CAEN Centro de Altos Estudios Nacionales
ESCUELA DE POSGRADO

Análisis de la protección de la información digital de las Fuerzas Armadas en el marco de la política de seguridad y defensa nacional en la región Lima, 2018

TESIS PARA OPTAR AL GRADO ACADÉMICO DE:

MAESTRO EN DESARROLLO Y DEFENSA NACIONAL

AUTOR:

Villarrubia Marcelo, Gabriel Ángel

ASESORES:

Doctor(a): José Apolaya Sotelo
Maestro(a): Humberto Zavaleta Ramos
Maestro(a): Sandor Tamayo Ampuero

LÍNEA DE INVESTIGACIÓN

Seguridad y Defensa Nacional

LIMA PERÚ

2021

Agradecimientos:

Al eterno Dios creador del cielo y la tierra por estar en su presencia y darme el espíritu de sabiduría para entender su palabra e intenciones sobre su justicia divina.

A mi querida familia por su incondicional apoyo y por darme la alegría de estar con ellos.

A nuestros destacados asesores metodológico y temático que, gracias a sus valiosos aportes permitieron concretizar esta investigación científica.

A la Dirección, Docentes y Alumnos participantes de esta prestigiosa casa de estudio, el Centro de Altos Estudios Nacionales que permitieron la consolidación de este informe de investigación final.

Dedicatoria:

Al Dios de Jacob, por brindarme la inteligencia y sabiduría en el recorrer de mi vida.

Al Centro de Altos Estudios Nacionales por acogerme en sus claustros de estudios y brindarme los conocimientos.

A mi esposa Marlene e hijos Daniel y Thiago por la comprensión y apoyo incondicional en realizar esta Tesis.

A mis profesores y asesores por hacer realidad este informe de investigación.

A todos mis compañeros de promoción que pertenecen a esta prestigiosa institución superior de estudio.

Índice

Página

Carátula..... i

Agradecimiento….....ii

Dedicatoria..... iii

Índice iv

Índice de tablas vii

Índice de figuras viii

Resumen… ix

Abstract…..... xi

Introducción..... 13

CAPÍTULO I

I. PLANTEAMIENTO DEL PROBLEMA..... 15

1.1. Descripción de la realidad problemática 16

1.2. Preguntas de investigación..... 18

1.3. Objetivos de la investigación 18

1.4. Hipótesis..... 19

1.5. Justificación y viabilidad…..... 19

1.6. Limitaciones de la investigación..... 20

CAPÍTULO II

II. ESTADO DEL CONOCIMIENTO.....21

2.1. Antecedentes de la investigación. 22

2.1.1 Investigaciones Internacionales 22

2.1.2 Investigaciones Nacionales.....24

2.2. Teorías 26

2.2.1 Protección de la información digital.....26

2.2.2 Políticas de seguridad de la información digital.....41

2.3. Marco conceptual.....46

CAPITULO III

III. METODOLOGÍA DE LA INVESTIGACIÓN 52

3.1. Enfoque de la investigación.....53

3.2. Tipo de investigación.....53

3.3. Método de investigación.....54

3.4. Escenario de estudio 54

3.5. Objeto de estudio 55

3.6. Observable(s) de estudio.....55

3.7. Fuentes de información.....56

3.8. Técnicas e instrumentos de y acopio de información.....56

3.8.1. Técnicas de acopio de información 56

3.8.2. Instrumentos de acopio de información.....58

3.9. Acceso al campo y acopio de información.....60

3.10. Análisis de información.....61

CAPITULO IV

IV. ANÁLISIS Y SÍNTESIS.....63

4.1. Análisis y síntesis de los resultados.....64

4.1.1 Categoría principal.....66

4.1.2 Categoría políticas de seguridad informática.....70

4.1.3 Categoría de infraestructura informática 77

4.1.4 Categoría de recursos económicos.....81

4.1.5 Categoría de amenazas y problemas.....85

4.1.6 Categoría de entidades informáticas 92

4.1.7 Relación entre macro categorías 95

Conclusiones.....96

Recomendaciones.....98

Propuesta para enfrentar la realidad problemática.....100

Referencias bibliográficas 102

Anexos 105

Anexo 01. Matriz de Consistencia

Anexo 02. Matriz de Categorías

Anexo 03. Guía de entrevista

Anexo 04: Agenda de entrevistas

Anexo 05. Ruta de documentos

Índice de tablas

Tabla 1: Elementos con sentido propio 64

Índice de figuras

Figura 1: Planos de actuación en la seguridad informática 29

Figura 2: Top de Amenazas detectadas en América Latina y el caribe..... 34

Figura 3: Pantalla de registro de las entrevistas 58

Figura 4: Ruta de análisis y síntesis de datos cualitativos..... 61

Figura 5: Mapeo temático de las categorías 66

Figura 6: Redes del mapeo temático de las macro categorías… 67

Figura 7: Reagrupación de las macro categorías..... 68

Figura 8: Relación de las macro categorías..... 69

Figura 9: MC1 Política de seguridad informática 70

Figura 10: MC2 Infraestructura informática 77

Figura 11: MC3 Recursos económicos..... 82

Figura 12: MC4 Amenazas y problemas..... 85

Figura 13: MC5 Entidades informáticas 93

Resumen

El presente informe de tesis cuyo título es “Análisis de la protección de la información digital de las Fuerzas Armadas en el marco de la Política de Seguridad y Defensa Nacional en la región Lima, 2018” es una investigación de enfoque cualitativo y está planteado de manera holística. Tuvo como principal objetivo, analizar la protección de la información digital de los centros de informática del Cuartel General del Ejército del Perú, y de los otros dos institutos armados ya sea la Marina de Guerra del Perú y la Fuerza Aérea del Perú en el marco de la ciberseguridad de la Política de Seguridad y Defensa Nacional.

La problemática observada evidencia que existe una limitada protección de la información digital que se encuentra en los centros de informática del Ejercito y de las Fuerzas Armadas, la cual se vería expuesta a las amenazas y ataques informáticos a las bases de datos de los diferentes institutos armados, a través de las redes informáticas presentes en el ciberespacio, y a su vez por las debilidades de ciberseguridad; todas ellas contempladas en el marco de la Política de Seguridad y Defensa Nacional.

El instrumento empleado fue la entrevista semiestructurada aplicada a diferentes especialistas e ingenieros que laboran en los centros de informática del Cuartel General del Ejército, así como también en los departamentos de la informática de la Marina de Guerra y de la Fuerza Aérea del Perú.

Los resultados del estudio concluyen que existe limitada protección de la información digital, así como también se evidencia una relativa vulnerabilidad frente a las ciberamenazas de los centros de informática del Ejercito de la Marina y de la Fuerza Aérea en el marco de ciberseguridad de la Política de Seguridad y Defensa Nacional.

Palabras claves: Protección de la información digital, Políticas de seguridad y defensa nacional- ciberseguridad- redes informáticas.

Abstract

The present qualitative approach thesis report, whose title consists of the "Analysis of the protection of digital information of the Armed Forces in the framework of the National Security and Defense Policy in the Lima region, 2018", proposed in a holistic way, Its main objective was to analyze the protection of digital information in the computer centers of the headquarters of the Peruvian Army, within the framework of cybersecurity of the National Security and Defense Policy.

The problem that was observed is that, there is a limited protection of the digital information found in the Army's computer centers, which would be exposing itself to computer threats and attacks on databases, using computer networks, and that they are present in cyberspace, and for having limited cybersecurity measures within the framework of the National Defense and Security Policy.

The consented elements were obtained through ten interviews with different specialists and engineers who work in the army's computer centers at headquarters.

The results conclude that, there is limited protection of the digital information of the Army's computer centers within the cybersecurity framework of the National Security and Defense Policy, being relatively vulnerable to cyber threats.

Key words: Protection of digital information, National defense and security policies.

Introducción

El presente informe de investigación titulado "Análisis de la protección de la información digital de las Fuerzas Armadas en el marco de la Política de Seguridad y Defensa Nacional en la región Lima, 2018", constituye una investigación abordada de forma holística. Es un estudio de enfoque cualitativo que tiene como principal objetivo, analizar la protección de la información digital de los centros de informática del Cuartel General del Ejército del Perú, de la Marina de guerra y de la Fuerza Aérea, en el marco de la ciberseguridad de la Política de Seguridad y Defensa Nacional. Presenta como problema principal, explicar y describir ¿Cuál es el estado de la protección de la información digital de los centros de informática del Ejército en el marco de la ciberseguridad de la Política de Seguridad y Defensa Nacional?

En la actualidad una de las formas más empleadas de interacción en el mundo se da por medio del ciberespacio en el cual utilizamos diferentes redes informáticas para trasmitir información, siendo que dicha información es digitalizada y que, al momento de transmitirla de una unidad de memoria o base de datos instalados previamente en un ambiente con una seguridad física pueden ser vulnerables de ser tomados o recogidos para fines diversos. Para que estos sistemas de seguridad de la información funcionen, la información es estructurada por protocolos y capas de internet para que pueda llegar a su destino final. Estos paquetes de información, a su vez contienen la dirección de las puertas de salida e ingreso de información las cuales pueden ser obtenidas por personas maliciosas que se aprovechan de algún error de seguridad del sistema, mediante la alteración y/o manipulación del software para robar la información, bloquear, modificar, chantajear a las persona e instituciones

que disponen información valiosa de personal y recursos económicos en sus respectivas bases de datos entre otros. En ese sentido, analizaremos la problemática de estudio planteado.

Este informe final de tesis cualitativa, tiene el siguiente esquema: El capítulo primero, consta del planteamiento del problema de investigación cualitativa, las preguntas de investigación que permitieron responder a los objetivos planteados. En el segundo capítulo, se describe el marco teórico, los antecedentes, bases teóricas y el marco conceptual de los observables determinados en el estudio. El tercer capítulo se describe la metodología, el enfoque, tipos y métodos de investigación, los escenarios de estudio, los observables, y los instrumentos de acopio de información para la investigación. El capítulo cuarto se realizó el análisis y síntesis describiendo los resultados obtenidos en las entrevistas e información obtenida.

Finalmente, tenemos las conclusiones y recomendaciones para luego presentar una propuesta de solución al problema planteado.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática

La posesión de grandes cantidades de información digital en los diferentes servidores y base de datos de los centros de informática del Ejercito y de las Fuerzas Armadas como instituciones públicas del Estado, son recursos valiosos y críticos que necesitan ser protegidos contra ataques y robos de información digital. Una de las problemáticas de poseer grandes cantidades de información digital, es la inseguridad que tienen los servidores y base de datos que están conectados e instalados a los sistemas y redes informáticas de los centros de informática del Ejército. En ese sentido, el Estado actualmente, si bien es cierto que dispone de la Secretaria de Gobierno Digital como organismo gestor de "procesos de innovación tecnológica y de transformación digital del Estado", no dispone aún de un organismo operativo o institución con infraestructuras, herramientas digitales, personal calificado, para que actué y proteja su información digital, según lo establece el concepto de ciberseguridad en la Política de Seguridad y Defensa Nacional del Perú.

Similares acontecimientos sobre la inseguridad de la protección de la información digital, están ocurriendo en otros países. Carbajal (2010) sostiene que "uno de los aspectos centrales de la protección de datos, quizá es uno de los menos tratados en nuestro país por parte de los órganos que han conocido esta materia se encuentra referido a la inseguridad" (p.57). Este tema de la protección de datos se torna relevante porque existe limitada seguridad de la información digital y si a esto sumamos los nuevos procedimientos de ataques cibernéticos que realizan los hackers, entonces resulta apropiado contar con un sistema idóneo de protección de la seguridad para contrarrestar los ataques contra los datos almacenados en los servidores.

El Ejército del Perú y los demás institutos armados a la fecha, no estarían asumiendo esta responsabilidad en forma eficaz y óptima para proteger la información digital de las amenazas existentes en la red informática de las instituciones públicas y privadas. Las instituciones y organismos del Estado peruano entre ellas el Ejército dentro de su infraestructura usan los datos e informaciones digitales, mediante las redes de

internet, las cuales han sufrido ataques por hackers mediante el cual sustraen o destruyen la información digital existente.

Los diferentes sistemas de redes informáticas y base de datos del Estado peruano, en especial el del Ejército del Perú, emplean limitadamente la ciberseguridad para proteger sus informaciones digitales ya que en su protección solo manejan antivirus, firewall adquiridos u otros aplicativos similares, pero estos no resultan lo suficientemente seguros para proteger de manera óptima estos sistemas de seguridad contra los ataques de los hackers.

Los hackers son usuarios que ingresan a todos aquellos sistemas de redes informáticas mediante vectores de ataque en el ciberespacio por la existencia de errores y vulnerabilidades existentes en él , a través de sistemas operativos, y softwares maliciosos que usan las puertas de entrada y salida de las redes informáticas, así como también usan las puertas o también denominados *universal serial bus* (USB) por las cuales el hacker consigue entrar al dominio de las redes informáticas para causar algún daño o robo de información.

Por otro lado, tenemos que, en el Ejercito del Perú existen las siguientes normas relacionadas con el tratamiento de la información y su protección tales como: Directiva Única para el Funcionamiento del Sistema de Telemática y Estadística del Ejército (DUFSITELE) la cual se refiere a normar el uso de la tecnología para el funcionamiento y envió de la información pero que no aborda el tema de protección de la misma. Por otro lado, también se tiene la Directiva N° 001 sobre los Lineamientos de Seguridad de la Información para la Ciberdefensa en el Ejército del Perú, que, a pesar de estar normado, no se estaría cumpliendo por el personal encargado la óptima protección de la información digital de los centros de informática del Ejército.

La problemática de estudio de la presente investigación consistió en explicar, cual es el estado de la protección de la información digital de los centros de informática del Ejército especialmente, institución que pertenece a las Fuerzas Armadas, todo esto

en el marco de la ciberseguridad de la Política de Seguridad y Defensa Nacional del Perú.

La protección de la información digital es de gran relevancia e importancia en el uso y empleo de las bases de datos conectadas a las redes informáticas.

1.2 Preguntas de investigación

De acuerdo a la problemática expuesta se presentan las siguientes preguntas de investigación:

P1 ¿Cuál es el estado de la protección de la información digital de los centros de informática del Ejército?

P2 ¿Cuál es el estado del desarrollo de software seguro para la protección de la información digital de los centros de informática del Ejército?

P3 ¿Cuál es el estado de las infraestructuras para la protección de la información digital de los centros de informática del Ejército?

1.3 Objetivos de la investigación

O1 Explicar el estado de la protección de la información digital de los centros de informática del Ejército.

O2 Explicar el estado del desarrollo de software seguro de los centros de informática del Ejército.

O3 Describir las infraestructuras para la protección de la información digital de los centros de Informática del Ejército.

1.4 Hipótesis

Las hipótesis de investigación planteada es la siguiente:
La limitada protección de la información digital de los centros de informática del ejercito constituye una vulnerabilidad frente a los ataques y sustracción de la información

Se plantea la hipótesis a fin de que sirva de guía en el proceso de la investigación. "En la investigación cualitativa las hipótesis son claves de interpretación que guían los primeros pasos en la recogida de datos" Ruiz (como se citó en Izcara 2014).

1.5 Justificación y viabilidad

La investigación se justifica en la medida en que contribuye con hallazgos importantes referidos al tema a fin de mejorar el estado actual de la protección de la información digital de los centros de informática del Ejército, institución que pertenece las Fuerzas Armadas del Perú.

Así mismo, la investigación contribuye a minimizar la problemática de los ataques a las redes informáticas en el robo o manipulación de la información digital, no solo del Ejército, sino que podrían los resultados ser generalizables a las otras dos instituciones de las fuerzas armadas.

Esta investigación también aporta con el fortalecimiento de conocimientos teóricos sobre la protección de la información digital. La Fundación Telefónica (2016) mediante la Editorial Ariel publica el libro "Ciberseguridad, la protección de la información en un mundo digital". En la actualidad la mayoría de países transmiten la información digital para remitirla mediante las redes de internet, y esta información necesita ser protegida para evitar ser robada o manipulada por personas indebidas o más conocidos como los hackers.

La viabilidad de la investigación, conforme al título planteado: Análisis de la protección de la información digital de las Fuerzas Armadas en el marco de la Política

de Seguridad y Defensa Nacional en la región Lima, 2018, se realizó reorientando el estudio solo al Ejército como institución que pertenece a las Fuerzas Armadas del Perú y siendo que, los ataques informáticos se dan utilizando el ciberespacio y espectro electromagnético contra la información digital y datos de personal y de la institución, que se encuentra alojada en las memorias y servidores de los centros informáticos del Ejército. Asimismo, la investigación fue posible, ya que el investigador conocía el entorno de la situación problemática y trabaja para el sector público del sector defensa.

1.6 Limitaciones de la investigación

La escasez de bibliografía específica de las categorías y sub categorías de estudios, otros trabajos previos sobre este tema, así como el tiempo es un factor de consideración, sin embargo, estas limitaciones fueron superadas.

Fernandez y Otros (2014) sostiene que “son realidades que van modificándose conforme transcurre el estudio y son fuente de datos” (p. 9).

De igual forma en el marco de una investigacion al plantear un problema, se requiere de la exploración y descripción de los hechos. Fernàndez y Otros (2014) afirma: “la investigación cualitativa se basa más en una lógica y proceso inductivo y van de lo particular a lo general” (p. 8).

CAPITULO II

ESTADO DEL CONOCIMIENTO

2.1 Antecedentes de la investigación

2.1.1 Investigaciones internacionales

Escalante y Vidarte (2018). ***Conflictos entre la gobernabilidad y soberanía en las organizaciones multilaterales: estudio fue la implementación de políticas de seguridad informática entre los años 2004-2006 en la Unión Europea***", de la Pontificia Universidad Católica del Perú, siguiendo la metodología cualitativa, tuvo como objetivo analizar las causas de la inexistencia de políticas públicas comunitarias en la Unión Europea que garanticen de manera eficaz la seguridad informática, concluye que: Las políticas públicas que buscan generar espacios virtuales seguros responden al uso que, el estado les ha dado a los sistemas informáticos para el almacenamiento de la información relevante para la consecución de sus intereses nacionales. Siendo así, se debe considerar que la información, en sí misma, tiene un gran valor para la toma de decisiones del Estado.

La Unión Europea es una organización comunitaria supranacional que, a la luz de lo expuesto en la presente investigación, es incapaz de generar políticas de seguridad informática de aplicación en todo el espacio comunitario. Esto debido a las constantes fricciones que se producen entre los intereses nacionales de los países con capacidad de influir en los procesos de toma de decisiones: Alemania, Reino Unido y Francia. La incapacidad de generar un apolítica comunitaria afecta la gobernabilidad informática en la materia, esto se ve materializado los múltiples ataques que se han sido señalados en el presente trabajo y que ha ocurrido en los últimos años. La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) tiene años de existencia y ha sido incapaz de generar un espacio comunitario seguro, de protección eficaz de la información y esto conllevo a que la Organización del Tratado Atlántico Norte (OTAN), una alianza militar independiente de la Unión Europea (UE), asuma un rol protagónico en esta materia y escenario.

Otra conclusión importante que refiere el estudio expresa: “la incapacidad de generar una política comunitaria informática en la materia, esto se ve materializado los múltiples ataques que han sido señalados en el presente trabajo y que la ENISA tiene años de existencia y ha sido incapaz de generar un espacio comunitario seguro, de protección eficaz de la información”.

Bugarini H, F. (2007). ***Una propuesta de seguridad en información: Caso Systematics de México, S.A***. en su tesis de Maestría realizado en el Instituto Politécnico Nacional, para obtener el grado de Maestría en Ciencias en Administración de Negocios, empleando la metodología mixta, con aspectos cuantitativos y cualitativos, y cuyo objetivo fue elaborar una propuesta que permita fomentar una cultura de seguridad informática, que minimice los riesgos en la continuidad del proceso y la eficacia del servicio de informática, lo que se conseguirá en función de que se identifiquen las amenazas y la atención se enfoque a los problemas relacionados a la seguridad y al tratamiento de la información dentro de la organización. Tuvo como resultado que: de las dos categorías de riesgos analizadas, observo que la organización “carece de medidas de seguridad adecuadas y que la falta conciencia del tema de la seguridad a nivel organizacional, aunque ya ha sufrido percances sumamente difíciles y costosos también que los usuarios no tienen cultura informática respecto a este tema” (p. 83). Otro resultado fue que: “el personal que labora en las empresas desconocen las amenazas informáticas por los usuarios de la misma evidenciando la dificultad para mostrar a la alta Dirección el valor estratégico que implican los esquemas de seguridad, teniendo dependencia tecnológica de las organizaciones a todos sus procesos debemos proteger la información para lo cual planteo una propuesta de seguridad informática” (p. 83). Como conclusión final nos dice que “la importancia que tiene la seguridad de la información en cualquier organización y tomando en cuenta las opiniones Symantec, respecto a que la información fluye mediante diversos medios y canales que la tecnología de la información ha sido diseñada considerando solo la escalabilidad, más que la seguridad, son vulnerables a la falsificación de las cuentas y potencialmente de fácil acceso a ataques de servicio, reflexionando sobre el impacto que causan los virus MBR, encriptado, oculto en archivos, diversos troyanos, gusanos, diversas amenazas como backdoors, spyware, sniffers, código malicioso,

keylogers, rootkits por corporativos dedicados a la protección de la información como Sophos, Panda Security, firmas como E&Y, PWC,CYBSEC, Websense UNISYS y centros de investigación a la detección de vulnerabilidades como el CERT e ISACA como se señaló que las pérdidas se pueden ocasionar ya sea en aspectos contables y su trascendencia en el factor financiero de la empresa afectada, se ha elaborado la propuesta para subsanar las carencias que tienen los usuarios para resguardar su información " (p. 86).

López (2016). ***Analíticas de Seguridad de código fuente de la Pontificia Universidad Carlos III de Madrid***, en su tesis siguió la metodología descriptiva, y tuvo como objetivo: la construcción de reglas que permitan detectar fallas o vulnerabilidades en el código fuente de las aplicaciones, concluye que: "la mayoría de empresas esperan demasiado tiempo para ejecutar el análisis de seguridad en sus aplicaciones. Es necesario incluir análisis de seguridad desde el inicio de la vida del software, o sea desde el plan de desarrollo". Otra conclusión importante que presenta el estudio es: "incluir la seguridad en el SDL (Secure Development Lifecycle) es la forma más adecuada de solucionar los problemas, si se espera al final del desarrollo los fallos se podrían convertir en daños económicos para las compañías y el precio de solucionarlos es siempre más caro si los fallos son detectados a posteriori" (p. 80).

2.1.2 Investigaciones nacionales

Zúñiga (2017). ***Ciberdefensa y su incidencia en la protección de la información del Ejercito del Perú. Caso: COPERE 2013-2014"***, estudio realizado en la Escuela de Post grado del Instituto Científico y Tecnológico del Ejercito (ICTE), para optar el grado académico de Magister en Ingeniería de Sistemas de Armas, en su tesis de investigación realizada, siguió la metodología cuantitativa, y tuvo como objetivo principal: determinar las dificultades que impiden el mejoramiento de la Ciberdefensa y su incidencia en la protección de la información del ejercito del Perú, concluye que: "Se presenta dificultades que impiden el mejoramiento de la Ciberdefensa y su incidencia en la protección de la información del Ejército del Perú, porque esta investigación ha probado la existencia de deficiencias en los programas de capacitación, al no disponer de Personal Militar o Civil que cuente con un

adecuado nivel de capacitación en Ciberdefensa; así como, no tener un nivel adecuado de conocimiento de la Norma Técnica Peruana NTP/ISO/IEC 17799 – "Código de buenas prácticas para la gestión de la seguridad de la información; la existencia de carencia de recursos disponibles para Ciberdefensa, al no disponer de un nivel adecuado de asignación presupuestal, para ser utilizado en Ciberdefensa; así como, no disponer de un nivel adecuado de funcionalidad de las infraestructuras estratégicas para el uso en ciberdefensa; la existencia de desconocimiento o aplicación incorrecta de los procedimientos de seguridad que dificultan el mejoramiento de la Ciberdefensa y su incidencia en la protección de la información del Ejército del Perú, como consecuencia que el personal Militar o civil no conoce o aplica adecuadamente los conceptos y principios básicos relacionados con ciberdefensa; y la existencia de incumplimientos de dispositivos normativos que puedan darse de forma internas o externas referidos al Decreto Supremo N° 66-2011-PCM, Plan de Desarrollo de la Sociedad de la Información en el Perú. La Agenda Digital 2.0., o Plan Estratégico Institucional "Bolognesi" o la Directiva Única de Funcionamiento del Sistema de Telemática y Estadifica del Ejercito (DUFSITELE) o la Directiva - Lineamientos de seguridad de la información para la Ciberdefensa en el Ejército del Perú, como consecuencia que el personal Militar o civil desconoce o no aplica las mencionadas disposiciones normativas…". De igual forma el estudio plantea la siguiente conclusión: La Agenda Digital 2.0., o Plan Estratégico Institucional "Bolognesi" o la Directiva Única de Funcionamiento del Sistema de Telemática y Estadifica del Ejercito (DUFSITELE) o la Directiva - Lineamientos de seguridad de la información para la Ciberdefensa en el Ejército del Perú, como consecuencia que el personal Militar o civil desconoce o no aplica las mencionadas disposiciones normativas.". Finalmente, presenta como conclusión que: se observa la existencia de carencias en el nivel asignación Presupuestal, Carencias en el nivel de Funcionalidad de las infraestructuras estratégicas y Carencias en el nivel de recursos 191 disponibles relacionados con ciberdefensa y su incidencia en la protección de la información del Ejército del Perú" (p. 206).

Inoguchi y Macha (2017). ***Gestión de Ciberseguridad y prevención de los ataques cibernéticos en las Pymes del Perú 2016***. Tesis de investigación realizada en la facultad de ingeniería de la Universidad San Ignacio de Loyola, la metodología cuantitativa, tuvo como objetivo determinar la gestión de ciberseguridad con la prevención de los ataques cibernéticos en las Pymes, concluye que: La empresa Zavala Cargo SAC tiene una falta del uso de planes contra ataques de seguridad cibernético que resguarden su información permitiendo así, una toma de decisiones más confiable. La importancia que se debe dar al resguardo de su información cibernética, ya que, si dicha información fuese robada o manipulada por personas ajenas a la empresa conllevaría a resultados adversos para la empresa misma, a tal punto de quebrar. Finalmente, como conclusión expresa los resultados de las pruebas de seguridad informática que se hizo a la empresa de Transporte Zavala Cargo SAC permitió evidenciar la falta de conocimiento de seguridad de la información cibernética de todo el recurso humano que labora en la empresa, así como todos los riesgos cibernéticos de información vital y privada de la misma. Dejando así a la empresa vulnerable a todos los riesgos cibernéticos de información vital y privada de las misma. La realización de nuestro trabajo permitió ayudar a que la empresa Transporte Zavala Cargo SAC.

2.2 Teorías

Para el desarrollo del estudio se tomaron las siguientes teorías:

Observables 1:

2.2.1 Protección de información digital

La protección de la información digital está dentro de la seguridad de la información y se encuentra estrechamente relacionada con la seguridad informática por lo cual es importante describir las bases teóricas necesarias para cumplir los objetivos de la investigación.

La protección de la información digital es el estado de certeza que un organismo, institución o persona tiene sobre la seguridad de la información digital o activos críticos que se encuentran grabados en una base de datos, servidores o unidades de memorias. Gómez (2011) afirma que:

> Las actividades cotidianas de las empresas y de las distintas Administraciones Públicas e, incluso, las de muchas otras instituciones y organismos, así como las de los propios ciudadanos, requieren del correcto funcionamiento de los sistemas y redes informáticas que las soportan y, en especial, de su seguridad (p. 38).

Seguridad informática

La seguridad informática está basada en la seguridad y protección de la información digital o datos que circula por las diferentes redes informáticas o de internet. De acuerdo a ello Gomez, (2011) afirma: "medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información" (p. 38). Son las medidas de seguridad digital o electrónica, que debe tener las redes informáticas, para evitar el ingreso de usuarios no autorizadas a las redes informáticas existentes.

Existen ciertas consideraciones que se debe tener en cuenta para proteger la información digital. (Gomez, 2011) sostiene "aspectos o cuestiones relacionados cuando se habla de Seguridad Informática" (p.38).

- Cumplimiento de las regulaciones legales aplicables a cada sector o tipo de organización.
- Control en el acceso a los servicios ofrecidos y la información guardada por un sistema informático.
- Control en el acceso y utilización de ficheros protegidos por Ley: contenidos digitales con derechos de autor ficheros con datos de carácter personal etc.
- Identificación de los autores de la información o de los mensajes.
- Registro del uso de los servicios de un sistema informático etc.

Objetivos de la seguridad y protección de la información

De acuerdo a lo expresado por Gómez (2011) los principales objetivos de la protección de la información se encuentran detallados de la siguiente manera:

> Objetivo 1: Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
>
> Objetivo 2: Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
>
> Objetivo 3: Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
>
> Objetivo 4: Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos (p. 40).

De igual forma Gómez (2011) expresa que para cumplir con estos objetivos una organización debe contemplar cuatro planos de actuación, tales como:

> Plano Técnico: Tanto a nivel físico como a nivel lógico. Corresponde la selección, instalación configuración y actualización de soluciones de hardware y software.
>
> Plano Legal: algunos países que en determinados sectores implantan una serie de medidas de seguridad (sector de servicios financieros y sector sanitario en Estados Unidos, protección de datos personales en todos los Estados miembros de la Unión Europea etc.). Debiendo tener el cumplimiento y adaptación a la legislación vigente.
>
> Plano Humano: sensibilización y formación de empleados y directivos definición de funciones y obligaciones del personal.

Plano Organizativo: definición e implantación de políticas de seguridad planes, normas, procedimientos y buenas prácticas de actuación.

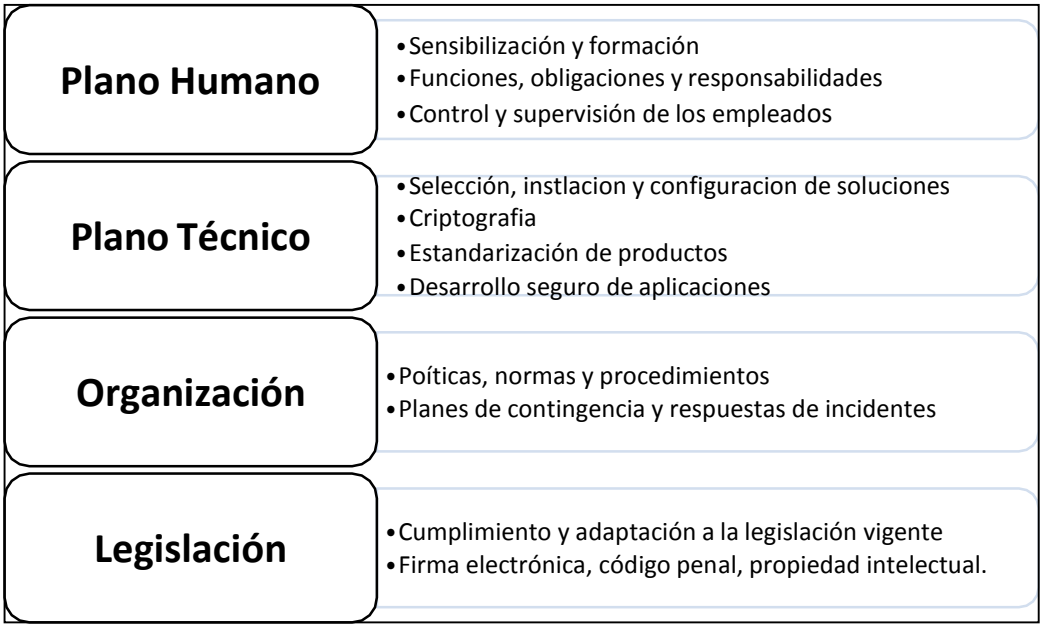

Figura 1 Planos de actuación en la seguridad informática

Fuente: Gómez (2011, p.41)

Servicios de seguridad de la información

Para la protección de la información, es necesario que existan ciertos servicios que contribuyan a incrementar la seguridad, no solo de la información sino del proceso que sigue, para ellos vamos a describir ciertos servicios o funciones (Gomez, 2011) nos expresa lo siguiente :

Confidencialidad

Mediante este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático solo podrá ser leído por su legítimo destinatario. Si dicho menaje cae en manos de terceras personas estas no podrán acceder al contenido del mensaje original. Por lo tanto, este servicio pretende garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de backup y/o de los datos trasmitidos a través de redes de comunicaciones (p. 42).

Autenticación

La autenticación está relacionada en identificar la procedencia del remitente de la información, de tal forma que el receptor de la información tenga la certeza que la información que está recibiendo es de procedencia conocida y segura. (Gomez, 2011) (p. 47). “La autentificación garantiza que la identidad del creador de un mensaje o documento es legítima, es decir, gracias a esta función, el destinatario de un mensaje podrá estar seguro de que su creador es la persona que figura como remitente de dicho mensaje.

Integridad

Este servicio de integridad se refiere a que la información recibida no haya sufrido modificaciones por hackers o usuarios al momento de ingresar ilícitamente a una red y base de datos que pueda manipular, agregar, modificar dicha información remitida.” (Gomez, 2011) nos dice “la integridad se encarga de garantizar que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión, a través de una red informática (p. 43).

No repudiación

La no repudiación se refiere a determinar fehacientemente el origen de la autoría, mediante el cual se identifica a la persona que creó el mensaje, para que, si en un futuro se necesite identificar el origen de creación del mensaje, este no pueda negarse en la responsabilidad de la creación de su mensaje. Gómez (2011) sostiene: "implementar un mecanismo probatorio que permita demostrar la autoría y envío de un determinado mensaje" (p 43).

Disponibilidad

La disponibilidad de la información digital a través del uso de las redes de internet debe estar a disposición del personal que lo necesita y para esto juega un papel muy importante la protección y seguridad, tanto en la trasmisión de los datos por las redes de internet, como la seguridad del software instalado en los servidores o computadores. (Gomez, 2011) sostiene que "de nada sirven los demás servicios de seguridad si el sistema informático no se encuentra disponible para que pueda ser utilizado por sus legítimos usuarios y propietarios" (p. 43). Normalmente algunos sistemas informáticos disponen de una red y base de datos alterno, caso una red no funcione entra en operación el sistema alterno.

Autorización

Mediante el servicio de autorización se persigue controlar el acceso de los usuarios a los distintos equipos y servicios ofrecidos por el sistema informático, una vez superado el proceso de autenticación de cada usuario. Para ello, se definen unas Listas de Control de Acceso (ACL) con la relación de usuarios y grupos de usuarios y sus distintos permisos de acceso a los recursos del sistema.

Consecuencias de la falta de seguridad en la información digital

La falta de seguridad o limitada protección de la información digital puede llegar a tener un costo muy alto para cualquier empresa que usa las tecnologías de la información y comunicaciones.

Dicho costo por la pérdida de información puede llegar a tener ciertos perjuicios para la organización. Gómez (2011) nos dice que "el impacto total para una organización puede resultar bastante difícil de evaluar, porque además de los posibles daños ocasionados a la información guardada, equipos y dispositivos de red, deberíamos tener en cuenta otros importantes perjuicios para la organización" (p. 49), esto puede ser:

> Horas de trabajo invertidas en las reparaciones y reconfiguración de los equipos, pérdidas ocasionadas por la indisponibilidad de diversas aplicaciones y servicios informáticos, robo de información confidencial y posible revelación a terceros, filtración de datos personales de usuarios registrados en los sistemas, posible impacto negativo a la imagen de la empresa ante terceros, retrasos en los procesos de producción perdidas de pedidos, posibles daños a la salud de las personas con pérdidas de vidas humanas, pago de indemnizaciones por daños y perjuicios a terceros.

La explicación a este fenómeno de perdida de la información por causas de "ataques que, en el caso de las empresas, tienen un impacto directo sobre la línea de flotación del negocio: 75,000 euros es el coste estimado de un ciberataque para una empresa promedio" (Iglesias, s.f.).

Gestión de riesgos en un sistema informático

Todo sistema informático actualmente necesita tener un proceso de gestión de riesgos, amenazas y vulnerabilidades para minimizarlos dado que ello va contribuir en tener una mejor protección de la información digital que se encuentran almacenadas en las memorias o discos duros de los servidores o de base de datos.

Riesgos

Gómez (2011) afirma: “El riesgo es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización “(p. 63). Al detectarse una vulnerabilidad se debe realizar la gestión para por lo menos minimizarla, debido que actualmente ningún sistema es cien por ciento seguro.

Amenazas

Markus Erb (s.f.) afirma: “una amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema”.

Conforme a la Figura 2 sobre las amenazas detectadas en América Latina y el Caribe. (López, 2019) a través de Symantec afirma que el correo electrónico es un fuerte vector de ciberataques, siendo el país más atacado Brasil, mientras tanto el Perú ocupa la posición séptima.

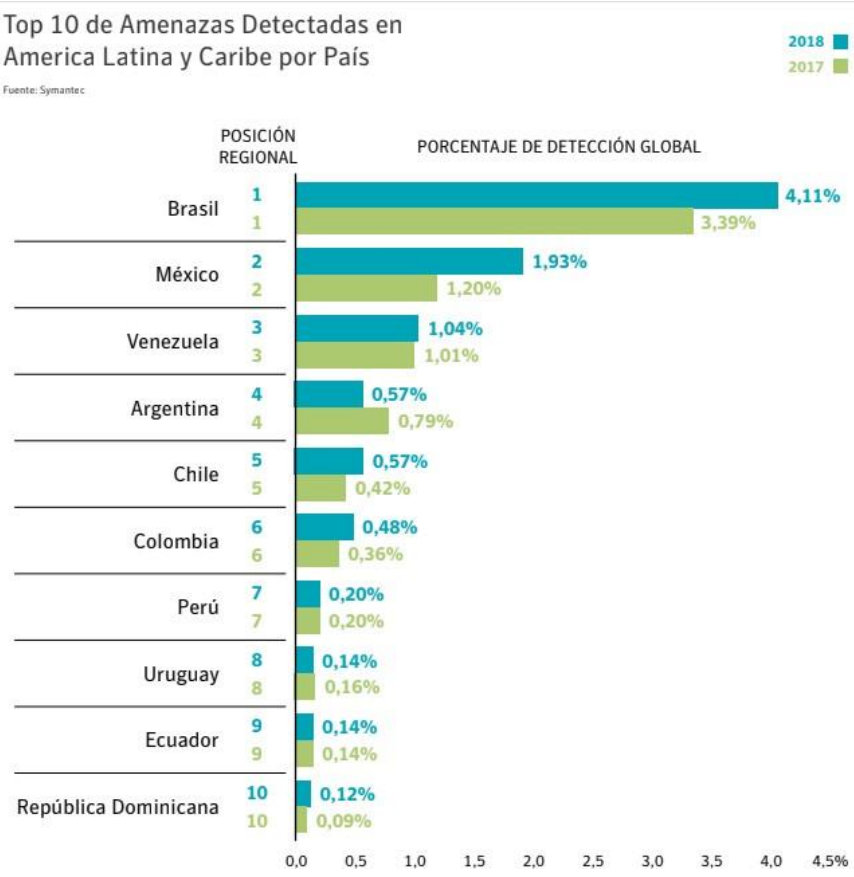

Figura 2 Top de Amenazas detectadas en América Latina y el caribe
Fuente: Symantec (2018)

Vulnerabilidades

Es la debilidad o fragilidad que posee un sistema informático frente a los riesgos existentes. Markus Erb (s.f.) afirma: "Las vulnerabilidades están en directa relación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño".

Para reducir o mitigar las vulnerabilidades se tiene que realizar el mantenimiento o el up grades a los diferentes sistemas informáticos existentes en una red. Harán (2020) afirma que "el último paquete de actualizaciones de seguridad publicado por Microsoft alcanzo un record en cuanto a las cantidades de vulnerabilidades mitigadas en una actualización" (Harán, 2020)

Incidentes de seguridad

Gómez (2011) afirma: “un incidente de seguridad es cualquier evento que tenga o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras” (p. 62).

Principios de defensa en profundidad

Este principio de la “defensa en profundidad” se refiere a la existencia de varios anillos o barreras de seguridad que se puede tener para proteger la información digital. (Gomez, 2011) sostiene que “si una de las barreras, es franqueada por los atacantes, conviene disponer de medidas de seguridad adicionales que dificulten y retrasen su acceso a información confidencial” (p. 51).

Gestión de la seguridad de la información digital

El término Gestión se encuentra relacionado con la administración de la seguridad de la información, siendo que la gestión de la seguridad de la información se refiere a la protección de la información digital como activos críticos que deben ser protegidos. Gómez (2011) sostiene que “parte del sistema general de gestión que comprende la política, la estructura organizativa, los recursos necesarios, los procedimientos y procesos necesarios para implantar la gestión de la seguridad de la información en una organización” (p. 52). Como se puede evidenciar la gestión es bastante amplia acerca de este concepto sin embargo únicamente se va a tratar aquellos puntos que son parte de la materia de investigación, tales como los recursos necesarios u otros que se estime conveniente.

Vector de ataque contra un objetivo

Los hackers cuando pretenden robar información de una base de datos, emplean como instrumento las redes informáticas o internet. Para poder ingresar a un servidor, computador u ordenador tienen que trazarse una ruta de ataque y para ello es preciso conocer detalladamente la ruta o vector de ataque caso contrario no podría ingresar

al computador y lograr sustraer la información pública, ya sea para venderla, destruirla o manipularla, etc.

Los hackers, para poder hacer el seguimiento de un objetivo de ataque tienen que conocer ciertas herramientas tales como:

- Nombre del dominio: Es la puerta de entrada principal de la dirección del protocolo de internet (IP). "El dominio se obtiene descartando el primer indicador por la izquierda de la siguiente dirección: www.arcos.es para este caso sería: arcos. es".
- Dirección IP: Identifica la dirección donde se va a realizar el ataque a través de los servicios disponibles.

Etapas de la seguridad de la información

La información digital sigue un proceso al ser remitida por las redes informáticas, en tal sentido para poder gestionar la seguridad de la información, esta se va dividir en fases o etapas. Gómez (2011) "podemos distinguir varias etapas o niveles de madurez en la Gestión de Seguridad de la Información" (p. 55). Estas etapas son:

> Implementación de medidas básicas de seguridad por sentido común, en esta primera etapa se considera las medidas de seguridad habituales existentes en la cuales la mayoría de las personas realizan en su computadora trabajos como, realizar copias de seguridad en un disco duro externo, instalar un antivirus de los muchos existentes, adaptación a los requisitos del marco legal y de las exigencias de los clientes. En esta parte las organizaciones y empresas evidencian cumplir alguna legislación existente tales como la protección de la propiedad intelectual, gestión integral de la seguridad de la información. En esta etapa, la organización mediante personal especialista planea e implanta normas, procedimientos de empleo y usos de la información y de las redes informáticas. Para tener una mejor referencia en "definición de una serie de políticas de seguridad, la implantación de planes y procedimientos de seguridad, el análisis y gestión de riesgos y la definición de un plan de respuesta a incidentes y de continuidad del negocio" (Gomez, 2011, p. 55).

Certificación de la Gestión de la seguridad de la información.

En esta última etapa, las organizaciones pretenden acreditarse con una empresa que les certifique mediante una evaluación de la calidad en la protección de sus activos informáticos en sus bases de datos. Y en ese sentido usan los llamado ISO 27001.

El autor señala lo siguiente: de acuerdo a la cuarta etapa se pretende llevar a cabo una certificación de la Gestión de la Seguridad de la Información, para obtener el reconocimiento de las buenas practicas implantadas por la organización y poder acreditarlo ante terceros (confianza y verificabilidad por parte de terceros): clientes, administraciones públicas y otras instituciones. Para ello, se recurre a un proceso de certificación basado en estándares como la ISO 2700.

Gestión del control de acceso a la información

La gestión del control de acceso a la información se relaciona con las medidas que se debe tener en el proceso de trámite y envío de la información o mensajes, en este caso implica el personal responsable encargado de la gestión y trámite de la información, para ello, dicho personal debe estar debidamente autorizado para administrar, gestionar reenviar, guardar la información y mensajes que tenga clasificación de reservado. (Areitio, 2008) sostiene que "la efectividad de mecanismo de un control de acceso depende casi por completo de la precisión y de la confianza en la información utilizada para la toma de decisiones de control de acceso. Debe tenerse mucho cuidado para asegurar que la información que describe la política de control de acceso solo pueda generarse o revisarse por un individuo previamente autorizado. Esta información estará sujeta, por tanto, a la propia política y al propio mecanismo de protección de control de acceso, a un nivel incluso más sensible que los objetivos protegidos por estos mecanismos" (p. 134). Cabe indicar que debe existir en cada institución una política clara, difundida, concientizada por parte de todo el personal que labora en una institución pública.

Permisos de control

Los permisos de control de acceso a la información, debe ser gestionados por personal especialista que tengan un cierto grado de responsabilidad dentro de la organización o institución pública, para ello se debe realizar un registro de todos los procesos para dicho control. Fundación Telefónica (2016) afirma que: "el control de acceso que permita controlar de una forma ordenada que objetos se conectan y si tienen derecho a conectarse" (p. 53). Resulta fundamental tener el control de los accesos mediante tablas registradas en la base de datos, caso sea necesario realizar procesos de auditoria como medio de control.

Amenazas contra la protección de la información digital

Hackers: son usuarios que ingresan a una red informática para tener acceso a la información digital. Gómez (2011) afirma: que los hackers son intrusos que se dedican a estas tareas como pasatiempo y como reto técnico: entran en los sistemas informáticos para demostrar y a poner a prueba su inteligencia y conocimientos de los entresijos de Internet, pero no pretenden provocar daños en estos sistemas. Sin embargo, hay que tener en cuenta que pueden tener acceso a información confidencial, por lo que su actividad está siendo considerada como un delito en bastantes países de nuestro entorno.

> Los hackers defienden sus actuaciones alegando que no persiguen provocar daños en los sistemas y redes informáticas, ya que solo pretenden mejorar y poner a prueba sus conocimientos. Sin embargo, el acceso no autorizado a un sistema informático se considera por sí mismo un delito en muchos países (p. 196).

Crackers: son personas con conocimiento de redes y lenguajes de programación que ingresan a una red informática para cometer ilícitos con la información digital y para obtener un beneficio económico. Gómez (2011) afirma: "son individuos con interés en atacar un sistema informático para obtener beneficios en forma ilegal o simplemente para provocar un daño a la organización propietaria del sistema" (p. 196). Los crackers son individuos con interés en atacar un sistema informático para obtener beneficios de forma legal o, simplemente, para provocar algún daño a la organización propietaria del sistema, motivados por intereses económicos, políticos, religiosos, etcétera.

Técnicas de hacking

Las técnicas de hacking que se define como "la búsqueda y explotación de vulnerabilidades de seguridad en sistemas o redes". En otras palabras, el **hacking** consiste en la detección de vulnerabilidades de seguridad, y también engloba la explotación de las mismas". Y las técnicas de hacking más comunes son el Phishing, Archivos adjuntos maliciosos, Robo de cookies, Keylogger, Ataques DDoS.

La señal de internet es un servicio que permite la trasmisión de datos o información a través del ciberespacio, por si sola es una vía de trasmisión que no requiere de hardware ni de software mientras que los sistemas o redes de informática para poder funcionar necesitan de ellos. En el desarrollo de esta investigación se trató mayormente la parte del software.

Los softwares son tipos de lenguajes de programación que consisten en un conjunto de sentencias, órdenes y comandos en forma lógica y ordenada, compuestos por algoritmos que, luego se ejecutan en las memorias y procesadores de los computadores. Estos normalmente son desarrollados sin tener en consideración niveles de seguridad desde su planeamiento e implementación.

El software también es conocido como una aplicación o programa informático que es desarrollado por personas conocidas como programadores. Dichos programas informáticos o aplicaciones desarrolladas muchas veces tienen ciertos errores o vacíos en la protección dejando puertas lógicas abiertas o direcciones web. Fundación Telefónica (2016) afirma que: "establece bien claro que la mayoría de los problemas de seguridad se concentran en las fases de diseño, mantenimiento y operación" (p. 105). Las personas mal intencionadas o conocidos como hackers se aprovechan de dichos errores o vacíos para poder vulnerar o ingresar maliciosamente a las bases de datos o servidores utilizando los puertos abiertos de las redes informáticas o internet.

Ciberseguridad

La ciberseguridad se relaciona con los diferentes tipos de herramientas existentes para la protección de la información digital que se encuentran grabados en los centros de datos, unidades de memorias o también conocidos como big data. Canes & Pastrana (2014) sostiene que:

> Es un conjunto de técnicas, herramientas y mecanismos que tienen como objetivo la protección de los sistemas, datos y usuarios que interaccionan en el ciberespacio. Hay numerosas herramientas de seguridad, como los conocidos cortafuegos los registros de eventos, o los Sistemas de Detección de Intrusiones (SDI). Estos analizan el tráfico entrante y buscan cualquier signo de intento de comprometer la seguridad de los sistemas. (P. 13).

Tipos de Ciberdelitos

Los Ciberdelitos son los delitos informáticos que cometen personas intrusas usando como herramienta la internet, redes informáticas, y las fallas y errores que tienen los softwares y aplicativos que se encuentran instalados en dichos ordenadores.

En cuanto a los tipos de delitos informáticos tenemos una clasificación en dos tipos de sentidos. (Hess, 2010) sostiene que “desde una perspectiva objetiva vamos a considerar como delito informático a cualquier fenómeno ilícito, cualquier conducta atípica, antijurídica, prevista en la legislación penal, en donde el objetivo del delito es un bien o servicio propio del mundo de la informática” (p. 130).

El segundo sentido es más funcional en el cual la persona que comete este tipo de delitos informáticos usan las redes informáticas, internet o las fallas del software o aplicativo instalados en los computadores para poder robar o manipular la información de una base de datos. (Hess, 2010) nos dice que “el sistema de cómputo ya no es el blanco de la conducta delictiva sino apenas una herramienta para cometer ilícitos contra terceras personas” (p. 130). Tanto las redes informáticas, como la internet, empleo de software malicioso aprovechando los errores que tiene un aplicativo instalado en un computador, estos son usados como herramientas e instrumentos para cometer los delitos informáticos.

Observables 2:

2.2.2 Política de seguridad de la información digital

Las políticas de seguridad y protección de la información digital son todas las normas y disposiciones escritas, aprobadas difundidas, socializadas con los responsables de la organización, que sirve como herramienta para poder dar estricto cumplimiento y compromiso a fin de salvaguardar y proteger los activos críticos de información digital. Aquino y otros (2010) afirma que “las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicio críticos que permiten a la institución crecer y mantenerse competitiva” (p.28) .

Política de seguridad y defensa nacional del estado peruano 2017

En la novena política de estado del Acuerdo Nacional que fue aprobado en el año 2002 por los diferentes partidos políticos y sociedad civil acordaron el compromiso para mantener una política que garantice la independencia soberanía e integridad territorial de acuerdo a los intereses nacionales del Perú.

Por otro lado, se continua el proceso de fortalecimiento de las normas para la protección de la información digital. "La Ley de Gobierno Digital, aprobada por Decreto Legislativo Nº 1412, establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos. Asimismo, define el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno. (p. 4).

Definición de Política de seguridad informática

Las políticas de seguridad informática tienen un sentido más amplio que, simplemente disposiciones legales, y normas técnicas dadas para realizar la comunicación y transferencia de la información. (Aquino, y otros, 2009) afirma:

> No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de lo que deseamos proteger y el porqué de ello, pues cada política de seguridad, es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos, así como un motor de intercambio y desarrollo en el ámbito de sus negocios. (p. 51).

Se puede definir a la política de seguridad informática como un conjunto de procedimientos que deben cumplir todos los involucrados en forma consciente y responsable para el tratamiento de la información como también se podría entender que "una política de seguridad informática es una forma de comunicarse con los usuarios, ya que la misma establecen un canal final de actuación del personal, en relación con los recursos y servicios informáticos de la organización" (Aquino, y otros, 2009, p.29).

La comunicación de los usuarios implica cierto conocimiento del tratamiento de la información desde el momento que sale de un computador hasta el momento que debe llegar al otro ordenador en forma segura.

Infraestructura para enfrentar ataques a los sistemas de información: Ciberseguridad

Las infraestructuras físicas pueden ser consideradas la tenencia del hardware, así como los servidores, estaciones de trabajo, equipos informáticos etc, que son parte del sistema que coadyuva con la seguridad de la información digital. El Decreto Supremo N° 012 (2017) establece que:

> Las tecnologías de la información están cada vez más integradas a la operación de infraestructura física, incluida la infraestructura critica por lo que hay un mayor peligro de que se pueda dañar o interrumpir el funcionamiento de las mismas poniendo en riesgo la economía y la vida cotidiana de millones de personas (p. 21).

La Política de Seguridad y Defensa Nacional (DS N° 012, 2017) refiere que:

> El ciberespacio y su infraestructura son susceptibles a una amplia gama de riesgos de amenazas tanto físicas como cibernéticas, por lo que una serie de actores podrían aprovechar estas vulnerabilidades para sustraer información e interrumpir el normal desarrollo y poner además en peligro o destruir la capacidad de prestar servicios (p. 21).

En cuanto a la infraestructura implica que las grandes instituciones públicas del estado peruano implementen sus políticas de seguridad informáticas internas, para proteger la información digital alojadas en los servidores o cuando viaje la información digital a través de las redes informáticas existentes, o sea toda una infraestructura informática que se dedique a la protección y seguridad de la información digital.

Una base de datos normalmente esta interconectada a otras redes informáticas en la cual podría ser atacado por intrusos mal intencionados, que quieran hacer daño a la infraestructura o para sustraer la información digital.

Implantación de un sistema de gestión de políticas de seguridad de la información.

Para implantar un Sistema de Gestión de Seguridad de la Información (SGSI) es necesario tener una guía conformada por diez (10) etapas o fases para la implantación en la organización.

> Las etapas son las siguientes: Definición de políticas de seguridad y de alcance del SGSI, Definición de responsabilidades y asignación de recursos, Identificación y Registro de activos , Análisis y Gestión de riesgos, Selección e implantación de controles de seguridad, Establecer un programa de mejora de la seguridad, Completar la documentación del SGSI, Revisión y auditoria del Proyecto de implantación del SGSI, Realización de la auditoria de certificación, Ejecutar las recomendaciones de la auditoria. (Gomez, 2011, p. 57).

Ley Nº 30999. Ley de Ciberdefensa

La Ley Nº 30999 Ley de Ciberdefensa fue publicada en el diario oficial El Peruano el 27 de agosto del año 2019, siendo presidente de la republica el ingeniero Martín Vizcarra. Consta de 14 artículos, 5 disposiciones complementarias finales, una disposición complementaria obligatoria. En esta ley en las disposiciones generales se expresa que la ciberdefensa está definida como la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional. Tiene como objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia. El ámbito de aplicación de la norma se circunscribe a la ejecución de operaciones de ciberdefensa frente a las amenazas o los ataques que afecten la seguridad nacional. Los órganos ejecutores lo constituyen las Fuerzas Armadas, es decir, el Ejercito, La Marina de Guerra y la Fuerza Aérea siendo regidos por el Comando Conjunto de las Fuerzas Armadas instituciones de calidad pertenecientes al Ministerio de Defensa. Tiene como finalidad defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio cuando estos afecten la seguridad nacional.

De igual forma en el capítulo I, el uso de la fuerza por parte de las Fuerzas Armadas se sujeta a las disposiciones contenidas en el artículo 51 de la Carta de las Naciones Unidas y a las normas regidas por el Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario. Toda vez que la legitima defensa está justificada en la medida en que ponga en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y los recursos claves para sostener las capacidades nacionales. El ejercicio de la legitima defensa se encuentra sujeto a los principios de legalidad, necesidad y oportunidad.

En el capítulo III La ley especifica que el Comando Conjunto de las Fuerzas Armadas está a cargo de la ciberdefensa y de los activos críticos nacionales y recursos claves cuando la capacidad de proteccion de sus operadores y/o del sector responsable de

cada uno de ellos y/o de la Dirección Nacional de Inteligencia sea sobrepasada a fin de mantener las capacidades nacionales, en el ámbito de la seguridad nacional. La Presidencia del Consejo de Ministros, como miembro del Consejo de Seguridad y Defensa Nacional, establece los protocolos de escalamiento, coordinación, intercambio y activación para lo indicado; ello se ejerce a través de la Secretaria de Gobierno Digital como ente rector del Sistema Nacional de Informática y de la Seguridad digital del país, quien emite los lineamientos y las directivas correspondientes.

2.3 Marco Conceptual

Son todos los términos que permitan comprender la propuesta.

Protección

(RAE, 2020) La Real Academia Española (RAE) afirma que es "la acción y efecto de proteger". También puede encontrarse referida al efecto de resguardar a una persona u objeto o cosa para que no le ocurra nada, o sea para colocarlo fuera de peligro.

Protección de la información digital

RAE (2020) afirma que: "la protección de datos es un sistema legal que garantiza la confidencialidad de los datos personales en poder de las Administraciones públicas u otras organizaciones". La protección de la información digital para este caso, no es una información impresa en un papel u otro medio similar, aquí vamos a tratar de la información digital en la cual son representados por dígitos del sistema binario compuestos por ceros "0" y unos "1", que se encuentra grabada en las bases de datos o unidades de memorias conocidos también como los discos duro en la cual necesitan ser protegidos contra las amenazas, así como el robo y destrucción de la información.

Medina (2006) afirma que la "seguridad de la información pudiera ser enfocada en proteger los activos de información de una organización contra pérdidas o uso

indebido" (p.10). Tenemos que la información y datos son recursos valiosos que debemos dar seguridad y protección.

La Política de Seguridad y Defensa Nacional (DS N° 012, 2017) refiere que "proteger el ciberespacio y su infraestructura se convierte en un asunto de Seguridad Nacional" (p. 21). También describe en la misma política que se fortalecerá e incrementará las capacidades militares y sus recursos humanos con la finalidad de garantizar la paz y tranquilidad de las personas para la consecución de los intereses nacionales.

DS N° 050 -2018- PCM (2018) que aprueba la definición de seguridad digital en el ámbito nacional establece:

> La seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación en su conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y la social, la seguridad nacional y los objetivos nacionales en dicho entorno (p. 2).

Seguridad de la información

Perafán y Caicedo (2014) nos dice que es "un estado especifico de la misma sin importar su formato, que nos indica un nivel o un determinado grado de seguridad de información, por ejemplo, que esté libre de peligro, daño o riesgo" (p. 19).

Norma Técnica Peruana (NTP-ISO/IEC 17799, 2007) afirma que "la información es un activo que como otros activos importantes del negocio tiene un valor para la organización y requiere en consecuencia una protección adecuada" (p. 7). El concepto de seguridad de la información está relacionado directamente con la protección de la misma.

Norma Técnica Peruana (NTP-ISO/IEC 27001, 2008) afirma que la seguridad de la información es "preservar la confidencialidad, integridad y disponibilidad de la información; además, también pueden ser involucradas otras características como

autenticación, responsabilidad, no-repudio y fiabilidad" (NTP-ISO/IEC 17799, 2005).

Sistema de Gestión de Seguridad de la Información (SGSI)

Norma Técnica Peruana (NTP-ISO/IEC 27001, 2008) afirma que la SGSI "es la parte del sistema integral de gestión, basado con un enfoque de riesgo del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información" (p. 4).

Es un sistema que es mencionado en la (NTP-ISO/IECC 17799, 2005) y nos "ayuda a proteger la información de un amplio rango de amenazas diferentes con lo que se asegura la continuidad del negocio, disminuir los daños generados en la organización y maximiza el retorno de las inversiones y las oportunidades de negocio".

Ciberdelito

Merino y Aliaga (2017) expresa que "una de las características del Ciberdelito es la distancia en la comisión del acto delictivo, la víctima y el victimario no están frente a frente" (p. 42. Esto se puede explicar que los que cometen este tipo de delito pueden estar en realidad en cualquier parte del mundo y en cualquier país o región incluso puede estar movilizándose de un lugar a otro tentando engañar a su víctima de su probable ubicación.

Desarrollo

El desarrollo consiste en realizar una secuencia de actividades en forma secuencial lógica y razonable de alguna actividad.

Desarrollo de software

Hidalgo (2014) sostiene que "el desarrollo de software no es cuestión de baladí, sino que, por su complejidad, requiere técnicas y procedimientos propios de una

ingeniería que es la ingeniería informática, una de cuyas partes es la ingeniería del software" (p. 4). El desarrollo de software implica hacer programas abstractos con una secuencia ordenada, lógica y por medios de algoritmos empleando un determinado lenguaje de programación.

Es importante precisar la necesidad de desarrollar un software de calidad propia, ya que permitiría independencia y seguridad sobre nuestros sistemas informáticos. De igual forma Hidalgo (2014) afirma que "la influencia del software en la eficiencia del sistema es mucho mayor que la del hardware" (p. 4 las criticas). Han existido responsabilidades por quienes desarrollan software, y "han desatado las críticas contra los fabricantes de software y de sus equipos informáticos, a raíz de las continuas vulnerabilidades descubiertas en sus productos" (Gómez 2011, p. 188).

De igual forma es importante precisar que de contar con el desarrollo de un software desde su inicio, se puede asegurar el sistema informático y con este los diferentes procesos administrativos y operativos empleados tanto en el Ejercito del Perú como en las otras dos Fuerzas Armadas.

El desarrollo de un software es una herramienta muy potente que hasta cierto punto se le puede considerar un arma digital que mediante el desarrollo eficaz y oportuno puede llegar a ser un instrumento estratégico para una nación.

Todo Estado o nación debe contar con el desarrollo de un software en cual se encuentre insertado dentro de las diferentes instituciones públicas entre ellas el Ejercito del Perú y las Fuerzas Armadas, de tal forma que desarrolle su propia entidad con infraestructura, personal y medios y así, proteger su información en la medida en que se encuentren interconectadas en las diferentes redes informáticas y de internet.

Software seguro y ciberseguridad

Hidalgo (2014) sostiene que "para hacer software seguro como hemos visto es forzosamente software de calidad, es necesario, en todas las fases del desarrollo, tener presentes dos puntos de vista fundamentales en la ingeniería del software seguro: los usuarios y los atacantes" (p. 8). A esto sumamos que los Hackers cada vez mejoran sus técnicas de ataque e intromisión en las redes informáticas ya se para robar o destruir la información y datos de un estado o nación.

Normalmente las instituciones de un estado optan por comprar un software de ciberseguridad para protegerse de ataques por los ciber delincuentes, sin embargo, para tener software de calidad en seguridad esta debe cumplir con las fases del desarrollo y estos se puede dar, si es que el programador implementa la seguridad desde su desarrollo, normalmente estos son realizados por las grandes empresas que venden dichos softwares.

Ciberseguridad

La ciberseguridad son todas las medidas de protección y seguridad con el que deben contar las redes informáticas y base de datos contra los ataques y robos de información por hackers y personas intrusas que practican estas modalidades de intromisión no autorizadas. La ciberseguridad "defiende nuestros sistemas y reacciona contra los atacantes. Para defender nuestros sistemas necesita promocionar el software seguro y, como hemos visto, para hacer software seguro se necesitan los puntos de vista del atacante y del usuario" (Hidalgo, 2008, p. 9).

Política de Seguridad y Defensa

La Política de Seguridad y Defensa Nacional (DS N° 012, 2017) refiere que son normas públicas para regular y satisfacer las necesidades que identifica como sujetos de la seguridad y defensa al Estado y a la persona humana, que viven en un determinado territorio (p. 15). La seguridad humana es en la actualidad relacionada con las personas y sus preocupaciones del día a día.

Ley de gobierno digital, DL N° 1412 (2018) establece que: "para el acceso a un servicio digital las entidades de la Administración Publica deben adoptar mecanismos o procedimientos de autenticación digital, considerando los niveles de seguridad a establecerse en la norma reglamentaria" (p. 6).

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Enfoque de la investigación

La investigación se desarrolló en el marco del enfoque cualitativo, debido a que se realizó el análisis de la protección de la información digital de los centros de informática del Ejército, en el marco de la ciberseguridad de la Política de Seguridad y Defensa Nacional, bajo el entendimiento de conocimientos de ingeniería, experiencias en desarrollo de software, políticas de protección y seguridad en ciberdefensa, desde el punto de vista del investigador, de los informantes, indagación e interpretación de documentos como la DUFSITELE y directivas, como parte de las políticas públicas vigentes. Hernandez, Fernandez, y Baptista (2014) sostiene que "el proceso de indagación es más flexible y se mueve entre las respuestas", (p. 9). El tema de investigación es actual y en constante cambio de la tecnología por lo que motiva el análisis y contribuye para la seguridad y protección de la información digital en instituciones públicas del estado.

3.2 Tipo de investigación

Esta investigación cualitativa se desarrolló en forma empírica, porque mediante el conocimiento del proceso de la protección de la información digital y de las políticas de seguridad y defensa nacional se va a proceder en describir dichos observables, acerca de la situación en que se encuentran.

> El investigador se introduce en las experiencias de los participantes y construye el conocimiento, siempre consciente de que es parte del fenómeno estudiado. Así en el centro de la investigación está situada la diversidad de ideologías y cualidades únicas de los individuos" (Hernandez, Fernandez, y Baptista, 2014, p. 9).

En esta investigación se incluyó al personal especialista con experiencia en el conocimiento y práctica de la realidad problemática, lo que permitió proporcionar conclusiones y recomendaciones a las autoridades competentes sobre la protección de la información digital existente en las bases de datos de los centros de informática del ejército.

3.3 Método de investigación

La investigación se desarrolló con el método Hermenéutico dentro del paradigma epistemológico "Hermenéutico-Interpretativo", la cual permitió analizar la protección de la información digital de los centros de informática, e interpretar la aplicación de las normas, directivas y políticas de seguridad y defensa, que dispone los departamentos de informática del ejército; conforme lo especifica Vargas (2011) "permite hacer interpretaciones de la realidad concreta, siempre que ésta sea vista como un texto que se pone en contexto" (p. 38). Se recogió la información de los observables en el mismo lugar de la realidad problemática, aplicando las técnicas de levantamiento de información de las infraestructuras existentes, hardware software y del personal especialista que labora en dicho lugar.

3.4 Escenario de estudio

El escenario donde se desarrolló la investigación para la recolección de datos, fue en los centros de informática del cuartel general del Ejército, ubicados geográficamente en el distrito de San Borja de la provincia de Lima, debido a que en ellas también se encuentra los departamentos de telemática, encargada de la protección de la información digital. Hernandez, Fernandez, y Baptista (2014) sostiene que "el escenario es el contexto en el cual se llevará a cabo la investigación" (p. 9). Dicha instalación es donde tiene las infraestructuras para la administración de la protección de la información digital, sin embargo, la información digital es usada en varios casos por las diferentes dependencias del Ejército en la cual están desplegadas a nivel nacional.

3.5 Objeto de estudio

El objeto de estudio se enfocó en la protección de la información digital. Lo que se analizó fue: cuál es el estado de la implementación de la protección de la información digital en los centros de informática del cuartel general del Ejército en el cumplimiento de la política de seguridad y defensa nacional, cuál es el estado de la implementación del desarrollo de software seguro y cuál es el estado de las infraestructuras para la protección de la información digital de los centros de informática del ejército, en el marco de la ciberseguridad de la Política de Seguridad y Defensa Nacional. El objeto de estudio debe ser elegido con un sentido de practicidad; de modo que la complejidad del mismo debe acoplarse a una limitación de tiempo y de recursos disponibles Martínez (como se citó en Izcara 2014)".

3.6 Observables de estudio

Los observables que se determinaron según la problemática de estudio son los siguientes

Observable 1

- Protección de la información digital

Observable 2

- Política de Seguridad Informática

Vargas (2010) expresa lo siguiente: "los observables permiten reconocer que cosas concretas de la realidad serán observadas y la pregunta le pone límites a la observación. Los observables tienen que estar perfectamente en línea con el resto de la investigación" (p. 42).

3.7 Fuentes de información

Las fuentes de información fueron todas las personas especialistas disponibles que laboran en los centros y oficinas de informática del cuartel general, que puedan aportar con su información en base a la experiencia vivida en el tema de la protección de la información digital, así mismo, se consideró toda la documentación acerca de las normas directivas y políticas de seguridad y defensa existente y disponibles en las dependencias encargadas de la protección de la información digital. Vargas (2011) sostiene que "las fuentes de informacion mismas que pueden ser personas, medios, objetos escritos edificios, etc.,exige la clarifiacion previa de los criterios que seran seleccionadas tales fuentes" (p. 82). Estos criterios se han seleccionado de acuerdo a los informantes que laboran en los centros de informática del ejército y tienen experiencia en dicho trabajo, acerca del conocimiento de la protección de la información digital de dicha organización. Los informantes seleccionados fueron: Jefe del departamento de telemática; ingenieros y oficiales que laboran en el desarrollo de software del departamento de telemática del; personal especialista en informática que ha laborado y conoce del tema de la protección de la información digital.

Como otras fuentes de información tenemos: Decreto Supremo N° 012-2017-DE, que aprueba la Política de Seguridad y Defensa Nacional y todas aquellas investigaciones con carácter de tesis para obtención de grado que obren en el Centro de Altos Estudios Nacionales entre otras.

3.8 Técnicas e instrumentos de acopio de información

3.8.1 Técnicas de acopio de información

Las técnicas de recojo y registro de información, se emplearon en los procesos de recolección de datos en esta investigación cualitativa. Para ello, es importante la selección previa del método, debido que la investigación responde a objetivos y al diseño del estudio. Además, la técnica implica una serie de procedimientos de actuación concreto y particulares que está asociado al método elegido (Latorre, Del Rincón y Arnal, 1996).

Para el desarrollo de las técnicas de recolección de datos que se emplearon en esta investigación fueron la entrevista semiestructurada y la Indagación documental.

La entrevista semiestructurada

Alvarez y Gayou (2003) sostiene que "la entrevista busco entender el mundo desde la perspectiva del entrevistado y desmenuzar los significados de sus experiencias" (p. 109). Para esta investigación se entrevistó al personal de profesionales y técnicos especialistas que labora en los centros de telemática del Ejercito, siendo un total de .. personal entrevistado, teniendo ellos como perfil profesional conocimientos de ingeniería de sistemas, ingeniería en telemática, desarrolladores de software y con experiencia aproximada de entre cinco a veinte años laborando en diferentes centros de telemática. Dentro de esta clasificación tenemos como instrumento la guía de preguntas, en la cual se indica la secuencia de las preguntas por realizar respecto al tema de la protección de la información digital.

Indagación documental

Constituye la relación de documentos buscados y rutas de sitios virtuales o reales. (Vargas, 2011) sostiene que "en esta etapa de observación implica el acopio de documentos escritos o digitales, textuales o iconográficos etc., con el objeto de ser interpretados hermenéuticamente obteniendo así de ellos información relevante para una investigación" (p.52). Se recurrió al uso del internet para la obtención de información acerca de la problemática del tema de estudio.

Vargas (2010) sostiene que "en el caso de las investigaciones de carácter cualitativo, el uso de dos o tres técnicas para poder obtener una masa crítica de información y poder triangularla, es decir, para conseguir corroboraciones, grados de consistencia" (p. 43). Con dichas técnicas seleccionadas es posible verificar o comprobar los observables disponibles en los escenarios existentes.

También se empleó el método de acopio de información. De tal forma que Hernández, Fernandez, y Baptista (2014) sostienen que "una fuente muy valiosa de datos cualitativos son los instrumentos, materiales y artefactos diversos. Nos pueden ayudar entender el fenómeno central de estudio" (p. 415).

3.8.2 Instrumentos de acopio de información

Los instrumentos que se utilizaron para el acopio de información de acuerdo a cada técnica son los siguientes:

Para poder materializar el acopio de información se realizó una Agenda de instrumentos conforme está redactado en el Anexo 04, lo cual nos permitió organizar a los informantes para la aplicación de los instrumentos.

Para la Técnica de Entrevista semiestructurada se empleó el instrumento:

Guía de preguntas

La preparación de la guía de preguntas fue fundamental debido a que son temas de actualidad en cuanto a la seguridad informática. Así mismo, para poder entender los diferentes términos y palabras técnicas que se emplean en el mundo de la computación y redes informáticas que muchas se relacionan con palabras y terminologías poco usadas en el quehacer diario y solamente es usado por especialistas en su área de investigación. La guía de preguntas nos permitió direccionar las interrogantes que se realizaron a los informantes, así mismo permitió reorientar, para alcanzar los objetivos planteados en la investigación en cuanto al análisis de la protección de la información digital de los centros de informática.

Alvarez y Gayou (2003) sostiene que "para su realización fue necesaria realizar una guía, como una actitud reflexiva del conocimiento que se pretende" (p. 111).

Para la Técnica de Indagación documental se empleó el instrumento:

Registros de documentos y rutas estratégicas de sitios virtuales

Los informantes nos proporcionaron las directivas, normas disponibles para poder realizar la indagación documental mediante el registro conforme se almaceno conforme el Anexo 05, que corresponde la relación de los documentos y rutas de sitios virtuales sobre el tema de estudio. Normalmente los informantes que laboran en el escenario de estudio nos narraron sus experiencias, que sirvieron como testimonio para la validación de la investigación.

Todos los registros de las entrevistas se almacenaron con el apoyo del software para análisis cualitativo denominado Atlas.ti, conforme la Figura 3.

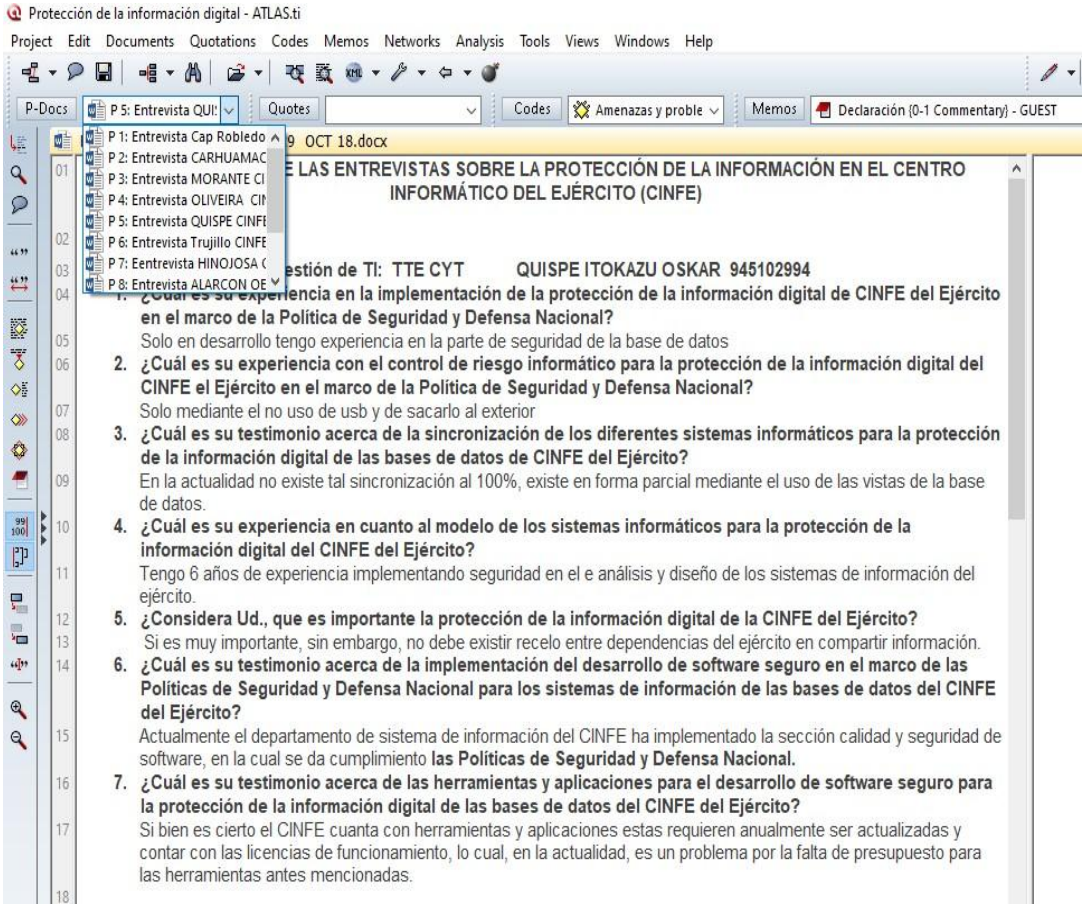

Figura 3 Pantalla de registro de las entrevistas

(Fuente: Programa Atlas.ti*.7)*

3.9 Acceso al campo y acopio de información

3.9.1 Acceso al campo

En esta etapa de trabajo de campo, se realizó en las infraestructuras de los centros y oficinas de informática del cuartel general del Ejército, institución que pertenece a las Fuerzas Armadas del Perú, y como informantes al personal especialista de ciencia y tecnología, que labora en la protección de la información de dichos centros. El acceso a este campo no hubo mayor problema para el investigador en vista que se realizó las coordinaciones necesarias con el personal responsable que labora en dicho lugar.

Además, defino mi rol como sujeto participante activo dentro de la investigación por tener conocimiento acerca de la realidad problemática de las observables materias de estudio.

3.9.2 Acopio de información

El acopio de información se realizó de manera personal por el propio investigador, yendo a las instalaciones de las oficinas y centros de informática del cuartel general del Ejército, para obtener la información directamente por los informantes, en la cual la mayoría son personal especialista en ciencia y tecnología. Hernandez, Fernandez, y Baptista (2014) sostiene que "el sitio inicial podría ser el campus de una institución, pero después tendríamos que cambiar los lugares de observación" (p. 366). También se visitó otros departamentos y oficinas que cumplen funciones similares a los centros de informática como por ejemplo la oficina económica del ejército, que dispone de servidores y especialistas en informática, otras dependencias no fueron consideras por ser de similares características y de menor envergadura.

Para alcanzar la seriedad y rigurosidad de estudio, se debió tener confiabilidad de los observables obtenidos en el trabajo de campo. "La confiabilidad está relacionada con la precisión, estabilidad, exactitud y consistencia de los resultados obtenidos; es decir el grado de acuerdo entre observadores independientes Ruiz (como se citó en Izcara, 2014)". Esta investigación se corroboro con otras tesis que mencionamos en los antecedentes.

3.10 Análisis de información

Para realizar el análisis de la información se hizo siguiendo las rutas o secuencias de acciones de datos cualitativos. En la Figura 4 se observó el procedimiento o secuencia del análisis desarrollado hasta llegar a un punto de saturación para luego proseguir con la etapa de síntesis en la cual se construye las unidades de análisis, nodos y categorías en la cual devela la realidad buscada. Luego del proceso de síntesis se procedió a la redacción de las categorías encontradas mediante una ordenación de las categorías para luego pasar a la obtención de los resultados mediante la interpretación y triangulación para llegar a las conclusiones del presente trabajo de investigación. Para la realización de estos procedimientos se utilizó como apoyo el software informático Atlas.ti.

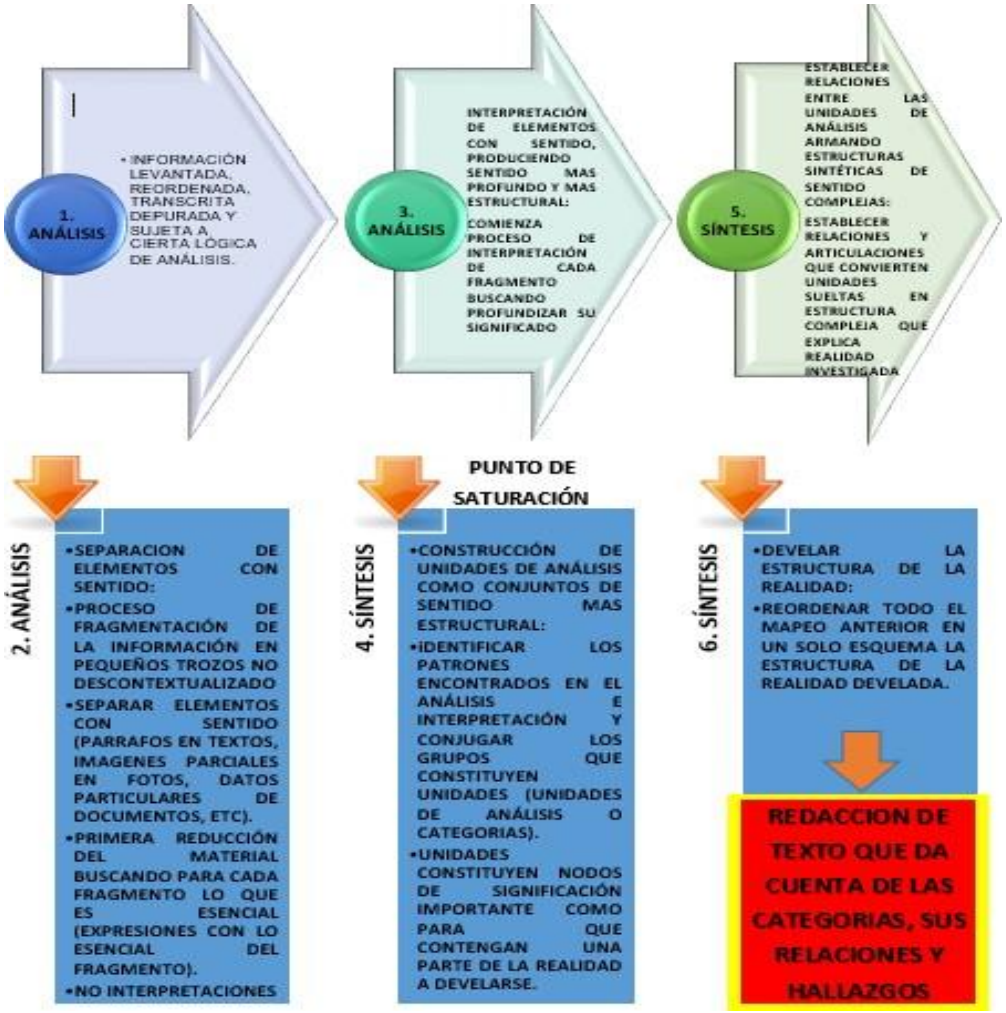

Figura 4 Ruta de análisis y síntesis de datos cualitativos

Fuente: Xavier Vargas Beal (2007, p.74)

Etapa reducción de información

La información recopilada en esta etapa, tuvo como propósito priorizar la mayor parte de la información de los observables obtenidos, y luego se filtró lo que realmente interesa de acuerdo a los objetivos planteados. Álvarez (como se citó en Izcara, 2014) el análisis del material cualitativo es la reducción. Y simplificación de los datos recabados mediante la eliminación interpretativa Tojar Hurtado (como se citó en Izcara, 2014). Para este caso la información que se obtendrá son: la infraestructura, material como hardware y software, y la información que proporcione el personal especialista de ciencia y tecnología que labora en los centros de informática del ejército.

Etapa de disposición y transformación de información

En esta etapa se planteó la estrategia o procedimiento de análisis de la información obtenida, para realizarlo con rigor científico y validez interna que amerita esta investigación. Shaw (como se citó en Izcara, 2014) nos dice:

> Son cinco las estrategias a seguir para obtener un elevado grado de validez interna o adecuación de los resultados a la realidad social y estas son: selección de personas ricas en información, saturación del campo de hablas en los discursos recogidos, permanencia prolongada en el campo, análisis de casos negativos, contraste con los actores sociales.

Este procedimiento se hizo en base a los objetivos planteados en esta investigación del enfoque cualitativo, con la asistencia del Atlas.ti, a fin de contribuir en solucionar una realidad problemática sobre la protección de la información digital que están en las bases de datos que dispone los centros de informática del Ejercito del Perú. Finalmente se realizó la redacción del informe final con los resultados obtenidos, producto del análisis de la información, de todas las etapas. y procesos de la revisión de la información proporcionada por los informantes acerca de los observables descritos.

CAPÍTULO IV

ANÁLISIS Y SÍNTESIS

4.1 Análisis y síntesis

El análisis se realizó de acuerdo a las categorías seleccionadas que surgieron de los elementos con sentido propio y de la propia esquematización de ellas. Para este proceso se utilizó como ayuda el programa computacional Atlas.ti., en la cual es una herramienta informática para realizar análisis cualitativo, permitiendo una mejor administración de la información conseguida.

Tabla 1 Elementos con sentido propio

N/O	ELEMENTOS CON SENTIDO	CATEGORIZACIÓN	MACRO CATEGORIAS
1	Usuarios	Contraseñas	
2	Software	Seguridad informática	
3	Informática	Sensibilización	
4	Seguridad informática	Ciberseguridad	Políticas de seguridad informática
5	Protección de la información digital	Leyes, Normas y Directivas	
6	DUFSITELE	Cumplimiento de las normas	
7	CINFE	Calidad del software	
8	Capacitación	ISO 9000	
9	Administración	Licencias informáticas	Recursos económicos para implementación
10	Sistemas perimetrales		
11	Informática/ Antivirus	Capacitación del Personal	
12	Licencias informáticas	Experiencia en desarrollo	Capacitación del personal
13	Desarrollo de software	Seguridad del software	
14	Deficiencias en Infraestructura	Software	
15	DITELE/ CINFE	Instalación de software	
16	Equipamiento	Aplicaciones Informática	
17	Campaña de Difusión	Sistemas perimetrales	Infraestructura informática

18	Renovación Licencia y antivirus	Informática	
19	Talleres de capacitación	Vigencia tecnológica	
20	Sensibilización	Sistema de información	
21	Implementación tecnológica	Sincronización	
22	Ciberseguridad	Secretaria de gobierno digital	
23	Software y Base de datos	CINFE/ COCIBER	
24	Sistema de información	DITELE	Entidades informáticas
25	Normas y Directivas	Obstáculos	
26	Robos de información	Idiosincrasia	
27	Hackers/ Crackers/Obstáculos	Falta de presupuesto para capacitación	Problemas /Amenazas
28	ISO 9000	Protección	Protección de
29	Licencias informáticas	Seguridad del software	información digital

Fuente: Elaboración propia

A partir de los resultados de la Tabla 1, se dio respuesta a las preguntas de investigación planteadas en los objetivos de la investigación. Se trata de realizar una lógica más interpretativa que esté orientada a los planteamientos originales según la problemática de estudio. Llegando luego al punto de saturación, para proceder a describir las categorías y macro categorías encontradas como las unidades de análisis.

En la Figura 5 tenemos a las categorías encontradas y se les ha agrupado para luego encontrar las macro categorías.

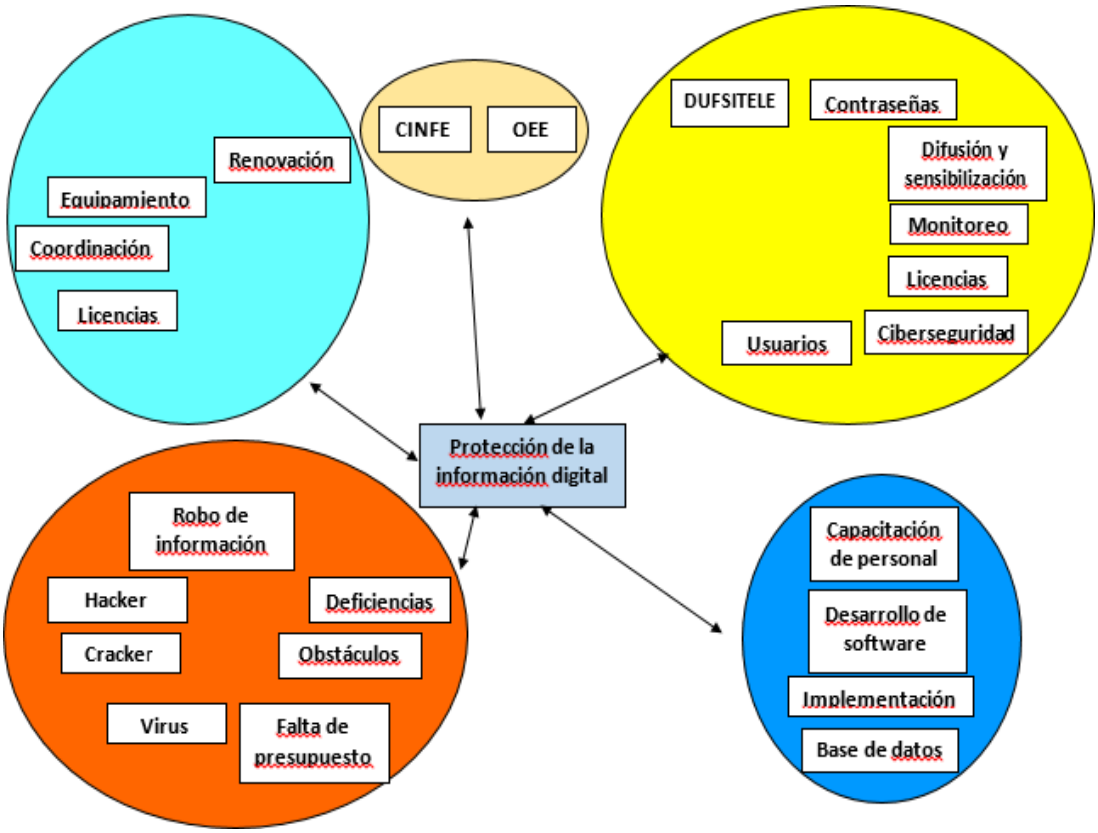

Figura 5 Mapeo temático de las categorías

(Fuente: Elaboración propia)

A continuación, se procede a describir las categorías principales, denominada "protección de la información digital", y también en un segundo plano las categorías a través de las macro categorías que están vinculadas con la categoría principal.

4.1.1 Categoría principal

Esta categoría principal de la investigación se denomina la "protección de la información digital" de los centros de informática del Ejército, en lo que concierne a tener la capacidad de ciberseguridad para proteger la información digital que deben tener las instituciones y entidades públicas del estado.

En la Figura 6 se observa la categoría principal, con las macro categorías donde nos muestra las redes y nodos de los mapas temáticos.

A partir de aquí, se establecen las relaciones y articulaciones que tienen las categorías encontradas de toda la estructura de la realidad problemática con la ayuda del Atlas.ti. Con esta categoría principal se detallan las siguientes Macro Categorías (MC):

MC1: Políticas de seguridad informática

MC2: Infraestructura informática

MC3: Recursos económicos

MC4: Amenazas y problemas

MC5: Entidades informáticas

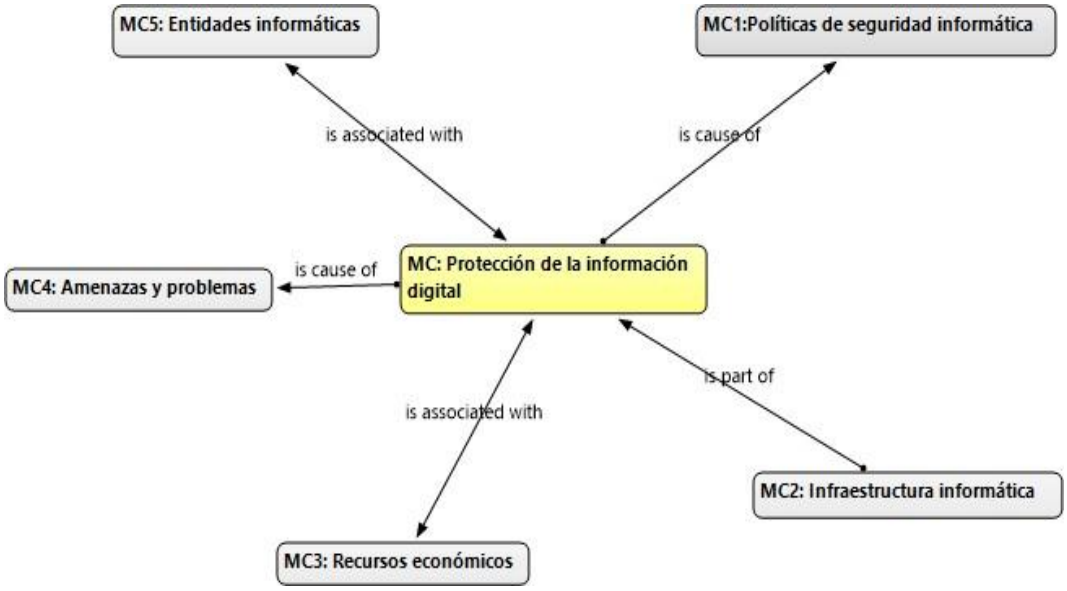

Figura 6 Redes del mapeo temático de las macro categorías

(Fuente: Programa Atlas.ti.*7)*

A partir de esta representación esquemática, según la Figura 7 se presenta el lenguaje esquemático el cual permite explicar a profundidad la realidad de esta investigación

de enfoque cualitativo a fin de poder dar respuesta a los objetivos planteados en el presente estudio. De esta manera se reordena en un solo esquema la develación de la estructura de la realidad problemática de las categorías y macro categorías con el observable de la protección de la información digital.

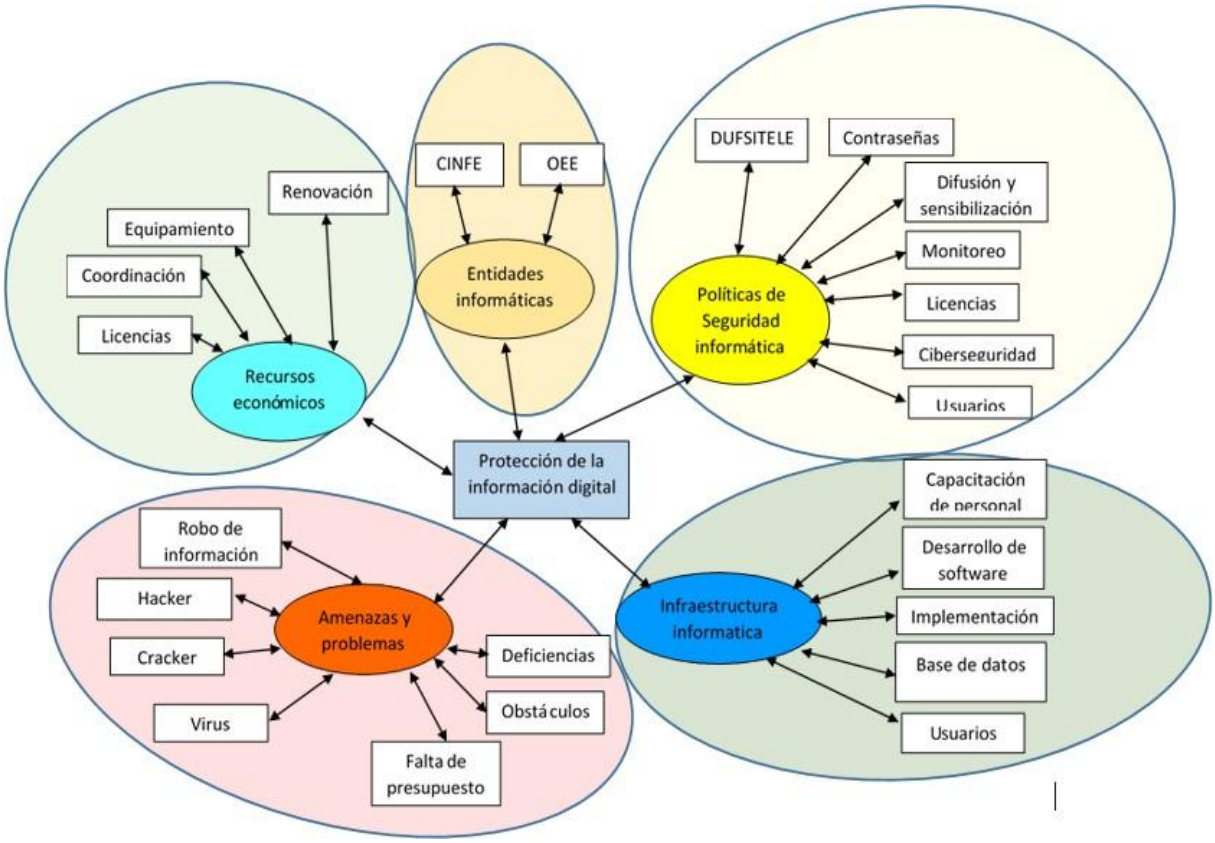

Figura 7 Reagrupación esquemática de las estructuras de las macro categorías

(Fuente: Elaboración propia)

Seguido de ello se procede en redactar el texto el cual se presentan las categorías, con sus relaciones y hallazgos, para luego pasar a dar respuesta a los objetivos planteados en esta investigación:

- Objetivo N° 01: Explicar el estado de la protección de la información digital de los centros de informática del Ejército del Perú.

- Objetivo N° 02: Incluir el estado de la implementación del desarrollo de software seguro para la protección de la información digital de los centros de informática del Ejército del Perú
- Objetivo N° 03: Incluir en el estado de las infraestructuras informática para la protección de la información digital de los centros de informática del Ejército del Perú.

La protección de la información digital de los centros de informática del cuartel general del Ejército consiste en describir las observables y evidencias encontradas que, para este caso tenemos las macro categorías tales como: Políticas de seguridad informática, la infraestructura informática, los recursos económicos, entidades informáticas, las amenazas y problemas que están ocurriendo en el entorno y contexto de dicha institución.

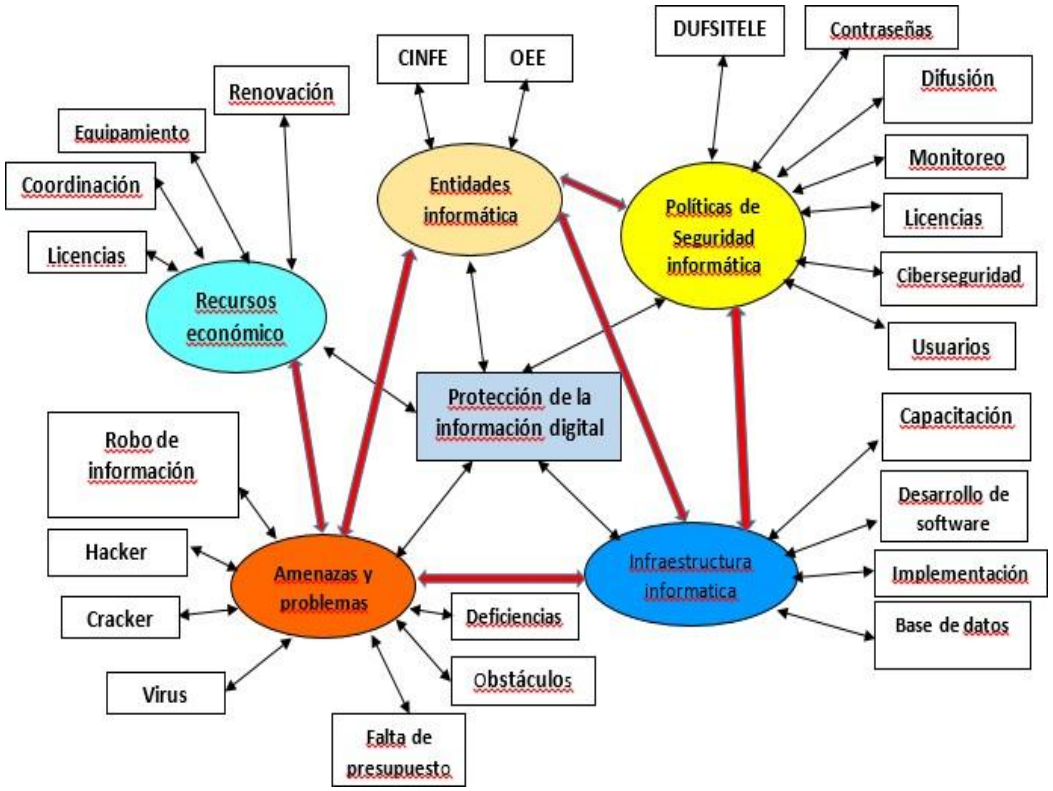

Figura 8 Relación de las macro categorías

(Fuente: Elaboración propia)

En la Figura 8 procedemos a redactar y describir el texto de las categorías con sus relaciones y hallazgos con las macro categorías encontradas que son parte de la categoría principal.

4.1.2 MC1: Políticas de seguridad informática

Esta categoría se encuentra relacionada la "protección de la información digital", de tal forma que se procedió en analizar de manera directa. En la Figura 9 se presentan las diferentes interrelaciones entre las categorías establecidas para realizar el análisis correspondiente.

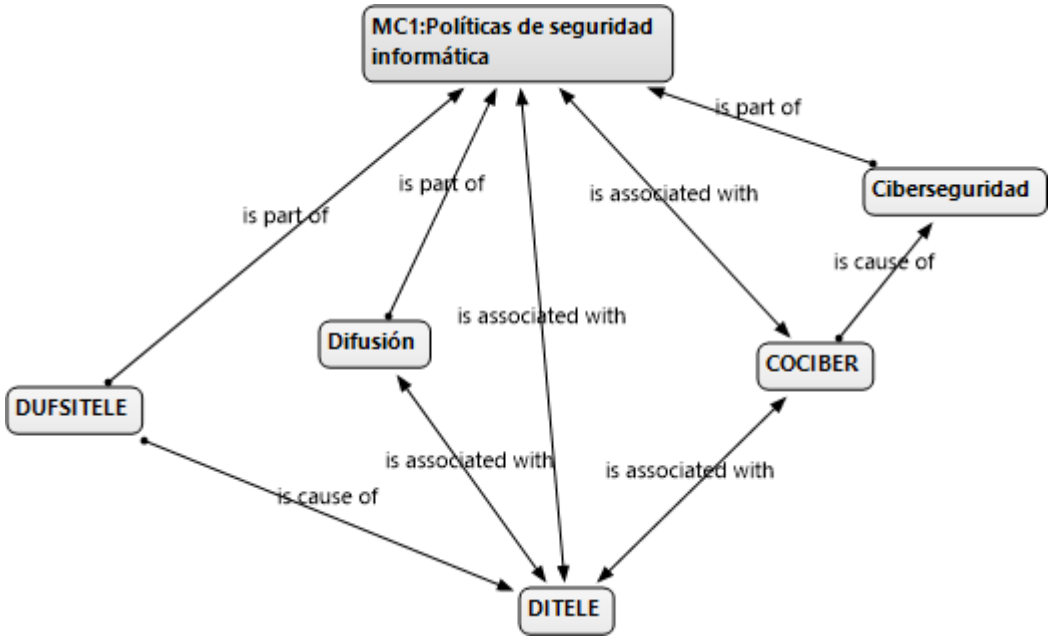

Figura 9 MC1: Política de seguridad informática

(Fuente: Programa Atlas.ti.*7)*

A partir de esta categoría se dio respuesta al Objetivo Específico N° 01 "Explicar el estado de la protección de la información digital los centros de informática del CGE en el marco de la ciberseguridad de la Política de Seguridad y Defensa Nacional".

Esta categorización compuesta se determinó por el método inductivo para poder agrupar los elementos con sentido común y a la vez esta subdividido por los

siguientes tipos de códigos, tal como se muestra en la Figura 6 y se detalla sus partes componentes a continuación:

- **Políticas de seguridad: ciberseguridad (Fundamentación:84 citas)**

El estado de la protección de la información digital se relaciona con las políticas de ciberseguridad informática en la cual procederemos analizar el Decreto Supremo N° 012-2017-DE del 2017, que aprueba la Política de Seguridad y Defensa Nacional.

Con respecto al Decreto Supremo N° 012-2017-DE (2017), que aprueba la Política de Seguridad y Defensa Nacional, solo describe en su diagnóstico en el ítem 4.2.14 Infraestructura para enfrentar ataques a los sistemas de información: Ciberseguridad. De ello se puede expresar la necesidad de contar con las diversas capacidades de respuesta para para enfrentar las amenazas y riesgos existentes en el ciberespacio, en la cual pueden realizar, ataques informáticos y perderse la información digital; esta política de seguridad aún falta su reglamentación motivo por el cual las instituciones aun no pueden definir bien sus funciones y responsabilidades. En una de las citas del personal especialista entrevistado nos dice que "se han establecido las políticas basadas en las buenas prácticas informáticas" aquí solo denota que se están rigiendo por las buenas prácticas pero, que no obedece a un planeamiento estratégico adecuado para establecer en forma eficiente y acorde con la reglamentación de la política se seguridad y defensa nacional en el ámbito de la protección de la información digital y de la ciberseguridad más aún que, los constantes cambios tecnológicos obliga que las entidades públicas deben en forma permanente estar actualizados.

Un ente rector del Sistema Nacional de informática adscrito a la Presidencia del Consejo de Ministros (PCM) es la Secretaria de Gobierno Digital (SEDGI) la cual se encuentra encargada de " formular, proponer y aprobar normas, estándares y lineamientos en materia de su competencia así como supervisar su cumplimiento" . (PCM-Secretaria de Gobierno Digital , 2017). Tenemos el Decreto legislativo N° 1412, que aprueba la ley de Gobierno digital (DL 1412 LEY DE GOBIERNO DIGITAL, 2018) la cual nos expresa lo siguiente:

> Establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública.

En el artículo 23.- Datos en el ítem 23.2 (DL 1412 LEY DE GOBIERNO DIGITAL, 2018) nos dice que:

> Las entidades de la Administración pública administran sus datos como un activo estratégico, garantizando que estos se recopilen, procesen, publiquen, almacenen y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, riesgos y la normatividad vigente en materia de gobierno digital, seguridad digital, transparencia, protección de datos personales y cualquier otra vinculante.

- **Entidades informáticas: DITELE, COCIBER CINFE (Fundamentación: 94 citas)**

La seguridad informática compete, a la protección de la información digital en lo que concierne a hardware y software, según la DUFSITELE (Dirección de Telemática del Ejército, 2017) nos dice:

Se puede expresar que la mayoría de las actividades de la seguridad informática es competencia y de responsabilidad de la COCIBER o Comando de Ciberdefensa en cuanto a la formulación, actualización de dicha directiva, más aún que, de acuerdo al avance de la tecnología vienen apareciendo nuevas herramientas, técnicas y procedimientos de seguridad informática.

Sin embargo, se ha podido observar que las actualizaciones y algunos desarrollos, de software lo hacen los propios usuarios de cada entidad sin contar con opinión favorable de la DITELE, más aún que, se ha creado el Comando de ciberdefensa encargado de la seguridad informática (COCIBER) y el Centro de Informática del

Ejercito (CINFE) que, se encuentra como organización independiente de la DITELE. Para fortalecer esta afirmación tenemos una declaración del personal entrevistado "con la creación del Comando del COCIBER y el CINFE, vienen coordinado acciones de defensa frente a malware o ataques en el ciberespacio."

La seguridad y protección de la información digital son muy importantes para las entidades públicas del estado, más aún para una institución castrense, prueba de ello tenemos que, en una manifestación, de uno de los especialistas al preguntársele: considera Ud., que es importante la protección de la información digital, nos dice "claro que sí, es de vital importancia ya que protege al activo más importante de la institución que es la información digital". Estos activos son normalmente considerados críticos, porque en ella está toda la información digital y datos del personal, que son los recursos más valiosos de la institución.

- **Políticas informáticas institucionales: DUFSITELE (Fundamentación: 38 citas)**

La Directiva Única de Funcionamiento del Sistema de Telemática del Ejército (DUFSITELE), es parte de las políticas informáticas institucionales del Ejercito, para su real y efectivo cumplimiento por los centros informáticos de todas las dependencias que se encuentran instaladas a nivel nacional de dicha institución, que pertenece a las FFAA del Perú.

(Dirección de Telemática del Ejército, 2017). Expresa lo siguiente que "la información digital existente en las bases de datos del CINFE" y la responsabilidad del monitoreo, debe ser ahora el COCIBER". Sin embargo, durante el periodo de la investigación, el COCIBER al termino del año 2018 fue desactivado para luego crearse en el año 2019, el Comando de Ciberdefensa y Telemática del Ejército (CITELE) que de acuerdo a lo expresado por el general Cesar Astudillo (2019/10/29) "que al contar con un Comando de Ciberdefensa nos va a ayudar a proteger nuestros activos nuestros sistemas de armas y base de datos, pues toda la data que maneja el Ejército en los diferentes comandos puede ser fácilmente alterada, reseteando toda la información, alterando todo el sistema de Comando de Personal y los estados de relevo; manifestó que este tipo de ataques son los más suaves que pueden hacer.

De igual forma se observa que dichas organizaciones del área de Telecomunicaciones e Informática, están en un proceso de reorganización, por lo tanto, la DUFSITELE se encontraría dentro de los cambios organizacionales y avances tecnológicos. Gómez (2011) afirma: Muchas organizaciones no han definido e implantado de forma eficaz unas adecuadas políticas y procedimientos de seguridad" (p. 171). La adecuación rápida de las organizaciones debe ser tal que en paralelo las políticas internas de seguridad informática sean implementadas en el más corto plazo para minimizar los riesgos y vulnerabilidades que están expuestos la información digital que se encuentran alojados en los servidores del Data Center.

- **Difusión (Fundamentación: 31 citas)**

El conocimiento de las políticas, normas y directivas para dar seguridad y proteger la información digital son importantes para que puedan ser cumplidas por todo el personal que manipula dicha información en una entidad pública, porque si no lo hacemos, entonces podríamos perder toda la información digital de la base de datos de la institución, para ello es necesario: concientizar a todos para que puedan cumplir dichas leyes y normas, realizar campañas de difusión en cumplimiento de las mismas. También uno de los ingenieros entrevistado manifestó que: "si es necesario, porque bastante personal del área de informática no conoce la DUFSITELE, y conociéndolo sería posible recomendar su empleo". Gómez (2011) afirma que "la falta de compromiso y de sensibilización de la Alta Dirección hacia estas cuestiones como una de las causas que explican esta preocupante situación en muchas organizaciones" (p. 179).

- **Ciberseguridad (Fundamentación: 22 citas)**

El tema de ciberseguridad es un nuevo campo de acción que se ha iniciado en los últimos años, debido a que la mayoría de personas interactúan con la información digital mediante las diferentes redes informáticas existentes y entre ellas tenemos la conexión a internet mediante la nube. Al realizar diversas operaciones cibernéticas como transacciones bancarias, compras por internet, etc. han aparecido los delitos informáticos y los ciberdelincuentes que ingresan a las redes informáticas mediante

procedimientos de manipulación, normalmente por software aprovechándose algún error en los sistemas operativos instalados para el funcionamiento de la base de datos para luego robar información y manipular o chantajear a las personas o instituciones públicas del Estado.

(DUFSITELE, 2017) afirma que "en cuanto a los sistemas de información que se instalan en el portal de información interno (Intranet) del Ejército son competencia de la DITELE. (http://sistemas.ejercito.mil.pe/SISMAS/)", sin embargo, tenemos que se ha sido inaugurado a finales del 2018 al Comando de Operaciones de Ciberdefensa (COCIBER) del Ejército, conforme lo manifiesta uno de los especialistas "pero como ya se creó el COCIBER, son ellos que deben monitorear dichos sistemas", además que, el sistema de información digital está a cargo del Centro de Informática del Ejercito (CINFE).

La ciberseguridad se relaciona con la protección de la información digital siendo que varias entidades están comprando software para proteger su información digital y a la vez están desarrollando ciertas aplicaciones o software para la seguridad informática. Hidalgo (2014) sostiene que "el desarrollo de software no es cuestión de baladí, sino que, por su complejidad, requiere técnicas y procedimientos propios de programación en cuanto a ingeniería informática, una de cuyas partes es la ingeniería del software" (p. 4). Por ello es necesario que sea implementado en forma adecuada el desarrollo de software en el CINFE desde su planeamiento con personal especialista de programadores, de tal forma que los anillos de seguridad sean robustos desde su concepción de la programación en el sistema.

De igual forma en el estudio también se pudo evidenciar la carencia de coordinación entre los centros de informática con la DITELE y CINFE para el desarrollo de software conforme ordena la DUFSITELE y esto se corrobora con la manifestación de uno de los especialistas entrevistados al decir que "hay entidades que desarrollan software que van en contra de la DUFSITELE" y con ello se puede tener el riesgo de

no guardar todas las medidas de seguridad para proteger la información digital, por otro lado las entrevistas arrojan la percepción que, la DUFSITELE está desactualizada e incompleta, y que dicta normas de manera general por lo que algunas entidades optan por buscar una solución para proteger o cuidar su información digital.

Como conclusión: De acuerdo al primer objetivo de estudio de la investigación en la cual se manifiesta que la protección de la información digital es muy importante, se puede expresar de acuerdo a los hallazgos que se encuentra están limitadamente protegidos en hardware y software, de tal forma que requieran de constante mantenimiento, renovación de licencias y actualizaciones. En cuanto al personal que labora necesita una constante capacitación y programa de incentivos para que realicen una mejor labor, así mismo existe la necesidad en desarrollar software propio, para incrementar los niveles de seguridad y a la vez ser menos dependientes de las empresas que proveen este servicio, porque tendríamos nuestro propio Know how. En cuanto al cumplimiento de las leyes, normas, directivas(DUFSITELE) y políticas de seguridad y defensa en el ámbito de la ciberseguridad se están realizando moderadamente, por lo que es necesario actualizar, difundir y concientizar al personal sobre su cumplimiento, debido que existen usuarios que realizan actualizaciones y upgrades sin contar con opinión favorable de la DITELE.

4.1.3 MC2: Infraestructura informática

Las infraestructuras informáticas están subdivididas en: infraestructura de instalaciones físicas, personal, hardware, software, etc.

La infraestructura es una categoría que hace referencia a la existencia de instalaciones apropiadas para que funcione toda organización informática compuestas por personas, hardware y software con la finalidad de proteger la información digital que, se encuentran almacenadas en memorias, servidores y base de datos de las instituciones de las FFAA. En la Figura 10 tenemos las diferentes interrelaciones entre las categorías y macro categorías establecidas para realizar el análisis correspondiente.

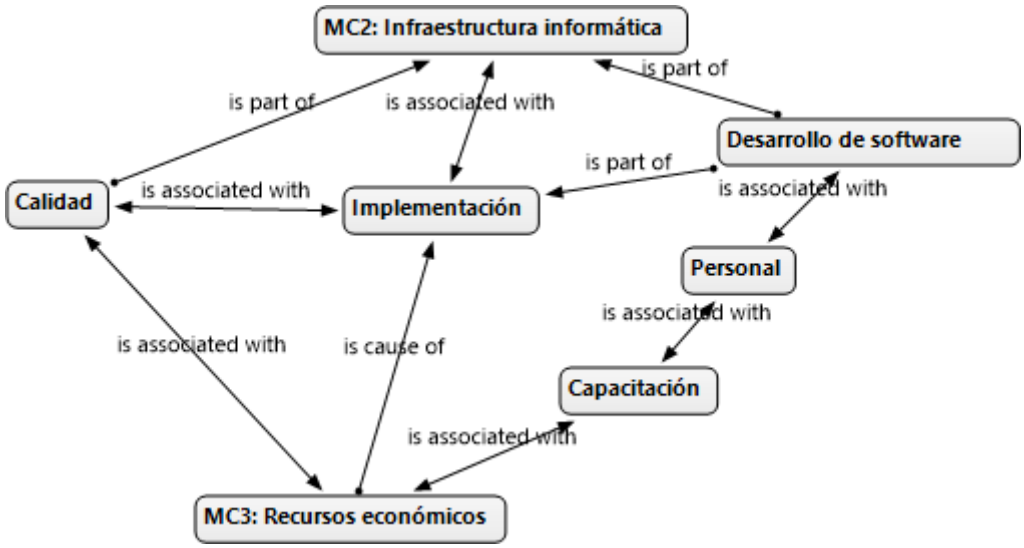

Figura 10 MC2: Infraestructura informática

(Fuente: Programa Atlas.ti *7)*

A partir de esta categoría se da respuesta al Objetivo N° 02 propuesto en la presente investigación "Explicar el estado del desarrollo de software seguro en el marco de la ciberseguridad de las Políticas de Seguridad y Defensa Nacional". Y de igual forma se da respuesta al Objetivo Especifico N° 03 que en el estudio se encuentra planteado de la siguiente manera: Describir el estado de las infraestructuras para la protección

de la información digital de los centros de informática del Ejército en el marco de la Política de Seguridad y Defensa Nacional".

Decreto legislativo N° 1412 (2018) que aprueba la ley de Gobierno Digital, en su Art 24, nos dice acerca de la Infraestructura Nacional de Datos y lo define como "conjunto articulado de políticas, normas, medidas, procesos, tecnologías digitales, repositorios y bases de datos destinadas a promover la adecuada recopilación, procesamiento, publicación, almacenamiento de datos que gestionan las entidades de la Administración Pública".

Esta categoría fue establecida usando el método deductivo y se estableció los siguientes códigos tales como:

- Capacitación del personal. (Fundamentación: 81 citas)

  La capacitación del personal que labora en los centros de informática requiere especial atención, esto mencionado por los especialistas entrevistados que laboran en esta área, que principalmente son compuestos por ingenieros del área de informática y de sistemas. El DL N° 1412 que aprueba la Ley del gobierno digital en el Articulo N° 18 e ítem 18.3 nos dice "capacitar en temas en materia de firmas electrónicas, firmas y certificados digitales, protección de datos personales, interoperabilidad, arquitectura digital, seguridad digital, datos abiertos y gobierno digital", asimismo, uno de los ingenieros manifiesta que, el principal obstáculo que afecta la implementación de la protección de la información digital en el CINFE es "la falta de capacitación del usuario final", luego se le pregunto, si, tiene algo más que agregar, y dijo: "que los lideres proporcionen los recursos necesarios para la capacitación del personal que se encuentra inmerso en el tema de ciberseguridad, siendo más ambicioso que esto se refleje en las escuelas de formación militar, donde debe haber una especialidad en ciberseguridad", todo ello refleja una profunda preocupación por la capacitación del personal en tema de ciberseguridad para que dicho personal, cuando llegue a trabajar en una dependencia que maneje la información digital, este se encuentre bien capacitado y pueda contribuir en incrementar los niveles de seguridad de la información digital.

- Desarrollo de software. (Fundamentación: 14 citas)

  El desarrollo de software en los centros de informática de las FFAA se realiza limitadamente sin embargo para aspectos de la protección de la información digital "todavía no se desarrolla aquí" según afirmación de los especialistas, ello demuestra dependencia tecnológica, porque cuando lo necesiten, van adquirirlo de empresas principalmente extranjeras, también considero que: "eso lo debe hacer el COCIBER". Sin embargo según la DL N° 1412 que aprueba la Ley del gobierno digital en su Artículo N° 5.3 Privacidad desde el diseño.- "En el diseño y configuración de los servicios digitales se adoptan las medidas preventivas de tipo tecnológico, organizacional, humano y procedimental" esto se explica que desde el diseño se realiza la planificación el desarrollo del software y se debe adoptar las medidas preventivas de tipo tecnológico que puede ser por hardware o software, si es por software entonces se aplicaría las técnicas y procedimientos en desarrollo de software seguro para proteger la información digital, mediante anillos de seguridad desde el inicio de la planificación para desarrollar el software. López (2016) concluye que "Es necesario incluir análisis de seguridad desde el inicio de la vida del software, o sea desde el plan de desarrollo" (p. 80).

- Implementación. (Fundamentación: 16 citas)

  La implementación de la protección de la información digital según los entrevistados, han manifestado que, es de vital importancia para que se implemente el desarrollo de software seguro para la protección de la información digital como parte de una excelente infraestructura tecnológica.

  La implementación actual para la protección de las informaciones digitales se da en diferentes capas, mediante la seguridad perimetral conforme lo manifiesta los especialistas, que se encuentra como administrador de equipos tales como: firewall, anti spam, filtrado de contenido, VPN SSL, y soluciones Endpoint.

- Calidad. (Fundamentación: 15 citas)

  La calidad del software puede brindar la seguridad de la transmisión de la información digital, así como el estado de confianza y privacidad para que dicha información llega a su destino sin interferencia evitando las ciberamenazas existentes en las redes. Gil (2015) sostiene que "tomando en cuenta la privacidad ya desde el primer momento, los diseñadores pueden desarrollar herramientas que aseguren un mayor grado de protección" (p. 136). Cuando el diseño del desarrollo es considerado desde su inicio para su implementación tienen mayor probabilidad de un estado de ciberseguridad.

  La explicación de la protección de la información digital no solo significa tener la seguridad del software contra el ataque que hace un hacker y pueda introducirse por las redes y base de datos para obtener o robar la información ilegalmente, sino que es necesario tener en consideración que "los sistemas de privacidad desde el diseño implican que las tecnologías sean construidas teniendo en cuenta la necesidad de la protección de la privacidad" (Gil Gonzales, 2015, p. 136).

A partir de esta categoría se da respuesta al Objetivo N° 02

Para dar respuesta a las preguntas que orientan la presente investigación cualitativa y poder llegar a las conclusiones que incluyen los objetivos del planteamiento del problema, esta macro categoría se analizó con las otras categorías y códigos que tengan relación con la protección de la información digital, tales como: políticas de seguridad, contraseñas, seguridad informática, la DUFSITELE, normas, directivas, licencias informáticas, monitoreo, campañas de difusión de ciberseguridad, y cumplimiento de las leyes.

Tenemos que, en cuanto al código de seguridad informática se relaciona con la protección de la información digital y se fundamenta con quince citas productos de las entrevistas realizada en los cuales se desprende que la seguridad informática es,

sinónimo de la protección de la información digital y son considerados por el personal que labora en los centros de telemática de las FFAA.

Como conclusión: De acuerdo con el tercer objetivo planteado que responde a las infraestructuras informáticas compuesta por: instalaciones modernas, equipamiento informático, sistemas perimetrales, recursos humanos capacitados en desarrollo de software, permite tener bases de datos implementadas, conectados e integradas con software seguro y de calidad para el servicio de los usuarios y clientes conectados para acceder a la información que necesitan, pero protegidos por un monitoreo a control remoto, y así se podría evitar el robo de información digital y/o el acceso de algún intruso para cometer algún delito informático.

4.1.4 MC3: Recursos económicos (Fundamentación: 47 citas)

Los recursos económicos son fundamentales para gestionar una eficaz protección de la información digital, y estos ocurren cuando se asigna presupuesto para los institutos castrenses puedan realizar los procesos de adquisición y selección de infraestructura informática por medio del sistema de contrataciones del estado. En la Figura 11 tenemos las diferentes interrelaciones entre las categorías y macro categorías establecidas para realizar el análisis correspondiente.

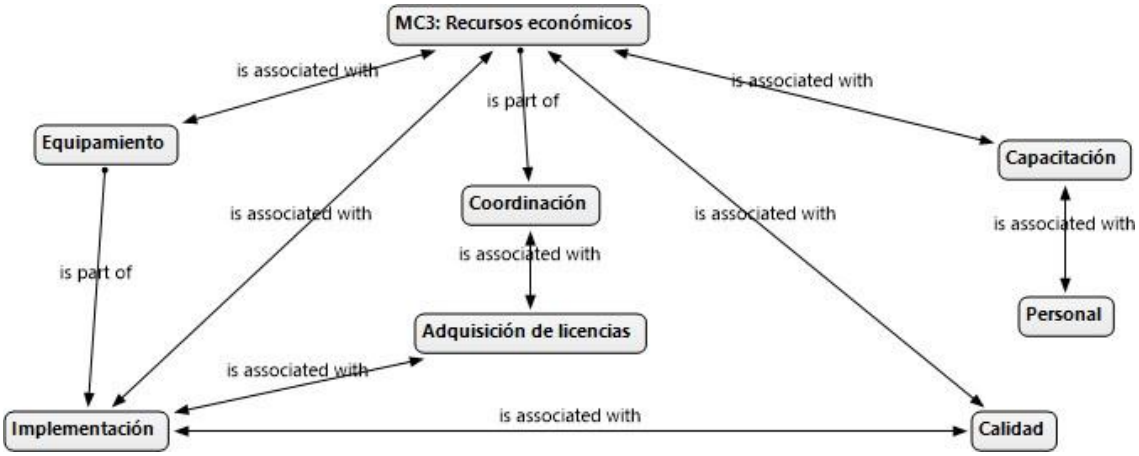

Figura 11 MC3: Recursos económicos

(Fuente: Programa Atlas.ti *7)*

La inversión en tecnología para la protección de la información digital es bastante onerosa, y se necesita de conocimiento y experiencia para entender y seleccionar, cual es la mejor tecnología que se pretende adquirir.

Los recursos económicos de esta categoría, consiste en disponer del presupuesto necesario para que los centros de informática puedan realizar inversiones para la implementación en infraestructura tecnológica, tales como: la adquisición de equipamiento en hardware y software, realizar la captación y capacitación del personal de desarrolladores en los diferentes lenguajes de programación que son necesarios para proteger la información digital de las entidades públicas del estado que pertenecen al sector Defensa.

Los recursos humanos que laboran en los centros de informática necesitan de capacitación constante porque el conocimiento científico en desarrollo de software, cada día aparecen nuevas técnicas y procedimientos para lenguajes de programación.

Los recursos pertenecen a una categoría de tercer nivel, siendo que está integrada a la categoría principal mediante el conector de “es parte de”. Esta categoría se

estableció por el método deductivo para agrupar los siguientes ítems conforme se detalla a continuación:

- Equipamiento (Fundamentación: 22 citas)

  Los equipamientos para la protección de la seguridad perimetral están conformados por: firewall routers, equipos VPN, equipos de filtrado web, antispam, etc., todos ellos son necesarios para la protección de los servidores de base de datos que están en le Data Center.

  Los ingenieros especialistas manifiestan que el "equipamiento de seguridad perimetral del Ejército permiten modernizar la seguridad frente ataques en el ciberespacio" en la cual se ha adquirido pero que, aún no es lo suficiente.

- Adquisición de licencias (Fundamentación: 15 citas)

  Para un buen funcionamiento de los diferentes sistemas instalados en los servidores del Data Center es necesario, que tengan su licencia de funcionamiento en la cual la mayoría tiene un año como periodos de vida, luego pasado ese tiempo, se tiene que adquirir una nueva licencia, y para ello implica presupuesto, pero ello es escaso siendo que, algunos usuarios optan por buscar informalmente los parches o cracks y estos mayormente traen software escondidos para robar información, según consideran los especialistas que: "la falta de recursos, y también del encargado de los DETELs realizan el uso excesivo de CRACKS, nadie desarrolla un software gratis, ahí hay algo que está por detrás para robar información."

- Capacitación del personal (Fundamentación: 7 citas)

  Teniendo los recursos económicos necesarios, es posible capacitar a nuestro personal que labora en el área de informática en las diferentes cursos y especialidades para desarrollar software en seguridad informática, redes, base de datos, integración y monitoreo de sistemas, etc.

- Presupuesto (Fundamentación: 81 citas)

  La categoría presupuesto está considerado en los recursos económicos lo cual existe 47 citas en esta problemática que limita la gestión para la protección de la información digital en base a las políticas de ciberseguridad que exige tener buenas infraestructuras en instalaciones, equipamiento de seguridad perimetral, capacitación del personal, comprar las licencias de funcionamiento, adquisición de antivirus, sistemas de protección de pozos atierra y presupuesto para incentivar al personal civil que labora en los centros de informática, etc. Zúñiga (2017) concluye que "la existencia de carencias de recursos disponibles para la ciberdefensa al no disponer de un nivel adecuado de asignación presupuestal para ser utilizado en ciberdefensa" (p. 200). Es fundamental disponer de los recursos económicos para dar soporte en software y hardware a los sistemas informáticos.

- Coordinación. (Fundamentación: 4 citas)

  La coordinación si bien es cierto tiene pocas citas, pero es fundamental para cerrar brechas que puedan potenciar alguna debilidad de los procesos para el cumplimiento de las políticas informáticas tales como: la DUFSITELE, en la cual se encuentra desactualizada, y es poco difundido, y que debería coordinarse entre las entidades comprometidas con este problema para actualizarlo e integrarlo de acuerdo a los avances tecnológicos para posteriormente ser socializado para todas las entidades informáticas disponibles en la institución .

A partir de esta categoría tenemos la respuesta para dos objetivos que son: el Objetivo N° 02 "Explicar el estado del desarrollo de software seguro en el marco de la ciberseguridad de las Políticas de Seguridad y Defensa Nacional" y al Objetivo Especifico N° 03" Describir el estado de las infraestructuras para la protección de la información digital de los centros de informática del CGE en el marco de la ciberseguridad de la Política de Seguridad y Defensa Nacional".

Como conclusión: Los bajos recursos económicos con los cuales se presupuesta en el Ejercito del Perú con respecto al sistema de seguridad de la información limitan la captación de personal especialista, adquisición de infraestructura informática modernas, adquisición de equipos de seguridad perimetral, servidores y licencias de funcionamiento para los diferentes softwares adquiridos; disponiendo de presupuesto permitiría incrementar la protección de la información digital acorde con las políticas de ciberseguridad y Defensa Nacional.

4.1.5 **MC4: Amenazas y problemas** (Fundamentación: 14 citas)

Las amenazas y problemas son riesgos que afectan la protección de la información digital. En la Figura 12 tenemos las diferentes interrelaciones entre las categorías y macro categorías establecidas para realizar el análisis correspondiente.

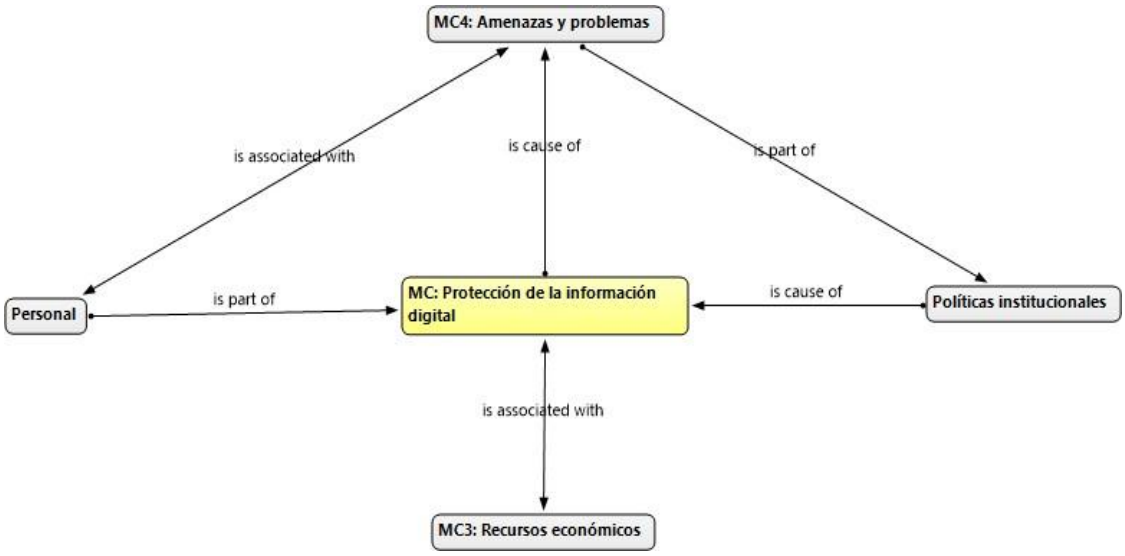

Figura 12 MC4: Amenazas y problemas

(Fuente: Programa Atlas.ti *7)*

Para un mejor análisis se ha subdividido en dos partes a las amenazas y problemas:

Amenazas

Según el enfoque de la Política de Seguridad y Defensa Nacional publicado mediante Decreto Supremo N° 012-2017-DE (DS012-2017-DE, 2017) describe a las amenazas como " riesgos y sus potenciales consecuencias, proteger el ciberespacio y su infraestructura se convierte en un asunto de Seguridad Nacional."

Las amenazas que actúan en el ciberespacio son múltiples y variadas, así como adopta nuevas formas y variaciones, según la Política de Seguridad y Defensa Nacional (DS012-2017-DE, 2017) nos dice:

> El ciberespacio y su infraestructura son susceptibles a una amplia gama de riesgos de amenazas tanto físicas como cibernéticas, por lo que una serie de actores podría aprovechar estas vulnerabilidades para robar información e interrumpir un proceso de transmisión de información digital, poniendo en riesgo, peligro o destruir la capacidad de prestar servicios; asimismo, el ciberespacio es particularmente difícil de proteger debido a la capacidad de estos actores de actuar virtualmente desde cualquier parte del mundo.

Los actores pueden actuar mediante el envío de diferentes tipos de amenazas cibernéticas tales como: virus, malware, hackers, crackers. Dichas amenazas se encuentran vinculados con la categoría principal mediante el conector de "es asociado de" protección de la información digital.

Las amenazas fueron establecidas por el método deductivo para poder agrupar los códigos que son afines a ellas y están conformada por los siguientes códigos según se muestra en la figura 7 y se destallan a continuación:

- Robo de información (Fundamentación: 03 citas)
  La sustracción de información digital se puede dar en cualquier parte donde se encuentre alojada o en transmisión dicha información, tales como en

unidades de almacenamiento de memoria, o cuando se encuentre siendo enviada o este viajando la información por las redes informáticas por los diferentes nodos existentes.

Para ello es necesario el desarrollo de software seguro como un medio alterno para proteger la información digital ya sea cuando este alojado en unidades de memoria, big data o cuando esta se encuentre siendo transmitida mediante señales analógicos o digitales.

Al consultarse a los especialistas, si desarrollaban software seguro para evitar la sustracción de información digital, se manifestó que: "eso es para el COCIBER", sin embargo, en el trayecto de la investigación, dicha entidad fue desactivada, creándose luego el CITELE, con esto se observa que existe limitaciones en su implementación por la coyuntura actual de reorganización.

- Virus (Fundamentación: 4citas)

  La existencia de virus en las redes informáticas actuales tales como: malware, fishing, troyanos, ramsonware, etc, es del día a día y existen en diversas modalidades para diferentes tipos de acciones para lo cual fue concebido y desarrollado por su creador. Los virus informáticos cada vez se tornan más robustos y sofisticados para cometer actos ilícitos con la información digital existentes. Gómez (2011) trata que los virus son "expertos informáticos que pretenden demostrar sus conocimientos construyendo virus y otros programas dañinos "(p. 197).

- Riesgos (Fundamentación: 7 citas)

  Los mecanismos de control de riesgos se dan con diferentes aplicaciones existentes para minimizar los intrusos a las bases de datos según esto, manifestó uno de los ingenieros, que "se controla con mecanismo de seguimiento de versiones mediante congelamiento de las aplicaciones por día en base a las versiones anteriores" por lo que, el control de riesgo se realiza, con limitadas acciones internas, para realizar protección de información digital de la base de datos, es necesario el monitoreo externo por otro ente que

sea de la misma red informática, para ello el especialista considera que " eso lo debe hacer el COCIBER", mediante el desarrollo de software seguro para proteger las redes informáticas y base de datos mediante un monitoreo externo a la red del CINFE. Gómez (2011) afirma que "el equipo responsable de la evaluación debe contar con un nivel adecuado de formación y experiencia previa" (p. 59). Aquí se explica la relación de las categorías de riesgos con la capacitación adecuada que debe tener el personal que labora en el sistema informático.

Con esta categoría se da respuesta a los siguientes objetivos: el Objetivo N° 01 "Explicar el estado de la protección de la información digital de los centros de informáticas Ejército en el marco de la ciberseguridad de las Política de Seguridad y Defensa Nacional" y al Objetivo Especifico N° 02 "Explicar el estado del desarrollo de software seguro en el marco de la ciberseguridad de la Políticas de Seguridad y Defensa Nacional".

Como conclusión: Las principales amenazas que limitan la protección de la información digital en el Ejercito del Perú de acuerdo a los hallazgos encontrados en el estudio son las siguientes : el limitado cumplimiento de las políticas de seguridad en los diferentes centros de informática, los virus, malware, fishing, troyanos, ramsonware, etc., el limitado desarrollo de software seguro, amenazas internas por parte del personal civil desafecto, probables hackers y crackers que son ciberdelincuentes de índole nacional e internacional y la existencia de instalaciones no adecuadas que protejan las bases de datos.

Problemas

A partir de esta categoría, se da respuesta al Objetivo N° 1: "Explicar el estado de la protección de la información digital de los centros de informática del Ejército en el marco de la ciberseguridad de la Política de Seguridad y Defensa Nacional".

Los problemas que se hace referencia en el estudio son los obstáculos y deficiencias que se tienen para proteger la información digital y las amenazas tales como los ciberataques que se puedan dar en contra de nuestros sistemas, redes y base de datos que se dispone en el Ejercito del Perú.

Un problema trascendental es la falta de actualización de las directivas y esto es, debido a que las tecnologías informáticas varían rápidamente en cuanto a sus contenidos, procedimientos y herramientas para dar seguridad a la información digital, así como por desconocimiento por el personal especialista, debido a la alta rotación existente cuando se realiza los procesos de cambios de colocación a las diferentes entidades de la institución.

Para tener un sistema informático con una debida y eficaz protección de la información digital es necesario invertir constantemente y estar a la vanguardia de la tecnología.

Asimismo, mediante la solución de los problemas de la protección de la información digital nos va permitir, la permanencia y supervivencia de la institución, porque es allí donde tenemos la base de datos para la administración y gestión de personal, recursos presupuestales, la gestión de bienestar, y gestión de derechos, etc.

Esta categoría de problemas de tercer nivel se relaciona mediante el conector “es causa de” la categoría principal.

Otros problemas a considerar son: deficiente difusión de las políticas de seguridad de la información por parte del personal responsable de cada entidad, las personas no leen las directivas y otros que consiguen leer, pero normalmente no lo comprenden en su contenido.

Esta categoría se estableció por el método deductivo para agrupar los siguientes ítems según como se detalla a continuación:

- Obstáculos (Fundamentación: 9 citas)

Dentro de los principales problemas y obstáculos que se ha podido observar para realizar una debida implementación de la protección de la información digital es la falta de los recursos económicos y esto lo manifiestan los entrevistados diciendo que: "es la falta de presupuesto lo que afecta la implementación de la seguridad de la información digital". Esta versión se puede confirmar con la actual publicación del DL N° 1412 que aprueba la Ley del gobierno digital en el Articulo N° 34.- Financiamiento, en la cual manifiesta que "la implementación de lo establecido en el presente Decreto Legislativo se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al tesoro público" por lo que se puede predecir que muy poco se podría hacer para realizar una efectiva implementación de la protección de la información digital debido a que se ha dado esta Ley pero, sin presupuesto adicional, lo cual se torna difícil implementar una efectiva seguridad de la información digital.

- Deficiencias (Fundamentación: 7 citas)

  Otras problemáticas observadas en las deficiencias para una debida implementación de la protección de la información digital son: la falta de recursos humanos capacitados, los limitados recursos económicos, la alta rotación de personal, la poca adquisición de tecnologías como firewall, siendo todo esto manifestado por los especialistas en la cual manifiestan que, "las principales deficiencias son: no hay un firewall interno que permita monitorear los sistemas o servidores ante un ataque y tener una alerta temprana. También la falta personal capacitado con nivel avanzado en infraestructura de seguridad, y también la falta de presupuesto".

- Idiosincrasia (Fundamentación: 4 citas)

Entendemos a la idiosincrasia al modo de ser de una persona en cuanto a sus características y peculiaridades, para este caso es la dejadez, la falta de interés o el propio desconocimiento que podría contribuir en esa dejadez al dejar de hacer y dejar pasar sin tomar las medidas correctivas. Según la entrevista los especialistas manifiestan: "que se le dé la importancia que le corresponde a la seguridad del equipamiento informático, ya que es el medio donde se almacena el activo más importante que es la información digital cuya pérdida sería de gran impacto".

- Falta de presupuesto (Fundamentación: 25 citas)

  Según lo que nos manifestado por varios especialistas que nos dicen: "la falta de presupuesto" es la principal problemática para mejorar la protección dela información digital. Esta problemática debe ser encarada por parte administrativa de la institución mediante diferentes estrategias como realizar alianzas con otras instituciones públicas y privadas asi como, las universidades e instituciones técnicas de enseñanza informática para poder desarrollar software seguro en la cual el beneficio sea para todos los entes que participan en su desarrollo e implementación.

- Falta de capacitación (Fundamentación: 81 citas)

  Según la entrevista los especialistas expresan que: "la falta personal capacitado en nivel avanzado en infraestructura de seguridad". Esta problemática puede bien ser encarado inicialmente mediante la captación de personal de procedencia universitaria y de instituciones tecnológicas educativas con cierto perfil de conocimiento en los diferentes tipos de lenguajes de programación, para después continuar su capacitación de acuerdo a sus potencialidades de cada profesional captado.

Como conclusión: Los principales problemas que limitan la protección de la información digital son: la falta de presupuesto, la falta de capacitación con el personal que labora en informática y base de datos, la falta de desarrollo de software seguro, la falta de difusión de las políticas de seguridad informática, el desconocimiento de la DUFSITELE, la poca importancia que se le da para proteger la información digital, los pocos firewall que existe en la seguridad perimetral, la falta de experiencia e idiosincrasia que existe con el personal civil, la falta de capacitación de nivel avanzado en infraestructura de seguridad informática, el desconocimiento por parte del comando del valor que tiene la protección de la información digital.

4.1.6 MC5: Entidades Informáticas (Fundamentación: 63 citas)

A partir de esta macro categoría, se da respuesta al Objetivo N° 1: "Analizar el estado de la protección de la información digital de los centros de informática del Ejército en el marco de la ciberseguridad y Política de Seguridad y Defensa Nacional", y también al Objetivo N° 3: "Describir el estado de las infraestructuras para la protección de la información digital de los centros de informática del Ejército en el marco de la Política de Seguridad y Defensa Nacional". En la Figura 13 tenemos las diferentes interrelaciones entre las categorías y macro categorías establecidas para realizar el análisis correspondiente.

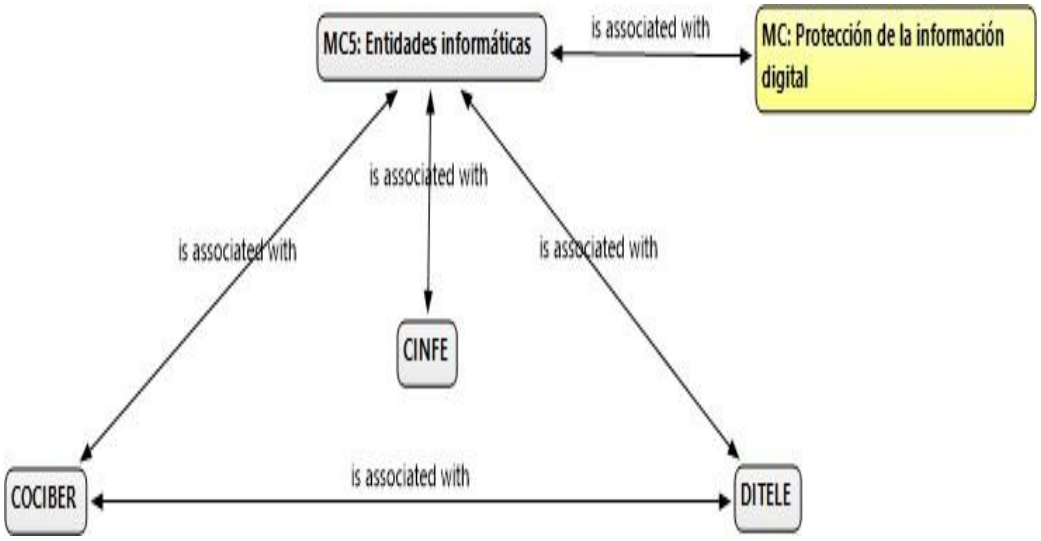

Figura 13 MC5: Entidades informáticas

(Fuente: Programa Atlas.ti *7)*

Existen diferentes actores externos e internos como entidades informáticas. En la parte externa esta la estructura del gobierno electrónico y principalmente la secretaria de gobierno digital; para la parte interna se cuenta con las siguientes entidades informáticas de la institución: DITELE, COCIBER y el CINFE.

- **Dirección de Telemática (DITELE):** (Fundamentación: 5 citas)

  La Dirección de Telemática como ente de dirección y planeamiento a nivel institución, es la encargada de normar los procedimientos conforme la secretaria de gobierno digital va emitiendo las diferentes Leyes.

  También esta entidad es la encargada de actualizar las normas, directivas y procedimientos en cuanto a comunicaciones, telemática e informática, así como el desarrollo y mantenimiento de software para todas las entidades de la institución.

- **Comando de Ciberdefensa (COCIBER):** (Fundamentación: 7 citas)

  El COCIBER con su creación de un año, ha sido reemplazado por el CITELE recientemente creado en la institución bajo los diferentes departamentos que lo componen, ellos van a permitir enfrentar las diferentes riesgos y amenazas en el ámbito dela ciberseguridad y ciberdefensa nacional. Así mismo, este comando tiene al CINFE el cual dentro de sus diferentes funciones tiene como objetivo dar mantenimiento y desarrollar software de diferentes tipos, aplicando el planeamiento, se conseguirá la privacidad de la información desde el "diseño y configuración de los servicios digitales se adoptan las medidas preventivas de tipo tecnológico, organizacional, humano y procedimental" (DL 1412 LEY DE GOBIERNO DIGITAL, 2018).

- **Centro de Informática (CINFE):** (Fundamentación: 5 citas)

El CINFE y el COCIBER dentro de la estructura organizacional en el área de informática, son la parte operativa para el desarrollo e implementación de los sistemas informáticos tanto en el ámbito administrativo como operacional.

Como conclusión: Las entidades informáticas que se encuentran inmersas dentro de las instituciones públicas y en especial en el Ejercito del Perú son de vital importancia en su funcionamiento, y de acuerdo con ello es importante considerar que deben contar con un interés especial del Comando ya sea desde los lineamientos presupuestarios hasta la inclusión en el plan de modernización digital y revolución científica en el marco de la globalización donde se tome en cuenta en principio una infraestructura adecuada, personal capacitado, actualizado y a la vanguardia de los últimos manejos cibernéticos, recursos suficientes para poder implementar y desarrollar software seguro, desde su planeamiento para luego ser instalados en los sistemas administrativos y operacionales, entre otros.

Relación entre Macro Categorías

Para un mejor entendimiento de la situación problemática y las relaciones entre las macro categorías existentes, según la Figura 7 debe observarse de forma holística, porque la concepción de cada realidad es la sumatoria de las partes de cada macro categoría que la componen a esta problemática de estudio, en las cuales interactúan con la macro categoría amenazas y problemas, que las afectan en forma trasversal.

La información digital que se encuentra alojada en la base de datos de los centros de informática del Ejército, institución que pertenece a las FFAA, son activos críticos nacionales deben ser incrementados las medidas de ciberseguridad mediante diferentes procesos, disposiciones, normas, directivas y políticas de seguridad y defensa nacional, para lo cual estos deben ser bien planificados eficientemente por las entidades informáticas para luego ser difundidos mediante sensibilización al personal militar, para que tomen conocimiento y lleven la puesta en práctica. Con la existencia de infraestructuras informáticas robustas, con eficiente capacitación del personal especialista en programación y desarrollo de software seguro desde su implementación en la base de datos es posible disponer un sistema informático con alto rango de ciberseguridad.

CONCLUSIONES

Primero:

Se evidencia que, en cuanto al estado de la protección de la información digital de los centros de informática del Ejército es muy importante, sin embargo, se encuentra limitadamente protegido en cuanto al hardware y software, en razón a los siguientes requerimientos:

- Necesidad de constante mantenimiento, adquisición de licencias y actualizaciones de los sistemas.
- El personal que labora en dichos centros necesita de una constante capacitación y requieren de incentivos o estímulos a fin de que realicen un idóneo desempeño laboral.
- En cuanto a la Políticas de Seguridad y Defensa Nacional, leyes, normas, directivas en el ámbito de la ciberseguridad no se están cumpliendo a cabalidad, por lo que es necesario actualizar, difundir y concientizar al personal sobre su cumplimiento.

- Necesidad de establecer coordinaciones con las nuevas entidades responsables con la seguridad informática, como son el CITELE, el CINFE, y DITELE; debiendo dichas entidades tener el nexo correspondiente con los entes de la Secretaria de Gobierno Digital que pertenece a la Presidencia del Consejo de Ministros.

Segundo:

En cuanto al estado del desarrollo de software seguro para mejorar la ciberseguridad en la protección de la información digital, esta se encuentra operando en forma limitada en los centros de informática del Ejército, existiendo la necesidad de captar y capacitar personal especialista en programación a fin de desarrollar nuestras propias herramientas de software y aplicativos para ciberseguridad, para incrementar los niveles de seguridad informática, y a la vez conseguir la independencia tecnológica al tener nuestro propio know how.

Tercero:

En relación a las infraestructuras para la protección de la información digital de los centros de Informática del Ejército, se evidencia que es importante destinar presupuesto adecuado y sostenible para garantizar su optimización y funcionamiento para una infraestructuras informáticas completamente modernizada la misma que estaría compuesta por: instalaciones, equipamiento informático, sistemas perimetrales y recursos humanos, colocándole a su vez a la par con los principales ejércitos del mundo.

RECOMENDACIONES

Primero:

Que el Comando del Ejército presten la debida importancia del estado actual en que se encuentra la implementación de la protección de la información digital que dispone en sus bases de datos de los diferentes centros de informática y que son empleados a través de las diferentes redes informáticas, debiendo asignar los recursos económicos financieros necesarios que permitan:

- La captación de personal especialista en lenguajes de programación asegurándoles su capacitación constante.
- El desarrollo de un software propio de tal manera que las redes puedan incrementar las capacidades de ciberseguridad informática.
- Se asegure el fiel cumplimiento de las normas de acuerdo a los lineamientos de la Política de Seguridad y Defensa Nacional en cuanto a ciberseguridad.

Segundo:

Que el Comando de Personal asegure la asignación y cambio de colocación de personal militar que tengan competencias profesionales en seguridad informática y desarrollo de software, administrándoles mediante un efectivo plan de carrera de tal forma que puedan permanecer en dichos centros, evitando la alta rotación por planes de cambio de colocación, todo ello con la finalidad de incrementar la protección de la información digital de las redes informáticas de los sistemas operativos y administrativos de la institución a nivel nacional.

Tercero:

Que el Comando del Ejército asigne los recursos presupuestales necesarios para asegurar las infraestructuras para la protección de la información digital de los centros de Informática del Ejército, la misma que está compuesta por: instalaciones, equipamiento informático, sistemas perimetrales, de todo el sistema que la componen.

PROPUESTAS

PARA ENFRENTAR LA REALIDAD PROBLEMÁTICA

a. Creación de un centro de Ciberdefensa

Que el Comando del Ejército gestione la creación de un Centro de Ciberdefensa teniendo en cuenta las experiencias de la creación del COCIBER y del CITELE con independencia administrativa y operativa con infraestructura informática compuesta por instalaciones, personal, redes, base de datos y computadores para alcanzar capacidades de realizar operaciones y acciones cibernéticas en el ciberespacio y así proteger la información digital no solo de los centros de informática de la institución, si no de los activos críticos de las instituciones públicas y privadas del Estado. Todo ello, implementado acorde con las normas alineadas con la política de ciberseguridad y Defensa Nacional.

b. Desarrollo de software para implementar las infraestructuras informática

Desarrollar un marco referencial de desempeño de competencias profesionales en la captación de personal con talento en sistemas de informática y desarrollo de software. De igual forma desarrollar una línea de capacitación continua en la adquisición de conocimientos y experiencia referida al tema. Acompañado a ello se debe procurar la ejecución de la inversión en un sistema de seguridad informática de última generación que responda a las actuales amenazas informáticas para que luego puedan desarrollar sistemas seguros para proteger la información digital de los centros de informática de la institución y de los activos críticos conformados por las redes informáticas y bases de datos del Ejercito del Perú.

Así mismo el personal que labore en dicho centro debe tener alta motivación e incentivos para que puedan producir en forma eficiente y eficaz.

c. Capacitación del personal

Es importante contemplar con un plan de capacitación con los recursos disponibles para el personal mediante especialistas contratados para todos los comandos y oficiales del alto mando y gestores del Estado Mayor del CGE a fin de sensibilizar según la planificación y programación que se realice.

REFERENCIAS BIBLIOGRÁFICAS

Alvarez -Gayou, J. (2003). *Como hacer investigación cualitativa.*

Aquino, R., Chavez, J., Vidal, L., Ferreyro, L., Alvez, A., & Carozo, E. (2009). *Manual de Gestión de incidente de seguridad informática.* Obtenido de www.proyectoamparo.net.

Areitio, J. (2008). *Seguridad de la información.* Paraninfo.

Biblioteca de la Universidad de Extremadura. (s.f.). *Que se entiende por velocidad lectora.* Obtenido de La lectura: https://biblioguias.unex.es/c.php?g=572102&p=3944889

Canes, M., & Pastrana, S. (2014).

Dirección de Telemática del Ejército. (2017). DUFSITELE.

DL 1412 LEY DE GOBIERNO DIGITAL. (2018). LEY DE GOBIERNO DIGITAL. *DECRETO LEGISLATIVO QUE APRUEBA LA LEY DE GOBIERNO DIGITAL*.

DS012-2017-DE. (2017). *https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-la-politica-de-seguridad-y-defen-decreto-supremo-n-012-2017-de-1600032-1/*.

DUFSITELE. (2017). Directiva unica de funcionamiento del sistema de telemática del Ejército.

Erb, M. (s.f.). *Gestión de Riesgo en la Seguridad Informática*. Obtenido de https://protejete.wordpress.com/about/

Escalante, O., & Vidarte, O. (2018). *Conflictos entre la gobernabilidad y la soberannia en las organizaciones multilaterales: estudio de la implementación de políticas de seguridad informática .*

Gamboa, C. (2010). *Seguridad cibernética una necesidad mundial.* San Jose: Impresión gráfica del Este S. A.

Gil Gonzales, E. (2015). *BIG DATA, PRIVACIDAD Y PROTECCIÓN DE DATOS.* Madrid: Agencia Española de Protección de Datos.

Gomez, A. (2011). *Enciclopedia de la Segurida informática.* Mexico: Alfaomega.

Harán, J. M. (2020). *Welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2020/06/10/actualizaciones-seguridad-junio-2020-microsoft/

Hernandez, R., Fernandez, C., & Baptista, P. (2014). *Metodologáa de la Investigación.* Mexico.

Hess, C. (2010). *Ciberseguridad en Costa Rica.* San José.

Hidalgo Tarrero, J. T. (11 de Agosto de 2014). *IEEE Ingeniería del software y Ciberseguridad.* Obtenido de IEEE: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO88-2014_Ingenieria_Software_Ciberseguridad_HidalgoTarrero.pdf

http://elperuano.pe. (2017). Obtenido de http://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-la-politica-de-seguridad-y-defen-decreto-supremo-n-012-2017-de-1600032-1/

Iglesias, A. (s.f.). *http://www.ticbeat.com/seguridad/los-mejores-repositorios-y-recursos-gratuitos-sobre-virus-y-ciberseguridad/*.

Inoguchi, A., & Macha, E. (2017). *Gestión de la ciberseguridad y prevencion de los ataques cibernéticos en las Pymes del Perú.*

Izcara, s. (2014). *Manual de Investigación Cualitativa.* Mexico D F: Fontamara.

Lopez, J. (2016). *Analíticas de seguridad de código fuente.* Madrid.

López, J. (2019). *Consumotic*. Obtenido de https://www.consumotic.mx/tecnologia/e-mail-principal-vector-de-ciberataques-symantec/

Medina Iriarte, J. (2006). *Repositorio Académico de la Universidad de Chile*. Obtenido de http://repositorio.uchile.cl/bitstream/handle/2250/108414/medina_j.pdf?sequence=4&isAllowed=y

Merino, F., & Aliaga, A. (2017). *Delitos informáticos y las salidas alternativas posibles revisadas desde el análisis económico del derecho.* Santiago.

NTP-ISO/IEC 27001. (2008). *Congreso.gob.pe*. Obtenido de http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C8D255B0DF2866580525831D00656B05/$FILE/1_isoiec27001.pdf

NTP-ISO/IECC 17799. (Marzo de 2015). *https://www.pmg-ssi.com/2015/03/ntp-isoiec-17799-norma-técnica-peruana/.* Obtenido de Norma técnica NTP-ISO/IEC 17799.

PCM-Secretaria de Gobierno Digital . (2017). Resolución de Secretaria de Gobierno Digital.

Perafán Ruiz, J. J., & Caicedo Cuchimba, M. (2014). *https://repository.unad.edu.co* . Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf?sequence=3&isAllowed=y

Proyecto AMPARO. (s.f.). *Gestión de incidente de seguridad informática.* Obtenido de www.proyectoamparo.net/.

RAE, R. A. (2020). *https://dle.rae.es/protecci%C3%B3n*. Obtenido de https://dle.rae.es/protecci%C3%B3n

Vargas, X. (2010).

Vargas, X. (2010). *Como hacer investigación cualitativa.*

Vargas, X. (2010). *Cómo hacer investigación cualitativa.*

Vargas, X. (2011). *¿Cómo hacer una investigación cualitativa?*

Zuñiga, J. (2017). *Ciberseguridad y su incidencia en la protección de la información del ejército del Perú. Caso:COPERE.*

ANEXOS

- Anexo 01. Matriz de Consistencia
- Anexo 02. Matriz de Categorías
- Anexo 03. Guía de entrevista
- Anexo 04: Agenda de aplicación de instrumentos
- Anexo 05. Ruta estratégica

ANEXO 01: MATRIZ DE CONSISTENCIA

TITULO: ANÁLISIS DE LA PROTECCIÓN DE LA INFORMACIÓN DIGITAL DE LAS FUERZAS ARMADAS EN EL MARCO DE LA POLÍTICA DE SEGURIDAD Y DEFENSA NACIONAL EN LA REGIÓN LIMA, 2018

PLANTEAMIENTO DEL PROBLEMA	OBJETIVOS	HIPOTESIS	OBSERVABLES	ENFOQUE	TIPO DE INVESTIGACIÓN
¿Cuál es el estado de la protección de la información digital de los centros de informática del ejército?	Explicar el estado de la protección de la información digital de los centros de informática del ejército	La limitada protección de la información digital de los centros de informática del ejercito constituye una vulnerabilidad frente a los ataques y sustracción de la información	Protección de la información digital. Políticas de Seguridad de la Información Digital	Cualitativo	Empírico
			METODO	**OBJETO**	**TECNICAS**
¿Cuál es el estado del desarrollo de software seguro para la protección de la información digital de los centros de informática del ejército?	Explicar el estado del desarrollo de software seguro de los centros de informática del ejército.		Hermenéutico	Empírico	Entrevista no estructurada Indagación documental
¿Cuál es el estado de las infraestructuras para la protección de la información digital de los centros de informática del ejército?	Describir las infraestructuras para la protección de la información digital de los centros de informática del ejército .		**INSTRUMENTOS** Guía de entrevista Relación de documentos buscados y ruta de sitios virtuales.		

ANEXO 02: MATRIZ DE CATEGORIAS

SUBCATEGORIAS (Codificación abierta)	MACROCATEGORIAS (Codificación axial)	METACATEGORIA (Codificación selectiva)
Contraseñas Deben ser entendidas como aquellos códigos secretos que se introducen en una máquina para poder acceder a una función informática.	**Política de Seguridad Informática** Se encuentra relacionada a la protección de la información digital.	**PROTECCION DE LA INFORMACION DIGITAL DE LAS FFAA** Concierne a tener la capacidad de ciberseguridad para proteger la información digital que deben tener las instituciones y entidades públicas del estado.
Seguridad Informática Conjunto de procedimientos que deben cumplir todos los involucrados respecto del tratamiento de la información. Es una forma de comunicarse con los usuarios en relación con los recursos y servicios informáticos.		
Ciberseguridad Se relaciona con la protección de la información digital.		
Leyes y normas Ley Nª 30999 Ley de Ciberdefensa publicada en el año 2019.		
Cumplimiento de normas Es la responsabilidad del respeto y subordinación respecto a las normas, reglamentos referidos a la confiabilidad de la información en busca de su protección.		
Sistemas perimetrales Sistemas que permite la seguridad del software.	**Recursos Económicos** Son fundamentales para gestionar una eficaz protección de la información digital y estos ocurren cuando se asigna presupuesto para los institutos castrenses puedan realizar los procesos de adquisición y selección de infraestructura informática por medio del sistema de contrataciones del Estado.	
Administración Administración para los sistemas.		
Licencias informáticas Son las autorizaciones para su empleo.		
Calidad del software Software sin errors de funcionamiento		
Equipamiento Relacionado a todo hardware para los sistemas.	**Infraestructura informática** Hace referencia a la existencia de instalaciones apropiadas para que funcione toda organización informática compuesta por personas, hardware y software con la finalidad de proteger la información digital.	
Instalación de software		
Aplicaciones informáticas Son los software instalados en los sistemas		
DITELE Se refiere a la Dirección de Telemática.	**Entidades informáticas** En la parte externa esta la estructura del gobierno electrónico y principalmente la secretaria de gobierno digital. En el aspecto interno se cuenta con DITELE, COCIBER Y el CINFE.	
Secretaria de gobierno digital		
CINFE Se refiere a los centros de informáticas		
COCIBER Comando de Ciberdefensa.		
Falta de presupuesto	**Problemas y amenazas** Son los que limitan el Sistema de protección de la información digital	
Idiosincracia		

ANEXO 03: GUÍA DE ENTREVISTA

Tema: Análisis de la protección de la información digital según la política de seguridad y defensa nacional

Introducción: Señores el propósito de esta entrevista es obtener información sincera para la elaboración de una tesis motivos por el cual, desde ya, se agradece su valiosa información y aportes.

Característica de la entrevista: Confidencial

Preguntas:

1. ¿Cuál es su experiencia en la implementación de la protección de la información digital de su departamento de informática en el marco de la Política de Seguridad y Defensa Nacional?

2. ¿Cuál es su experiencia con el control de riesgo informático para la protección de la información digital de su departamento de informática en el marco de la Política de Seguridad y Defensa Nacional?

3. ¿Cuál es su testimonio acerca de la sincronización de los diferentes sistemas informáticos para la protección de la información digital de las bases de datos de su departamento de informática?

4. ¿Cuál es su experiencia en cuanto al modelo de los sistemas informáticos para la protección de la información digital de su departamento de informática?

5. ¿Considera Ud., que es importante la protección de la información digital de su departamento de informática?

6. ¿Cuál es su testimonio acerca de la implementación del desarrollo de software seguro en el marco de las Políticas de Seguridad y Defensa Nacional para los sistemas de información de las bases de datos de su departamento de informática?

7. ¿Cuál es su testimonio acerca de las herramientas y aplicaciones para el desarrollo de software seguro para la protección de la información digital de las bases de datos de su departamento de informática?

8. ¿Cuál es su experiencia en cuanto al desarrollo de software seguro para evitar el robo de información digital por personal malicioso de su departamento de informática?

9. Acerca de la Política de Seguridad y defensa. Diga Ud., ¿cuál es su experiencia en cuanto al cumplimiento de dichas Leyes, Normas y Directivas?

10. Actualmente ¿Cuál es su testimonio acerca del cumplimiento de las Normas, Directivas (DUFSITELE) para la protección y seguridad de la información digital que debe tener la base de datos de su departamento de informática?

11. ¿Cómo se monitorea la implementación de la protección de la información digital existente en las bases de datos de su departamento de informática?

12. A su criterio ¿Cuáles son los principales obstáculos que afectan la implementación de la protección de la información digital de su departamento de informática?

13. Cree Ud., ¿necesaria una campaña de difusión y sensibilización con las autoridades y personal en general sobre la importancia en el cumplimiento de la DUFSITELE?

14. A su criterio ¿Cuáles son las principales deficiencias en cuanto a infraestructura para la protección de la información digital de su departamento de informática?

15. Actualmente acerca de la Infraestructura para la protección de la información. Diga Ud., ¿cuál es su testimonio para una mejor implementación y desarrollo de software seguro para evitar perdida y robo de información digital?

16. A su criterio ¿Cuáles son los principales obstáculos que afectan la implementación de una infraestructura adecuada para la protección de la información digital de su departamento de informática?

17. ¿Tiene Ud. algo más que agregar o manifestar en la presente entrevista?

Gracias por su participación.

Fuente: Elaboración propia

ANEXO 04: AGENDA DE APLICACIÓN DE INSTRUMENTO PARA RECOPILACIÓN DE INFORMACIÓN (GUÍA DE ENTREVISTA)

N/O	Zona de entrevista	Nombre del entrevistado	Fecha y hora de la entrevista	Dependencia	Puesto desempeñado	Obs
01	Cuartel General	Luis Alberto SOTO HUAMAN	05 1000 Oct 18	Centro de Informática	Asistente Analista de sistema	
02	Cuartel General	Giovanna Mariela HINOJOSA FLORES	05 1030 Oct 18	Centro de Informática	Sistema Analista principal de sistemas	
03	Cuartel General	David Oliver NINAHUAMAN HURTADO	05 1100 Oct 18	Centro de Informática	Ing. Sistemas Administrador de Base de Datos	
04	Cuartel General	Manuel ALARCON CALDERON	15 1000 Oct 18	Centro de Informática	Jefe de DETEL de la OEE	
05	Cuartel General	Luis TRUJILLO LAURA	22 0920 Oct 18	Centro de Informática	Ingeniería de Sistemas	
06	Cuartel General	ROBLEDO COVEÑAS Miguel Angel	22 0940 Oct 18	Centro de Informática	Jefe Departamento Infraestructura Telemática	
07	Cuartel General	Fernando MORANTE ALTAMIRANO	22 1000 Oct 18	Centro de Informática	Jefe Sección Programación	
08	Cuartel General	Victor MARISCAL CARHUAMACA	22 1020 Oct 18	Centro de Informática	Jefe Sección Calidad Software	
09	Cuartel General	OLIVEIRA AREVALO Karl Hans	22 1040 Oct 18	Centro de Informática	Jefe de Data Center	
10	Cuartel General	QUISPE ITOKAZU Oscar	22 1100 Oct 18	Centro de Informática	Jefe de Sección de TI	

Fuente: Elaboración propia

ANEXO 05: RUTAS ESTRATÉGICAS: RELACIÓN DE DOCUMENTOS BUSCADOS Y RUTA DE SITIOS VIRTUALES O REALES DONDE PUEDEN SER ENCONTRADOS EL TEMA DE PROTECCIÓN DE LA INFORMACIÓN DIGITAL Y CIBERSEGURIDAD

N°	INFORMACIÓN	DOCUMENTO	DEPENDENCIA O UBICACIÓN DEL DOCUMENTO
1	Políticas del Estado Peruano. • 9na Política: Seguridad Nacional.	Acuerdo Nacional (2002).	En poder del investigador
2	Marco Legal que aprueba la Política de Seguridad y Defensa Nacional, • Ámbito de aplicación. • Financiamiento. • Implementación.	Decreto Supremo N° 012-2017-DE del 20 de Diciembre del 2017 que aprueba la Política de Seguridad y Defensa Nacional.	En poder del investigador
3	• Objetivo de Política N° 1 • Lineamientos de Política de Seguridad y Defensa	Política de Seguridad y Defensa Nacional del Estado Peruano (2017)	En poder del investigador

4	• Objetivos sectoriales. • Lineamientos estratégicos del sector Defensa	Plan estratégico sectorial multianual del Ministerio de Defensa 2016-2021.	Ministerio de Defensa (CARÁCTER SECRETO)
5	• Objetivos institucionales. • Acciones estratégicas del sector Defensa	Plan estratégico Institucional del Ministerio de Defensa (PEI)	Ministerio de Defensa (CARÁCTER DE SECRETO)
6	Marco Normativo de la Dirección de Telemática	DUFSITELE	Acceso limitado
7	• Departamento de Seguridad Nacional en España	http://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/ciberseguridad	Acceso al investigador
8	• Experiencia en España en Ciberseguridad.	https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos	Acceso al investigador
09	• Experiencia en el Reino de España. Plan estratégico de	https://www.es-ciber.com/plan-estrategico-concienciacion-	Acceso al investigador

	concienciación en Ciberseguridad	ciberseguridad-fortaleciendo-al-eslabon-mas-debil-la-cadena/	
10	Definiciones para el Marco conceptual	https://acuerdonacional.pe/políticas-de-estado/definición	Acceso al investigador
11	Definiciones para el Marco conceptual	http://www.perulinux.pe/capacitaciones/curso-de-ciberseguridad/	Acceso al investigador
12	Definiciones para el Marco conceptual	https://www.cisco.com/c/es_pe	Acceso al investigador
13	Definiciones para el Marco conceptual	https://www.peruciberseguro.org/	Acceso al investigador
14	Estrategia de Ciberseguridad Nacional 2016-2021 Reino Unido	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643420/Spanish_translation_-_National_Cyber_Security_Strategy_2016.pdf	Con acceso y en poder del investigador

Fuente: Elaboración propia