar sus especificaciones; aprovechar las características, posibilidades en provecho de nuestra Formación Académica Especializada.

3. Después de hallar en la Hipótesis Específica 2 que 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. Se llegó a la conclusión de que la falta de conocimiento de la estructura y responsabilidades de la asignatura de Guerra Cibernética, no nos

proporciona una visión sistemática del ciberespacio y potenciar las capacidades de los Cadetes del arma de Comunicaciones de la EMCH “CFB”. El conocimiento del ciberespacio nos permitirá potenciar nuestra Formación Académica Especializada y aplicar los conocimientos impartidos mediante la materialización de lo que se aprendería en la asignatura de Guerra Cibernética.

4. Después de hallar en la Hipótesis Específica 2 que el valor calculado para la Chi cuadrada (0.315) es mayor que el valor que aparece en la tabla (0.05) para un nivel de confianza de 95% y un grado de libertad. Se llegó a la conclusión de que la falta de conocimiento sobre la aplicación de la asignatura de Guerra Cibernética en las operaciones terrestres no nos proporciona los elementos necesarios para poder aplicar sus especificaciones; potenciar la ejecución de las operaciones ofensivas y defensivas en provecho de nuestra Formación Académica Especializada.

RECOMENDACIONES

Como recomendación y tomando en consideración es el ciberespacio se está convirtiendo en un nuevo escenario de conflicto, debemos:

1. Solicitar se gestione convenios con el Ejército de Brasil, a fin de que se capacite a instructores que puedan generar doctrina para nuestro Ejército, que vaya acorde específicamente con nuestra realidad, posibilidades y limitaciones.

2. Solicitar que una vez se cuente con oficiales capacitados en Guerra Cibernética, se proceda a dictar la asignatura en la Escuela Militar de Chorrillos Coronel Francisco Bolognesi.

3. Es necesario que a nivel Escuela Militar de Chorrillos se solicite la participación de oficiales especialistas en Guerra Electrónica de la ECOM, a fin de generar y potenciar prácticas de Guerra Cibernética haciendo uso del internet en la Escuela Militar, en provecho de nuestra Formación Académica Especializada.

4. Por último, debemos tener en cuenta que la ciberguerra no pertenece a la ciencia ficción, sino que es un hecho que se puede hacer realidad en cualquier instante, aunque de momento no se haya producido ningún ataque de este tipo en una infraestructura vital; es por ello que debemos brindarle la importancia que requiere para nuestra Formación Académica Especializada, que está orientada a nuestro futuro como oficiales del arma de Comunicaciones.

REFERENCIAS BIBLIOGRÁFICAS

- Díaz del Rio (2010). En su artículo titulado: *"La Ciberseguridad en el Ámbito Militar"*.
  Ministerio de Defensa. España.

- Espinosa (2012). En su tesis titulada: *"Guerra Cibernética: Un problema estratégico*
  con envolvimiento de las Fuerzas Armadas". Escuela Superior de Guerra. Rio de Janeiro. Brasil

- KUEHL (2009). *From Cyberspace to Cyberpower: Defining the Problem, Information*
  Resources Management. Estados Unidos. College-National Defense University.

- Maness & Valeriano (2012). Persistent Enemies and Cyberwar: *Rivalry Relations in an*
  Age of Information Warfare. En: D. Reveron. Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World (pp. 139 – 157) Washington, Estados Unidos: Georgetown University Press.

- Manual de Campanha EB70-MC-10.232 Guerra Cibernética, 1ª Edição, 2017

- Pantano (2014). En su artículo titulado: *"Ciberguerra".* Universidad de Palermo-Argentina

- Ruef, A., Shakarian, J. & Shakarian, J. (2013). *"Introduction to Cyber-Warfare: A*
  multidisciplinary approach!". Massachusetts, Estados Unidos: Elsevier.

- Sain (2016). En su artículo titulado: *"¿Qué es la Ciberguerra?".* Revista Pensamiento

Penal. Argentina

- Sánchez (2009). En su artículo publicado en la Revista Política y Estrategia N° 114:
  "Internet: Una Herramienta Para Las Guerras En El Siglo XXI". Academia Nacional de Estudios Políticos y Estratégicos. Madrid. España

- Sánchez, H. y Reyes, C. (2006). *"Metodología y diseño de investigación científica".*
  Lima. Universitaria.

- Schreier (2012). *On Cyberwar*. Ginebra, Suiza: DCAF.

- Shakarian (2011, Abril). Stuxnet: *Cyberwar Revolution in Military Affairs*. En: Air &
  Space Power Journal, pp. 50 – 59.

- Suarez (2015). Tesis para optar el Título Profesional de Abogado: *"La Ciberguerra y*
  la aplicación de los Principios del Derecho Internacional Humanitario".
  Universidad San Martin de Porres. Lima. Perú

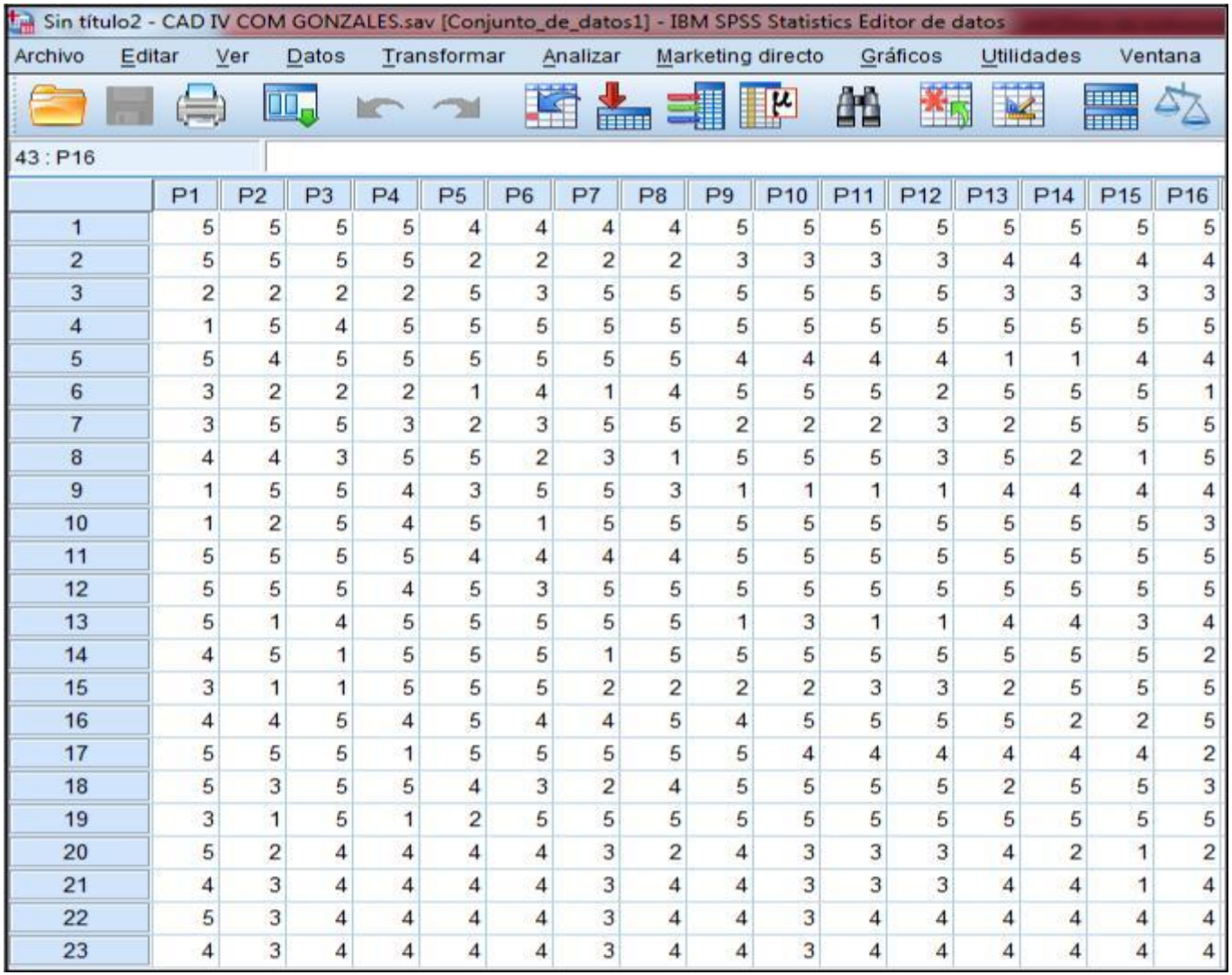
- Taylor, F. y Carter, J. (2010). *"Cyberspace Superiority Considerations. Conflict and*
  Cooperation in Cyberspace: The Challenge to National Security in Cyberspace". Editores: Yannakogeorgos, Panayotis; y Lowther, Adam
  Taylor y Francis Group, CRC Press. p. 13.

- Trujillo (2013). En su artículo titulado: *"Guerra de 5ª Generación; la conquista de las*
  mentes". Lima. Perú

ANEXOS

1. Base de Datos
2. Matriz de Consistencia
3. Instrumento de Recolección
4. Documento de Validación del Instrumento
5. Constancia de entidad donde se efectuó la investigación
6. Compromiso de autenticidad del Instrumento.
7. Ley N° 30999
8. Carta de las Naciones Unidas
9. Decreto Legitimo N° 1141

Anexo 1. Base de datos de la Asignatura de Guerra Cibernetica y la Formación Académica Especializada del Cadete de Cuarto año de Comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16
1	5	5	5	5	4	4	4	4	5	5	5	5	5	5	5	5
2	5	5	5	5	2	2	2	2	3	3	3	3	4	4	4	4
3	2	2	2	2	5	3	5	5	5	5	5	5	3	3	3	3
4	1	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5
5	5	4	5	5	5	5	5	5	4	4	4	4	1	1	4	4
6	3	2	2	2	1	4	1	4	5	5	5	2	5	5	5	1
7	3	5	5	3	2	3	5	5	2	2	2	3	2	5	5	5
8	4	4	3	5	5	2	3	1	5	5	5	3	5	2	1	5
9	1	5	5	4	3	5	5	3	1	1	1	1	4	4	4	4
10	1	2	5	4	5	1	5	5	5	5	5	5	5	5	5	3
11	5	5	5	5	4	4	4	4	5	5	5	5	5	5	5	5
12	5	5	5	4	5	3	5	5	5	5	5	5	5	5	5	5
13	5	1	4	5	5	5	5	5	1	3	1	1	4	4	3	4
14	4	5	1	5	5	5	1	5	5	5	5	5	5	5	5	2
15	3	1	1	5	5	5	2	2	2	2	3	3	2	5	5	5
16	4	4	5	4	5	4	4	5	4	5	5	5	5	2	2	5
17	5	5	5	1	5	5	5	5	5	4	4	4	4	4	4	2
18	5	3	5	5	4	3	2	4	5	5	5	5	2	5	5	3
19	3	1	5	1	2	5	5	5	5	5	5	5	5	5	5	5
20	5	2	4	4	4	4	3	2	4	3	3	3	4	2	1	2
21	4	3	4	4	4	4	3	4	4	3	3	3	4	4	1	4
22	5	3	4	4	4	4	3	4	4	3	4	4	4	4	4	4
23	4	3	4	4	4	4	3	4	4	3	4	4	4	4	4	4

24	5	4	4	4	4	4	3	4	4	5	4	4	4	4	4	4
25	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
26	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
27	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
28	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
29	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
30	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
31	4	4	4	5	4	5	4	4	4	4	4	4	4	4	4	4
32	5	5	4	5	4	5	4	4	4	4	4	4	4	4	4	5
33	4	5	4	5	4	5	4	4	4	4	4	5	5	4	4	5
34	5	5	4	5	4	5	4	4	4	4	4	5	5	5	5	5
35	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5
36	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
37	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
38	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
39	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
40	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
41	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
42	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Anexo 2. Matriz de consistencia de la Asignatura de Guerra Cibernetica y la Formación Académica Especializada del Cadete de Cuarto año de Comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	DISEÑO METOLOGÓGICO E INSTRUMENTOS
General ¿Cuál es la relación que existe entre la asignatura de Guerra Cibernética y la Formación Académica Especializada del cadete de 4° año de Comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019? ***Específicos*** ¿Cuál es la relación que existe entre los Fundamentos de la asignatura de Guerra Cibernética y la Formación Académica Especializada del cadete de 4° año de Comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019? ¿Cuál es la relación que existe entre la Estructura y Responsabilidades de la asignatura de Guerra Cibernética y la Formación Académica Especializada	***General*** Determinar cuál es la relación que existe entre la asignatura de Guerra Cibernética y la Formación Académica Especializada del cadete de 4° año de Comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019. ***Específicos*** Establecer cuál es la relación que existe entre los Fundamentos de la asignatura de Guerra Cibernética y la Formación Académica Especializada del cadete de 4° año de Comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019. Establecer cuál es la relación que existe entre la Estructura y Responsabilidades de la asignatura de Guerra Cibernética y la Formación Académica Especializada del cadete de 4° año de Comunicaciones de la Escuela	***General*** La asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada del cadete de 4° año de Comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019. ***Específicas*** Los Fundamentos de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada del cadete de 4° año de Comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019. La Estructura y Responsabilidades de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada del cadete de 4° año de Comunicaciones	La Asignatura de Guerra Cibernética	Fundamentos	• Principios de empleo • Características de la guerra cibernética • Posibilidades de la guerra cibernética • Limitaciones de la guerra cibernética	**TIPO DE INVESTIGACIÓN** Básico **DISEÑO** No Experimental- Corte Transversal **ENFOQUE** Cuantitativo **POBLACIÓN** Cadetes de Comunicaciones **MUESTRA** 62 Cadetes de Comunicaciones **TÉCNICA** Se ha aplicado: • Investigación documental • Investigación de campo **INSTRUMENTOS** Se utilizó: • Cuestionarios • Encuestas
				Estructura y Responsabilidades	• Visión Sistémica • Capacidades del Sistema de Guerra Cibernética del Ejército	
				Aplicación en Operaciones Terrestres	• Operaciones Combinadas • Operaciones Ofensivas • Operaciones Defensivas • Operaciones de Información	
				Empleo de comunicaciones para todas las armas	• Organización de comunicaciones • Fundamentos de empleo • Personal de comunicaciones de las UU tipo batallón • Procedimientos de explotación y constitución de equipos básicos de comunicaciones	

del cadete de 4° año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019? ¿Cuál es la relación que existe entre la Aplicación en Operaciones Terrestres de la asignatura de Guerra Cibernética y la Formación Académica Especializada del cadete de 4° año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?	Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019. Establecer cuál es la relación que existe entre la Aplicación en Operaciones Terrestres de la asignatura de Guerra Cibernética y la Formación Académica Especializada del cadete de 4° año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.	de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019. La Aplicación en Operaciones Terrestres de la asignatura de Guerra Cibernética se relaciona significativamente con la Formación Académica Especializada del cadete de 4° año de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.	Formación Académica especializada	Sistema de comunicaciones satelital VSAT	• Generalidades • Estación base • Estaciones fijas • Unidades móviles	**MÉTODOS DE ANÁLISIS DE DATOS** Estadística SPSS22
				Medios de comunicación en campaña	• Equipo de radio PRC – 6020 HF • Equipo de radio PRC – 730 VHF • Equipo de radio PRC – 710 VHF/UHF • Equipo de radio SELEX UHF	
				Fundamentos de comando y control	• Generalidades • Definiciones, principios y funciones del C2 • Componentes de un sistema de comando y control • Software de comando y control Wiracocha	

Anexo 3: Instrumento de Recolección de Datos

Encuesta

Instrucciones:

Gracias por su colaboración en contestar el presente cuestionario, es anónimo.

Por favor coloque una X en la respuesta que usted considere pertinente.

---

1. ¿Cree usted que las características de empleo de la Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH "CFB"?

   ( ) NUNCA

   ( ) CASI NUNCA

   ( ) A VECES

   ( ) CASI SIEMPRE

   ( ) SIEMPRE

2. ¿Cree usted que las posibilidades de empleo de la Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH "CFB"?

   ( ) NUNCA

   ( ) CASI NUNCA

   ( ) A VECES

   ( ) CASI SIEMPRE

   ( ) SIEMPRE

3. ¿Cree usted que las características de empleo de la Guerra Cibernética se relacionan con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH "CFB"?

   ( ) NUNCA

   ( ) CASI NUNCA

   ( ) A VECES

   ( ) CASI SIEMPRE

   ( ) SIEMPRE

4. ¿Cree usted que las posibilidades de empleo de la Guerra Cibernética se relacionan con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

   ( ) NUNCA

   ( ) CASI NUNCA

   ( ) A VECES

   ( ) CASI SIEMPRE

   ( ) SIEMPRE

5. ¿Considera usted que la Visión Sistemática de la Estructura y Responsabilidades de la Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

   ( ) NUNCA

   ( ) CASI NUNCA

   ( ) A VECES

   ( ) CASI SIEMPRE

   ( ) SIEMPRE

6. ¿Considera usted que las Capacidades del Sistema de Guerra Cibernética se relacionan con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

   ( ) NUNCA

   ( ) CASI NUNCA

   ( ) A VECES

   ( ) CASI SIEMPRE

   ( ) SIEMPRE

7. ¿Considera usted que la Visión Sistemática de la Estructura y Responsabilidades de la Guerra Cibernética se relacionan con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

   ( ) NUNCA

   ( ) CASI NUNCA

   ( ) A VECES

( ) CASI SIEMPRE

( ) SIEMPRE

8. ¿Considera usted que las Capacidades del Sistema de Guerra Cibernética se relacionan con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

   ( ) NUNCA

   ( ) CASI NUNCA

   ( ) A VECES

   ( ) CASI SIEMPRE

   ( ) SIEMPRE

9. ¿Cree usted que la aplicación de las operaciones ofensivas de la Guerra Cibernética se relaciona con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

   ( ) NUNCA

   ( ) CASI NUNCA

   ( ) A VECES

   ( ) CASI SIEMPRE

   ( ) SIEMPRE

10. ¿Cree usted que la aplicación de las operaciones defensivas de la Guerra Cibernética se relaciona con el sistema de comunicaciones satelital VSAT dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

    ( ) NUNCA

    ( ) CASI NUNCA

    ( ) A VECES

    ( ) CASI SIEMPRE

    ( ) SIEMPRE

11. ¿Cree usted que la aplicación de las operaciones ofensivas de la Guerra Cibernética se relaciona con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

    ( ) NUNCA

( ) CASI NUNCA

( ) A VECES

( ) CASI SIEMPRE

( ) SIEMPRE

12. ¿Cree usted que la aplicación de las operaciones defensivas de la Guerra Cibernética se relaciona con los medios de comunicación de campaña dentro de la Formación Especializada de los Cadetes de Comunicaciones de la EMCH “CFB”?

( ) NUNCA

( ) CASI NUNCA

( ) A VECES

( ) CASI SIEMPRE

( ) SIEMPRE

13. ¿Considera usted que, atendiendo a la Formación Especializada, el Empleo de las Comunicaciones para todas las Armas es influido por la Asignatura de Guerra Cibernética?

( ) NUNCA

( ) CASI NUNCA

( ) A VECES

( ) CASI SIEMPRE

( ) SIEMPRE

14. ¿Considera usted que, atendiendo a la Formación Especializada, el Sistema de Comunicaciones Satelital VSAT es influido por la Asignatura de Guerra Cibernética?

( ) NUNCA

( ) CASI NUNCA

( ) A VECES

( ) CASI SIEMPRE

( ) SIEMPRE

15. ¿Considera usted que, atendiendo a la Formación Especializada, los Medios de Comunicación en Campaña son influidos por la Asignatura de Guerra Cibernética?

( ) NUNCA

( ) CASI NUNCA

( ) A VECES

( ) CASI SIEMPRE

( ) SIEMPRE

16. ¿Considera usted que, atendiendo a la Formación Especializada, los Fundamentos de Comando y Control son influidos por la Asignatura de Guerra Cibernética?

( ) NUNCA

( ) CASI NUNCA

( ) A VECES

( ) CASI SIEMPRE

( ) SIEMPRE

ANEXO 4. VALIDACION DE INSTRUMENTO POR EXPERTO

1era EVALUACION POR JUICIO DE EXPERTOS

TITULO DE LA TESIS.

La Asignatura de la Guerra Cibernetica y la Formación Académica Especializada de los cadetes de Comunicaciones de la “Escuela Militar de Chorrillos Coronel Francisco Bolognesi” 2019.

AUTORES.

- CAD IV COM GONZALES CONCHA, Luis Angel
- CAD IV COM RAMOS CASTILLO, Gustavo Alfonso

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

CRITERIOS	DESCRIPCION	VALOR ASIGANDO POR EL EXPERTO									
		10	20	30	40	50	60	70	80	90	100
1.CLARIDAD	Está formado con el lenguaje adecuado										
2.OBJETIVIDAD	Esta expresado en conductas observables										
3.ACTUALIDAD	Adecuado de acuerdo al avance de la ciencia										
4.ORGANIZACION	Existe una cohesión lógica entre sus elementos										
5.SUFICIENCIA	Comprende los aspectos requeridos en cantidad y calida										
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.METODOLOGIA	El diseño responde al propósito de la investigación										
10.PERTINENCIA	Es útil y adecuado para la investigacion										

PROMEDIO DE VALORACION DEL EXPERTO…….

OBSERVACIONES REALIZADAS POR EL EXPERTO……
……..

GRADO ACADEMICO DEL EXPERTO……

INSTITUCION DONDE LABORA……

APELLIDO Y NOMBRE DEL EXPERTO……

FIRMA DEL EXPERTO……

POST FIRMA DEL EXPERTO……

DNI DE EXPERTO……

ANEXO 4. VALIDACION DE INSTRUMENTO POR EXPERTO

2da EVALUACION POR JUICIO DE EXPERTOS

TITULO DE LA TESIS.

La Asignatura de la Guerra Cibernetica y la Formación Académica Especializada de los cadetes de Comunicaciones de la “Escuela Militar de Chorrillos Coronel Francisco Bolognesi” 2019

AUTORES.

- CAD IV COM GONZALES CONCHA, Luis Angel
- CAD IV COM RAMOS CASTILLO, Gustavo Alfonso

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

CRITERIOS	DESCRIPCION	VALOR ASIGANDO POR EL EXPERTO									
		10	20	30	40	50	60	70	80	90	100
1.CLARIDAD	Está formado con el lenguaje adecuado										
2.OBJETIVIDAD	Esta expresado en conductas observables										
3.ACTUALIDAD	Adecuado de acuerdo al avance de la ciencia										
4.ORGANIZACION	Existe una cohesión lógica entre sus elementos										
5.SUFICIENCIA	Comprende los aspectos requeridos en cantidad y calida										
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.METODOLOGIA	El diseño responde al propósito de la investigación										
10.PERTINENCIA	Es útil y adecuado para la investigacion										

PROMEDIO DE VALORACION DEL EXPERTO…….

OBSERVACIONES REALIZADAS POR EL EXPERTO……
……..

GRADO ACADEMICO DEL EXPERTO……

INSTITUCION DONDE LABORA……

APELLIDO Y NOMBRE DEL EXPERTO……

FIRMA DEL EXPERTO……

POST FIRMA DEL EXPERTO……

DNI DE EXPERTO……

ANEXO 4. VALIDACION DE INSTRUMENTO POR EXPERTO

3era EVALUACION POR JUICIO DE EXPERTOS

TITULO DE LA TESIS.

La Asignatura de la Guerra Cibernetica y la Formación Académica Especializada de los cadetes de Comunicaciones de la "Escuela Militar de Chorrillos Coronel Francisco Bolognesi" 2019

AUTORES.

- CAD IV COM GONZALES CONCHA, Luis Angel
- CAD IV COM RAMOS CASTILLO, Gustavo Alfonso

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

CRITERIOS	DESCRIPCION	VALOR ASIGANDO POR EL EXPERTO									
		10	20	30	40	50	60	70	80	90	100
1.CLARIDAD	Está formado con el lenguaje adecuado										
2.OBJETIVIDAD	Esta expresado en conductas observables										
3.ACTUALIDAD	Adecuado de acuerdo al avance de la ciencia										
4.ORGANIZACION	Existe una cohesión lógica entre sus elementos										
5.SUFICIENCIA	Comprende los aspectos requeridos en cantidad y calida										
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.METODOLOGIA	El diseño responde al propósito de la investigación										
10.PERTINENCIA	Es útil y adecuado para la investigacion										

PROMEDIO DE VALORACION DEL EXPERTO…….

OBSERVACIONES REALIZADAS POR EL EXPERTO……
……..

GRADO ACADEMICO DEL EXPERTO……..

INSTITUCION DONDE LABORA……

APELLIDO Y NOMBRE DEL EXPERTO……

FIRMA DEL EXPERTO……..

POST FIRMA DEL EXPERTO……..

DNI DE EXPERTO……..

ANEXO N° 5: CONSTANCIA EMITIDA POR LA INSTITUCIÓN DONDE SE REALIZÓ LA INVESTIGACIÓN.

Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”

DEPARTAMENTO DE INVESTIGACIÓN Y DOCTRINA.

El que suscribe, Jefe del Departamento de Investigación y Doctrina de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi, deja:

CONSTANCIA

Que los bachilleres de COMUNICACIONES, GONZALES CONCHA LUIS ANGEL, RAMOS CASTILLO GUSTAVO ADOLFO, identificados con DNI: 70333823, 72617133, respectivamente, han realizado en nuestro ámbito institucional, la tesis dirigida a la población académica nacional e internacional.

Dicha investigación ha sido realizada en el año 2019, para la obtención del Título de Licenciado en Ciencias Militares, con mención en Administración.

Título: “LA ASIGNATURA DE GUERRA CIBERNÉTICA Y LA FORMACION ACADÉMICA ESPECIALIZADA DE LOS CADETES DE COMUNICACIONES DE LA ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI” 2019”

Se expide la presente constancia a solicitud de los interesados para los fines que sean pertinentes.

Chorrillos, de diciembre, 2019

ESCUELA MILITAR DE CHORRILLOS “Coronel Francisco Bolognesi”

O-224396679-O+
Christian SOLDEVILLA PALACIOS
TTE CRL EP.
Jefe del DIDOC de la EMCH ”CFB”

ANEXO 6: Compromiso de Autenticidad del Documento

Los Cadetes de cuarto año de Comunicaciones GONZALES CONCHA, Luis Angel, RAMOS CASTILLO, Gustavo Alfonso, autores del trabajo de investigación titulada: La Asignatura de Guerra Cibernetica y la Formación Académica Especializada de los Cadetes de Comunicaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” 2019

Declaran

Que el presente trabajo ha sido íntegramente elaborado por los suscritos y que no existe plagio alguno, presentado 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 nuestra responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión, tanto en los documentos como en la información aportada.

Nos afirmamos y ratificamos en los expresado, en sal de lo cual firmarnos el presente documento.

Chorrillos, …de …… del 2019

……..	……..……
GONZALES CONCHA, Luis	**RAMOS CASTILLOS, Gustavo**

ANEXO 7: Ley N° 30999

EL PRESIDENTE DE LA REPÚBLICA
POR CUANTO:
LA COMISIÓN PERMANENTE DEL
CONGRESO DE LA REPÚBLICA;
Ha dado la Ley siguiente:

LEY DE CIBERDEFENSA

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto

La presente ley tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley.

Artículo 2. Finalidad

Defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

Artículo 3. Ámbito de aplicación

El ámbito de aplicación de la norma se circunscribe a la ejecución de operaciones de ciberdefensa en y mediante el ciberespacio frente a las amenazas o los ataques que afecten la seguridad nacional.

Artículo 4. Definición

Entiéndase por ciberdefensa a la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional.

Artículo 5. Órganos ejecutores

Las Fuerzas Armadas, que están constituidas por el Ejército, la Marina de Guerra y la Fuerza Aérea, y el Comando Conjunto de las Fuerzas Armadas son instituciones con calidad de órganos ejecutores del Ministerio de Defensa.

TÍTULO II
DE LA CIBERDEFENSA
CAPÍTULO I
LAS CAPACIDADES DE CIBERDEFENSA Y LAS OPERACIONES EN Y MEDIANTE EL CIBERESPACIO

Artículo 6. De las capacidades de ciberdefensa

Es el uso de conocimiento, habilidades y medios para realizar operaciones en y mediante el ciberespacio a fin de asegurar su empleo por las fuerzas propias.

Artículo 7. De las operaciones militares en el ciberespacio

Es el eficiente y eficaz empleo de las capacidades de ciberdefensa por parte de los órganos ejecutores del Ministerio de Defensa, de acuerdo a sus funciones y en el ámbito de sus respectivas competencias, contra las amenazas o los ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

Artículo 8. De la planificación y ejecución de las operaciones en el ciberespacio

La planificación y ejecución de las operaciones de ciberdefensa a cargo del Comando Conjunto de las Fuerzas Armadas responde al mandato conferido en la Constitución Política del Perú, así como al cumplimiento de las responsabilidades asignadas en las leyes que regulan su naturaleza jurídica, competencias, funciones y estructura orgánica, las disposiciones contenidas en la presente ley, y los tratados y acuerdos internacionales de los que el Perú es parte y resulten aplicables.

CAPÍTULO II
DEL USO DE LA FUERZA EN Y MEDIANTE EL CIBERESPACIO

Artículo 9. Del uso de la fuerza por las Fuerzas Armadas

El uso de la fuerza por la Fuerzas Armadas en y mediante el ciberespacio se sujeta a las disposiciones contenidas en el artículo 51 de la Carta de las Naciones Unidas y el presente dispositivo legal, y está regido por las normas del Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario que sean aplicables.

Artículo 10. De la legítima defensa

Toda amenaza o ataque en y mediante el ciberespacio que ponga en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales, da lugar al ejercicio del derecho de legítima defensa.

Artículo 11. Requisitos para el ejercicio del uso de la fuerza

El ejercicio del derecho de legítima defensa en el contexto de las operaciones de ciberdefensa está sujeto a los principios de legalidad, necesidad y oportunidad.

En el caso de conducir una operación de respuesta en y mediante el ciberespacio que contenga un ataque deliberado, debe realizarse de acuerdo a ley.

CAPÍTULO III
DE LA SEGURIDAD DE LOS ACTIVOS CRÍTICOS NACIONALES Y RECURSOS CLAVES

Artículo 12. Del control y de la protección de los activos críticos nacionales y recursos claves

El Comando Conjunto de las Fuerzas Armadas está a cargo de la ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores y/o del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia sea sobrepasada, a fin de mantener las capacidades nacionales, en el ámbito de la seguridad nacional.

Artículo 13. De los protocolos de escalamiento, coordinación, intercambio y activación

La Presidencia del Consejo de Ministros, en su calidad de miembro del Consejo de Seguridad y Defensa Nacional, establece los protocolos de escalamiento, coordinación, intercambio y activación para lo indicado en la presente ley.

Esta función se ejerce a través de la Secretaría de Gobierno Digital en su calidad de ente rector del Sistema Nacional de Informática y de la seguridad digital en el país, quien emite los lineamientos y las directivas correspondientes.

Artículo 14. Modificación del artículo 32 del Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital

Modifícase el artículo 32 del Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, el cual queda redactado de la siguiente manera:

“Artículo 32.- Gestión del Marco de Seguridad Digital del Estado Peruano

El Marco de Seguridad Digital del Estado Peruano tiene los siguientes ámbitos:

a. Defensa: El Ministerio de Defensa (MINDEF), en el marco de sus funciones y competencias, dirige, norma, supervisa y evalúa las normas en materia de ciberdefensa.

[…].”

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Reglamentación en materia de ciberdefensa

La Presidencia del Consejo de Ministros, en coordinación con el Ministerio de Defensa, aprueba el reglamento de la presente ley, en un plazo máximo de noventa (90) días, contados a partir del día siguiente de su publicación en el diario oficial El Peruano.

SEGUNDA. Modificaciones a normas de las Fuerzas Armadas en materia de ciberdefensa

El Ministerio de Defensa, en un plazo de noventa (90) días, contados a partir de la fecha de entrada en vigencia de la presente ley, presenta las modificaciones, derogaciones e incorporaciones a las normas correspondientes a las Fuerzas Armadas en materia de la presente ley.

TERCERA. Recursos críticos de Internet

Se reconoce a las entidades que gestionen recursos críticos de Internet (nombres de dominio, números IP y protocolos) en su naturaleza de entidades vinculadas a la ciberdefensa, debiendo mantener mecanismos de comunicación de incidentes que pudieran afectar la capacidad de ciberdefensa nacional.

CUARTA. Desarrollo de currículos de educación superior en materia de ciberdefensa

La Presidencia del Consejo de Ministros, en su calidad de ente rector en materia de seguridad digital, coordina con el Ministerio de Defensa y el Ministerio de Educación la pertinencia del desarrollo de contenidos especializados en materia de seguridad digital, que incluye la ciberdefensa, en las instituciones de educación superior universitaria y tecnológica, a nivel de pregrado y postgrado. Para ello,

establece instrumentos de cooperación interinstitucional con entidades del sector privado, la academia, la sociedad civil y la comunidad técnica.

QUINTA. Aplicación de recursos especiales

Los procesos para las capacidades de ciberdefensa deben considerarse dentro del alcance de la aplicación de los artículos 30 y 31 del Decreto Legislativo 1141.

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogatoria

Deróganse o déjense en suspenso, según el caso, las disposiciones legales y reglamentarias que se opongan a lo establecido por la presente ley o limiten su aplicación, con la entrada en vigencia de la presente ley.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los nueve días del mes de agosto de dos mil diecinueve.

PEDRO C. OLAECHEA ÁLVAREZ CALDERÓN

Presidente del Congreso de la República

KARINA BETETA RUBÍN

Primera Vicepresidenta del Congreso de la República

AL SEÑOR PRESIDENTE DE LA

REPÚBLICA POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiséis días del mes de agosto del año dos mil diecinueve.

MARTÍN ALBERTO VIZCARRA

CORNEJO Presidente de la República

SALVADOR DEL SOLAR LABARTHE

Presidente del Consejo de Ministros

1801519-5

ANEXO 8: Carta de las Naciones Unidas

CARTA DE LAS NACIONES UNIDAS

Firmada en San Francisco, Estados Unidos el 26 de junio 1945 entrada en vigor: 24 de octubre de 1945, de conformidad con el artículo 110

Capítulo VII: Acción en Caso de Amenazas a la Paz, Quebrantamientos de la Paz o Actos de Agresión (Artículos 39-51)

Artículo 51

Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales.

ANEXO 9: Decreto Legislativo N° 1141

Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI

Artículo 30º.- Rendición de cuentas de recursos especiales

30.1 Constituyen recursos especiales aquellos destinados a atender los gastos de naturaleza reservada de la actividad de inteligencia, que de hacerse en forma pública, pondrían en riesgo la seguridad nacional, la integridad del personal de inteligencia o sus fuentes de información. Los recursos especiales no pueden ser destinados para cubrir aumentos y/o pagos de haberes ordinarios y/o gastos de carácter personal, tanto del personal de la Dirección Nacional de Inteligencia – DINI como a cualquier personal de los componentes del Sistema de Inteligencia Nacional - SINA.

30.2 El Director de Inteligencia Nacional establece bajo responsabilidad, mediante Directiva clasificada como secreta, el procedimiento para la autorización, ejecución, sustentación y control de la rendición de cuentas de los recursos especiales utilizados por el Sistema de Inteligencia Nacional - SINA; siendo sus disposiciones de obligatorio cumplimiento por todos los componentes del sistema.

30.3 La Directiva debe contar con la previa opinión favorable de la Contraloría General de la República; requisito sin el que dicho documento no tiene efecto legal alguno.

30.4 Es responsabilidad del Director de Inteligencia Nacional poner en conocimiento de los demás componentes del Sistema de Inteligencia Nacional - SINA, la Directiva a que alude el presente artículo.

30.5 Los funcionarios y demás personal del Sistema Nacional de Control garantizan la debida reserva y el carácter de secreto de la información, de conformidad con lo establecido en el artículo 4° del presente Decreto Legislativo.

30.6. La Dirección Nacional de Inteligencia deberá dar cuenta de uso de los gastos de naturaleza reservada de la actividad de inteligencia al Presidente del Consejo de Ministros por lo menos dos (02) veces al año.

Artículo 31º.- Contrataciones que se efectúan con cargo a recursos especiales

Las contrataciones que se efectúen con cargo a los recursos especiales a que se refiere el artículo anterior, para actividades de inteligencia, que de hacerse en forma pública, pondrían en peligro la seguridad nacional, las fuentes de información o la integridad del personal de los componentes del Sistema de Inteligencia Nacional - SINA, tienen la clasificación de secreto y se rigen por la normativa de la materia.