ESCUELA MILITAR DE CHORRILLOS

“CORONEL FRANCISCO BOLOGNESI”

“SISTEMA DE INFORMACIÓN DE VIGILANCIA Y LA CIBERSEGURIDAD EN LAS INSTALACIONES PARA LOS CADETES DE LA ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI, AÑO 2019”

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

PRESENTADO POR:

DIAZ NOA CARMEN DIANA

LLIQUE CRUZADO JHOSSELYN

LIMA – PERÚ

2019

ASESOR Y MIEMBROS DEL JURADO

ASESOR: Mg, Paucar Luna Anastasio

TEMÁTICO: Crl Vigo Salirosas Pedro

METODOLÓGICO: Grl.

PRESIDENTE DEL JURADO:

Dr. Bernabe Moreno Hugo

MIEMBROS DEL JURADO:

Dr. Gavidia Orjuela Cesar

Dr. La torre Padron Oscar

DEDICATORIA

Dedicamos este producto de investigación científica a nuestros seres queridos, especialmente a quienes confiaron en nosotros de manera incondicional, en nuestro esfuerzo de formación profesional, académica, científica y para quienes les brindamos nuestros corazones de orgullo por los objetivos alcanzados.

AGRADECIMIENTO

A la gloriosa Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", alma mater del Ejército del Perú, por la oportunidad de realizar nuestros estudios de Formación profesional, científica, humanística que nos permitió culminar con éxito nuestra Tesis.

A las autoridades y docentes de la Escuela Militar de Chorrillos "coronel Francisco Bolognesi", que colaboraron en el proceso de producción de este trabajo.

PRESENTACIÓN

Señores miembros del Jurado:

En cumplimiento de lo establecido en el Reglamento de elaboración y sustentación de Tesis de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, presentamos a consideración del jurado la Tesis titulada: "SISTEMA DE INFORMACIÓN DE VIGILANCIA Y LA CIBERSEGURIDAD EN LAS INSTALACIONES PARA LOS CADETES DE LA ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI, AÑO 2019".

El objeto del estudio busca determinar la relación que existe entre el Sistema de Información de Vigilancia y la Ciberseguridad en las instalaciones de los cadetes de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi; con el propósito que, a la luz de los resultados obtenidos, plantear las recomendaciones pertinentes, que contribuyan a la superación de la situación problemática y constituya un real aporte al mejoramiento de la Ciencia Militar. El estudio es fruto de la participación mancomunada de los autores, teniendo como responsable de los aspectos Lógicos y Temáticos al Srta. Díaz Noa Carmen Diana y como responsable de los aspectos Epistemológicos y Metodológicos al Srta. Lique Cruzado Joselyn.

Por lo expuesto, señores miembros del jurado, pongo a vuestra disposición esta investigación para ser evaluada esperando merecimiento de aprobación.

Los Autores

ÍNDICE

ÍNDICE DE TABLAS

INDICE DE GRAFICOS

RESUMEN

La presente investigación titulada “SISTEMA DE INFORMACIÓN DE VIGILANCIA Y LA CIBERSEGURIDAD EN LAS INSTALACIONES PARA LOS CADETES DE LA ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI, AÑO 2019”, tiene como objetivo general, establecer la relación entre el Sistema de Informacion de Vigilancia y la ciberseguridad en las instalaciones de los cadetes de la Escuela Militar de Chorrillos.

El diseño de investigación fue cuantitativo, no experimental y descriptivo. También se utilizaron los instrumentos tipo cuestionario, para determinar en qué medida se relaciona entre el Sistema de Información de Vigilancia y la ciberseguridad en las instalaciones de los estudiantes cadetes de Inteligencia. Estos instrumentos fueron aplicados a una muestra de estudiantes cadetes seleccionados de manera aleatoria. Finalmente, los resultados obtenidos evidencian que los estudiantes cadetes que comprendieron y manejaron las utilidades de los Sistema de Información de Vigilancia obtuvieron un mayor nivel en la ciberseguridad en las instalaciones durante el proceso de formación profesional de los cadetes de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, investigación realizada el año 2019.

Palabras Claves: Sistemas de Información de Vigilancia. – Ciberseguridad en las instalaciones

ABSTRACT

The present investigation entitled “SYSTEM OF SURVEILLANCE INFORMATION AND CYBER SECURITY IN THE INSTALLATIONS OF THE CADETES OF THE MILITARY SCHOOL OF CHORRILLOS CORONEL FRANCISCO BOLOGNESI, YEAR 2019” has as a general objective, to establish the relationship of the Surveillance Information System and the Cybersecurity in the facilities of the cadets of the Military School of Chorrillos.

The research design was quantitative, non-experimental, transversal, exploratory and descriptive. The questionnaire-type instruments were also used to determine the extent to which Cybersecurity relates to the Security of Computer Systems in the facilities of the Intelligence cadet students. These instruments were applied to a sample of randomly selected cadet students. Finally, the results obtained show that the cadet students who understood and managed the utilities of the Computer Systems obtained a higher level in cybersecurity in the facilities during the professional training process of the intelligence cadets of the Military School of Chorrillos “Colonel Francisco Bolognesi”, research carried out in 2019.

Keywords: System of surveillance information - Cybersecurity in facilities

INTRODUCCIÓN

La investigación titulada: "SISTEMA DE INFORMACIÓN DE VIGILANCIA Y LA CIBERSEGURIDAD EN LAS INSTALACIONES PARA LOS CADETES DE LA ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI, AÑO 2019", tuvo por finalidad estudiar las condiciones experienciales, de capacitación y de empleo de el Sistema de Informacion de Vigilancia y la ciberseguridad en las instalaciones; teniendo la Variable "Sistema de Informacion de Vigilancia" como dimensiones: 1) Herramienta de trabajo en las cuadras, 2) Redes sociales, y 3) Adicción al Internet; de manera que los cadetes obtengan un mayor nivel de Ciberseguridad en las instalaciones y se apropien de las competencias necesarias que incrementen el nivel de formación profesional.

El problema que aborda esta investigación es acerca del conocimiento de la seguridad de los sistemas de información de vigilancia, entiéndase de sus características, funciones, posibilidades, limitaciones, técnicas y herramientas de trabajo en relación con la Ciberseguridad en las instalaciones de los cadetes de Inteligencia de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2019.

Para abordar este tema de investigación ha sido necesaria dividir el presente informe en 05 capítulos:

El Capítulo I, Problemas de investigación, presenta los aspectos importantes tales como; el planteamiento del problema las cuales buscamos una explicación del Sistema de Información de Vigilancia y la ciberseguridad en las instalaciones, dando así la formulación del problema, donde la justificación es fortalecer la seguridad informática, siendo las limitaciones una de ella el tiempo donde las actividades de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" ocupa gran parte del tiempo disponible y la viabilidad donde se contaron con docentes especializados en Tecnologías de la información y comunicaciones.

El Capítulo II Marco Teórico, presenta los antecedentes, son en base a las variables independiente y dependiente, como investigaciones tanto nacionales como internacionales, las bases teóricas de las dos variables de estudio y la definición de términos. Desarrollando la hipótesis general y específica, las variables expresando en la definición conceptual y operacionalización de las mismas.

El Capítulo III, Marco Metodológico, se aclaran los aspectos metodológicos tales como el enfoque, tipo, diseño, método de estudio, la población y muestra, las técnicas e instrumentos de recolección de datos, así como los métodos de análisis de datos.

En el Capítulo IV, Resultados, se presenta una descripción de los resultados, la interpretación y discusión de los mismos.

Finalmente, las Conclusiones y Recomendaciones, en donde se plantearon los aspectos más relevantes alcanzados producto del presente trabajo y que permitieron establecer las conclusiones y como también plantear las recomendaciones.

Asimismo, se ha establecido al término de la investigación y con las pruebas de hipótesis que existe una relación significativa entre el Sistema de Información de Vigilancia y la ciberseguridad de las instalaciones de los cadetes de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

CAPÍTULO I. PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema.

La Unión Internacional de Telecomunicaciones ha informado en mayo de 2017, que de los 940 millones de personas que habitan los países menos desarrollados, sólo 89 millones están conectadas. El organismo internacional ha señalado que más de 3 millardos de personas en el mundo usan actualmente Internet, sin embargo, otros 4 millardos que residen en los países más pobres del planeta siguen sin estar conectadas. Estos 4 millardos de personas representan dos terceras partes de la población que reside en los países en desarrollo, y no tienen perspectivas a corto plazo para poder tener acceso a las nuevas tecnologías de la información (TIC en adelante).

De hecho, de los 940 millones de personas que viven en los Países Menos Desarrollados sólo 89 millones usan Internet, lo que indica una penetración de tan solo 9,5%. No obstante, la proporción de hogares que tienen acceso a Internet pasó de un 18% en 2005 a un 46% en 2015. Actualmente, hay más de 7 millardos de líneas de móvil en el mundo, cuando en el año 2000 eran solo 738 millones. Bajo este contexto, en los países se ha iniciado una serie de medidas, esto es legislaciones en materia de terrorismo, ciberdelincuencia, la creación de organismos de certificación electrónica y resguardo frente a posibles ataques cibernéticos bien hacia sus ciudadanos o contra la misma soberanía de los Estados cuando se accede a los sistemas de información, redes o a las infraestructuras de comunicación en general.

Hoy más que nunca, se observa una concienciación creciente de la necesidad de controlar los riesgos informáticos operacionales debido a la utilización extensiva de las nuevas tecnologías, a la existencia de una infraestructura de información mundial y a la aparición de nuevos riesgos. Además, también es cierto que la transformación de las sociedades en sociedades de la información, gracias a la integración de nuevas tecnologías en todas sus actividades e infraestructuras, aumenta la dependencia de los individuos, de

las organizaciones y de los Estados, de los sistemas de información y de las redes. Esto constituye un riesgo de primer orden que debe contemplarse inclusive como un riesgo de seguridad. Sin embargo, los países en desarrollo se enfrentan a la necesidad de formar parte de la sociedad de la información asumiendo el riesgo de su dependencia de las tecnologías y de los proveedores de las mismas intentando que la brecha digital existente no dé lugar a una brecha de seguridad y menos aún a una dependencia más estrecha de entidades que controlen sus necesidades y los medios de seguridad de las tecnologías de la información.

En consecuencia, las infraestructuras de telecomunicaciones y los servicios y actividades que éstas permiten desarrollar y generar, deben plantearse, concebirse, instalarse y administrarse en términos de seguridad. La seguridad es la piedra angular de toda actividad y debe contemplarse como un servicio que permite crear otros y generar valor añadido (cibergobierno, cibersalud, ciberenseñanza, etc.) con independencia de las tecnologías. No obstante, hasta el momento, las herramientas básicas de comunicación disponibles no cuentan con los medios suficientes ni necesarios para establecer o garantizar un nivel mínimo de seguridad. Los sistemas informáticos conectados en red son recursos accesibles a distancia y blancos potenciales de ataques informáticos.

Esto incrementa los riesgos de intrusión en los sistemas y ofrece un terreno favorable para la realización y propagación de ataques y delitos. Los ataques pueden afectar a la capacidad de tratamiento, salvaguarda y comunicación del capital de información, de los valores y materiales y de los símbolos, y al proceso de producción o de decisión de los que los poseen. Así pues, las redes de telecomunicaciones y la apertura de los sistemas plantean problemas de seguridad informática, complejos y multiformes, que son relativamente difíciles de controlar y que pueden tener consecuencias y repercusiones críticas sobre el funcionamiento de las organizaciones y de los Estados. De la capacidad de controlar la seguridad de las informaciones, de los procesos, de los sistemas, y de las infraestructuras dependen los factores críticos de éxito de las economías.

La interconexión extensiva de sistemas, la interdependencia de las infraestructuras, el aumento de la dependencia de las tecnologías digitales, las amenazas

y los riesgos, exigen dotar a los individuos, las organizaciones y los Estados de medidas, procedimientos y herramientas que permitan mejorar la gestión de los riesgos tecnológicos y de la información. Así surge la denominada ciberseguridad. Los retos del dominio de los riesgos tecnológicos son propios del siglo XXI y exigen un planteamiento global a nivel internacional y su integración en el proceso de la seguridad de los países en desarrollo. No basta con establecer puntos de acceso a las redes de telecomunicación, es indispensable desplegar infraestructuras y servicios informáticos fiables, susceptibles de mantenimiento, robustos y seguros, para respetar los derechos fundamentales de las personas y de los Estados.

La protección de los sistemas y de la información de valor debe complementarse y armonizarse con la protección de los individuos y de su intimidad digital (privacidad). La entrada en la sociedad de la información sin un riesgo excesivo y aprovechando las experiencias obtenidas de los países en desarrollo, sin que la ciberseguridad se convierta en un factor adicional de exclusión, constituye un nuevo reto para los países en desarrollo. Se afirma, que el tema de la ciberseguridad es fundamental para sustentar un modelo tecnológicamente coherente. Las perturbaciones del tendido eléctrico o los problemas causados a los sistemas financieros por injerencias en las redes de las TIC son concretas y constituyen amenazas para la seguridad nacional. Las personas malintencionadas en línea son numerosas, están bien organizadas y son muy diversas van desde organizaciones políticas, delincuentes, terroristas o activistas.

Navarro (2015) recientemente ha asegurado que Internet es “la gran arma” del terrorismo yihadista y abogó por la cooperación internacional en la lucha contra el terrorismo de inspiración internacional. Agrega Navarro (2015), “existen más de 30.000 páginas yihadistas que hoy circulan por la red, por lo que argumentó que los estados democráticos deben buscar una “respuesta congruente” con las nuevas amenazas. Estos grupos mal intencionados disponen de herramientas cada vez más sofisticadas y complejas, y adquieren experiencia con el tiempo; el número creciente de plataformas conectadas no hace más que ofrecerles nuevos vectores de ataque.

Es imposible volver a los tiempos primitivos, razón por la cual la ciberseguridad debe formar parte integrante e indivisible del progreso tecnológico. Lamentablemente,

como afirman ABI Research y la Unión Internacional de Telecomunicaciones (2014), la ciberseguridad todavía no se considera esencial en muchas estrategias tecnológicas nacionales e industriales. Los esfuerzos para aumentar la ciberseguridad son numerosos pero eclécticos y dispersos. Las disparidades en la penetración de Internet, el desarrollo tecnológico, el dinamismo del sector privado o las estrategias públicas significan que la ciberseguridad evoluciona de lo particular a lo general, lo que es natural cuando existen esas disparidades entre Estados, sector público y privado e incluso sectores industriales. Ahora bien, una cultura mundial de la ciberseguridad tendría más éxito en esencia, si evolucionara de lo general a lo particular. La divulgación de información y la cooperación son fundamentales para afrontar las amenazas internacionales.

1.2. Formulación del problema

1.2.1 Problema General

¿En qué medida la Ciberseguridad se relaciona con la Seguridad de los Sistemas Informáticos en las instalaciones para los cadetes de la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2019?

1.2.2 Problemas específicos

1.2.2.1 Problemas Específicos 1

¿En qué medida la Ciberseguridad se relaciona con la Seguridad de los Sistemas Informáticos en las instalaciones para los cadetes de la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2019?

1.2.2.2 Problema específico 2

¿En qué medida la prevención de ataques Cibernéticos se relaciona con la Seguridad de los Sistemas Informáticos para los cadetes de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2019?

1.3. Objetivos

1.3.1 Objetivo general

Determinar en qué medida la Ciberseguridad se relaciona con la Seguridad de los Sistemas Informáticos en las instalaciones para los cadetes de la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2019.

1.3.2 Objetivos Específicos

1.3.2.1 Objetivo Específico 1

Determinar en qué medida la Ciberseguridad se relaciona con la Seguridad de los Sistemas Informáticos en las instalaciones para los cadetes de la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2019.

1.3.2.2 Objetivo Específico 2

Determinar en qué medida la prevención de ataques cibernéticos se relaciona con la Seguridad de los Sistemas Informáticos para los cadetes de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2019.

1.4. Justificación de la investigación

1.4.1. Justificación teórica

Los ataques cibernéticos no son solo problemas de las instalaciones militares, también el Estado se involucra en este tema, por ello con el

objetivo de fortalecer la seguridad informática, el 22 de octubre del año 2013 el Gobierno nacional aprobó la ley N° 30096 – Ley de Delitos Informáticos. Capítulo II, Art. 2 Acceso ilícito a la información: "El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado". Capítulo II, Art. 3 Atentado contra la integridad de datos informáticos: "El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa". Capítulo II, Art. 4 Atentado contra la integridad de sistemas informáticos. "El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

1.4.2. Justificación metodológica

Con esta investigación ayudaremos a fomentar una cultura de prevención y detección de riesgos cibernéticos en las instalaciones de los cadetes de Inteligencia de la Escuela Militar, se dará a conocer sobre el peligro que representa no estar preparado para los diferentes ataques cibernéticos que existen actualmente y se brindará información de cómo elaborar los planes de acción y estrategias basadas en minimizar los riesgos.

1.4.3. Justificación practica

Esta investigación es importante porque los estudios realizados por los cadetes de inteligencia en ciberseguridad señalan que los ataques cibernéticos han evolucionado, los hackers están desarrollando softwares maliciosos, cada vez más sofisticados con el fin de buscar vulnerabilidades en los sistemas interconectados para sustraer información digital con el fin de lograr su objetivo. Para ello aplicaremos la elaboración de planes, acciones y estrategias para minimizar los riesgos, las instalaciones tendrán el enfoque necesario para establecer un sistema informático que garantice la seguridad cibernética.

1.5. Limitaciones

Para realizar la investigación nos encontramos con diversas limitaciones, una de ellas es el tiempo, ya que las actividades de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" ocupan gran parte del tiempo disponible para la ejecución de este trabajo. Asimismo, limitado acceso a bibliotecas públicas y privadas por el régimen de internado vigente.

1.6. Viabilidad de la investigación

La presente investigación fue viable ya que se contaron con los siguientes recursos:

1.6.1. Humanos

Se contó con los docentes especializados en Tecnologías de la información y comunicaciones (TIC) y docentes especialistas en Ciberseguridad y Ciberdefensa, los cuales permitieron acceder a las bases de datos e información sobre el estudio del arte, de la variable Ciberseguridad en las instalaciones y la variable Seguridad en los Sistemas Informáticos.

1.6.2. Financieros

Se contó con la capacidad económica suficiente para cubrir los gastos que demandaron la investigación.

1.6.3. Materiales

Se contó con bibliografía actualizada y relacionada con el tema de investigación. Si bien los antecedentes locales y nacionales fueron reducidos; en el extranjero, a través de la vía on-line, se ubicaron varias tesis que se relacionan con las variables de estudio y permitieron establecer el proceso de discusión de los resultados. Estas tesis fueron presentadas en la sección de antecedentes de la investigación.

CAPITULO II. MARCO TEÓRICO

2.1 Antecedentes

2.1.1 Investigaciones realizadas en el ámbito internacional.

Valdebenito (2018), artículo científico: "Un fantasma recorre la web. Aproximación crítica al trabajo digital y cibervigilancia". El objetivo del presente trabajo es introducir al debate entre el tecno-entusiasmo y el tecno-escepticismo, y la necesidad que esto implica a la hora de formular estrategias de intervención que lidien con problemas vinculados a Internet. Se sostiene una hipótesis doble: que Internet, como red de circulación de información, refleja las dinámicas de explotación propias de la economía global capitalista; y que pensarla como espacio de libertad, constituye una mitificación de esta en omisión del contexto general de lucha de clases que la configura y da soporte. Nociones como las de "prosumidor" y "trabajo digital" permiten entender la concatenación y características de los distintos procesos presentes en la cadena de valor de la industria de hardware y software, vital para su funcionamiento. De tal modo, la consideración sobre problemas como ciberamenazas no puede realizarse desde fetiches tecno-céntricos, sino mediante un análisis de sus funciones en cuanto a niveles y procesos partes de una economía política digital extendida globalmente. Las conclusiones indican que Internet expresa contradicciones propias del régimen de producción capitalista, y se invita a la discusión sobre las tácticas que podrían articularse ante ellas.

León, Castellano y Vargas (2006), artículo científico: "Valoración, selección y pertinencia de herramientas de software utilizadas en vigilancia tecnológica. Revista de ingeniería e investigación. Facultad de ingeniería, Universidad nacional de Colombia. El entorno actual de desarrollo industrial y empresarial ha planteado la necesidad de incorporar en el aparato productivo distintos elementos diferenciadores que permitan anticipar los cambios tecnológicos. En este contexto, la vigilancia tecnológica (VT) surge como una

metodología enfocada a analizar estos cambios para identificar retos y oportunidades, apoyándose principalmente en las tecnologías de la información (TI), mediante la búsqueda, captura y análisis de datos e información. El presente artículo propone generar criterios para la escogencia y la utilización eficientes de las herramientas de software con distintas características, requerimientos, capacidades y costos, que pueden ser utilizados en la vigilancia. Inicialmente se realiza una aproximación a los distintos modelos desarrollados en VT, haciendo énfasis en la identificación y análisis de las diversas fuentes de información, por su cobertura, aporte al proceso de vigilancia, tipo de insumos informático y acceso. Posteriormente se proponen algunos criterios para la valoración, selección y análisis de pertinencia por contexto, de acuerdo al perfil y necesidad individual de cada institución o sistema productivo, para el uso de este tipo de herramientas. Finalmente se describen algunos de los paquetes de software existentes en el mercado para la realización de proyectos de vigilancia, relacionándolos con su complejidad, sus características de proceso y sus costos.

Araujo (2015), tesis para optar el Título de Ingeniero: “Implementación de un sistema de videovigilancia para los exteriores de la Universidad Politécnica Salesiana, mediante minicomputadores y cámaras Rapsberry”. La presente investigación tuvo como objetivo general el implementar y articular el sistema de video vigilancia para solucionar una parte importante del problema de la seguridad ciudadana en el distrito de Pueblo Libre entre el 2016 y 2020, la que tiene a cargo la Gerencia de Seguridad Ciudadana de la Municipalidad, que cuenta con un aproximado de 200 trabajadores, y una cantidad aproximada de 189 equipos de video vigilancia, habiendo concluido y recomendado la cantidad y tipos de equipos de video vigilancia que faltan, los puntos sensibles donde se requieren las cámaras, la descentralización del centro de control y la articulación con la Policía Nacional, Serenazgo y los Comités de Juntas vecinales del distrito de Pueblo Libre. El método utilizado en la investigación es el deductivo, de enfoque cualitativo, el diseño es de estudio de casos, hermenéutico Interpretativo, cuya información es de un período específico, que se desarrolló al aplicar las preguntas de acuerdo al problema del tema en

investigación y el cuestionario de entrevista no estructurada, que brindaron información sobre cámaras de video, del incremento, la descentralización, los puntos sensibles y la articulación con la Policía, serenazgo y la juntas vecinales, que realizado el diagnostico se pudo determinar que puesta en práctica este estudio de investigación, se puede obtener la respuesta oportuna para la emergencia en el distrito. La investigación recomienda que, para proponer una buena seguridad en el distrito de Pueblo Libre, se requiere de seis (06) centrales de control de Video Vigilancia descentralizados, aparte del centro de control principal, la instalación de sesenta (60) equipos de cámaras de video vigilancia, en los lugares recomendados y la coordinación con Serenazgo, PNP y Juntas Vecinales.

2.1.2 Investigaciones realizadas en el ámbito nacional.

Sierra (2017), Tesis para optar el grado de Maestro: "Propuesta del sistema de videovigilancia en la seguridad ciudadana del distrito de Pueblo Libre 2016-2020". Escuela de Postgrado, Universidad César Vallejo. La presente investigación tuvo como objetivo general el implementar y articular el sistema de video vigilancia para solucionar una parte importante del problema de la seguridad ciudadana en el distrito de Pueblo Libre entre el 2016 y 2020, la que tiene a cargo la Gerencia de Seguridad Ciudadana de la Municipalidad, que cuenta con un aproximado de 200 trabajadores, y una cantidad aproximada de 189 equipos de video vigilancia, habiendo concluido y recomendado la cantidad y tipos de equipos de video vigilancia que faltan, los puntos sensibles donde se requieren las cámaras, la descentralización del centro de control y la articulación con la Policía Nacional, Serenazgo y los Comités de Juntas vecinales del distrito de Pueblo Libre. El método utilizado en la investigación es el deductivo, de enfoque cualitativo, el diseño es de estudio de casos, hermenéutico Interpretativo, cuya información es de un período específico, que se desarrolló al aplicar las preguntas de acuerdo al problema del tema en investigación y el cuestionario de entrevista no estructurada, que brindaron información sobre cámaras de video, del incremento, la descentralización, los

puntos sensibles y la articulación con la Policía, serenazgo y la juntas vecinales, que realizado el diagnostico se pudo determinar que puesta en práctica este estudio de investigación, se puede obtener la respuesta oportuna para la emergencia en el distrito. La investigación recomienda que, para proponer una buena seguridad en el distrito de Pueblo Libre, se requiere de seis (06) centrales de control de Video Vigilancia descentralizados, aparte del centro de control principal, la instalación de sesenta (60) equipos de cámaras de video vigilancia, en los lugares recomendados y la coordinación con Serenazgo, PNP y Juntas Vecinales.

Obregón (2016), Tesis para optar el título profesional de Ingeniero de Sistemas: "Seguridad y monitoreo basado en cámaras IP para la institución educativa La Libertad, 2016". Desde los años 90, los sistemas de vigilancia basada en cámaras IP han sido un importante factor para la seguridad y prevención de robos. Estos sistemas constan, principalmente, de una cámara que se encarga de capturar la imagen, un monitor donde se controla la información, las cámaras IP tienen la particularidad de grabar en su memoria; ya que es necesario para almacenar los videos e imágenes capturados. El tema de investigación trata sobre: "Seguridad y monitoreo basado en cámaras IP para institución educativa La libertad de Huaraz en el año 2016". El objetivo es diseñar un sistema de video vigilancia utilizando tecnología IP que mejore la percepción sobre el control y seguridad en la institución educativa La libertad de Huaraz en el año 2016, el cuál permita vigilar y controlar a toda la población Libertana para así poder disminuir los problemas que aquejan.

2.2 Bases teóricas.

2.2.1 Seguridad en los Sistemas de Información de Vigilancia

2.2.1.1 Empleo del internet.

En estos tiempos el Internet ha superado todas las incógnitas mediante la

gran gama que nos brinda, con todos los servicios de los cuales podemos encontrar con tan sólo escribir una simple palabra en el buscador, hasta los diferentes aspectos que relaciona a dicha definición.

Valdebenito (2018) manifestó en su teoría, que el Internet se centraliza mediante la implementación de las reglas por un conjunto de protocolos que garantiza de una manera eficiente las redes físicas de una manera globalizada, pero sin dejar de utilizar la lógica que muy importante para un alcance en el aspecto mundial del conocimiento (p.40).

En el diccionario de la RAE (2014) se le considera al Internet como una conexión entre todas las computadoras mediante el protocolo de uso, para su comunicación de una manera muy rápida y eficaz al momento de interactuar información unas con otras (p.25).

Para poder enfatizar mejor el tema podemos decir que en un entorno globalizado las computadoras se conectan o interactúan entre ellas mediante la interconexión mediante los enlaces, sea éstas en redes grandes con redes pequeñas. Porque tienen un lenguaje garantizado, enfocándose mediante los protocolos para repartir dichos recursos al momento de especificar una orden se conoce como TCP/IP.

2.2.1.2 Servicios de internet

La red posee una serie de servicios que, en mayor o menor medida, tienen que ver con las funciones de información, comunicación e interacción. Algunos de los servicios disponibles en Internet son:

a) Buscadores
b) correo electrónico
c) wikis
d) foros Web
e) chat

f) redes sociales
g) Weblog, blogs o bitácoras Valdebenito (2014) p. 45.

Para León, Castellanos y Vargas (2006) lo clasifica de la siguiente manera:

a) World Wide Web
b) Correo electrónico
c) Listas de distribución
d) Foros web (e) Weblog
e) Transferencia de archivos FTP
f) Intercambio de archivo P2P
g) Archie
h) Chats o IRC (InternetRelay Chat), audio y videoconferencia, mensajería instantánea y llamadas telefónicas vía Internet
i) Gopher
j) (f) redes sociales
k) (g) wikis.

Algunas palabras del entorno tecnológico que se utiliza cuando se trabaja en el Internet:

- Buscadores.
- Wikis.
- Correo electrónico.
- Redes sociales.

2.2.1.3 El trabajo digital.

Las transformaciones asociadas a la masiva adopción de dispositivos inteligentes en el mundo actual plantean una serie de desafíos altamente complejos en su estudio e intervención Valdebenito (2018). Internet, en tanto red de circulación de información, no puede ser entendida como elemento

abstraído de las lógicas que operan sobre los fenómenos constitutivos de la realidad concreta, sino como reflejo o extensión de ellos Ferré (2006) p.56. Si bien existen vulnerabilidades que son propias de su infraestructura, estas no son fetichizadas tecnocéntricamente, sino que son estudiadas a partir del modo en que son explotadas en un contexto económico y político general. En dicho proceso se involucran tantos actores como usuarios de Internet existen, resumidos en gobiernos, corporaciones y sociedad civil Ferré, (2006) p.67.

Pese a que el diseño de la red de redes se ha desarrollado en un proceso en el que se distinguen ciertos intereses clave que configuran su código técnico, no se le debe esencializar positiva o negativamente, sino que se debe estudiar como parte de una totalidad histórica, económica, política y cultural. Internet se puede entender como una herramienta que evidencia diferentes contradicciones en su uso. Por ejemplo, el problema de la vigilancia masiva sobre la población, y el lucro derivado de la explotación de los datos producidos por millones de internautas (Ferré, 2006, p.48). Datos que son apropiados y explotados por corporaciones de diferentes industrias —publicitaria y tecnológica principalmente— transformándolos en información dotada de valor comercial y financiero. En base a la plusvalía derivada del trabajo digital, compañías como Facebook o Google se enriquecen en base a la especulación realizada sobre los datos recolectados de sus usuarios, conformando una estructura de clases entre propietarios de plataformas y proletariados digitales no reconocidos como tal, este problema se entiende como extensión de dinámicas de explotación propias del mundo offline.

De igual modo, prácticas como robos bancarios cometidos por delincuentes informáticos constituyen una mera extensión de lógicas de funcionamiento del mundo offline, y no fenómenos originados por la red de redes. El ciberdelito, por lo tanto, no corresponde esencialmente a algo nuevo y, tal como en el mundo fuera de línea, justifica la introducción de sofisticados sistemas de cibervigilancia Morcillo (2003) p.69. La infraestructura de Internet, controlada por gobiernos y corporaciones, además de monitorear todas y cada una de las acciones realizadas por los usuarios de la red, cumple

una función política de control y económica de explotación. La crítica ante ello, proveniente desde el panopticismo, indica que la gestión de la infraestructura técnica de Internet es formulada y empleada con propósitos de control biopolítico. Pero en el fondo, lo que justifica la introducción de millonarias inversiones en su perfeccionamiento deriva de los beneficios económicos, comerciales y financieros, percibidos por corporaciones de la industria digital. La respuesta orquestada desde ciertos sectores de la sociedad civil ante ello ha sido articulada acudiendo a valores culturales individualistas y políticos democráticos. Por ejemplo, demandas por privacidad y transparencia en línea expresan sus limitaciones en no englobar adecuadamente la complejidad que el fenómeno implica desde su origen hasta la configuración de su actualidad.

Según Morcillo (2003) p.69, de reducirse a una cuestión basada puramente en la protección del anonimato en Internet, los intentos de intervención serán limitados. La Deep web, así como diferentes técnicas criptográficas, permiten conservar el anonimato en Internet; pero el problema no se reduce a ello, sino a todas las condiciones de precariedad y explotación situadas en los distintos procesos productivos de la cadena de valor de la industria digital. La infraestructura de Internet se configura a partir de una compleja y enorme red de servidores, cables submarinos, antenas, satélites, entre otros. La cadena de producción involucra diversos procesos de explotación medioambiental y de mano de obra, entre las que se encuentran industrias extractivas de minerales como cobalto, litio y oro, y de fabricación en compañías como Foxconn, conocida por sus deplorables condiciones de trabajo, millonarias ganancias que aumentan año a año y gigantescos clientes directos como Apple, Microsoft o Samsung. Sus instalaciones juegan un rol fundamental en la demanda tecnológica contemporánea.

Si a lo anterior se agregan los procesos de desecho acelerado por obsolescencias programadas y su daño ambiental, se ilustran las contradicciones internas de los procesos de valorización y acumulación de una economía de capitalismo digital Morcillo (2003) p.77. Operando desde la base de un régimen altamente globalizado en el que gobiernos compiten por atraer

inversión extranjera abaratando costos laborales y medioambientales de producción, la precarización de estos parece ser la tendencia mundial de todo proceso productivo. Pero el capital encuentra formas de explotación y apropiación de ganancias no sólo a partir de las fuerzas productivas, sino también desde la mercancía donde se originan términos como el de prosumidor o de consumidor productivo como parte de una economía digital extendida globalmente Morcillo (2003) p.78. La gestión de la infraestructura de Internet, debido a sus altos costos de instalación y mantenimiento bajo el orden actual, es propiedad de las mismas corporaciones propietarias del tráfico de la red. Compañías como AT&T y Google establecen un oligopolio de la red, ante el que gobiernos y otras instituciones regulatorias adhieren mediante diferentes estrategias de cooperación. Guiados por la superación de brechas digitales y de desarrollo de infraestructura de telecomunicaciones a nivel territorial, terminan reproduciendo las lógicas de explotación y acumulación que las sustentan.

Las agencias de seguridad gubernamental también explotan sus propios beneficios, además de la explotación derivada del control del tráfico de datos por parte de corporaciones, se han identificado diferentes tácticas como la weaponization en contextos generales de ciberguerra. Dicha práctica convierte ordenadores, mediante exploits u otros malwares, en armas para la ejecución de tácticas de ciberguerra, ciberdelito o ciberterrorismo, ejemplificando la fragilidad en las distintas fases de la edificación de este sistema sociotécnico Morcillo (2003) p.85. Ahora bien, esto no debe conducir a la generación de un fetiche esencialista ni determinista de Internet en un sentido positivo o negativo. Internet no es por sí mismo explotación, vigilancia o libertad. La traducción práctica de esta idea es que, tanto diagnósticos como intervenciones realizadas sobre los problemas dados en el funcionamiento de Internet, no se pueden centrar en la cosa en sí. Ello significaría un reduccionismo inadecuado para abordar tanto los desafíos conceptuales de su delimitación como las prácticas para la solución de sus problemas.

A un fenómeno multidimensional - como lo es la configuración y funcionamiento de Internet - se debe aplicar un análisis que articule a lo menos

tres dimensiones o niveles fundamentales. El primero de ellos, y que posee cierta centralidad respecto de los dos siguientes, corresponde al económico y, en específico, a las distinciones acerca de los distintos procesos de valorización que ocurren en Internet. Le sigue el político, en el que se despliegan diferentes tácticas orientadas a consolidar un aparato institucional y jurídico encargado de normalizar el curso de las actividades del nivel económico. Finalmente, se encuentra el cultural en el que se comprenden todos los procesos propios de la configuración de un sistema de creencias, valoraciones, imaginarios y/o representaciones, desde los cuales se legitima la ordenación de los dos primeros. Las discusiones relativas a problemas derivados de la existencia de ciberamenazas deben considerar tales elementos de contexto para lograr su adecuada delimitación.

La relevancia de ello radica, en que usualmente las alternativas que formulan estrategias de protección de los "usuarios" de la red omiten aspectos económicos, políticos y culturales de fondo (Morcillo, 2003, p.83). Promoviendo, por ejemplo, derechos de privacidad basados en valores neoliberales de responsabilidad individual y/o de participación en espacios democráticos. La limitación de estos es que al ignorar las condiciones de explotación que dan soporte a Internet, sus propuestas no permiten terminar con su problema de base: la monopolización de la infraestructura y del tráfico de datos de la red. Elementos como ciberamenazas deben comprenderse desde una economía política digital por sobre concepciones tecnocéntricas, pesimistas o entusiastas. El potencial de ello es caracterizar las funciones que cumplen ciertas prácticas englobadas en nociones como ciberterrorismo, ciberdelitos, o cibervigilancia en procesos de valorización, de conformación de estructuras regulatorias, o de promoción de principios valóricos, imaginarios, creencias o representaciones.

2.2.1.4 La vigilancia tecnológica.

La vigilancia tecnológica (VT) es un concepto inherente a la gestión de tecnología (GT), la cual involucra procesos de planeación, dirección, control y

coordinación del desarrollo e implementación de la información para entender y anticiparse a los cambios tecnológicos, haciendo una detección temprana de eventos que representan oportunidades o amenazas potenciales. Sin embargo, su concepto trata no solo con la identificación desde el punto tradicional de detección, sino que de acuerdo con los recursos de las empresas y su personal, puede tener distintos alcances y significados como Escorsa y Maspons (2001) p. 36: a) vigilancia pasiva (scanning), cuya intención es descubrir información de interés para la empresa en diferentes fuentes de información; b) vigilancia activa (monitoring), búsqueda regular de información sobre actividades seleccionadas, para proveer un conocimiento actual, este tipo de vigilancia puede enfocarse a la búsqueda puntual de un determinado tema (search); c) whatching: Siendo el significado más general incluye tanto al scanning como al monitoring, e incorpora un trabajo de observación, análisis y difusión de la información.

De esta manera, la Vigilancia Tecnológica implica un trabajo importante de análisis en términos de definir los avances en las distintas áreas tecnológicas, difundirlos a la gente correcta y apoyar en la toma de decisiones estratégicas. Estos métodos de anticipación requieren a su vez de esquemas de búsqueda de información que permitan abordar de manera eficiente la consecución de información del entorno y traducirlo en conocimiento tal para solventar las necesidades y retos del desarrollo tecnológico, los cuales no siempre son correctamente identificados y adecuadamente implementados en modelos de gestión, conduciendo generalmente a una ausencia en los resultados efectivos. Identificar y definir una necesidad real y clara de información presenta uno de los mayores desafíos en términos de priorizar lo que es clave de ser objeto de vigilancia, en el ámbito tecnológico.

Escorsa y Maspons (2001) p. 39 señala que en cada proyecto desarrollado en Vigilancia Tecnológica asocia permanentemente y de manera individual distintas problemáticas, recursos, conocimiento, etc., lo que conlleva a caracterizar un número limitado de áreas de estudio. Empleando la metodología de factores críticos de vigilancia (FCV) - desarrollados en 1979

por Rockard - que definen áreas estratégicas de las organizaciones productivas, es posible identificar los factores a vigilar. Tomando como punto inicial estos factores, se establecen los procesos clave para la consecución de la información, el procesamiento, análisis y difusión de los resultados, lo cual a su vez permite definir elementos estratégicos que soporten una toma adecuada de decisiones en cada factor analizado. El modelo se fundamenta en un proceso de retroalimentación que vuelve a iniciar una vez que la organización ha definido una nueva necesidad de información. Finalmente, Escorsa y Maspons (2001) p. 42 plantean un proceso de VT enfocado en el análisis de fuentes documentales como las bases de datos, y lo trasladan a un espacio en el cual el diseño de estrategias conduce necesariamente a generar impactos en distintas áreas del desarrollo tecnológico.

De manera análoga a un sistema o modelo de computación, en el cual la calidad de los resultados depende en gran medida del insumo con el que son alimentados, la validez de los resultados de la vigilancia tecnológica depender· de las fuentes de información, sus procesos y herramientas de análisis, así como de la competencia del equipo de profesionales responsables del proyecto. Por ello es relevante tener fuentes de información confiables y adecuadas para soportar eficientemente cada fase de la vigilancia y de esta manera reducir el tiempo de análisis y toma de decisiones acertadas.

2.2.1.5 Disponibilidad de información.

Las fuentes de información, siendo uno de los factores que más influyen en la calidad de los resultados de una vigilancia, se pueden clasificar, de acuerdo con su acceso o posibilidad de procesamiento, en dos grupos: 1) Fuentes de información física: entre ellas se destacan las visitas a ferias y exposiciones, entrevistas con expertos en el tema, visitas técnicas, seminarios, talleres, entre otros. Este tipo de fuentes se convierten en un aliado estratégico muy valioso cuando se dirigen a la toma de decisiones. 2) Fuentes de información online: surgen principalmente con la aparición de la Internet; su

disponibilidad en medios digitales facilita ampliamente acceso, socialización, almacenamiento y procesamiento de información. Este último tipo de fuentes se ve representado, por ejemplo, en innumerables bases de datos (artículos, revistas, patentes, etc.), las cuales, además de organizar grandes volúmenes de información, permite en muchos casos su acceso libre o a bajos costos. Antes de la aparición de la internet, la búsqueda de información era un proceso extenso, dispendioso y con limitaciones de cobertura Bahamón (2016) p. 44.

Esta tecnología derivó no solo en una reducción del tiempo, sino en una avalancha de datos e información. Destaca el conocimiento técnico de la humanidad registrado en patentes, este se incrementa anualmente en aproximadamente unas 600.000. Siendo el objeto de interés las fuentes de información disponibles electrónicamente y la literatura científica y tecnológica, estas se pueden agrupar a su vez en dos subgrupos de acuerdo a la calidad de la fuente: a) Fuentes informales: son de contenido de libre acceso, pero no tienen un respaldo técnico definido en cuanto a su construcción, datos de origen y procesamiento. De este tipo se encuentran las charlas u opiniones en foros electrónicos, la información de diferentes páginas web que no tengan un asidero real; b) Fuentes formales: Son fuentes confiables, que pueden ser usadas con fines de vigilancia sin necesidad de corroborarlas, como, entre otras, los artículos científicos, las patentes, las bases de datos Bahamón (2016) p. 46.

Este tipo de fuente es la más recomendable de usar como un insumo adecuado para realizar proyectos de vigilancia para el desarrollo tecnológico. Bases de datos de artículos científicos: constituyen una de las principales herramientas para realizar seguimiento de las tecnologías más recientes dado que en algunos casos los temas que abordan son previos al desarrollo de patentes relacionadas. Adicionalmente, son elementos más científicos que técnicos dado que su aprovechamiento práctico no está demostrado. Entre las posibilidades que ofrece el uso de los artículos científicos como insumo de los proyectos de VT están: a) identificación de los autores, tecnologías y países; b)

Áreas temáticas de mayor desarrollo y emergentes; c) instituciones involucradas; d) fuentes de información adicionales (bibliografía); e) autores referenciados (bibliografía).

Bases de patentes: las patentes son uno de los tipos particulares de documento científico y tecnológico de mayor nivel de elaboración, donde se plasman los avances más importantes en cada área del conocimiento aplicado y del desarrollo tecnológico.

Las fuentes de información descritas anteriormente contienen, por lo general, extensas y elevadas cantidades de datos, lo que en VT resulta útil. Sin embargo, para efectos de análisis, costos y tiempo, resulta extenuante analizar cada registro obtenido como resultado de las búsquedas en las bases de datos, que en ocasiones pueden ser miles, razón por la cual es pertinente apoyarse en tecnologías que permitan efectuar las fases operativas de vigilancia con mayor agilidad y eficiencia Bahamón (2016) p. 53.

Las TI han tenido recientemente una evolución que las promovió de ser simples programas informáticos y máquinas, a ser soporte para las funciones de gestión, almacenamiento, análisis y comunicación de la información. Las TI involucran las nuevas tecnologías asociadas a Internet, el almacenamiento de datos, los sistemas de información, las comunicaciones, entre muchas otras, representado en: a) herramientas de búsqueda, localización, acceso, monitoreo y adquisición de información; b) tecnología de filtrado, captura, análisis y agregación de valor según las necesidades específicas, determinadas previamente; c) tecnología de registro, almacenamiento y recuperación contextual de la información, gestión documental; d) soporte para la segmentación y el mapeo de los recursos y necesidades de la organización, particularmente los recursos y necesidades de conocimiento y las actividades generadoras de conocimiento Bahamón (2016) p. 58.

2.2.1.6 Herramientas informáticas usados en los proyectos de vigilancia tecnológicas.

Sobre la base de un sistema de vigilancia o monitoreo, la adecuada definición de cada fase del proceso y de la correspondiente selección de las fuentes de información, las TI abordadas desde el punto de herramientas, cobran importancia en la medida que puedan ser integradas a los proyectos de Vigilancia Tecnológica. Sin embargo, por las características particulares de: los procesos productivos, las fuentes de información, los recursos tecnológicos y humanos disponibles, entre otros, es pertinente definir el tipo de herramientas informáticas que mejor se adecúan para cada situación. Las herramientas de VT constituyen un factor clave a la hora de traducir la información del entorno en resultados que se puedan involucrar en procesos de toma de decisiones; sin embargo, no es adecuado que estas se constituyan en el fundamento y base estructural de los procesos desarrollados. Conocer las características de estas herramientas brinda la posibilidad de identificar más acertadamente que tipos de fuentes se pueden consultar y los resultados que son factibles de obtener, reduciendo considerablemente tiempo y dinero. El principal enfoque se dirige hacia la búsqueda, análisis e interpretación de herramientas para fuentes informales Bahamón (2016) p. 76.

A nivel de criterios de valoración, las distintas herramientas de programas informáticos pueden ser definidas y analizadas en un conjunto de atributos, tanto funcionales (encaminados a la operación de la herramienta - procesos medulares), como no funcionales. Existen cinco atributos entre funcionales como no funcionales, de modo que se obtenga una idea general de las características de algunas de las herramientas de software que pueden apoyar los proyectos de vigilancia tecnológica: a) la descripción: general de la herramienta y sus principales características; b) el apoyo al ciclo de la VT: nivel de incidencia de la herramienta en cada fase; c) los procesos estadísticos asociados: elementos de procesamiento de la herramienta para establecer relaciones no triviales a través de procesamiento estadístico; d) el sistema: define la capacidad y los requerimientos de máquina y programas informáticos preinstalados para poder usar la herramienta (programa en ordenador, en servidor, mixto, etc.; e) el licenciamiento: costo y acceso a las

herramientas Bahamón (2016) p. 81.

Ficha Técnica para evaluar software de VT (vista previa de una herramienta)					
Producto:	Matheo Pathent			**Versión:**	3.0
Casa Productora:	Matheo Software			**Web:**	http://www.matheo-software.com/home_en.asp
Descripción General				 *Imagen de la herramienta*	
Descarga automáticamente la familia de patentes, creando automáticamente una base de datos Crea automáticamente las familias de patentes Genera gráficos de frecuencias y redes. Asiste al usuario en la conformación de clústeres Otros					
Vol de Información	Grandes Volúmenes				
Req. de Sistema	Win. 98/Me/NT4/2000/XP				
Arquitectura	Stand Alone				
Apoyo al ciclo de VT				**Licencia**	Demo (gratuito), Completo (€$600)
FASE				**Página de descarga**	http://www.matheo-software.com/home_en.asp
Planeación	X			**Procesos Estadísticos Asociados**	
Búsqueda	X			**Est. Básica**	Si
Análisis	X			**Est. Avanzada**	No
Inteligencia y Comunicación			X	**Tipo de Info.**	Estructurada → Patentes

	Ashton y Klevans (1997)		*Vargas y Castellanos (2005)*
	Necesidades Planeación de actividades Fuentes y Métodos	Planeación	Información previa Planeación
	Recolección de fuentes de información	Selección de las fuentes de información y Acopio	Preparación de la Búsqueda Búsqueda en bases de datos
	Análisis de Datos	Análisis	Depuración y convalidación de registros Procesamiento de Registros Análisis e Interpretación de los resultados
	Entrega de Información Evaluación de los resultados Uso de los resultados	Difusión de resultados Procesos de decisión Acciones	Diseño de estrategias Impactos

Tabla 1. Fases de los procesos de la vigilancia tecnológica.

Fuente: (Bahamón, 2016)

Tabla 2. Ejemplo de la valoración de una herramienta para la YT: Software Matheo Patent.

Fuente: Bahamón (2016)

2.2.1.7 Selección de las herramientas de software usados en la vigilancia tecnológica.

Posterior a la valoración, se deben comparar diferentes herramientas en función de su aporte en los procesos de vigilancia, teniendo en cuenta en su posible implementación los recursos en hardware y software requeridos, los costos, el capital intelectual necesario.

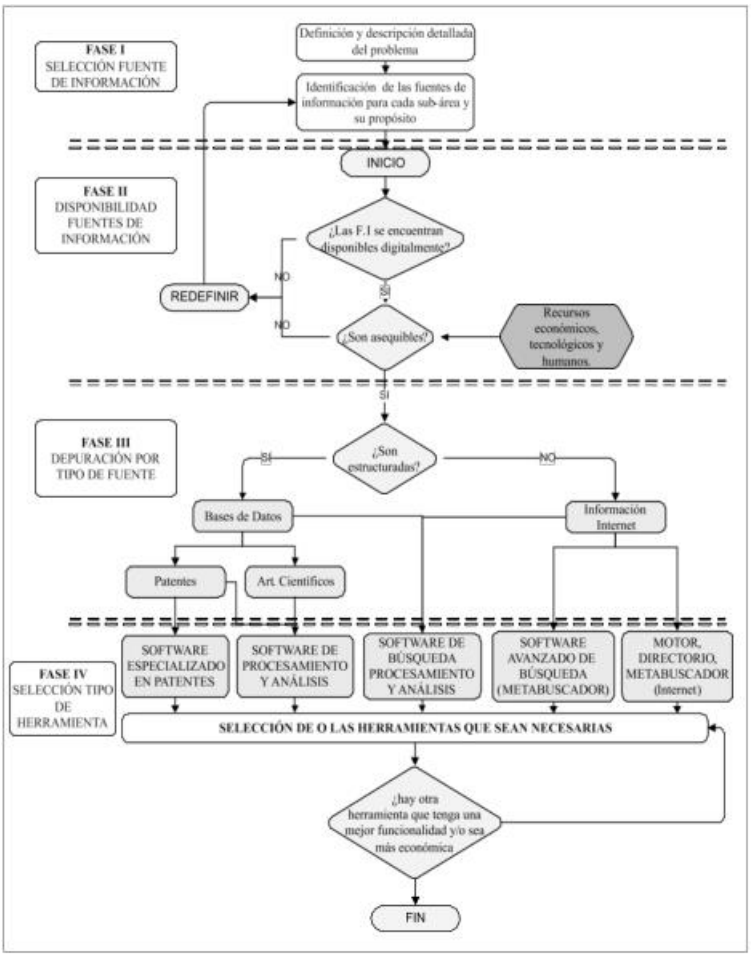


Tabla 3. Metodología para la selección de herramientas de *software* para la YT.

Fuente: Bahamón (2016)

FASE I - Selección fuente de información. Proveniente de la definición de los factores críticos de vigilancia - FCV, su importancia se centra en el establecimiento de los aspectos clave que definen la ejecución del proyecto. Para Bahamón (2016) p. 66, el planteamiento debido del problema ha de considerar un elemento descriptivo (problema - realidad - enforno), un elemento constitutivo (variables que inciden) y un elemento formal (cuerpo lógico de la investigación). En este último componente es relevante que el problema pueda ser descompuesto en aspectos cada vez más pequeños con la finalidad de poderlos evaluar en unidades más reducidas, "definir un problema significa especificarlo en detalle y con precisión. Cada cuestión y

aspecto subordinado que deban responderse han de ser delimitados. Deben determinarse los límites de la investigación. Con frecuencia es necesario revisar estudios previos con el objeto de determinar con exactitud lo que se ha de hacer".

FASE II: Acceso a las fuentes de información. Las distintas fuentes de información resultan útiles para los proyectos de VT en cuanto puedan ser procesadas y analizadas por el personal encargado de este elemento. De acuerdo con los distintos formatos en los que se disponen las fuentes de información consideradas anteriormente y en el marco del uso de las herramientas de *software*, resulta útil que estas estén disponibles digitalmente dada su facilidad de procesamiento, el amplio volumen de información tratado y su importancia establecida en la Fase I. En caso de no estar disponible una fuente clave para el proyecto de VT en este formato, se deben contemplar distintas posibilidades tecnológicas existentes de conversión, ya sea a través de medios como la transcripción o el escaneo, por mencionar algunos. Luego, un elemento prioritario que se debe tener en cuenta, son las condiciones de acceso real a esta fuente de información, las cuales no son generalmente sencillas de cumplir, por variables como el costo, por ejemplo, de las bases de datos de artículos científicos o de patentes.

FASE III: Depuración por tipo de fuente. Es una fase que define el tipo de programas informáticos que se requiere a las características de las fuentes de información determinadas. Como se mencionó, las fuentes de información tecnológica de tipo secundario podían ser determinadas en base a su contenido en tres grupos: páginas de internet, bases de datos de artículos científicos y de patentes, lo que puede reducirse por su construcción en dos grupos: información no estructurada (internet), información estructurada en bases de datos. De esta forma, en el caso de la información estructurada, permitirá acceder a un grupo más reducido y específico de herramientas de software (fase IV), pertinente para su procesamiento y análisis.

FASE IV: Selección del tipo de herramienta. Una vez abordados los

pasos anteriores, se debe seleccionar la herramienta adecuada para los proyectos de VT. En cuanto al tipo de información que pueden abordar los programas informáticos se estableció una clasificación subjetiva que los divide de acuerdo a si su especialización se encuentra en las páginas *web*, los artículos científicos, las patentes, o un conjunto de varios de ellos.

En este sentido, las herramientas se pueden clasificar desde la perspectiva de su uso en la vigilancia en cinco categorías:

1. Motores, directorios, metabuscadores disponibles en internet: constituyen una fuente de acceso a la información de una relativa buena calidad y son de acceso libre.

2. *Software* avanzado de búsqueda (metabuscador): programas que funcionan con las mismas características de los metabuscadores pero que ofrecen la posibilidad de generar análisis más detallados, guardar las búsquedas y generar reportes. Su acceso es más restringido, aunque ofrecen en su mayoría versiones demostrativas. Son programas de instalación en el computador

3. Software de búsqueda, procesamiento y análisis: en su mayoría aplicaciones complementarias a programas o paquetes de software de gran capacidad que analizan estadísticamente la información a fin de encontrar las relaciones más significativas. Son programas de instalación en el computador.

4. Software especializado en patentes: son programas desarrollados para evaluar cienciométricamente las patentes (exclusivamente) y determinar las relaciones más significativas. Son programas de instalación en el computador.

5. Software de procesamiento y análisis de información: son herramientas de orden superior en el ciclo de la vigilancia tecnológica, ya que, además de permitir la búsqueda de información en cualquier fuente, la procesan y

analizan a través de algoritmos complejos de acuerdo a las necesidades de información. Otorgan a su vez elementos para la formulación y solución de problemas, como las relaciones entre distintos elementos. Son programas de instalación en el computador.

2.2.2 Sistemas de Información de Vigilancia.

2.2.2.1 Procesos, cadenas y valores en Internet.

La rápida expansión global de Internet y su penetración en la cotidianidad del orden mundial ha generado un debate que es posible resumir entre dos posturas: el tecno-entusiasmo y el tecno-escepticismo. Cada una posee cierta heterogeneidad interna, la primera se caracteriza por la frecuente defensa del potencial democrático que significa la conformación de un escenario altamente tecnologizado en la era actual Bahamón (2016) p. 49). Por ejemplo, las tecnologías de información y de las comunicaciones (en adelante TICS) permiten empoderar a la ciudadanía en la difusión de abusos e injusticias que sufra por parte de los poderosos. Favoreciendo la libertad de expresión se pueden rastrear hitos clave en el uso realizado de dispositivos móviles y redes sociales de Internet durante las Primaveras Árabes como episodio revolucionario.

La crítica fundada desde el tecno-escepticismo apunta a develar los fetiches tecnológicos y la omisión de las variables estructurales de contexto que usualmente sostienen argumentos tecno-entusiastas. La conformación de un escenario globalmente integrado debe entenderse desde una perspectiva histórica y no puramente técnica. Ello permite problematizar el hilo de las decisiones políticas y económicas realizadas en torno a la inversión en desarrollo tecnológico. Al examinar con detención, muchas de ellas se enmarcan en el transcurso de diferentes tipos de conflictos comerciales, bélicos o sociales. Si se presta especial atención a cuestiones prácticas de acceso y dominio tecnológico en la sociedad es posible identificar la progresión de diferentes dinámicas de exclusión generadas en torno al dominio técnico, y no

al revés; expresadas en muchos casos, además, en el fortalecimiento de asimetrías de poder en términos geográficos.

El desarrollo técnico, bajo las condiciones de producciones globales y contemporáneas, exhibe en la práctica una orientación hacia la contribución de la acumulación de capital por parte de quienes lo comandan. Como parte de ciclos de producción económica, este parece colaborar más con el enriquecimiento de las corporaciones de la industria tecnológica que lo dirige por sobre la emancipación de los oprimidos del mundo. Pese a que se ha explorado en diversas investigaciones el vínculo entre el uso de redes sociales de Internet y ciclos de movilización ciudadana, este no está exento de contradicciones. En primer lugar, las movilizaciones sociales poseen una trayectoria que, si bien contiene cierta relación histórica con el desarrollo de medios técnicos de producción, distribución y circulación de información, no es estrictamente causal. Pareciera ser que su surgimiento responde más bien a la agudización de diferentes cuestiones políticas, como crisis de legitimidad de un sistema político, o económicas, como abruptas inequidades materiales en un país determinado.

A lo anterior se suman las denominadas brechas digitales referidas a la distribución desigual en el uso y manejo de recursos como TICS en la sociedad, posibles de describir siguiendo variables como edad, nivel educacional, zona de residencia (urbana o rural), entre otras. Constituye una limitación reconocida incluso por tecnoentusiastas. Suponer que la ciudadanía se configura en base a una distribución equitativa de recursos es un error puesto que la masificación del uso de TICS se traduce, en muchos casos, en la generación de nuevas asimetrías sociales. Esto constituye un arma de doble filo: empodera a quienes se familiarizan con ellas y discrimina a aquellos que no. Lo tecnológico, entendido desde una globalidad económica digital y distinciones tecno-escépticas, instala la duda acerca de si acaso es tan beneficioso como se plantea por el tecno-entusiasmo.

Hechos englobados por ellas corresponden básicamente a dos. En primer

lugar, la generación y reproducción de nuevas asimetrías al interior de la sociedad, en base a las inequidades de dominio o habilidades técnicas de los sujetos. Segundo, el beneficio corporativo y gubernamental en cuanto a explotación y vigilancia, derivado de la penetración de diferentes TICS, principalmente de aquellas smart. De tal modo, la valoración de lo digital como condición de posibilidad y realización del empoderamiento y/o emancipación se fundaría en un fetiche tecnológico, que además terminaría reproduciendo dominaciones de clase en base a la propiedad de los medios de producción tecnológica y digital. El tecno-optimismo representa, en resumen, un idealismo en vista de la omisión de las condiciones materiales que contextualizan el diseño y desarrollo de nuevas tecnologías. Igualmente es imposible entender el desarrollo tecnológico en su complejidad si se le piensa únicamente en términos técnicos.

Nociones como las de código técnico permiten examinar la naturalización técnica que se realiza de ciertos requisitos que ocultan en realidad propósitos culturales, económicos y/o políticos Bahamón (2016) p. 98. Ejemplos de ello pueden encontrarse en la configuración técnica de los smartphones, dotados hoy en día de dos cámaras web, tres micrófonos, sistemas de geolocalización GPS, y una vida útil que no supera los tres años. Es innegable que la comunicación es indispensable para la ciudadanía, sea en contextos de catástrofe o de movilización social, pero ¿Qué sucede cuando el diseño del hardware permite la implementación de tácticas opresivas por parte de agentes de seguridad del Estado? Desde este debate es posible entender que Internet se encuentra lejos de ser un medio colectivo de producción y circulación de información, sino que es diseñado, configurado y operado por agentes específicos como gobiernos y corporaciones. De hecho, las capas que conforman su arquitectura son propiedad de grandes corporaciones y consorcios internacionales, entre las que figuran compañías como Google, AT&T, y Facebook. Las que precisamente poseen la red de cables submarinos mediante los cuales fluye la información, o los balones de helio, propiedad de Google, que proveen de conexión Wi-fi a lugares remotos y proyectos de cables específicos como Tannat y Monet.

Por cuestiones de costo e inversión asociadas a la instalación, mantenimiento y actualización de lo que constituye finalmente la espina dorsal del Internet, resulta asunto exclusivo para agentes con capacidad de inversión de grandes capitales. Esto configura en la práctica un sistema altamente monopolizado en el que las mismas compañías propietarias de la infraestructura son las que controlan el tráfico de datos. Tales elementos difícilmente permiten sostener que Internet es sinónimo de libertad o emancipación social. Rastreando elementos fundamentales de su composición se hallan contradicciones presentes en diferentes niveles. La instalación de macrosistemas técnicos compuestos a partir de cables, servidores, antenas, entre otros, responde a decisiones que van más allá de parámetros técnicos. Interseccionadas con aspectos políticos y económicos, son recubiertas usualmente con discursos de inclusión y reducción de brechas digitales. El tecno-escepticismo permite enfatizar, al mismo tiempo, en los sucesos que marcan la gestión de acuerdos de cooperación intersectorial entre gobiernos y corporaciones.

Así, la constitución de un orden jurídico e institucional se realiza acorde al sostenimiento de procesos de producción y acumulación de datos tendientes a su explotación y valorización bajo lógicas comerciales y financieras capitalistas. Es el lucro derivado de los usos de la información producida por prosumidores en dispositivos de su manufactura, operados en sus servidores y bajo sus licencias de software en colaboración con organismos regulatorios, lo que conforma esta gran economía digital. Innovación, manejo de información y su posterior financiarización en bolsas de valores, conforman la puesta en marcha de un modelo de negocios basado en una economía de capitalismo digital. En tal aspecto se deben reconocer los intentos por implementar una economía política basada en criptomonedas como los bitcoins.

No obstante, y pese a basarse en Comunes, más que brindar soluciones a los debates sobre la crisis financiera, plantea interrogantes pertinentes de abordar una vez resueltos aspectos fundamentales de los intermediarios y

propietarios de la circulación de información en Internet. Tampoco es posible afirmar que Internet permite superar las inequidades socioeconómicas del mundo offline, por el contrario, al operar bajo lógicas comercial-financieras de producción y acumulación, las potencialidades que esta entrega se restringe a segmentos con capacidad adquisitiva, contraviniendo discursos pro inclusión y democratización de la red. Más aún, en la cadena de producción propia de dispositivos e insumos necesarios para su uso se encuentran grandes multinacionales de la industria manufacturera de hardware y softwares.

Contrario a la apreciación positiva que se pudiera tener de estas, se caracterizan, en general, por poseer regímenes laborales de alta precariedad. Foxconn, corporación taiwanesa y principal fabricante de componentes electrónicos, constituye su ejemplo por antonomasia. Con trabajadores suicidas que protestan por mejores condiciones laborales, clientes de renombre como Apple y Microsoft, y exuberantes ganancias lucrativas, ilustra patentemente las contradicciones internas del modo de producción capitalista en la industria tecnológica Bahamón (2016) p. 107. La procedencia de materias primas necesarias para la manufactura de dispositivos como teléfonos, computadores, o tablets, así como su posterior desecho, involucra también condiciones de rápido deterioro humano y medioambiental. Distinguible a partir de sucesos propios de la lógica extractivista presente en la industria minera de litio, cobalto y oro situada en el tercer mundo, ha implicado un alto costo a países africanos como el Congo. La demanda de materias prima aumenta en la medida que aparatos electrónicos son crecientemente requeridos por el mercado, lo que se traduce, además, en la generación de toneladas de chatarra tecnológica.

En tal sentido, si se consideran, por ejemplo, los diseños que contienen desarrollos que hablan de una obsolescencia programada, la situación empeora aún más. En el caso de la industria de softwares la precariedad y exclusión es vivida por desarrolladores de compañías de la India y Silicon Valley: Exigencia desmesurada, jornadas laborales que no dan espacio a descansos, despiadada competitividad entre empleados termina por ocasionar en muchos de sus trabajadores de cuello blanco síndromes de burnout. Ahora bien, en el caso de

la mano de obra de cuello azul, las labores de limpieza, mantenimiento de maquinaria y manipulación de objetos tóxicos, entre otras, son realizadas principalmente por mujeres y/o migrantes. Disfunciones respiratorias que van desde la silicosis al cáncer del pulmón, enfermedades a la piel, abortos espontáneos, y enfermedades congénitas expresan la reproducción de una economía política del trabajo racista y sexista que mutila trabajadores, destruye familias y el ecosistema. En consideración de los procesos involucrados en la configuración y manufactura de requerimientos necesarios para el uso de Internet ¿puede sostenerse que es sinónimo de libertad?, por lo que es necesario considerarla desde aspectos propios que configuran el funcionamiento de los procesos de movilización social.

En primer lugar, es difícil sostener que estos se encuentran determinados por la disponibilidad de TICS para quienes los ejecutan. Su lectura de los actos de censura gubernamental sobre Internet en el transcurso de las Primaveras Árabes sostiene que ante tal amenaza al ejercicio de libertades civiles se generó una efervescencia de masas. Violentos enfrentamientos entre civiles y fuerzas de orden público, intervención de la comunidad internacional, y derrocamiento de regímenes dictatoriales fueron consecuencias de tales acontecimientos. No obstante, la respuesta desde el tecno-escepticismo esbozada disecciona tal argumento. Su conclusión indica que las Primaveras Árabes no pueden ser entendidas en omisión de las condiciones históricas y estructurales en las que se sitúan. Su explicación enfatiza en las altas desigualdades económicas propias de los países de oriente medio, la existencia de un sistema político autoritario y centralizado, y la propagación de valores liberales de democracia y libertad. Sin caer en romanticismos de suma de factores, tales elementos deben articular una explicación realista sobre lo ocurrido, por sobre idealismos fundados en fetiches tecnológicos. Más aún cuando las condiciones sobre las que opera la propiedad de la infraestructura han contribuido a la generación de nuevas y perfeccionadas formas de control social cimentadas en la red de redes. Se trata de la cibervigilancia, la cual se comprende como parte de un complejo entramado de ciberamenazas para los usuarios de Internet.

2.2.2.2 Amenazas y seguridad en Internet.

El concepto de ciberamenazas remite a un conjunto heterogéneo y cambiante de riesgos existentes en la red, partes de un proceso de expansión y consolidación de una economía digital de carácter global Bahamón (2016) p. 102. El aumento de la cantidad de internautas, la cantidad de tiempo que estos permanecen conectados a Internet, y dispositivos de los que cada uno dispone, es manifestación del sostenido crecimiento de su productividad. La penetración de Internet se ha dado en diferentes áreas sociales y comerciales que van desde actividades lúdicas recreativas, operaciones financieras y gestión de sistemas fundamentales para el funcionamiento de una ciudad, hasta transporte o energía. Esto es problemático a la hora de considerar la vulnerabilidad propia de los sistemas informáticos que ha involucrado igualmente una extensión de los límites de la actividad delictual, originando diferentes repertorios de ciberdelitos.

Phising, pharming, robos a particulares mediante adulteración de cuentas bancarias, tráfico de armas, estupefacientes y/o pornografía, son algunos repertorios de los denominados ciberdelitos. La evolución de amenazas como estas, además de la introducción de nuevos virus y malwares aumenta a ritmos exponenciales. En 1994 se hablaba de la generación diaria de un nuevo virus, cifra que para el 2017 aumentó a 323.000 malwares diarios. Su importancia reside en que el rango de sucesos de acciones ciberdelictuales involucra igualmente ataques a las denominadas infraestructuras críticas. Comprendiendo aquellas redes de sistemas físicos y virtuales vitales para el funcionamiento de un país. Se destacan entre ellas instalaciones de servicios de emergencia, salud, agua, energía eléctrica, gasoductos, transporte, agricultura, financieros, comerciales, defensa, químicas, comunicación e información, entre otros.

No existe certeza sobre las eventuales consecuencias que tendría la ejecución de un bien planificado ciberataque sobre ellas. Todas ellas son vulnerables en contextos de ciberguerra o de ataques ciberterroristas Ferré (2005) p. 68.

Apagones masivos, descarrilamientos de trenes, descoordinación de vuelos aéreos, destrucción de datos bancarios e, incluso, pérdida de control de sistemas de gestión militar, serían parte de sus repertorios. Ejemplos concretos pueden rastrearse en el sabotaje del sistema de suministro eléctrico a Ucrania en el año 2005, del sistema bancario de Estonia en el año 2007 y del sistema nuclear de Irán mediante el malware Stuxnet Ferré (2005) p. 79.

Estos presuponen un manejo técnico por parte de quienes los ejecutan, quienes resguardan su privacidad empleando tácticas de criptografía y protegen el anonimato de sus acciones desde, por ejemplo, la Deep web Ferré (2005) p. 97. Dificultando su seguimiento por parte de policías y otros agentes de seguridad ciberdelictual, su existencia nutre el desarrollo de una compleja industria de ciberseguridad. Compañías como Kaspersky o Eset destacan en dicho ámbito, además de las acciones realizadas por diferentes ejércitos mediante sus departamentos de ciberguerra que han reaccionado ante las vulnerabilidades de los sistemas informáticos. La respuesta de estas se encamina actualmente en implementar procedimientos de monitoreo y mitigación de ciberataques, similar a las estrategias de policías del mundo offline. No obstante, las estimaciones para el año 2016 sobre los costos de sus daños indican un aproximado de US $400 billones, mientras que la inversión en ciberseguridad marca un aproximado de US $175 billones Ross (2016).

Estas acciones no corresponden a la aparición de prácticas o fenómenos nuevos debido a la introducción de nuevas tecnologías informáticas. El delito, el terrorismo, y la guerra poseen una historia muy anterior a ellas y, en dicho sentido, sólo representan expresiones de su actualización en la era digital. Suponer lo contrario sería caer en fetiches tecno-centristas. Ahora bien, lo que sí podría corresponder a algo relativamente reciente es la entrada de técnicas de vigilancia poblacional masiva desde gobiernos y corporaciones. Pese a los conocidos ejemplos del siglo XX del FBI de John Edgar Hoover, o la Gestapo, y la Stasi, el perfeccionamiento de lo que se entiende hoy por cibervigilancia es algo sin antecedentes. Para su ejecución se desarrollan acuerdos comerciales entre distintos agentes corporativos y gubernamentales como parte de una

economía política de la vigilancia, entre propietarios de la infraestructura y de los sistemas regulatorios vigentes. Ello ha contribuido a la popularización de ciertas iniciativas que sostienen que Internet, uno de los más grandes inventos de la humanidad, sería, pese a todo, un facilitador del totalitarismo. Sistemas como Echelon, Prism, Xkeyscore, y Tempora, además de la difusión de casos como el de Cambridge Analytica, ilustran tales nociones Ferré (2005) p. 96.

El escenario se configura a partir de actores que cumplen funciones específicas en procesos concretos de la conformación de una totalidad económica, política y cultural: las corporaciones se benefician de diferentes procesos de valorización de los datos producidos por los internautas, y, al mismo tiempo, agentes gubernamentales conforman sistemas políticos que permiten la operación de procesos productivos. En cuanto a la prensa y medios de comunicación, estos colaboran con conformación de un sistema de creencias que desplaza el conflicto de clases presente en tales procesos.

Para el tecno-entusiasmo la cibervigilancia, pese a todo, el enunciado de que Internet es un espacio de libertad. “Pese a ser vigilado, no puede ser controlado”, señaló Castells en una entrevista televisiva. Más allá de la lucha contra el delito, terrorismo, o carreras armamentísticas entre Estados, la construcción de sistemas de cibervigilancia constituye también una promesa de solucionismo técnico en sistemas proclives a modernizarse. Sistemas de iluminación, control de tráfico, entre otros, son proclives a la intervención de soluciones Smart a sus rendimientos. Pero el terrorismo no se detendrá por la introducción de más cámaras de vigilancia en las ciudades, ni el ciberterrorismo por el monitoreo de ciberamenazas, ya sea por vulnerabilidades internas de la infraestructura o por elementos que la sobrepasan. Igualmente, las soluciones de smart cities han estado lejos de contribuir, por ejemplo, a la eficiencia energética al estar cooptada por intereses conservadores de gobiernos y corporaciones, engendrando nuevas formas de estigmatización y criminalización espacial.

2.3 Definiciones de Términos Básicos

Ataques Cibernéticos de Países: Los problemas del mundo donde vivimos se extienden en el mundo del ciberespacio. Pocos años atrás se viene registrando ciberataques estratégicos como, por ejemplo, el ciberataque al País de Estonia en 2007 que produjo la inhabilitación pasajera de muchas instalaciones militares críticas, otro caso es el ciberataque del País de Rusia al País Georgia en 2008 el cual trajo como consecuencia la invasión terrestre, otro caso es el ciberataque al País de EEUU, el cual se descubrió que la base del ataque se encontraba en el territorio del País de China.

Ataques Cibernéticos de Empresas Privadas: Muchas empresas privadas tienen como obtener a como dé lugar obtener los procesos técnicos operarios industriales de otras empresas privadas o estatales las cuales representan una rivalidad.

Ataques Cibernéticos Terroristas, Absolutismo o extremismo de Política o de Ideología: Dichos terroristas y agrupaciones fanática extremistas emplean el espacio cibernético para planear sus operaciones, luego ejecutarlas y al final publicitarlas para demostrar su superioridad intelectual cibernética contra sus oponentes, esto con el fin de reclutar más partidarios para continuar con los ataques.

Ataques Cibernéticos de Bandas Criminales Organizadas: Las bandas del crimen organizado también conocidas como cibergangs han emprendido acciones en las redes de internet, básicamente en redes de internet privadas de empresas.

Ataques Cibernéticos de Hacktivistas: Desde el 2011, los hacktivistas han creado un movimiento masivo denominado “el hacktivismo”. Dicho movimiento se ha transformado en una de los riesgos más grandes para todas las organizaciones privadas y estatales de muchos países.

Ataques Cibernéticos de Bajo perfil: Estos ataques son realizados

comúnmente por individuos de un alto saber en las ciencias de la informática, y ello les permite llevar a cabo sus ciberataques por razones muy diversa como los son venganzas, sabotaje, rivalidades, investigación, cólera e ira de despido de la empresa, siempre son temas de motivo personal.

Ataques Cibernéticos de Personas con Accesos Autorizados: También conocidos como insiders, intruders o privilegiados, este segmento son unas de las mayores amenazas para la seguridad de la información en la entidades privadas y estatales de todos los países, por lo general son personas que están infiltradas en un una entidad o grupo y está descontenta o disconforme como el modo de pensar de la misma agrupación a la que pertenece, pero esta como integrante para poder robar la información sin mucho esfuerzo ya que cuenta con accesos a la red privada donde la información se encuentra. También se les pude señalar como espía infiltrado por un Estado enemigo de otro, también hay casos de empleados de la organización que son cautivados y contratados por bandas de terroristas o cibercriminales.

2.4 Formulación de hipótesis

2.4.1 Hipótesis general

El Sistema de información de vigilancia se relaciona significativamente con la Ciberseguridad en las instalaciones para los cadetes de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2019

2.4.2 Hipótesis específicas

2.4.2.1 Hipótesis específica 1

La gestión de la Ciberseguridad se relaciona significativamente con el sistema de información de vigilancia para los

cadetes de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2019.

2.4.2.2 Hipótesis específica 2

La Prevención de los ataques cibernéticos se relaciona significativamente con el sistema de información de vigilancia para los cadetes de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2019.

2.5 Variables

2.5.1 Definición conceptual

Variable independiente (x)

Sistemas de Información de Vigilancia:

La ciberseguridad es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. La Ciberinteligencia (Cyberintelligence en inglés o nuestro servicio CYBINT®) se refiere a las actividades de inteligencia en los procesos de la Ciberseguridad que se ocupan de analizar (Intenciones-oportunidades de los ciberactores) y prevenir, identificar, localizar y atribuir ataques o amenazas.

Variable dependiente (y)

Ciberseguridad en las instalaciones:

La Ciberseguridad en las instalaciones configura un conjunto de acciones preventivas y reactivas por parte de las organizaciones y sistemas

tecnológicos con el objetivo de proteger la información en pro de resguardar la confidencialidad, disponibilidad e integridad de datos.

2.5.2 Definición operacional.

VARIABLE	DIMENSIONES	INDICADORES
V (x) Sistemas de Información de Vigilancia	Gestión de la Ciberseguridad	- Infraestructuras tecnológicas - Gestión de conocimiento sobre seguridad e información - Diseminación de información - Interpretación de la información
	Prevención de los ataques cibernéticos	- Mecanismos de prevención y protección - Tipos de ataque cibernéticos - Tipos de defensa cibernética - Probabilidad de amenaza y magnitud de daño.
V (y) Ciberseguridad en las instalaciones	Analógico	- Nivel de seguridad - Capacidad de almacenamiento
	Digital	- Percepción sobre la mejora de control y seguridad - Velocidad del video a fin de promover una visión óptima en tiempo real

CAPITULO III.
MARCO METODOLÓGICO.

3.1 Enfoque de investigación.

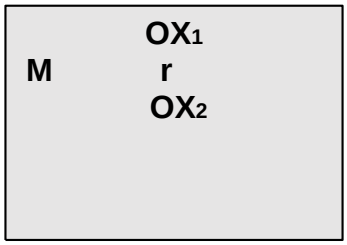
La investigación será de enfoque Cuantitativo, por cuanto será necesario dimensionar las variables del objeto de estudio, en dimensiones e indicadores para describir e inferenciar su correlación.

3.2 Tipo.

El tipo de investigación corresponde a la Investigación Básica, pues no tiene propósitos aplicativos inmediatos; busca ampliar y profundizar el caudal de conocimientos científicos existentes acerca de la realidad y pretende correlacionar las variables de estudio.

3.3 Diseño.

La investigación siguió un diseño no experimental**,** transeccional y descriptivo, dado que no se manipularon las variables de estudio, al contrario, se observaron tal y como se presentaron en su contexto natural, para después analizarlos. Los datos se recolectaron en un sólo momento y el propósito fue describir las variables, y analizar su incidencia e interrelación en un momento dado Hernández, R., Fernández, C. y Baptista, P. (1999). El siguiente esquema corresponde a este tipo de diseño:



Donde "M" es la muestra donde se realiza el estudio, los subíndices "X_1, X_2," en cada "O" nos indican las observaciones obtenidas en cada de dos variables distintas (X_1,X_2), y finalmente la "r" hace mención a la correlación que existentes entre variables estudiadas:

3.4 Método.

El trabajo de investigación, aplicó el método deductivo, el cual es el procedimiento o camino que sigue el investigador para hacer de su actividad una práctica científica. El método hipotético-deductivo tiene varios pasos esenciales: observación del fenómeno a estudiar, creación de una hipótesis para explicar dicho fenómeno, deducción de consecuencias o proposiciones más elementales que la propia hipótesis, y verificación o comprobación de la verdad de los enunciados deducidos comparándolos con la experiencia. Este método obliga al científico a combinar la reflexión racional o momento racional (la formación de hipótesis y la deducción) con la observación de la realidad o momento empírico (la observación y la verificación).

3.5 Población y muestra.

Debido a que la población de estudio es muy pequeña, se considera su totalidad como parte de la muestra, siendo un total de 120 cadetes de la Escuela Militar de Chorrillos.

3.6 Técnicas e instrumentos de la recolección de datos

3.6.1 Descripción de los instrumentos.

3.6.1.1 Cuestionario sobre el sistema de información de vigilancia.

3.6.1.1.1 Objetivo: Recoger las apreciaciones de los cadetes sobre los sistemas de información de vigilancia.

3.6.1.1.2 Estructura: el cuestionario considera 10 interrogantes organizada por dimensiones.

3.6.1.1.3 Analógico, Digital.

Criterio de confiabilidad valores	
No es confiable	-1 a 0
Baja confiabilidad	0.01 a 0.49
Moderada confiabilidad	0.5 a 0.75
Fuerte confiabilidad	0.76 a 0.89
Alta confiabilidad	0.9 a 1

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,763	10

El coeficiente obtenido es de 0.763, lo cual permitió decir que el test en su versión de 10 ítems tiene una baja confiabilidad.

Existe la posibilidad de determinar si al excluir algún ítems o pregunta del cuestionario aumente o disminuya el nivel de confiabilidad interna que presenta el cuestionario, esto nos ayudaría a mejorar la construcción de las preguntas u oraciones que utilizaremos para capturar la opinión o posición que tiene cada individuo.

Estadísticas de total de elemento

	Alfa de Cronbach si el elemento se ha suprimido
¿Cómo consideras que esta el nivel de seguridad en la Escuela Militar?	,678
¿Cómo consideras el nivel de control de seguridad en la Escuela Militar?	,678
¿Cómo percibes el nivel de riesgo que pone en peligro la vida o la integridad física?	,786
¿Cómo percibes la necesidad de adoptar medidas para garantizar la seguridad en la Escuela Militar?	,782
¿Cómo consideras que una solución tecnológica con cámaras IP puede mejorar el control y seguridad?	,678
¿Qué nivel consideras que una solución tecnológica puede contribuir para prevenir las situaciones de riesgo?	,791
¿Considera que con el sistema de información de video vigilancia se reducirían los robos y hurtos en la Escuela Militar?	,678

¿Considera que con el sistema de video vigilancia se reduciría los actos de desorden e indisciplina en la Escuela Militar?	,797
¿Considera que con la implementación del sistema de video vigilancia se mejorara el control y seguridad de la Escuela Militar?	,779
V(x) Sistema de información de vigilancia	,711

El cuadro anterior nos demuestra que el test en su totalidad presenta gran consistencia interna, lo cual no se modifica significativamente ante la ausencia de alguno de los ítems.

Este proceso compromete el deseo inequívoco de búsqueda de una mejora continua en el proceso de investigación, luego de varios tratamientos, consejos y reformulaciones de las preguntas alcanzaremos el siguiente nivel de índices con ausencia de los ítems.

3.6.1.2 Cuestionario sobre la Ciberseguridad en las instalaciones.

3.6.1.2.1 Objetivo: Recoger las apreciaciones de los cadetes sobre la Ciberseguridad en las instalaciones.

3.6.1.2.2 Estructura: el cuestionario considera 10 interrogantes organizada por dimensiones.

3.6.1.2.3 Gestión de la ciberseguridad, Prevención de los ataques cibernéticos.

3.7 Validez y confiabilidad de los instrumentos. (Anexo 4 y 5)

3.7.1 Cuestionario sobre el sistema de información de vigilancia.

Para comprobar la validez del instrumento, primero se sometió a juicio de expertos en el tema del sistema de información. Segundo se aplicó una prueba piloto a una muestra de 10 cadetes.

En cuanto a la confiabilidad se determinó la consistencia interna mediante el Alfa de Cronbach, cuyos resultados fueron los siguientes:

- Análisis de fiabilidad de la escala: 0.77
- El índice de consistencia es mayor (alfa = 0.65) y se le considero aceptable.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,568	10

El coeficiente obtenido es de 0.568, lo cual permite decir que el test en su versión de 09 ítems tiene una baja confiabilidad.

Existe la posibilidad de determinar si al excluir algún ítem o pregunta del cuestionario aumente o disminuya el nivel de confiabilidad interna que presenta el cuestionario, esto nos ayudaría a mejorar la construcción de las preguntas u oraciones que utilizaremos para capturar la opinión o posición que tiene cada individuo.

Estadísticas de total de elemento

	Alfa de Cronbach si el elemento se ha suprimido
¿En la escuela militar de chorrillos existen normas o practicas enfocadas en la ciberseguridad?	,567
¿Cree usted que la ciberseguridad sea importante en la escuela militar?	,474
¿Dentro de la escuela militar existe algún personal encargado de la ciberseguridad?	,579
¡En la escuela militar se realizan análisis de gestión de riesgos informáticos?	,567

¿Existen planes de contingencia ante un ciberataque?	,532
¿Sabe usted qué medidas tomar ante un ciberataque?	,596
¿existen herramientas que aseguran su información digital?	,474
¿En la escuela militar asignan presupuesto destinado a la ciberseguridad?	,532
¿en la escuela militar se realiza capacitación y prevención ante amenazas cibernéticas?	,587
V(y) Ciberseguridad en las instalaciones	,473

El cuadro anterior nos demuestra que el test en su totalidad presenta gran consistencia interna, lo cual no se modifica significativamente ante la ausencia de alguno de los ítems.

Este proceso compromete el deseo inequívoco de búsqueda de una mejora continua en el proceso de investigación, luego de varios tratamientos, consejos y reformulaciones de las preguntas alcanzaremos el siguiente nivel de índices con ausencia de los ítems.

3.7.2 Ciberseguridad en las instalaciones.

Al igual que él cuestionario se determinó la validez a través del juicio de los expertos en ciberseguridad sobre el promedio académico de los cadetes y las capacidades que deben evaluarse para lograr la competencia en las asignaturas. Se tomó referencia del mismo 10 cadetes que participaron en el cuestionario.

3.8 Métodos de análisis de datos.

Luego de establecida la validez de lis instrumentos, realizada por los expertos, se coordinó con las autoridades de la Escuela Militar de Chorrillos coronel Francisco Bolognesi, para la aplicación de dichos instrumentos.

Se aplicaron los instrumentos de la siguiente manera: primero el cuestionario sobre el sistema de información de vigilancia y una semana después Sobre la Ciberseguridad en las instalaciones.

Los datos se trasladaron a hojas de cálculo a través de una plantilla que se elaboró en base a los indicadores o ítems aplicados.

Con ayuda de un experto se procesaron los datos empleando el paquete estadístico SPSS V.22. se emplearon los estadísticos: promedio, desviación estándar y distribución de frecuencia. Para establecer la relación entre las variables se usó la prueba de Rho Spearman. Así como el coeficiente alfa de Cronbach para la fiabilidad de los instrumentos.

3.9 Aspectos éticos.

Esta investigación tomó en cuenta los principios jurídicos y éticos de una investigación original. Se respetó los créditos, las opiniones de terceros y toda propiedad intelectual de las fuentes consultadas a través de un registro de referencias de acuerdo al APA, 6ta edición en inglés y 3era en español, que evidencian que esta investigación es inédita.

La investigación también respetó los derechos de confidencialidad y las acciones realizadas para llevar a cabo esta; es decir, contó con el consentimiento de los participantes de la muestra.

CAPÍTULO IV
RESULTADOS:

4.1. Descripción.

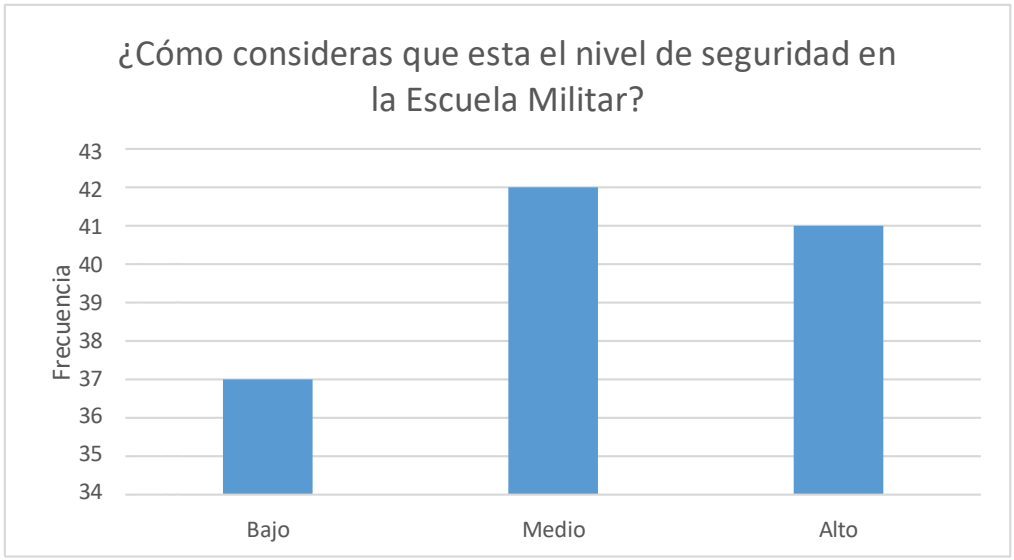
4.1.1. Variable N° 1.

Tabla Nª 4.-

¿Cómo consideras que esta el nivel de seguridad en la Escuela Militar?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	37	30,8	30,8	30,8
	Medio	42	35,0	35,0	65,8
	Alto	41	34,2	34,2	100,0
	Total	120	100,0	100,0	

Gráfico Nº 1.-



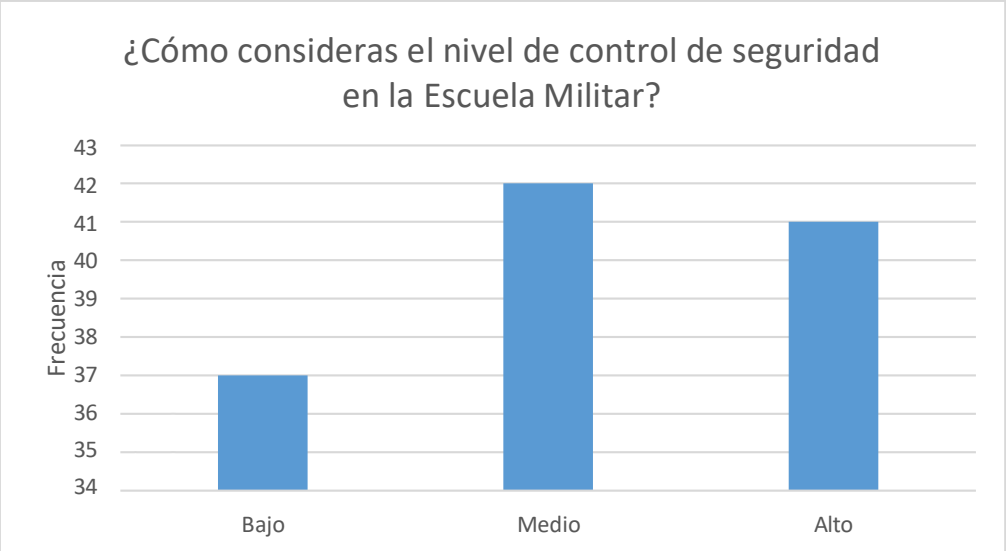
En el gráfico se puede observar que el 35% de los cadetes manifiestan que es medio el nivel de seguridad en la escuela militar, un 34% que es alto y un 30% manifiestan que es bajo. Esto refleja que en su mayoría los cadetes consideran que esta elevado el nivel de seguridad en la Escuela Militar.

Tabla Nº 5.-

¿Cómo consideras el nivel de control de seguridad en la Escuela Militar?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	37	30,8	30,8	30,8
	Medio	42	35,0	35,0	65,8
	Alto	41	34,2	34,2	100,0
	Total	120	100,0	100,0	

Gráfico Nº 2.-



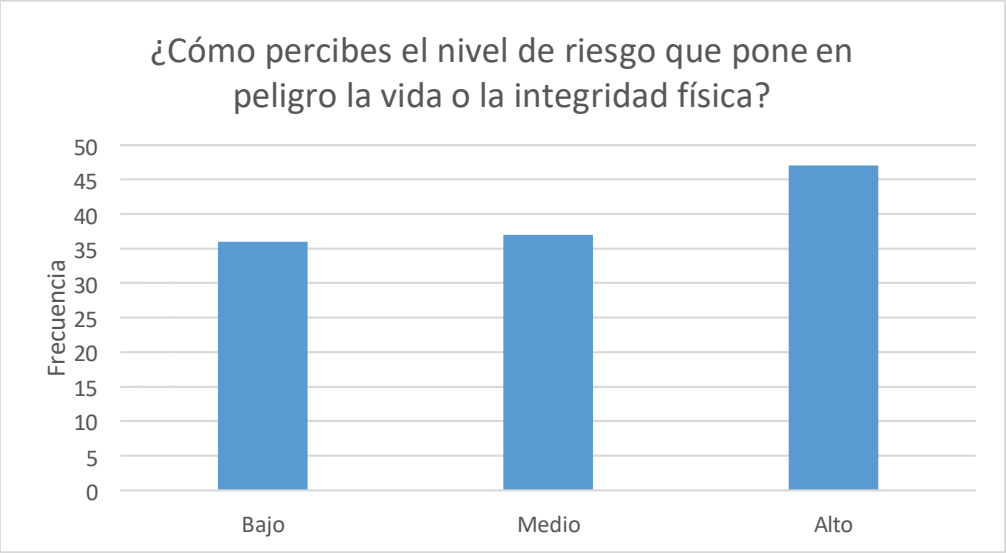
En el gráfico se puede observar que el 35% de los cadetes consideran que es medio el nivel de control de seguridad en la escuela militar, un 34% que es alto y un 30% manifiestan que es bajo. Esto refleja que en su mayoría los cadetes consideran que esta elevado el control de seguridad en la Escuela Militar.

Tabla Nº 6.-

¿Cómo percibes el nivel de riesgo que pone en peligro la vida o la integridad física?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	36	30,0	30,0	30,0
	Medio	37	30,8	30,8	60,8
	Alto	47	39,2	39,2	100,0
	Total	120	100,0	100,0	

Gráfico Nº 3.-



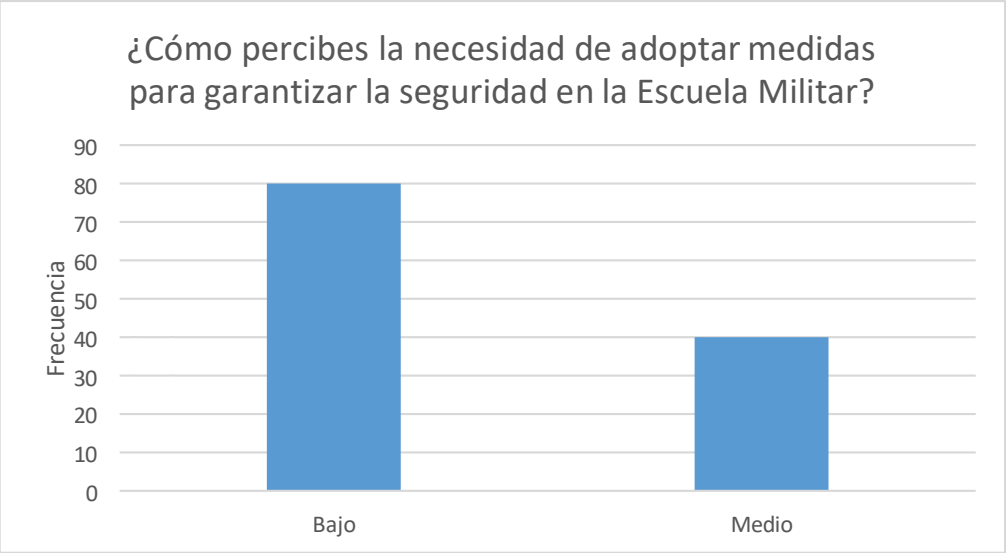
En el gráfico se puede observar que el 39% de los cadetes consideran que perciben alto el nivel de riesgo que pone en peligro la vida o la integridad física, un 31% que es medio y un 30% manifiestan que es bajo. Esto refleja que en su mayoría los cadetes consideran elevado el nivel de riesgo que pone en peligro la vida o la integridad física.

Tabla Nº 7.-

¿Cómo percibes la necesidad de adoptar medidas para garantizar la seguridad en la Escuela Militar?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	80	66,7	66,7	66,7
	Medio	40	33,3	33,3	100,0
	Total	120	100,0	100,0	

Gráfico Nº 4.-



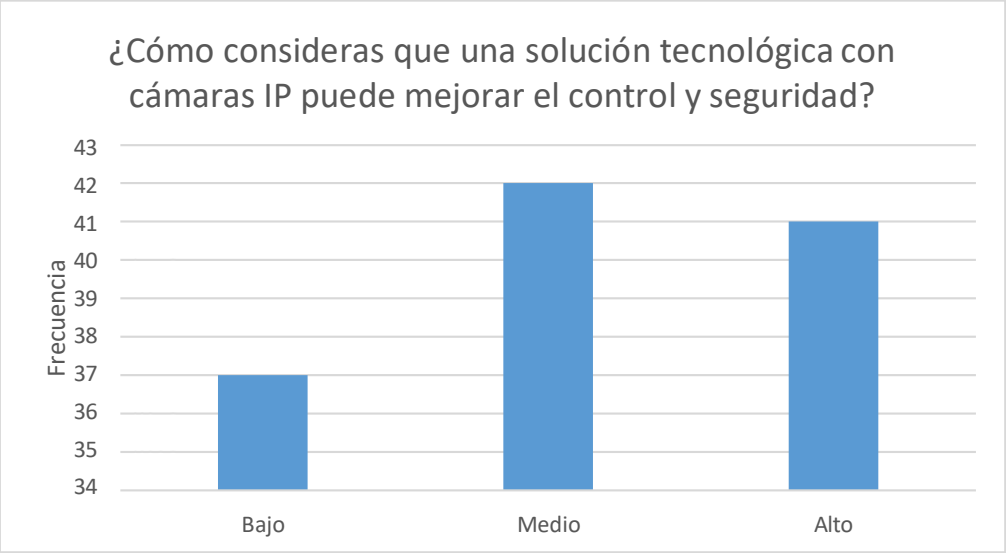
En el gráfico se puede observar que el 66% de los cadetes consideran que perciben baja la necesidad de adoptar medidas para garantizar la seguridad en la Escuela Militar, un 33% que es medio manifiestan que es medio. Esto refleja que en su mayoría los cadetes consideran baja la necesidad de adoptar medidas para garantizar la seguridad en la Escuela Militar.

Tabla N º 8.-

¿Cómo consideras que una solución tecnológica con cámaras IP puede mejorar el control y seguridad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	37	30,8	30,8	30,8
	Medio	42	35,0	35,0	65,8
	Alto	41	34,2	34,2	100,0
	Total	120	100,0	100,0	

Gráfico N º 5.-



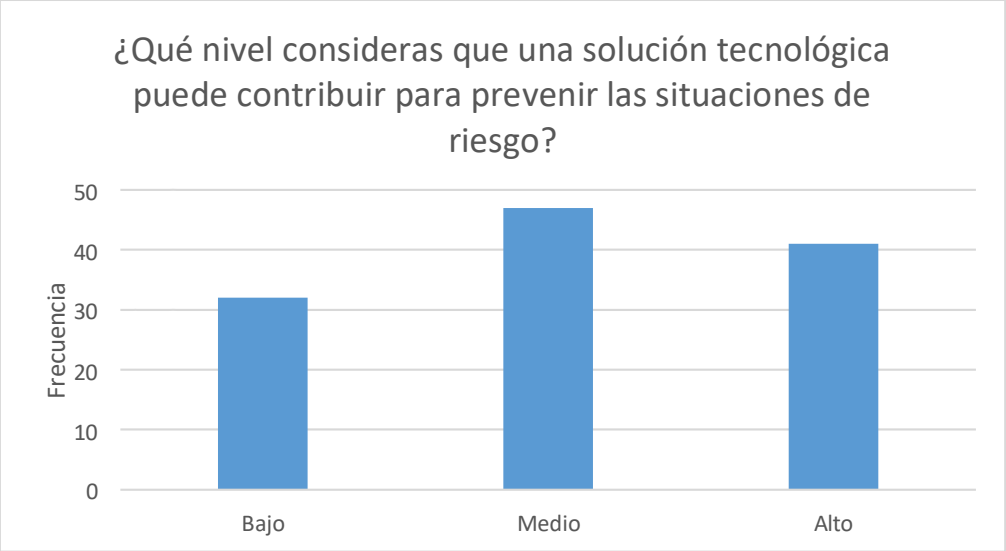
En el gráfico se puede observar que el 35% de los cadetes consideran que es medio que una solución tecnológica con cámaras IP puede mejorar el control y seguridad, un 34% que es alto y un 30% manifiestan que es bajo. Esto refleja que en su mayoría los cadetes consideran elevada que una solución tecnológica con cámaras IP puede mejorar el control y seguridad.

Tabla Nº 9.-

¿Qué nivel consideras que una solución tecnológica puede contribuir para prevenir las situaciones de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	32	26,7	26,7	26,7
	Medio	47	39,2	39,2	65,8
	Alto	41	34,2	34,2	100,0
	Total	120	100,0	100,0	

Gráfico Nº 6.-



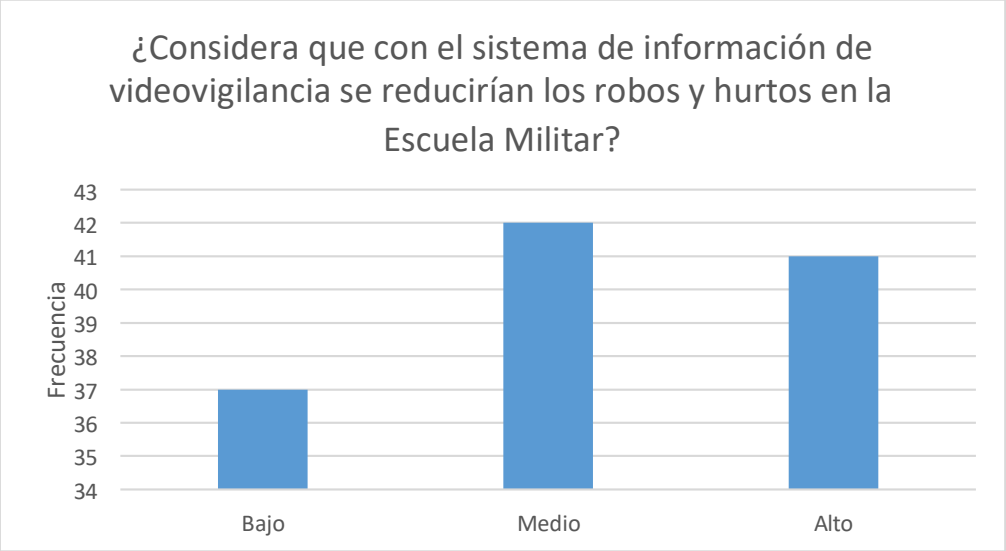
En el gráfico se puede observar que el 39% de los cadetes consideran que es medio que una solución tecnológica puede contribuir para prevenir las situaciones de riesgo, un 34% que es alto y un 26% manifiestan que es bajo. Esto refleja que en su mayoría los cadetes consideran elevada que una solución tecnológica puede contribuir para prevenir las situaciones de riesgo.

Tabla Nº 10.-

¿Considera que con el sistema de información de videovigilancia se reducirían los robos y hurtos en la Escuela Militar?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	37	30,8	30,8	30,8
	Medio	42	35,0	35,0	65,8
	Alto	41	34,2	34,2	100,0
	Total	120	100,0	100,0	

Gráfico Nº 7.-



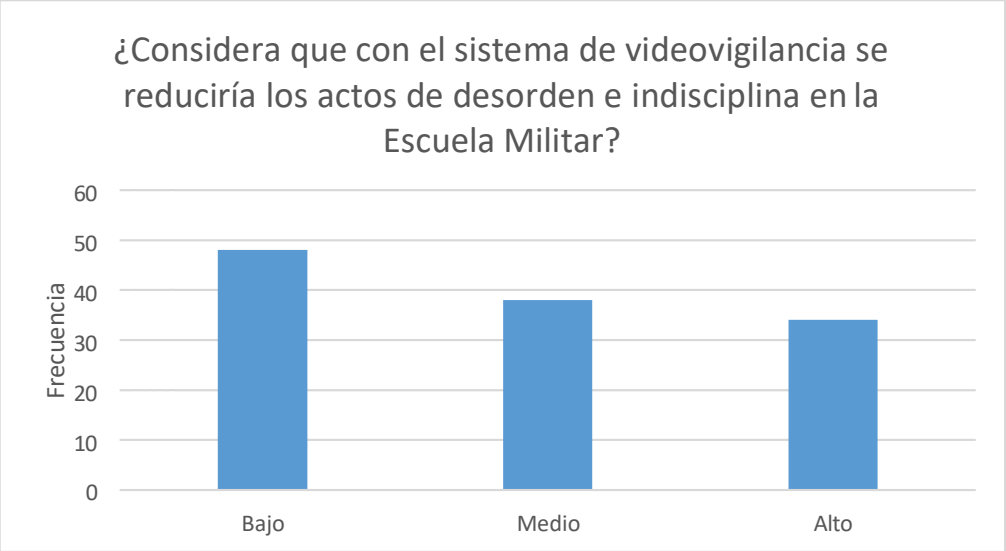
En el gráfico se puede observar que el 35% de los cadetes consideran que es medio que con el sistema de información de videovigilancia se reducirían los robos y hurtos en la Escuela Militar, un 34% que es alto y un 30% manifiestan que es bajo. Esto refleja que en su mayoría los cadetes consideran elevado que con el sistema de información de videovigilancia se reducirían los robos y hurtos en la Escuela Militar.

Tabla Nº 11.-

¿Considera que con el sistema de videovigilancia se reduciría los actos de desorden e indisciplina en la Escuela Militar?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	48	40,0	40,0	40,0
	Medio	38	31,7	31,7	71,7
	Alto	34	28,3	28,3	100,0
	Total	120	100,0	100,0	

Gráfico Nº 8.-



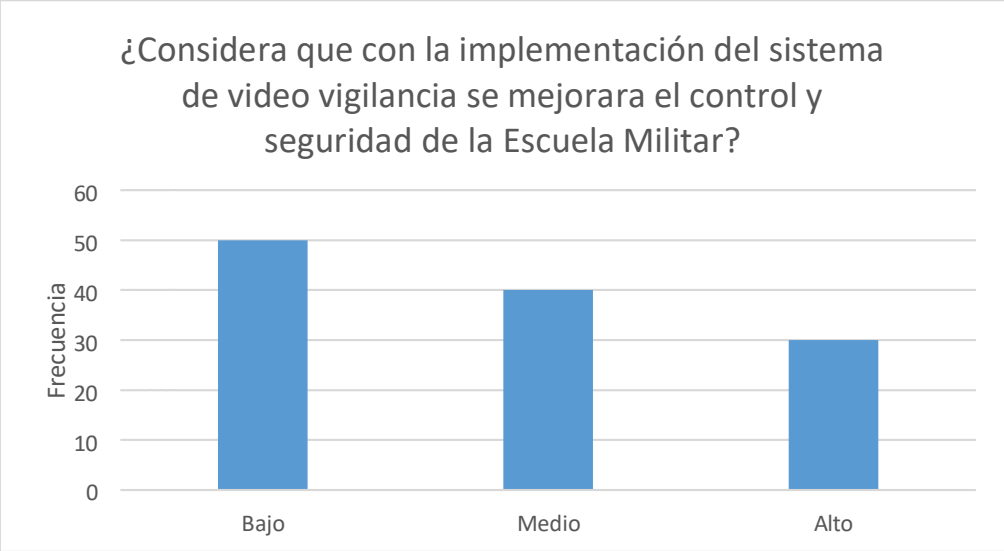
En el gráfico se puede observar que el 40% de los cadetes consideran que es bajo que con el sistema de videovigilancia se reduciría los actos de desorden e indisciplina en la Escuela Militar, un 31% que es medio y un 28% manifiestan que es alto. Esto refleja que en su mayoría los cadetes consideran elevado que con el sistema de videovigilancia se reduciría los actos de desorden e indisciplina en la Escuela Militar.

Tabla Nº 12.-

¿Considera que con la implementación del sistema de video vigilancia se mejorara el control y seguridad de la Escuela Militar?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	50	41,7	41,7	41,7
	Medio	40	33,3	33,3	75,0
	Alto	30	25,0	25,0	100,0
	Total	120	100,0	100,0	

Gráfico Nº 9.-



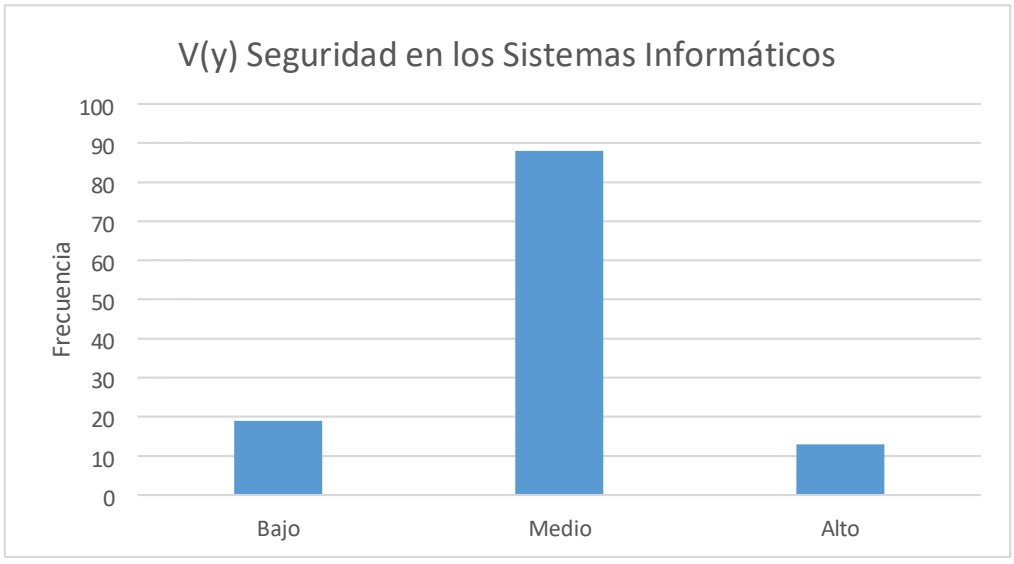
En el gráfico se puede observar que el 41% de los cadetes consideran bajo que con la implementación del sistema de video vigilancia se mejorara el control y seguridad de la Escuela Militar, un 33% que es medio y un 25% manifiestan que es alto. Esto refleja que en su mayoría los cadetes consideran bajo que con la implementación del sistema de video vigilancia se mejorara el control y seguridad de la Escuela Militar.

Tabla Nº 13.-

V(y) Seguridad en los Sistemas Informáticos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	19	15,8	15,8	15,8
	Medio	88	73,3	73,3	89,2
	Alto	13	10,8	10,8	100,0
	Total	120	100,0	100,0	

Gráfico Nº 10.-



En el gráfico se puede observar que el 73% de los cadetes consideran medio la Seguridad en los sistemas de Información, un 15% que es bajo y un 10% manifiestan que es alto. Esto refleja que en su mayoría los cadetes consideran elevado la Seguridad en los Sistemas Informáticos.

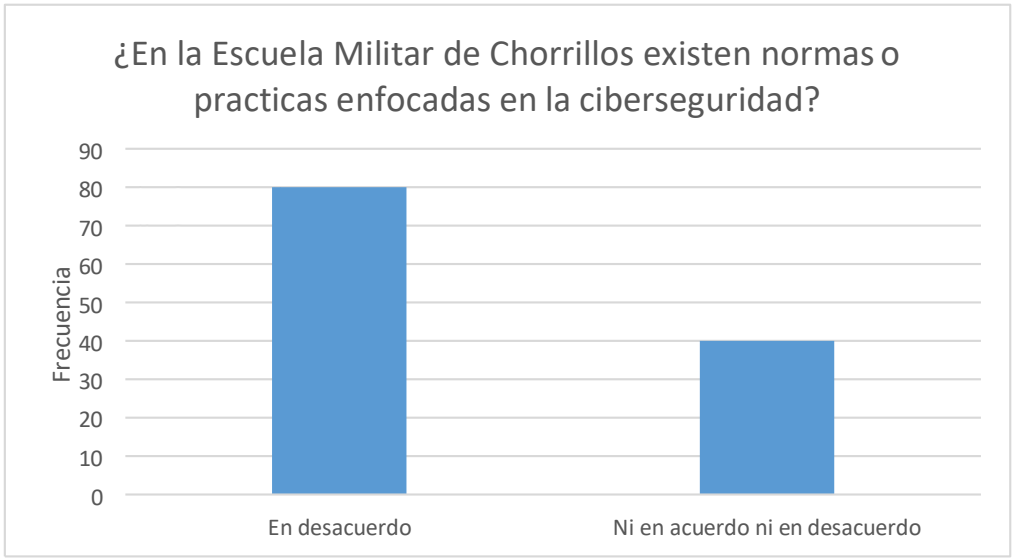
4.1.2. Variable N° 2

Tabla Nº 14.-

¿En la Escuela Militar de Chorrillos existen normas o practicas enfocadas en la ciberseguridad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	80	66,7	66,7	66,7
	Ni en acuerdo ni en desacuerdo	40	33,3	33,3	100,0
	Total	120	100,0	100,0	

Gráfico Nº 11.-



En el gráfico se puede observar que el 66% de los cadetes están en desacuerdo con que en la Escuela Militar de Chorrillos existen normas o practicas enfocadas en la ciberseguridad y un 33% manifiestan que están ni acuerdo ni desacuerdo. Esto refleja que la mayoría de cadetes están en desacuerdo con que en la Escuela Militar de Chorrillos existen normas o practicas enfocadas en la ciberseguridad.

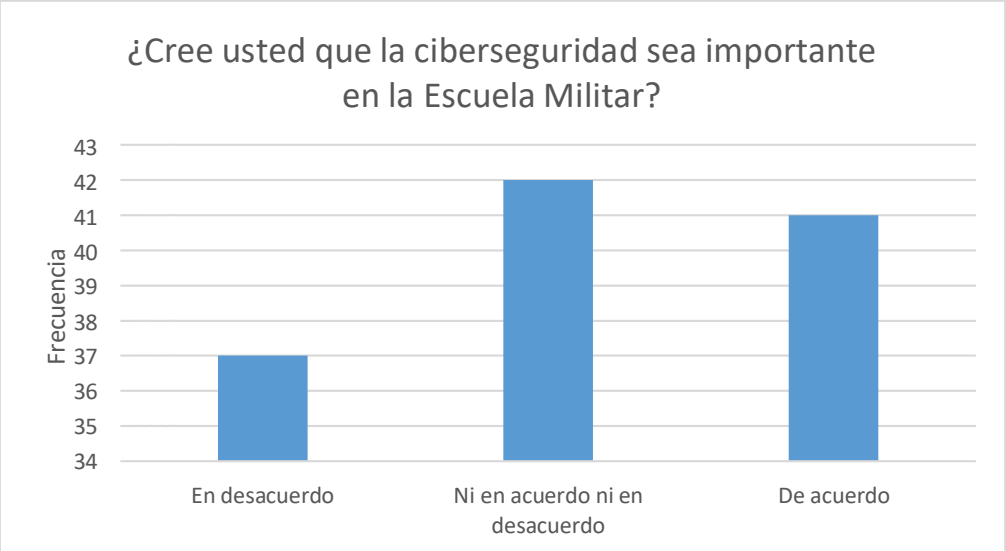
.

Tabla Nº 15.-

¿Cree usted que la ciberseguridad sea importante en la Escuela Militar?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	37	30,8	30,8	30,8
	Ni en acuerdo ni en desacuerdo	42	35,0	35,0	65,8
	De acuerdo	41	34,2	34,2	100,0
	Total	120	100,0	100,0	

Gráfico Nº 12.-



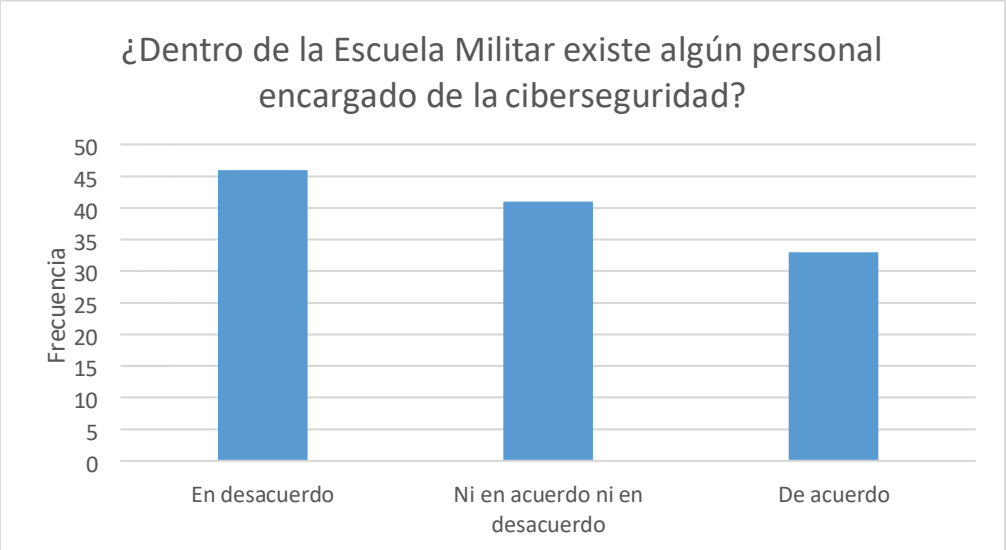
En el gráfico se puede observar que el 35% de los cadetes están ni acuerdo ni desacuerdo con la ciberseguridad sea importante en la Escuela Militar; un 34% están de acuerdo y un 30% manifiestan que están en desacuerdo. Esto refleja que la mayoría de cadetes están en acuerdo y ni desacuerdo con que la ciberseguridad sea importante en la Escuela Militar.

Tabla N º 16.-

¿Dentro de la Escuela Militar existe alguna personal encargado de la ciberseguridad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	46	38,3	38,3	38,3
	Ni en acuerdo ni en desacuerdo	41	34,2	34,2	72,5
	De acuerdo	33	27,5	27,5	100,0
	Total	120	100,0	100,0	

Gráfico Nº 13.-



En el gráfico se puede observar que el 38% de los cadetes están en desacuerdo con que dentro de la Escuela Militar exista alguna personal encargado de la ciberseguridad; un 34% están de ni acuerdo ni en desacuerdo y un 27% manifiestan que están de acuerdo. Esto refleja que la mayoría de cadetes están en desacuerdo con que dentro de la Escuela Militar existe alguna personal encargado de la ciberseguridad.

Tabla Nº 17.-

¿En la Escuela Militar se realizan análisis de gestión de riesgos informáticos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	80	66,7	66,7	66,7
	Ni en acuerdo ni en desacuerdo	40	33,3	33,3	100,0
	Total	120	100,0	100,0	

Gráfico Nº 14.-

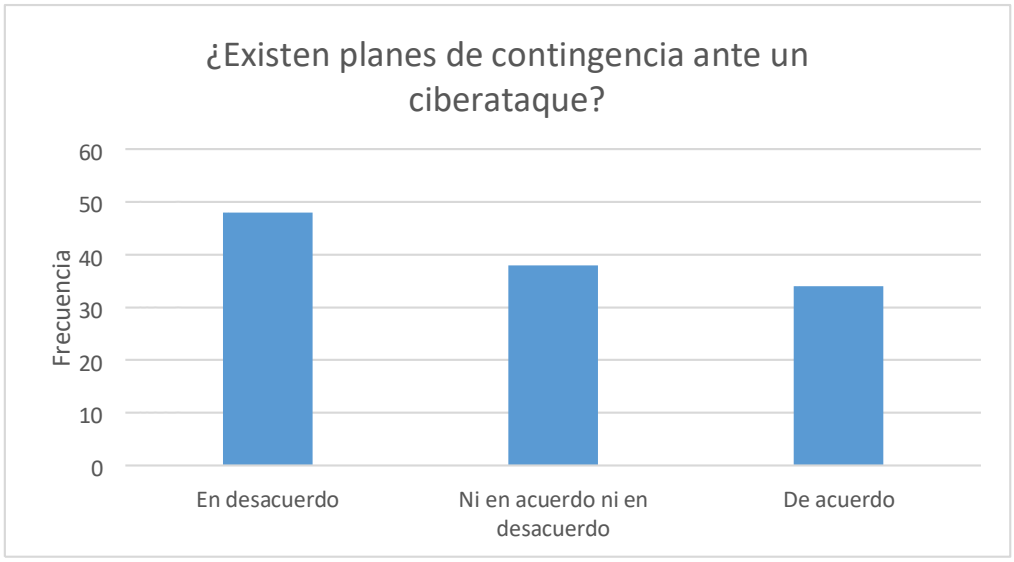
En el gráfico se puede observar que el 66% de los cadetes están en desacuerdo con que en la Escuela Militar se realizan análisis de gestión de riesgos informáticos y un 33% manifiestan que están ni de acuerdo ni en desacuerdo. Esto refleja que la mayoría de cadetes están en desacuerdo con que dentro de la Escuela Militar se realizan análisis de gestión de riesgos informáticos.

Tabla Nº 18.-

¿Existen planes de contingencia ante un ciberataque?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	48	40,0	40,0	40,0
	Ni en acuerdo ni en desacuerdo	38	31,7	31,7	71,7
	De acuerdo	34	28,3	28,3	100,0
	Total	120	100,0	100,0	

Gráfico Nº 15.-



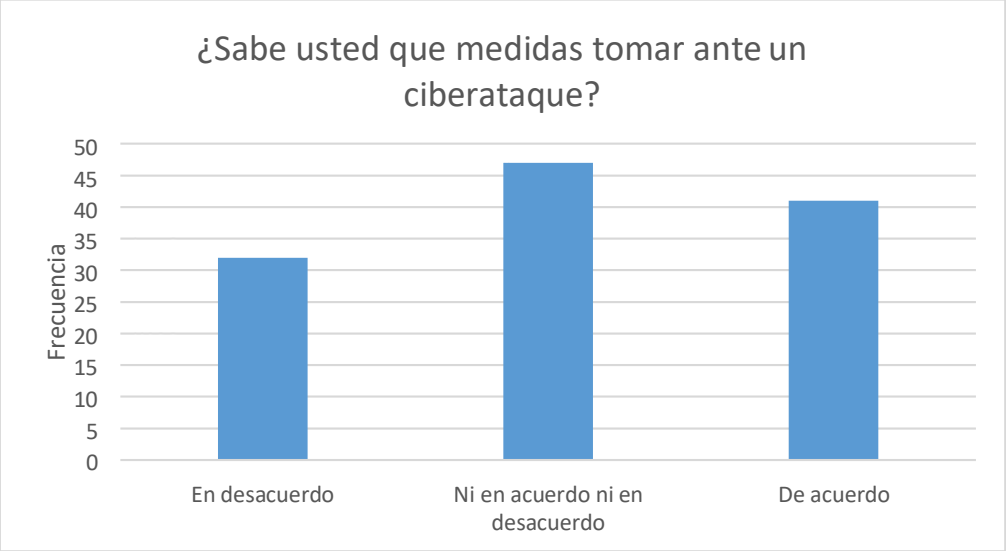
En el gráfico se puede observar que el 40% de los cadetes están en desacuerdo con decir que existen planes de contingencia ante un ciberataque; el 31% están ni acuerdo ni en desacuerdo y un 28% manifiestan que están de acuerdo. Esto refleja que la mayoría de cadetes están en descuerdo en decir que existen planes de contingencia ante un ciberataque.

Tabla N° 19

¿Sabe usted qué medidas tomar ante un ciberataque?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	32	26,7	26,7	26,7
	Ni en acuerdo ni en desacuerdo	47	39,2	39,2	65,8
	De acuerdo	41	34,2	34,2	100,0
	Total	120	100,0	100,0	

Gráfico Nº 16.-



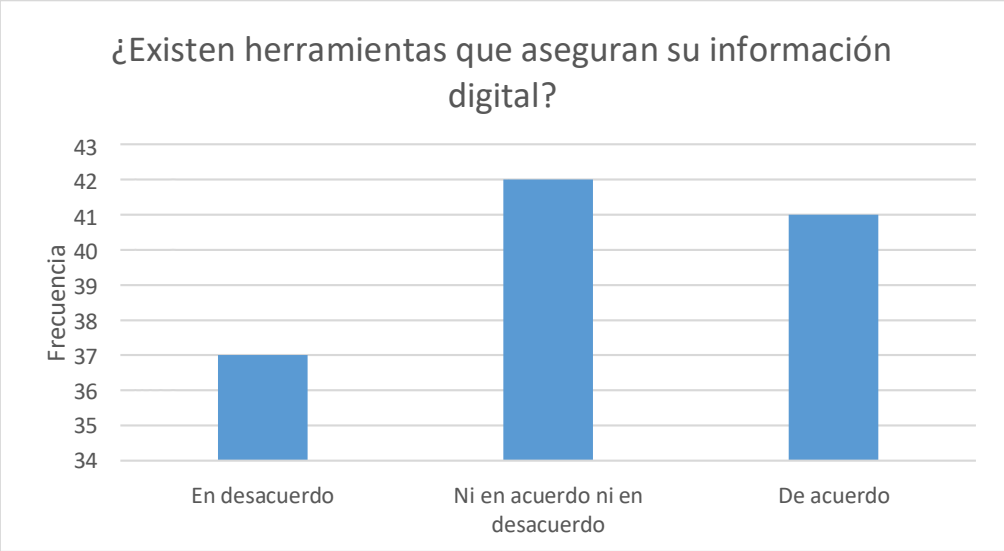
En el gráfico se puede observar que el 39% de los cadetes están ni acuerdo ni en desacuerdo con saber qué medidas tomar ante un ciberataque; el 34% están de acuerdo y un 26% manifiestan que están de desacuerdo. Esto refleja que la mayoría de cadetes están ni acuerdo ni en descuerdo con saber qué medidas tomar ante un ciberataque.

Tabla Nº 20.-

¿Existen herramientas que aseguran su información digital?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	37	30,8	30,8	30,8
	Ni en acuerdo ni en desacuerdo	42	35,0	35,0	65,8
	De acuerdo	41	34,2	34,2	100,0
	Total	120	100,0	100,0	

Gráfico Nº 17.-



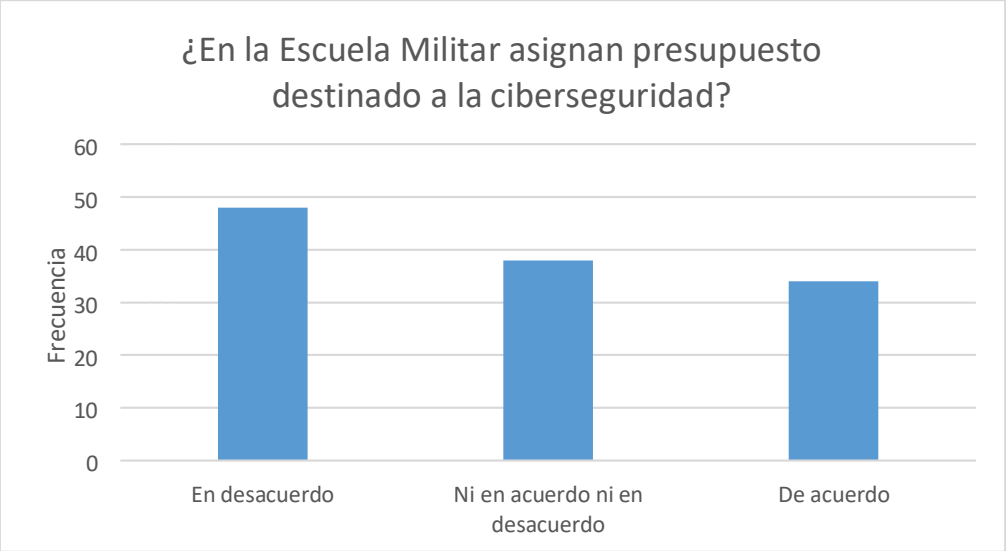
En el gráfico se puede observar que el 35% de los cadetes están ni acuerdo ni en desacuerdo con saber si existen herramientas que aseguran su información digital; el 34% están de acuerdo y un 30% manifiestan que están de desacuerdo. Esto refleja que la mayoría de cadetes están ni acuerdo ni en descuerdo con saber si existen herramientas que aseguran su información digital.

Tabla Nº 21.-

¿En la Escuela Militar asignan presupuesto destinado a la ciberseguridad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	48	40,0	40,0	40,0
	Ni en acuerdo ni en desacuerdo	38	31,7	31,7	71,7
	De acuerdo	34	28,3	28,3	100,0
	Total	120	100,0	100,0	

Gráfico Nº 18.-



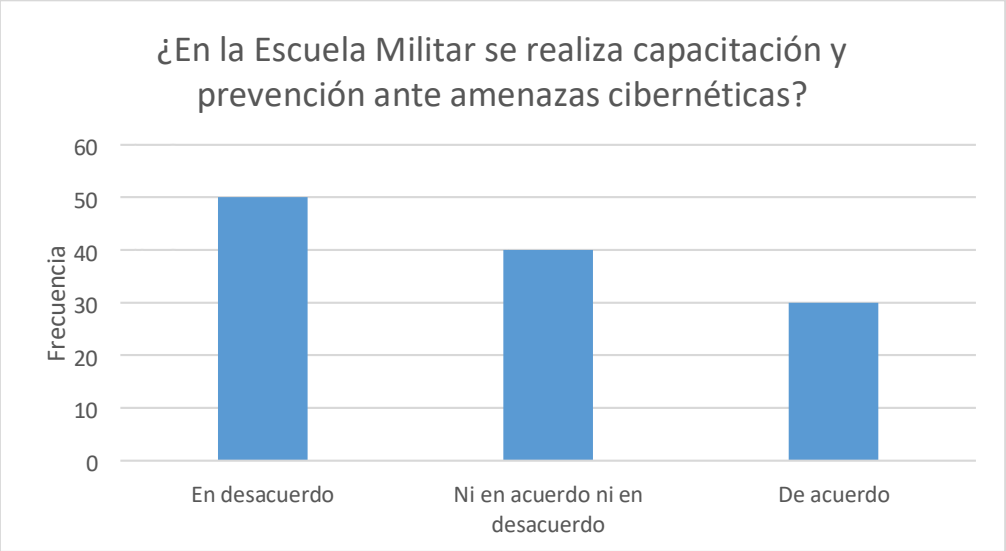
En el gráfico se puede observar que el 40% de los cadetes están en desacuerdo con que en la Escuela Militar asignan presupuesto destinado a la ciberseguridad; el 31% están no están ni de acuerdo ni en desacuerdo y un 28% manifiestan que están de acuerdo. Esto refleja que la mayoría de cadetes de acuerdo con que en la Escuela Militar asignan presupuesto destinado a la ciberseguridad.

Tabla Nº 22.-

¿En la Escuela Militar se realiza capacitación y prevención ante amenazas cibernéticas?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	50	41,7	41,7	41,7
	Ni en acuerdo ni en desacuerdo	40	33,3	33,3	75,0
	De acuerdo	30	25,0	25,0	100,0
	Total	120	100,0	100,0	

Gráfico Nº 19



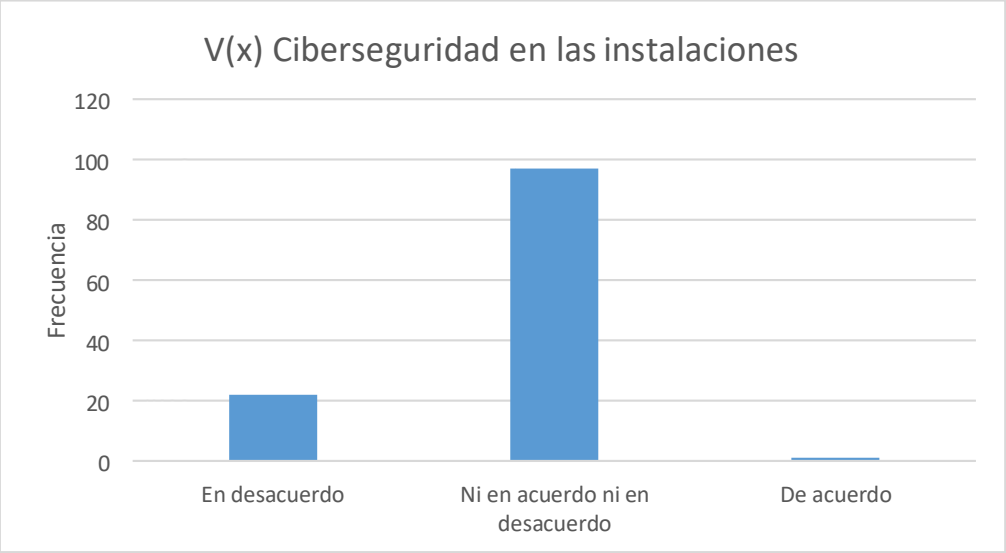
En el gráfico se puede observar que el 41% de los cadetes están en desacuerdo con que en la Escuela Militar se realiza capacitación y prevención ante amenazas cibernéticas; el 33% están no están ni de acuerdo ni en desacuerdo y un 25% manifiestan que están de acuerdo. Esto refleja que la mayoría de cadetes de acuerdo con que en la Escuela Militar se realiza capacitación y prevención ante amenazas cibernéticas.

Tabla Nº 23-

V(x) Ciberseguridad en las instalaciones

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	22	18,3	18,3	18,3
	Ni en acuerdo ni en desacuerdo	97	80,8	80,8	99,2
	De acuerdo	1	,8	,8	100,0
	Total	120	100,0	100,0	

Gráfico Nº 20



En el gráfico se puede observar que el 80% de los cadetes no están ni acuerdo ni desacuerdo con la ciberseguridad en las instalaciones; el 18% en desacuerdo y un 1% manifiestan que están de acuerdo. Esto refleja que la mayoría de cadetes no están ni acuerdo ni en desacuerdo con la ciberseguridad en las instalaciones.

4.2. Interpretación

En la prueba de la hipótesis general y las específicas, que constituyen hipótesis de relación, se empleó Rho de Spearman, para determinar el grado de asociación entre las dos variables de estudio. El valor estadístico de Rho de Spearman, con una significación bilateral de $p < 0.05$ permitirá, finalmente, decidir si se rechaza o se acepta la hipótesis nula de la hipótesis de estudio formulada.

4.2.1. Prueba de hipótesis general.

H1: Existe relación significativa entre la Ciberseguridad con la Seguridad de los Sistemas Informáticos en las instalaciones de los cadetes de inteligencia de la Escuela Militar de Chorrillos, año 2019.

Ho: No existe relación significativa entre la Ciberseguridad con la Seguridad de los Sistemas Informáticos en las instalaciones de los cadetes de inteligencia de la Escuela Militar de Chorrillos, año 2019.

Correlaciones

		V(x) Ciberseguridad en las instalaciones	V(y) Seguridad de los Sistemas Informáticos
V(x) Ciberseguridad en las instalaciones	Correlación de Pearson	1	,604**
	Sig. (bilateral)		,000
	N	120	120
V(y) Seguridad de los Sistemas Informáticos	Correlación de Pearson	,604**	1
	Sig. (bilateral)	,000	
	N	120	120

**. La correlación es significativa en el nivel 0,01 (bilateral).

El valor de Rho de Spearman (1,00; sig. = 0.000) es estadísticamente significativo al nivel de $p < 0.05$, lo cual permite afirmar que existe relación significativa entre las variables “Ciberseguridad en las instalaciones con la seguridad en los Sistemas Informáticos”. Es decir, se observa que, a mayor implementación de los Sistemas Informáticos, mayor es la tendencia con la Ciberseguridad en las instalaciones.

Decisión: en vista de lo resultados encontrados, se decide rechazar la hipótesis nula de la hipótesis general del estudio.

4.2.2. Prueba de hipótesis especifica.

4.2.2.1. Relación entre la gestión de la Ciberseguridad y la Seguridad de los Sistemas Informáticos

H1: Existe relación significativa entre la gestión de la Ciberseguridad y la Seguridad de los Sistemas Informáticos de los cadetes de inteligencia de la Escuela Militar de Chorrillos, año 2019.

Ho: No existe relación significativa entre la gestión de la Ciberseguridad y la Seguridad de los Sistemas Informáticos de los cadetes de inteligencia de la Escuela Militar de Chorrillos, año 2019.

Correlaciones

		V(x) Gestión de la Ciberseguridad en las instalaciones	V(y) Seguridad de los Sistemas Informáticos
V(x) Gestión de la Ciberseguridad en las instalaciones	Correlación de Pearson	1	,443**
	Sig. (bilateral)		,000
	N	120	120
V(y) Seguridad de los Sistemas Informáticos	Correlación de Pearson	,443**	1
	Sig. (bilateral)	,000	
	N	120	120

**. La correlación es significativa en el nivel 0,01 (bilateral).

El valor de Rho de Spearman (,443; sig. = 0.000) es estadísticamente significativo al nivel de $p < 0.05$, lo cual es indicativo de que existe asociación significativa entre la variable: entre el método de aprendizaje basado en problemas y programa de especialización en pavimentos.

Decisión: en consecuencia, teniendo en cuenta los resultados obtenidos, se dispone de suficiente evidencia para rechazar la hipótesis nula.

4.2.2.2. Relación entre la Prevención de los ataques cibernéticos y la Seguridad de los Sistemas Informáticos

H1: Existe relación significativa entre la Prevención de los ataques cibernéticos y la Seguridad de los Sistemas Informáticos de los cadetes de Inteligencia de la Escuela Militar de Chorrillos, año 2019.

Ho: No existe relación significativa entre la Prevención de los ataques cibernéticos y la Seguridad de los Sistemas Informáticos de los cadetes de Inteligencia de la Escuela Militar de Chorrillos, año 2019.

Correlaciones

		V(y) Seguridad de los Sistemas Informáticos	Prevención de los ataques cibernéticos
V(y) Seguridad de los Sistemas Informáticos	Correlación de Pearson	1	,736**
	Sig. (bilateral)		,000
	N	120	120
Prevención de los ataques cibernéticos	Correlación de Pearson	,736**	1
	Sig. (bilateral)	,000	
	N	120	120

**. La correlación es significativa en el nivel 0,01 (bilateral).

El valor de Rho de Spearman (,736; sig. = 0.000) es estadísticamente significativo al nivel de $p < 0.05$, lo cual significa que existe asociación significativa entre la variable Prevención de los ataques cibernéticos y la Seguridad de los Sistemas Informáticos de los cadetes de inteligencia de la muestra seleccionada.

Decisión: considerando los resultados encontrados, se decide rechazar la hipótesis nula.

4.3. Discusión de los resultados.

La Ciberseguridad en las instalaciones y la Seguridad de los Sistemas Informáticos:

La hipótesis general planteó que existe relación entre el sistema de información de vigilancia con la Ciberseguridad en las instalaciones de los cadetes de Inteligencia de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, y

fue rechazada por el valor de Rho de Spearman (,604; sig. = 0.000), estadísticamente no significativo al nivel de $p<0.05$, lo cual rechaza la hipótesis de investigación. Es decir, se observa que, a mayor nivel de Seguridad de los Sistemas Informáticos existe una fuerte correlación positiva con Ciberseguridad en las instalaciones en los cadetes de inteligencia de la Escuela Militar de Chorrillos de la muestra investigada.

Los resultados de la presente investigación, fueron obtenidos a través de un cuestionario aplicado a los 24 cadetes de la sección inteligencia de la Escuela Militar de Chorrillos, quedando registro de la actividad mencionada, los cuestionarios llenados.

En el caso de la herramienta utilizada, fueron sometidas al criterio de tres jueces expertos quienes observaron y recomendaron mejoras y optimizaciones para la obtención de resultados lo más precisos posible. La técnica empleada permitió realizar el análisis de fiabilidad correspondiente, certificando la validez de los resultados que se consiguieron.

Los resultados obtenidos corresponden en efecto, al estudio de la Ciberseguridad en las instalaciones y la Seguridad de los Sistemas de Información de los cadetes de inteligencia pudiendo generalizarse a los cadetes de las otras armas, servicios y de otros años académicos de la Escuela Militar, por cuanto les seria de la misma utilidad de mejoramiento de si formación profesional en el Ejercito.

Lo que sí se puede generalizar es la metodología empleada en la investigación, ya que las herramientas y el instrumento empleado cumplen la función de averiguar al detalle y recopilar la información necesaria sobre las variables de estudio.

Dentro de las limitaciones que existieron en el desarrollo de la investigación, se puede citar a las dos consideraciones más importantes: los horarios y la accesibilidad a las fuentes de información y bibliotecas.

Es necesario analizar problema por problema al detalle, de modo que se observe las causas y efectos que se ocasionan; pero más importante aún, poder medir los impactos de la aplicación de una teoría, en un ambiente caracterizado por constantes cambios, en función de variables exógenas la mayoría de las veces.

Así, la teoría será una guía que permita establecer las bases para el estudio de la Ciberseguridad en las instalaciones y la Seguridad de los Sistemas Informáticos; al final esta deberá ser puesta en práctica con nuevos paradigmas, herramientas y modelos de calidad orientados hacia la consecución de los objetivos planteados; teniendo en cuenta que la mejora en la Seguridad de los Sistemas Informáticos son el objetivo a alcanzar por los cadetes de la sección de inteligencia de la Escuela Militar.

Se puede concluir que el estudio sobre la Ciberseguridad en las instalaciones y su relación con la Seguridad de los Sistemas Informáticos que ofrece la presente investigación, recurre a un enfoque que busca asegurar no solo la

mejora académica y tecnológica, sino una mejora significativa en la calidad de las medidas de ciberseguridad de los estudiantes cadetes militares.

CONCLUSIONES

1. Desde la perspectiva de la variable Ciberseguridad se observa una creciente necesidad de controlar los riesgos informáticos debido a la nueva tecnología, se puede afirmar que los factores más relevantes y fuertes son básicamente: a) Comprenden que la Ciberseguridad es importante en la Escuela Militar; b) Saben qué medidas tomar ante un Ciberataque; c) Existen herramientas que aseguren su información digital.
2. En consecuencia, las infraestructuras de las comunicaciones y los servicios permiten desarrollar y administrarse nuevos términos de seguridad por lo que es necesario profundizar el problema de estudio, como una futura línea de investigación, sobre las medidas de seguridad que debe adoptar los sistemas de información de vigilancia y ciberseguridad de instalaciones, ampliándolos a otras armas y servicios, cuya distinción son sus propias estructuras y culturas organizacionales
3. Por otro lado, se ha constatado que el internet es “la gran arma” del terrorismoy existen más de 30 000 páginas terroristas que circulan por la red sin embargo un 66.7% de estudiantes cadetes que percibe en forma baja la necesidad de adoptar medidas para garantizar la seguridad de los cadetes.

RECOMENDACIONES

1. Incrementar actividades o programas sobre el empleo del internet y los sistemas de información de vigilancia (talleres, seminarios, cursos, ejercicios grupales) con el fin de satisfacer necesidades de formación profesional del cadete que favorezcan el equilibrio de su desarrollo y educación digital en ciberseguridad.
2. Coordinar y utilizar la información de tutoriales instructivos y guías de procedimientos con el fin de brindar apoyo oportuno al cadete en situaciones que lo requieran de acuerdo a las armas y servicios lo requieran.
3. Que las autoridades directivas de la escuela militar implementen talleres de estrategia de afrontamiento encaminados a capacitar en el uso de sistemas de información de vigilancia, del internet, uso y búsqueda en bases de datos, uso de motores de búsqueda por los cadetes.

Anexo 1: Base de datos

Título: "CIBERSEGURIDAD Y SU RELACIÓN EN LA SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS EN LAS INSTALACIONES PARA LOS CADETES DE LA ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI, AÑO 2019"

Sistema de información de vigilancia												Ciberseguridad en las instalaciones											
Analógico						Digital					X	Gestión de la ciberseguridad					Prevención de los ataques cibernéticos						X
P1	P2	P3	P4	P5	X	P6	P7	P8	P9	X		P10	P11	P12	P13	X	P14	P15	P16	P17	P18	X	
2	2	3	2	2	2	3	2	4	2	3	2	2	2	3	2	2	4	3	2	4	2	3	3
4	4	3	3	4	4	3	4	2	4	3	3	3	4	3	3	3	2	3	4	2	4	3	3
2	2	4	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	3	2	2	2	2	2
3	3	2	3	3	3	4	3	2	2	3	3	3	3	4	3	3	2	4	3	2	2	3	3
2	2	3	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	3	2	2
4	4	3	2	4	3	3	4	4	3	4	3	2	4	4	2	3	4	3	4	4	3	4	3
4	4	3	2	4	3	4	4	2	3	3	3	2	4	4	2	3	2	4	4	2	3	3	3
4	4	4	2	4	4	4	4	4	3	4	4	2	4	3	2	3	4	4	4	4	3	4	3
3	3	2	3	3	3	2	3	3	2	3	3	3	3	3	3	3	3	2	3	3	2	3	3
3	3	3	2	3	3	4	3	2	3	3	3	2	3	2	2	2	2	4	3	2	3	3	3
4	4	4	2	4	4	4	4	4	2	4	4	2	4	4	2	3	4	4	4	4	2	4	3
3	3	2	2	3	3	3	3	4	2	3	3	2	3	2	2	2	4	3	3	4	2	3	3
4	4	4	3	4	4	3	4	4	3	4	4	3	4	4	3	4	4	3	4	4	3	4	4
2	2	4	2	2	2	4	2	3	2	3	3	2	2	2	2	2	3	4	2	3	2	3	2
4	4	3	2	4	3	4	4	4	3	4	4	2	4	3	2	3	4	4	4	4	3	4	3
4	4	3	2	4	3	3	4	3	3	3	3	2	4	2	2	3	3	3	4	3	3	3	3
2	2	2	2	2	2	3	2	2	2	2	2	2	2	3	2	2	2	3	2	2	2	2	2
3	3	2	3	3	3	3	3	2	3	3	3	3	3	4	3	3	2	3	3	2	3	3	3
3	3	2	3	3	3	2	3	2	3	3	3	3	3	2	3	3	2	2	3	2	3	2	3
2	2	3	3	2	2	4	2	3	2	3	3	3	2	3	3	3	3	4	2	3	2	3	3
4	4	2	3	4	3	2	4	3	4	3	3	3	4	4	3	4	3	2	4	3	4	3	3
4	4	2	2	4	3	3	4	3	3	3	3	2	4	2	2	3	3	3	4	3	3	3	3
4	4	3	2	4	3	3	4	4	4	4	4	2	4	3	2	3	4	3	4	4	4	4	3
2	2	4	2	2	2	4	2	3	3	3	3	2	2	3	2	2	3	4	2	3	3	3	3
3	3	4	3	3	3	4	3	4	4	4	3	3	3	3	3	3	4	4	3	4	4	4	3
2	2	3	3	2	2	4	2	2	4	3	3	3	2	4	3	3	2	4	2	2	4	3	3
4	4	4	2	4	4	3	4	3	3	3	3	2	4	4	2	3	3	3	4	3	3	3	3
3	3	4	3	3	3	3	3	2	4	3	3	3	3	2	3	3	2	3	3	2	4	3	3
2	2	4	2	2	2	3	2	4	4	3	3	2	2	2	2	2	4	3	2	4	4	3	3
4	4	3	2	4	3	4	4	2	2	3	3	2	4	4	2	3	2	4	4	2	2	3	3
3	3	2	2	3	3	4	3	3	2	3	3	2	3	3	2	3	3	4	3	3	2	3	3
4	4	3	2	4	3	2	4	4	2	3	3	2	4	2	2	3	4	2	4	4	2	3	3

3	3	4	2	3	3	3	3	4	2	3	3	2	3	3	2	3	4	3	3	4	2	3	3
3	3	4	2	3	3	4	3	2	3	3	3	2	3	2	2	2	2	4	3	2	3	3	3
4	4	4	2	4	4	3	4	3	4	4	4	2	4	3	2	3	3	3	4	3	4	3	3
2	2	4	2	2	2	2	2	4	2	3	2	2	2	4	2	3	4	2	2	4	2	3	3
3	3	4	2	3	3	4	3	2	4	3	3	2	3	2	2	2	2	4	3	2	4	3	3
3	3	4	3	3	3	3	3	2	2	3	3	3	3	4	3	3	2	3	3	2	2	2	3
2	2	4	2	2	2	2	2	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2
2	2	4	2	2	2	3	2	2	4	3	3	2	2	3	2	2	2	3	2	2	4	3	2
4	4	2	3	4	3	3	4	3	4	4	3	3	4	2	3	3	3	3	4	3	4	3	3
3	3	2	2	3	3	2	3	3	4	3	3	2	3	2	2	2	3	2	3	3	4	3	3
2	2	2	2	2	2	4	2	4	3	3	3	2	2	2	2	2	4	4	2	4	3	3	3
2	2	2	2	2	2	4	2	2	2	3	2	2	2	3	2	2	2	4	2	2	2	2	2
4	4	3	2	4	3	2	4	4	3	3	3	2	4	3	2	3	4	2	4	4	3	3	3
4	4	4	3	4	4	4	4	3	2	3	4	3	4	4	3	4	3	4	4	3	2	3	3
2	2	3	2	2	2	2	2	3	2	2	2	2	2	2	2	2	3	2	2	3	2	2	2
2	2	4	2	2	2	3	2	4	3	3	3	2	2	3	2	2	4	3	2	4	3	3	3
4	4	4	2	4	4	3	4	2	4	3	3	2	4	2	2	3	2	3	4	2	4	3	3
4	4	3	2	4	3	3	4	4	2	3	3	2	4	2	2	3	4	3	4	4	2	3	3
4	4	2	2	4	3	4	4	2	3	3	3	2	4	2	2	3	2	4	4	2	3	3	3
2	2	4	2	2	2	3	2	4	2	3	3	2	2	3	2	2	4	3	2	4	2	3	3
2	2	2	2	2	2	2	2	2	2	2	2	2	2	4	2	3	2	2	2	2	2	2	2
3	3	3	2	3	3	3	3	4	2	3	3	2	3	4	2	3	4	3	3	4	2	3	3
2	2	3	3	2	2	2	2	3	2	2	2	3	2	2	3	3	3	2	2	3	2	2	2
4	4	3	2	4	3	3	4	4	4	4	4	2	4	3	2	3	4	3	4	4	4	4	3
3	3	2	2	3	3	2	3	2	4	3	3	2	3	3	2	3	2	2	3	2	4	3	3
4	4	4	2	4	4	2	4	2	3	3	3	2	4	4	2	3	2	2	4	2	3	3	3
3	3	2	2	3	3	3	3	2	3	3	3	2	3	4	2	3	2	3	3	2	3	3	3
3	3	2	2	3	3	2	3	4	2	3	3	2	3	4	2	3	4	2	3	4	2	3	3
4	4	3	3	4	4	3	4	2	2	3	3	3	4	2	3	3	2	3	4	2	2	3	3
4	4	2	3	4	3	4	4	3	4	4	4	3	4	3	3	3	3	4	4	3	4	4	3
3	3	3	3	3	3	2	3	2	3	3	3	3	3	4	3	3	2	2	3	2	3	2	3
3	3	2	3	3	3	2	3	4	3	3	3	3	3	3	3	3	4	2	3	4	3	3	3
3	3	3	3	3	3	4	3	2	2	3	3	3	3	2	3	3	2	4	3	2	2	3	3
3	3	3	3	3	3	2	3	4	2	3	3	3	3	4	3	3	4	2	3	4	2	3	3
4	4	4	3	4	4	3	4	2	2	3	3	3	4	4	3	4	2	3	4	2	2	3	3
3	3	2	3	3	3	3	3	3	2	3	3	3	3	2	3	3	3	3	3	3	2	3	3
2	2	3	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	3	2	2
3	3	2	2	3	3	3	3	4	4	4	3	2	3	3	2	3	4	3	3	4	4	4	3
4	4	4	3	4	4	2	4	3	4	3	4	3	4	4	3	4	3	2	4	3	4	3	3
3	3	2	3	3	3	3	3	3	4	3	3	3	3	2	3	3	3	3	3	3	4	3	3
3	3	4	3	3	3	3	3	2	4	3	3	3	3	4	3	3	2	3	3	2	4	3	3

4	4	3	2	4	3	4	4	4	4	4	4	2	4	2	2	3	4	4	4	4	4	4	3
4	4	4	2	4	4	4	4	2	3	3	3	2	4	2	2	3	2	4	4	2	3	3	3
3	3	4	2	3	3	2	3	3	2	3	3	2	3	2	2	2	3	2	3	3	2	3	2
3	3	2	3	3	3	4	3	3	3	3	3	3	3	4	3	3	3	4	3	3	3	3	3
2	2	3	3	2	2	3	2	3	3	3	3	3	2	2	3	3	3	3	2	3	3	3	3
4	4	4	2	4	4	4	4	2	3	3	3	2	4	4	2	3	2	4	4	2	3	3	3
4	4	3	2	4	3	2	4	3	2	3	3	2	4	2	2	3	3	2	4	3	2	3	3
4	4	4	2	4	4	4	4	4	3	4	4	2	4	2	2	3	4	4	4	4	3	4	3
2	2	2	2	2	2	4	2	3	3	3	2	2	2	3	2	2	3	4	2	3	3	3	3
2	2	2	2	2	2	4	2	3	4	3	3	2	2	2	2	2	3	4	2	3	4	3	3
3	3	2	3	3	3	4	3	3	2	3	3	3	3	2	3	3	3	4	3	3	2	3	3
3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3	4	3	3
4	4	4	3	4	4	2	4	3	3	3	3	3	4	4	3	4	3	2	4	3	3	3	3
3	3	4	2	3	3	3	3	2	3	3	3	2	3	2	2	2	2	3	3	2	3	3	2
4	4	2	2	4	3	3	4	2	4	3	3	2	4	3	2	3	2	3	4	2	4	3	3
2	2	2	3	2	2	4	2	2	2	3	2	3	2	2	3	3	2	4	2	2	2	2	2
2	2	4	2	2	2	4	2	4	2	3	3	2	2	4	2	3	4	4	2	4	2	3	3
3	3	2	2	3	3	2	3	4	3	3	3	2	3	2	2	2	4	2	3	4	3	3	3
4	4	4	2	4	4	4	4	2	3	3	3	2	4	4	2	3	2	4	4	2	3	3	3
3	3	2	2	3	3	4	3	2	2	3	3	2	3	4	2	3	2	4	3	2	2	3	3
2	2	4	2	2	2	4	2	3	4	3	3	2	2	3	2	2	3	4	2	3	4	3	3
3	3	3	2	3	3	3	3	3	4	3	3	2	3	3	2	3	3	3	3	3	4	3	3
4	4	3	2	4	3	3	4	2	2	3	3	2	4	3	2	3	2	3	4	2	2	3	3
3	3	3	2	3	3	2	3	2	2	2	3	2	3	4	2	3	2	2	3	2	2	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2
2	2	3	3	2	2	4	2	2	3	3	3	3	2	3	3	3	2	4	2	2	3	3	3
4	4	4	2	4	4	3	4	3	2	3	3	2	4	3	2	3	3	3	4	3	2	3	3
2	2	4	2	2	2	4	2	4	3	3	3	2	2	4	2	3	4	4	2	4	3	3	3
2	2	4	3	2	3	3	2	3	2	3	3	3	2	3	3	3	3	3	2	3	2	3	3
2	2	3	2	2	2	4	2	4	4	4	3	2	2	3	2	2	4	4	2	4	4	4	3
2	2	3	3	2	2	3	2	2	3	3	2	3	2	2	3	3	2	3	2	2	3	2	2
4	4	4	3	4	4	4	4	3	2	3	4	3	4	3	3	3	3	4	4	3	2	3	3
4	4	3	2	4	3	2	4	2	4	3	3	2	4	2	2	3	2	2	4	2	4	3	3
3	3	2	2	3	3	2	3	4	2	3	3	2	3	4	2	3	4	2	3	4	2	3	3
3	3	4	2	3	3	4	3	4	2	3	3	2	3	3	2	3	4	4	3	4	2	3	3
4	4	4	3	4	4	3	4	3	2	3	3	3	4	2	3	3	3	3	4	3	2	3	3
3	3	3	2	3	3	2	3	3	2	3	3	2	3	2	2	2	3	2	3	3	2	3	2
2	2	2	3	2	2	2	2	3	2	2	2	3	2	2	3	3	3	2	2	3	2	2	2
3	3	4	2	3	3	2	3	2	2	2	3	2	3	2	2	2	2	2	3	2	2	2	2
3	3	4	3	3	3	4	3	2	3	3	3	3	3	3	3	3	2	4	3	2	3	3	3
2	2	4	2	2	2	3	2	2	3	3	2	2	2	3	2	2	2	3	2	2	3	2	2

2	2	2	2	2	2	3	2	4	3	3	2	2	2	3	2	2	4	3	2	4	3	3	3
2	2	4	2	2	2	4	2	3	4	3	3	2	2	2	2	2	3	4	2	3	4	3	3
3	3	2	2	3	3	3	3	4	2	3	3	2	3	2	2	2	4	3	3	4	2	3	3
2	2	3	2	2	2	3	2	2	3	3	2	2	2	3	2	2	2	3	2	2	3	2	2
3	3	4	3	3	3	3	3	3	2	3	3	3	3	2	3	3	3	3	3	3	2	3	3
4	4	4	2	4	4	2	4	2	4	3	3	2	4	4	2	3	2	2	4	2	4	3	3

ANEXO 2: MATRIZ DE CONSISTENCIA

TITULO: CIBERSEGURIDAD Y SU RELACIÓN EN LA SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS EN LAS INSTALACIONES PARA LOS CADETES DE LA ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI, AÑO 2019

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES / DIMENSIONES / INDICADORES			INSTRUMENTOS / METODOLOGIA
P. GENERAL	**O. GENERAL**	**H. GENERAL**	**Variable X**	**DIMENSIONES**	**INDICADORES**	**TIPO**
¿En qué medida el sistema de información de vigilancia se relaciona con la ciberseguridad en las instalaciones de los cadetes de inteligencia de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2019?	Determinar en qué medida el sistema de información de vigilancia se relaciona con la ciberseguridad en las instalaciones de los cadetes de inteligencia de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2019.	El Sistema de información de vigilancia se relaciona significativamente con la Ciberseguridad en las instalaciones de los cadetes de inteligencia de la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2019.	V (x) Sistema de información de vigilancia	Analógico	-Nivel de seguridad -Solución de problemas	Cuantitativo Básica Transversal
				Digital	- Percepción sobre la mejora de control y seguridad - Nivel de apreciación del sistema de información de vigilancia	DISEÑO: Descriptivo, Correlacional No experimental
Problemas Específicos	**Objetivos Específicos**	**Hipótesis Especificas**	**Variable Y**	**DIMENSIONES**	**INDICADORES**	**TÉCNICAS E INSTRUMENTOS**
Problema Especifico 1	**Objetivo Especifico 1**	**Hipótesis Especifica 1**	V (y) Ciberseguridad en las instalaciones	Gestión de la ciberseguridad	- Infraestructuras tecnológicas - Gestión de conocimiento sobre seguridad e información - Diseminación de información - Interpretación de la información	Encuestas: Cuestionario Revisión documental: Ficha bibliográfica
¿En qué medida la gestión de la Ciberseguridad en las instalaciones se relaciona con el sistema de información de vigilancia de los cadetes de inteligencia de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2019?	Determinar en qué medida la gestión de la Ciberseguridad en las instalaciones se relaciona con el sistema de información de vigilancia de los cadetes de inteligencia de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2019	La gestión de la Ciberseguridad se relaciona significativamente con el sistema de información de vigilancia de los cadetes de inteligencia de la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2019.				
Problema Especifico	**Objetivo Especifico 2**	**Hipótesis Especifica 2**		Prevención de los ataques cibernéticos	- Mecanismos de prevención y protección - Tipos de ataque cibernéticos - Tipos de defensa cibernética - Probabilidad de menaza y magnitud de daño.	
¿En qué medida la prevención de los ataques cibernéticos se relaciona con el sistema de información de vigilancia de los cadetes de inteligencia de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2019?	Determinar en qué medida la prevención de los ataques cibernéticos se relaciona con el sistema de información de vigilancia de los cadetes de inteligencia de la Escuela Militar de Chorrillos Coronel Francisco Bolognesi, año 2019.	La Prevención de los ataques cibernéticos se relaciona significativamente con el sistema de información de vigilancia de los cadetes de inteligencia de la Escuela Militar de Chorrillos coronel Francisco Bolognesi, año 2019.				

Anexo 3. Cuestionario de la variable X

Sistema de información

En este cuestionario no hay respuestas "correctas" o "equivocadas", Nos interesa solo su opinión. Sus respuestas serán tratadas con alto grado de confiabilidad y no afectarán su evaluación. Marque con "X" en los cuadros (1, 2, 3, 4,5) de cada afirmación de acuerdo a los valores mostrado en la tabla.

Escala de valores	
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy alto

Observaciones (precisar si hay suficiencia):

_____

_____

	Preguntas	1	2	3	4	5
1	¿Cómo consideras que esta el nivel de seguridad en la escuela militar?					
2	¿Cómo consideras el nivel de control de seguridad en la escuela militar?					
3	¿Cómo percibes el nivel de riesgo que pone en peligro la vida o la integridad física?					
4	¿Cómo percibes la necesidad de adoptar medidas para garantizar la seguridad de los cadetes?					
5	¿Cómo consideras que una solución tecnológica con cámaras IP puede mejorar el control y seguridad?					
6	¿Qué nivel consideras que una solución tecnológica puede contribuir para prevenir las situaciones de riesgo?					
7	¿Considera que con el sistema de información de videovigilancia se reducirían los robos y hurtos en la escuela militar?					
8	¿Considera que con el sistema de videovigilancia se reduciría los actos de desorden e indisciplina en la escuela militar?					
9	¿Considera que con la implementación del sistema de video vigilancia se mejorara el control y seguridad de la escuela militar?					

Opinion de aplicabilidad: Aplicable ( ) Aplicable después de corregir ( )
No aplicable ( )
Apellido y nombre del juez validador. Dr / Mg:
……. DNI:
……..
Especialidad del validador: ……..
……. De …….. del 2019

Anexo 3. Cuestionario de la variable Y
Ciberseguridad en las instalaciones

En este cuestionario no hay respuestas “correctas” o “equivocadas”, Nos interesa solo su opinión. Sus respuestas serán tratadas con alto grado de confiabilidad y no afectarán su evaluación. Marque con “X” en los cuadros (1, 2, 3, 4,5) de cada afirmación de acuerdo a los valores mostrado en la tabla.

Escala de valores	
1	Muy en desacuerdo
2	En desacuerdo
3	Ni en acuerdo ni en desacuerdo
4	De acuerdo
5	Muy de acuerdo

Preguntas		**1**	**2**	**3**	**4**	**5**
1	¿En la escuela militar de chorrillos existen normas o practicas enfocadas en la ciberseguridad?					
2	¿Cree usted que la ciberseguridad sea importante en la escuela militar?					
3	¿Dentro de la escuela militar existe algún personal encargado de la ciberseguridad?					
4	¡En la escuela militar se realizan análisis de gestión de riesgos informáticos?					
5	¿Existen planes de contingencia ante un ciberataque?					
6	¿Sabe usted que medidas tomar ante un ciberataque?					
7	¿existen herramientas que aseguran su información digital?					
8	¿En la escuela militar asignan presupuesto destinado a la ciberseguridad?					
9	¿en la escuela militar se realiza capacitación y prevención ante amenazas cibernéticas?					

FORMATO DE VALIDACIÓN DE INSTRUMENTO POR EXPERTO

TÍTULO DEL TRABAJO DE INVESTIGACIÓN /TESIS:

"SISTEMA DE INFORMACIÓN DE VIGILANCIA Y LA CIBERSEGURIDAD EN LAS INSTALACIONES DE LOS CADETES DE INTELIGENCIA DE LA ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI, AÑO 2019"

AUTORES:

DIAZ NOA, Carmen Diana.

LUQUE CRUZADO, Jhosiy

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

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

PROMEDIO DE VALORACIÓN DEL EXPERTO: 96%

OBSERVACIONES REALIZADAS POR EL EXPERTO:

GRADO ACADÉMICO DEL EXPERTO: Doctor en Educación

INSTITUCIÓN DONDE LABORA: Escuela Superior de Guerra del Ejército - Escuela de Postgrado

APELLIDOS Y NOMBRES DEL EXPERTO: GALINDO HEREDIA José Antonio

FIRMA:

POST FIRMA: Dr. José A. Galindo Heredia

DNI: 43231422

REFERENCIAS

- ✓ Araujo (2015). Tesis para optar el título de ingeniero: “Implementación de un sistema de videovigilancia para los exteriores de la universidad politécnica salesiana, mediante minicomputadores y cámaras Rapsberry.
- ✓ Bahamón (2016). Construcción de indicadores de gestión bajo el enfoque de sistemas., Universidad Icesi, Departamento Académico de Sistemas, Colombia.
- ✓ Escorsa y Maspons (2001). De la Vigilancia tecnológica a la Inteligencia competitiva., Prentice Hall, Madrid.
- ✓ Ferré (2006). Internet y su impacto en la sociedad actual., Disponible en: http://www.upm.es/canalUPM/notasprensa/Doc2005t02402.html, Acceso en febrero de 2006.
- ✓ León, Castellanos y Vargas (2006). Articulo científico: “Valoración, selección y pertinencia de herramientas de software utilizadas en vigilancia tecnológica. Revista de ingeniería e investigación. Facultad de ingeniería, Universidad nacional de Colombia.
- ✓ Morcillo (2003). Vigilancia e inteligencia competitiva: fundamentos e implicaciones., Disponible en: hffp://www.madrimasd.org/revisfa/revistat7/tribuna/ tribunal.asp, Acceso en julio de 2005., España: Madrid revista U. t7, julio, 2003.
- ✓ RAE (2014). Real academia de la lengua española. Madrid, España.
- ✓ Obregón (216). Tesis para optar el título profesional de ingeniería de sistemas: “Seguridad y monitoreo basado en cámaras IP para la institución educativa La Libertad, 2016”. Escuela profesional de ingeniería de sistema, universidad católica

los ángeles de Chimbote.

- ✓ Sierra (2017). Tesis para optar grado de maestro: “Propuesta del sistema de videovigilancia en la seguridad ciudadana del distrito de pueblo libre 2016 – 2020”. Escuela de postgrado, Universidad Cesar vallejo,

- ✓ Valdebenito (2018). “Un fantasma recorre la web. Aproximación articulo científico critica al trabajo digital y cibervigilancia”. Facultad de ciencias sociales, universidad de Valparaíso. Chile