ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

TESIS DE GRADO

CAPACIDAD MILITAR DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ EN LAS OPERACIONES MILITARES EN EL CIBERESPACIO, 2021

AUTOR

Bach Alexander Bladimir PAMPA URIETA
0000-0002-6781-8099

Para optar el Grado Académico de

MAESTRO EN CIENCIAS MILITARES

Con mención en Planeamiento Estratégico y Toma de decisiones

ASESOR METODOLÓGICO:

Mg. Adrián Víctor CAMACHO SORIANO
0000-0003-1961-9666

ASESOR TEMÁTICO:

Mg. Neyelko Miguel ACOSTA ARANIBAR
0000-0003-1506-4763

2023

Conformidad de Jurado de sustentación de tesis

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

DEPARTAMENTO GESTIÓN DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN DE TESIS No 010 – 2023/ DGI

En la Escuela Superior de Guerra del Ejército - Escuela de Postgrado, a los veinte días del mes de abril del año dos mil veintitrés, siendo las 0850 horas, se reunió el jurado evaluador conformado por los docentes:

❖	Doctora	BERTHA MILAGROS VILLALOBOS MENESES	Presidente
❖	Maestro	DE LA CRUZ GRAJEDA ABRAHAM FELIX	Secretario
❖	Doctor	HUGO RICARDO PRADO LOPEZ	Vocal

Designados según Resolución de Expedito para Sustentación de Tesis **N° 010-2023/SIE/DGI/ESGE-EPG** del 13 de marzo del 2023, para evaluar la sustentación presencial y defensa de la Tesis de Grado titulada **"CAPACIDAD MILITAR DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ EN LAS OPERACIONES MILITARES EN EL CIBERESPACIO, 2021"**, presentado por los Bachiller **ALEXANDER BLADIMIR PAMPA URIETA**, para optar el Grado Académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de decisiones, de acuerdo a lo establecido en el artículo 45° de la Ley Universitaria N° 30220.

Luego de atender la sustentación presencial, defensa de la tesis de grado y realizadas las preguntas de rigor, el jurado acordó concederle la calificación de Aprobado por UNANIMIDAD

En mérito del cual, el jurado Aprueba (aprueba / no aprueba) que se le otorgue el Grado Académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de decisiones.

Firmado, en Chorrillos a los veinte días del mes de abril del 2023.

DRA. BERTHA MILAGROS VILLALOBOS MENESES
PRESIDENTE

MG. DE LA CRUZ GRAJEDA ABRAHAM FELIX
SECRETARIO

DR. HUGO RICARDO PRADO LOPEZ
VOCAL

Autorización para publicación y uso

A través del presente documento, yo Bach. Alexander Bladimir PAMPA URIETA autorizo a la Escuela Superior de Guerra del Ejército-Escuela de Postgrado la publicación del texto completo o parcial de la tesis de grado titulada “Capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio, 2021.” presentada para optar al grado académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones en el Repositorio Institucional y en el Repositorio Nacional de Tesis (RENATI) de la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU), de conformidad al marco legal y normativo vigente. La tesis se mantendrá permanente e indefinidamente en el Repositorio para beneficio de la comunidad académica y de la sociedad. En tal sentido autorizo gratuitamente y en régimen de no exclusividad los derechos estrictamente necesarios para hacer efectiva la publicación, de tal forma que el acceso al mismo sea libre y gratuito, permitiendo su consulta e impresión, pero no su modificación. La tesis puede ser distribuida, copiada, exhibida y usada también con fines académicos siempre que se indique la autoría y no se podrán realizar obras derivadas de la misma.

Chorrillos, 10 de noviembre del 2022

Alexander Bladimir PAMPA URIETA

DNI: 42194606

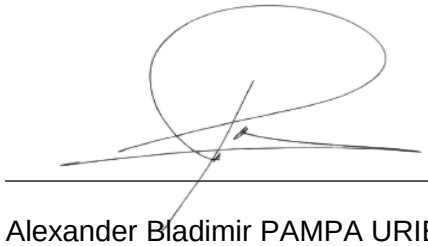
Declaración Jurada de Autoría

Mediante el presente documento, Yo, Bach. Alexander Bladimir PAMPA URIETA, identificado con Documento Nacional de Identidad N° 42194606 , con domicilio en Torres de Matellini sector “A” block N° 14 departamento N° 104, Chorrillos , provincia y departamento de Lima, graduado de la X Maestria en Ciencias Militares con mención en Planeamiento Estratégico de la Escuela Superior de Guerra-Escuela de Posgrado del Escuela Superior de Guerra del Ejército-Escuela de Postgrado (ESGE-EPG) declaro bajo juramento que:

Soy el autor de la investigación titulada: “Capacidad militar de Ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio, 2021”, que presento a los doce días del mes de julio del año 2021, ante esta institución con fines de optar el grado académico de Magister en Ciencias Militares con mencion en Planeamiento Estrategico y Toma de Decisiones.

Dicha investigación no ha sido presentada ni publicada anteriormente por ningún otro investigador ni por el suscrito, para optar otro grado académico ni título profesional alguno. Declaro que se ha citado debidamente toda idea, texto, figura, fórmulas, tablas y a otros que corresponde al suscrito o a otro en respeto irrestricto a los derechos del autor. Declaro conocer y me someto al marco legal y normativo vigente relacionado a dicha responsabilidad.

Declaro bajo juramento que los datos e información presentada pertenecen a la realidad estudiada, que no han sido falseados, adulterados, duplicadas ni copiados. Que no he cometido fraude científico, plagio o vicios de autoría; en caso contrario, eximo de toda responsabilidad a la Escuela Superior de Guerra del Ejército-Escuela de Postgrado y me declaro como el único responsable.



Alexander Bladimir PAMPA URIETA

DNI 42194606

Agradecimiento

En el continuo conocer de la vida, de los amplios conocimientos que uno va adquiriendo, desde la escuela hasta los estudios superiores, somos artistas de nuestro conocimiento, lo tallamos de acuerdo a nuestro enfoque, con esfuerzo, dedicación y sacrificio. A través de mi carrera militar entendí que el éxito radica en la perfección del talento y nos ayuda a ser mejores, mis padres Marco y Cecilia, por la primera experiencia de tener un computador de niño y despertar en mi la pasión por la tecnología y ser mi aliento desde el cielo, la inteligencia militar por medio del cual puse mi capacidad al máximo con un enfoque nuevo, del empleo de la cibernética en las operaciones de inteligencia.

Índice

CAPITULO III: METODOLOGÍA DE LA INVESTIGACIÓN

CAPITULO IV: ANÁLISIS Y SÍNTESIS

CAPITULO V. DIALOGO TEÓRICO – EMPÍRICO

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

Lista de tablas

Lista de figuras

Resumen

La investigación tiene como propósito explicar la situación actual de la capacidad militar de Ciberdefensa del Ejército del Perú, y analizar las operaciones militares en el ciberespacio, 2021. La investigación tiene un enfoque cualitativo, de tipo teórica - empírica, con el método hermenéutico interpretativo. Se empleó el muestreo no probabilístico empleando la muestra: de voluntarios realizada a seis (05) expertos de Ciberdefensa. Este estudio se realizó mediante una guía de entrevista al personal que labora en el Centro de Ciberdefensa del Ejército (CECIBER) y especialistas en Ciberdefensa Desarrollándose estableciendo categorías: Capacidad militar de defensa, operaciones militares en el ciberespacio. Los principales resultados explican que en la región se está desarrollando la capacidad militar de Ciberdefensa en diferentes países, cabe mencionar que el Ejército del Perú creó el CECIBER, con muchas limitaciones siendo estas tecnológicas, personales, de procesos, el no disponer de un soporte tecnológico, es una variable crítica en vista que ello está relacionado con el presupuesto institucional, la necesidad de disponer de personal especialista en Ciberdefensa complica la implementación de la Ciberdefensa dentro del Ejército. Asimismo, las operaciones militares en el ciberespacio son un desafío para el Ejército del Perú, en vista que es un nuevo dominio sin supremacía ni superioridad sobre las diferentes ciberamenazas. La articulación de las capacidades operativas hace necesario de poseer una doctrina acorde a los requerimientos operacionales, siendo la conclusión más importante que mientras no se disponga de un centro de ciberdefensa con óptimas capacidades operativas, las operaciones militares en el ciberespacio por parte del Ejército del Perú aun serán limitadas.

Palabras clave: capacidad militar de Ciberdefensa, operaciones militares, ciberespacio, Ciberdefensa.

Abstract

The purpose of the research is to explain the current situation of the Military Cyber Defense Capacity of the Peruvian Army, and to analyze the military operations in cyberspace carried out by the Army Cyber Defense Center, 2021. The research has a qualitative approach, of a Theoretical type - empirical, with the interpretive hermeneutical method. Non-probabilistic sampling was used using the sample: of volunteers made to six (05) Cyber defense experts. This study was carried out through an interview guide for personnel working at the Army Cyber Defense Center (CECIBER) and specialists in Cyber Defense Developing by establishing categories: Military defense capacity, military operations in cyberspace. The main results explain that in the region the military capacity of Cyber defense is being developed in different countries and in their Armies, however in the Peruvian Army the CECIBER was created with many limitations, these being technological, personal, process, not having of a technological support, is a critical variable since it is related to the institutional budget, the need to have specialized Cyber defense personnel complicates the implementation of Cyber defense within the Army. Likewise, military operations in cyberspace are a challenge for the Peruvian Army, since it is a new domain without supremacy or superiority over the different cyber threats. The articulation of operational capabilities makes it necessary to have a doctrine in accordance with operational requirements, the most important conclusion being that as long as there is no Cyber Defense center with optimal operational capabilities, military operations in cyberspace by the Army will still be limited.

Keywords: military cyber defense capabilities, military operations, cyberspace, cyberdefense.

Introducción

La Ciberdefensa es tiene por finalidad emplear sus capacidades operativas para hacer frente a ciberataques asi como defenderse de ellas, dicha capacidad permite contener y neutralizar ataques realizados contra nuestros sistemas de redes comunicaciones e informática para permitir el cumplimiento de los obejtivos establecidos, todo ello debe estar enmarcado en las normativas establecidas asi como procedimientos tácticos, operacionales, que se encuentran a cargo de los órganos ejecutores del Ministerio de Defensa. La la conducción de las operaciones tienen como responsable Comando Conjunto de las Fuerzas Armadas (CCFFAA), en base a la Resolución Ministerial N° 388-2019-DE/CCFFAA (Comando Operacionales y Comando Especiales), establece que dentro del Comando Operacional se encuentra el Comando Operacional de Ciberdefensa, asignándole como misión planear, organizar dirigir y conducir operaciones especiales conjuntas en el ciberespacio, con el fin de neutralizar ciberataques sobre nuestras fuerzas, medios de alto valor y activos críticos, asimismo la Ciberdefensa de los Activos Críticos Nacionales (ACN), están a cargo del Comando Conjunto de las FF.AA, cuando la capacidad de protección de sus operadores y/o sector responsable y de la Dirección de Inteligencia Nacional (DINI) sean sobrepasadas. Según D.S N° 007- 2019-DE (Directiva Nacional de Seguridad y Defensa para la protección de Activos Críticos) el Ministerio de Defensa es el responsable de la protección de los ACN a partir de un tercer momento, a través de CCFFAA y sus IIAA. LA Ley N° 30999 (Ley de ciberdefensa) establece claramente el objeto de la Ciberdefensa en el Perú en base a ello en el Ejército del Perú se han realizado los esfuerzos para implementar la Ciberdefensa dentro de la institución, creándose Ciberdefensa, Telemática del Ejército (CITELE) teniendo como órgano de ejecución al Centro de Ciberdefensa del Ejército (CECIBER), dentro de dicho Centro se han establecido las tres capacidades de Ciberdefensa del Ejército, respuesta, defensa, explotación, llevándose por medio de estas la ejecución de operaciones empleando para ello tareas tácticas. Asimismo, dichas capacidades tienen como pilares procesos adecuados para repuesta antes incidentes, una óptima tecnología siendo esta una deficiencia identificada en vista que la tecnología para Ciberdefensa aún no ha sido implementada, otra falencia identificada es la del personal, en vista que las operaciones demandan de personal calificado especialista con perfil profesional adecuado a los requerimientos para realizar operaciones militares de ciberdefensa.

CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema

El ciberespacio es un dominio nuevo y disruptivo para las organizaciones militares y civiles, para lo cual, la Secretaria de Gobierno Digital (SEGDI), entidad que pertenece a la Presidencia de Consejo de Ministros (PCM) y encargada de formular, establecer políticas nacionales en materia digital, conforme a lo antes mencionado la SEGDI desde el 2017 ha realizado esfuerzos para que las organizaciones estatales y privadas, tomen medidas activas en temas de seguridad digital, siendo este considerado el primer nivel de defensa en materia de seguridad digital. El estado ha identificado a través de la Dirección Nacional de Inteligencia (DINI) Activos Críticos Nacionales (ACN) siendo estos imprescindibles para mantener y desarrollar las capacidades nacionales, cuya afectación, perturbación o destrucción no permite soluciones alternativas inmediatas, generando grave perjuicio a la Nación.

En el Estado Peruano la seguridad digital en un tercer nivel, la responsabilidad recae sobre las FF. AA, para tal fin se crea El Comando Operacional de Ciberdefensa con Resolución Ministerial N° 0388-2019 DE/CCFFAA de fecha 25 de marzo del 2019, el Comando Operacional de Ciberdefensa (2019) afirma lo siguiente:

> Planea, organiza, dirige y conduce operaciones militares conjuntas de Ciberdefensa en el ciberespacio, ejerciendo el comando y control de las operaciones de Ciberdefensa, con la finalidad de defender, explorar y responder amenazas y ataques realizados en y mediante el ciberespacio, que alteren o impidan el normal funcionamiento de nuestras redes digitales, sistemas de información, telecomunicaciones, Activos Críticos Nacionales y recursos claves que afecten la Seguridad Nacional. (p. 2)

El COCID cuenta con tres comandos de Ciberdefensa (Ejército, Marina y Fuerza Aérea) entidad orgánica del Comando Conjunto de las Fuerzas Armadas (CCFFAA) y el 30 de octubre del 2018 se crea el Comando de Ciberdefensa del Ejército (COCIBER) dentro del Ejército del Perú, siendo a partir de la fecha una preocupación para el comando del Ejército establecer nuevos lineamientos en esta nueva capacidad de ámbito global, ya creados las entidades militares era de suma importancia la necesidad establecer normativas que respalden todas las operaciones militares en el ciberespacio, el 14 de octubre de 2019, se promulga la Ley N° 30999 “Ley de Ciberdefensa” sin reglamentación a la fecha. tiene por finalidad regular las operaciones militares en y mediante el ciberespacio a cargo de los

órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley.

Durante todo este tiempo, no se ha podido establecer lineamientos, así como procedimientos a seguir en los escenarios de ciberguerra, apoyo a las operaciones militares y en la protección de los ACN (Activos Críticos Nacionales) y Recursos Claves por parte de la Ciberdefensa del Ejército del Perú frente a ciberamenazas e incidentes cibernéticos, ya que de materializarse una ciberguerra, un ataque cibernético en un ACN afectaría la estabilidad de un País, determinando la vulnerabilidad como Estado frente a las ciberamenazas e incidentes cibernéticos, enfocándonos al Ejército del Perú, de no establecerse procedimientos operativos tácticos y operacionales de continuidad frente a los tres escenarios identificados, seríamos una fuerza con capacidades muy limitadas en este nuevo ámbito, ya que países de la región están fortaleciendo esta capacidad de Ciberdefensa de manera oportuna y acelerada, tratando de implementarla en su totalidad, debemos de tener cuenta que las amenazas son globales y transnacionales y el Ejército del Perú debe fortalecer los tres pilares fundamentales de la Ciberdefensa (tecnología, personas y procesos), al crear la Ciberdefensa y Telemática del Ejército (CITELE), lo ha creado de una manera limitada carente de los tres pilares anteriormente indicados, en vista que a la fecha, no posee la tecnología necesaria para hacer frente a las ciberamenazas e incidentes cibernéticos, en lo que refiere a personal no dispone de elementos especialistas, en vista que la Ciberdefensa requiere de personal altamente especialista en diferentes tecnologías con especialización continua en el tiempo, en lo que refiere a procesos no se ha establecido procesos o procedimientos operativos en escenarios de ciberguerra, apoyo a las operaciones militares ni vínculos necesarios con los ACN identificados, esta última se enfoca posturas problemáticas, la primera el Ejército del Perú no cuenta con el personal necesario para establecer los procedimientos necesarios en vista que los ACN emplean tecnología de tipo industrial, siendo esta ajena al Ejército del Perú, la segunda que los directivos que conducen a las entidades identificadas como ACN no confían la seguridad perimetral de tecnología que dispone las fuerzas militares. Asimismo, debemos establecer que el ciberespacio es un nuevo dominio como los ya existentes (tierra, mar, aire espacio).

Siendo estas algunas de las problemáticas identificadas se puede inferir que es difícil establecer una protección cibernética adecuada, acorde a la situación globalizada en lo que refiere a tecnología, por cuanto urge fortalecer los tres pilares de la Ciberdefensa en vista que Ley de Ciberdefensa establece que los órganos ejecutores del Ministerio de Defensa son los responsables de seguridad digital de los ACN.

La capacidad de Ciberdefensa no solo está relacionada en la protección de los ACN, sino también en apoyo a las operaciones militares, como se plantea en el Manual de

Operaciones ME 1-13, Ejército del Perú, “operaciones militares comprenden operaciones ofensivas que se orientan a destruir o derrotar al enemigo y las operaciones defensivas. Derrotan un ataque enemigo, ganan tiempo, economizan fuerzas o desarrollan condiciones favorables para pasar a las operaciones ofensivas” (Ejército del Perú, 2015, p. 4).

En un contexto global las fuerzas militares de varios países se encuentran conformando dependencias en el ámbito de la Ciberdefensa, tal es el caso de EE. UU a través de su cibercomando, apoyando esta entidad en las operaciones militares propias de las fuerzas norteamericanas, en diferentes regiones del mundo en un entorno ofensivo a través del empleo de ciberarmas desarrolladas por la misma entidad a medidas de sus requerimientos operacionales. Por otro lado, tenemos a Rusia conformando sus propias fuerzas en el ámbito de la ciberdefensa en apoyo a sus operaciones militares, debemos de tener en consideración que la mayoría de los ciberataques identificados han podido ser referenciados en esta parte del mundo.

China es uno de los países que más ha invertido y fortalecido su fuerza de operaciones en el ciberespacio conformando un gran ejército exclusivo para operar en este ámbito.

En América del Sur, Brasil es el país que más ha desarrollado la Ciberdefensa conformando su Escuela de Defensa Cibernética.

En el ámbito nacional el Ejército del Perú desde el año 2015 viene capacitando a personal militar en este ámbito cibernético, siendo este esfuerzo insuficiente a los grandes requerimientos que necesita una implementación óptima de la capacidad de ciberdefensa. Al no poseer una doctrina de empleo de la ciberdefensa en operaciones militares, nos limita en demasía la integración y la sincronización con otros elementos de apoyo, asimismo el empleo de la ciberdefensa no es exclusivo a un área operaciones, por lo contrario las amenazas cibernéticas llevan al empleo de la ciberdefensa a un ámbito global, requiriendo que la capacidad ofensiva de ciberdefensa se desarrolle en base a fundamentos ofensivos como la sorpresa y oportunidad, la protección de la infraestructura cibernética crítica de una fuerza sean estos (sistemas de comando y control, sistema armas, etc.) se realicen de una manera física y lógica, la exploración tenga que realizarse de una manera oportuna y segura ya que a través de esta capacidad operativa se podrá accionar de una manera ofensiva o defensiva según el ambiente operacional lo demande. Debemos de inferir que el ciberespacio es un nuevo ámbito donde también se debe maniobrar por medio de operaciones militares ofensivas, defensivas y que enfrente tenemos a un adversario anónimo e invisible y con una magnitud desconocida para nuestra fuerza. Ante la carencia de una doctrina del empleo de la ciberdefensa, nuestra fuerza se encuentra en una posición desventajosa para la realización de operaciones militares en el ciberespacio o como en apoyo a las operaciones de combate terrestres que según el Manual ME 1-13, según el Ejército del Perú (2015) “el conjunto de encuentros terrestres; decisivos, de relativa o de poca importancia para el desarrollo de la

guerra, comprende la maniobra, el apoyo de combate y el servicio de combate como un sistema" (p. 6)

infiriendo que los procedimientos de conducción y ejecución de operaciones de Ciberdefensa en base a las capacidades operativas de defensa, explotación y respuesta frente a ciberamenazas por parte del Centro de Ciberdefensa del Ejército del Perú, por cuanto resulta necesario a fin de reducir la brecha de vulnerabilidad frente a las ciberamenazas e incrementar capacidad operativa de respuesta ofensiva oportuna de acuerdo a ley.

Asimismo, debemos entender que las ciberamenazas no son direccionadas solo por adversarios civiles, sino también algunos estados que financian a organizaciones que tienen como finalidad obtener información de interés o causar un efecto de la disrupción de las capacidades de una nación, así como en las infraestructuras cibernéticas militares. Es por ello la necesidad de fortalecer los pilares de la ciberdefensa con el propósito de tener unas capacidades acordes a los requerimientos de hacer frente tanto a las ciberamenazas en el ciberespacio y estar en condiciones de hacer frente en un escenario de ciberguerra, apoyo a las operaciones militares y protección a los activos críticos nacionales.

1.2 Justificación de la investigación

La investigación responde al interés profesional del investigador por denotar la relevancia de lo que representa en la actualidad la ciberdefensa en un entorno global y como esta se vincula con nuestro entorno nacional, a fin de permitir que el instituto adopte e implemente de una manera adecuada y optima la capacidad militar de ciberdefensa.

De lo anterior se establece que la importancia del fenómeno investigado se enfatiza en la necesidad de establecer el diseño operativo en base al empleo de la Ciberdefensa frente a las nuevas amenazas en un nuevo domino denominado ciberespacio, la que se debe articular con diferentes entidades públicas como privadas, nacionales como internacionales, entendiendo que la capacidad de ciberdefensa obedece a la integración y trabajo colaborativo de capacidades inherentes a ciberdefensa como la protección, explotación y respuesta dentro de un marco normativo Ley de Ciberdefensa N° 30999 y satisfacer también las necesidades propias de la institución.

El aporte de la investigación se enfoca, en la solución al problema de determinar el diseño operativo de empleo de la capacidad militar de ciberdefensa del Ejército del Perú con las operaciones militares en el ciberespacio, que cumpla con las expectativas institucionales, así como las establecen la Ley de Ciberdefensa, además de participar en el tratamiento correcto de todos los procesos que esta propuesta de diseño en todas sus etapas en la vinculación con la capacidad de Ciberdefensa.

Esta investigación se justifica metodológicamente ya que se utilizó métodos y técnicas que servirán de guía para futuras investigaciones, cabe señalar que el tema a desarrollar no ha sido investigado por la comunidad científica en el Perú, es por ello que con este estudio se dará un aporte a la metodología en la en capacidad de ciberdefensa del Ejército del Perú.

1.3 Delimitaciones de la investigación

La presente investigación se llevó a cabo en la provincia de Lima, debido a la recopilación de información en vista que se tuvo como referencia la experiencia, observación y estudio de las operaciones de Ciberdefensa en el Ejército del Perú, por medio del CECIBER en el presente año 2021, La delimitación, la cual se llevó a cabo durante los meses de enero a diciembre del 2021.

.

1.4 Limitaciones de la investigación

Algunas restricciones se darán en el hecho de acceder al entorno de la capacidad de ciberdefensa implementado en el Ejército del Perú a través del Centro de Ciberdefensa del Ejército, donde se produce el problema a investigar, estos serán minimizados, puesto a que el investigador ha laborado en dicha dependencia en años anteriores y podrá obtener algunos permisos para ingresar al lugar señalado.

La falta de trabajos de investigación y personal con experiencia en el tema tratado, dentro de la institución, se podrá minimizar gracias al estudio de otras instituciones.

1.5 Formulación del problema

Problema 1

¿Cómo se emplea la capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio?

Problema 2

¿Cómo se relaciona la capacidad militar de ciberdefensa del Ejército del Perú en la protección de los Activos Críticos Nacionales?

Problema 3

¿Cuál es el enfoque de diseño para el empleo de la capacidad militar de ciberdefensa del Ejército del Perú en apoyo a las operaciones militares?

1.6 Objetivos de la investigación

Objetivo 1

Analizar la capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio.

Objetivo 2

Analizar la capacidad militar de ciberdefensa del Ejército del Perú en la protección de los activos críticos nacionales.

Objetivo 3

Proponer un enfoque de diseño a través de buenas prácticas para el empleo de la capacidad militar de ciberdefensa del Ejército del Perú en apoyo a las operaciones militares.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 Antecedentes nacionales

Saenz (2020) en su investigación, titulada “La ciberdefensa en el sistema de mando y control en la 9na Brigada Blindada”, cuyo objetivo es hacer conocer nuevos enfoques operacionales, siendo la tecnología, más allá de la variable tradicional, la tecnología ha modificado la forma de establecer operaciones militares influyendo en los ejércitos de un nuevo mundo. El cual concluye que los sistemas de armas de los ejércitos se orienta a una demanda hacia las tecnologías emergentes han facilitado y siguen en las operaciones militares ya sea dando soporte a las operaciones o como participación directa en las operaciones a través de operaciones militares de ofensiva o defensiva, como ya otros ejércitos han implementado esta capacidad , también representa una debilidad las vulnerabilidad la implementación lenta en vista que las amenazas seas estos hackers informáticos o ciberterroristas vienen realizando y empleando el ciberespacio como medio de sus accionar.

Emanuel (2019) en su tesis para obtener el grado de Maestro en Ciencias Militares, titulada “Capacidad de respuesta del Centro de Ciberdefensa en las operaciones y acciones militares”, señala que en nuestro país mediante la Ley de Gobierno Digital Nº 1412 que tiene por finalidad establecer el marco de gobernanza del gobierno digital, el Ejército del Perú es una de las instituciones dentro de las Fuerzas Armadas que desde el año 2018 ha implementado un Centro de Ciberdefensa (CECIBER), y existe preocupación por la institución la consolidación del CECIBER en operaciones y acciones militares, para poder brindar seguridad a la institución, así como entidades públicas y privadas que la requieran.

En sus tesis de Vilcarromero Zubiate y Vilchez Linares (2018), titulada “Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones”, establecen analizar la situación y el problema actual que el Perú presenta en materia de ciberseguridad, nos indica que el ente encargado de los protocolos de seguridad de las tecnologías de la información del estado es la oficina nacional de gobierno electrónico, y como tal se encarga de liderar los proyectos, la normatividad, y las diversas actividades que el material de gobierno electrónico realiza el Estado.

Según Vilcarromero sería la ONGE la responsable, toma también un rol importante la secretaria de gobierno digital adscrita al PCM quien da los lineamientos generales en temas digitales en el Perú.

Acuerdo Nacional

Debemos mencionar que el Acuerdo Nacional declara que la seguridad Nacional es una tarea que involucra a la sociedad en su conjunto, estrechando el vínculo existente entre nuestra Fuerzas Armadas (Marina, Ejército, Fuerza Aérea) con la Defensa y Seguridad Nacional y la sociedad en conjunto.

Plan Bicentenario 2021

En el Eje estratégico N° 03: Estado y gobernabilidad, que en Seguridad y Defensa Nacional según Ministerio de Defensa (2013) "se debe Optimizar el funcionamiento del Sistema de Seguridad y Defensa Nacional para defender los intereses permanentes del Perú" (p. 123). Las fuerzas militares deben estar en una constante optimización y modernización, por cuanto para un optima protección del ciberespacio las FF. AA deben poseer un adecuado funcionamiento alineado a os requerimientos globales para hacer frente a las amenazas. En el objetivo específico N° 04 Nos establece una acción estratégica, según el Ministerio de defensa (2013) "Involucrar a la sociedad en el Sistema de Seguridad y Defensa Nacional para enfrentar las amenazas internas y aquellas denominadas "nuevas amenazas" de tipo transnacional, como el narcoterrorismo, y otras que puedan surgir" (p. 180). Estableciendo una posible prospectiva que surjan nuevas amenazas en un nuevo ámbito, en nuestro caso sería el ciberespacio.

Políticas del Sector Defensa

Dentro de la política general del sector defensa 2017-2021 establece de disponer de capacidades militares necesarias para garantizar la independencia, soberanía e integridad territorial de la república.

Asimismo, dentro del Objetivo N° 01: disponer de capacidades militares necesarias para garantizar la independencia, soberanía e integridad territorial de la república, el planeamiento estratégico militar debe contemplar acciones en el ciberespacio de investigación, prevención, detección y respuesta que protejan las infraestructuras criticas ante ciberataques. En lo que refiere a la Plan Estratégico Sectorial Multianual (PESEM) en el Sector Defensa 2017 -2021 establece como objetivo estratégico N° 01: Garantizar la defensa nacional teniendo como acción estratégica el desarrollar la Ciberdefensa protegiendo la infraestructura crítica del estado de ciberataques.

En lo que refiere al plan estratégico institucional 2021 – 2023 como objetivo estratégico N° 05: establece desarrollar la capacidad institucional. Asimismo, en Plan de Transformación Institucional del Ejercito del Perú, establece como objetivo estratégico N° 04. El desarrollar la ciberdefensa institucional.

La II Conferencia de Ciberdefensa del hemisferio occidental, organizada por la Junta Interamericana de Defensa (JID) y la Fundación Interamericana de Defensa (FID), reunió a más de 800 líderes y autoridades del contexto militar los días 28 y 29 de septiembre del 2020 para generar oportunidades de cooperación entre los principales actores en ciberdefensa. Es importante destacar la participación de diversos sectores en la conferencia, tales como: militar, gubernamental, académico, el sector privado, y organizaciones internacionales, entre otros; con la finalidad de establecer las bases para la cooperación en ciberdefensa a corto y largo plazo. Según el Comando Conjunto (2016)" la capacidad militar que permite impedir, contener y neutralizar ataques realizados en el ciberespacio contra nuestros sistemas de redes de comunicaciones e informática; para permitir el cumplimiento de los roles estratégicos" (p. 4).

Política de Seguridad y Defensa Nacional (D.S N° 012-2017)

La cual contiene tres (03) objetivos y veintinueve (29) lineamientos, el objetivo N° 01 vinculado menciona: "conjunto de previsiones y acciones que el Estado genera y ejecuta permanentemente para garantizar la soberanía, independencia e integridad territorial, así como la protección de los intereses nacionales" dicho objetivo sería vinculante a la capacidad militar de ciberdefensa.

Estableciendo como una problemática infraestructura para enfrentar ataques a los sistemas de información: Ciberseguridad cuyo concepto según el Congreso de la República del Perú (2017) afirma:

> Las tecnologías de la información están cada vez más integradas a la operación de infraestructura física, incluida la infraestructura crítica, 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. A la luz de estos riesgos y sus potenciales consecuencias, proteger el ciberespacio y su infraestructura se convierte en un asunto de seguridad nacional. (p. 3)

Secretaria de Seguridad y Defensa Nacional (SEDENA)

SEDENA nos menciona un enfoque de seguridad definiéndolo: "como el conjunto de Previsiones y acciones que el Estado genera y ejecuta permanentemente para garantizar la soberanía, independencia, integridad territorial y la protección de los intereses nacionales" (SEDENA, 2014, p. 14).

El estudio realizado sobre seguridad nacional resulta de mucha importancia porque estos reflejarán los pilares de la ciberdefensa en el Ejército del Perú, en vista que dicha

capacidad será un actor en un escenario global donde la tecnología y el hombre, mantendrán una nueva sinergia para hacer frente a nuevas amenazas del ciberespacio.

Libro Blanco

Asimismo, en lo que refiere al Libro Blanco según el Ministerio de Defensa (2005), establece:

> Tiene como propósito esencial dar a conocer a la ciudadanía y a los países amigos, que el Perú se guía por los principios de respeto al derecho internacional, fiel cumplimiento de los tratados, solución pacífica de controversias, respeto a la soberanía de los Estados y a las fronteras internacionales, no intervención y prohibición de la amenaza o del uso de la fuerza; en concordancia con los principios de las Cartas de la OEA y de la ONU. (p. 67)

Dentro del enfoque que establece el Libro Blanco nos menciona que la seguridad es multidimensional en vista que integra multiplicidad de factores y riesgos.

En el año 2003 en la “Declaración de la seguridad para las Américas” dada en México nos vierte un enfoque multidimensional estableciendo que los “campos de la actividad humana y traspasa las fronteras de los estados, además de amenazas tradicionales y desafíos como la pobreza, corrupción, exclusión social, desastres naturales, ataque cibernético, entre otros, que fungen como factores asociados a las nuevas amenazas” (Salcedo, 2017, p. 16)

2.1.2 Antecedentes internacionales

En la investigación de Vergara Evergisto y Trama Gustavo (2017) denominada “Operaciones militares cibernéticas: planeamiento y ejecución en el nivel operacional, Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de la República de Argentina” plantea que Las acciones en el ciberespacio significan conflictos de voluntades e intereses, han surgido nuevos términos como ciberseguridad, ciberdefensa, ciberoperaciones, ciberguerra y debido a que un conflicto puede causar un gran daño igual o mayor que la de una contienda militar física. Se concluye que estas nuevas capacidades que se vienen adoptando por las fuerzas militares requieren de nuevas tecnologías y personal especialista para hacer frente a los desafíos y exigencias propias del ciberespacio como quinto dominio para ello es necesario desplegar más esfuerzo e incorporar nuevas tecnologías ello tiene una decisión estratégica para una ejecución táctica en vista que toda esta implementación requieres de un presupuesto ambicioso para que las fuerzas actúen y tengan una actitud ofensiva defensiva acorde a los requerimientos del ciberespacio y velar por la seguridad nacional.

CEEAG (2017) *d*esarrolló la investigación denominada “La Ciberguerra: sus impactos y desafíos” *determinando* que el ciberespacio es considerado como el quinto dominio, junto con lo terrestre, marítimo, aéreo y el espacio, por esta razón debe existir especial preocupación acerca del concepto de ciberguerra, que sigue los lineamientos de ser una herramienta más en una estrategia de acción. Ejemplos de sabotaje de Israel a la capacidad nuclear de Irak, espionaje de países orientales a otras potencias, son presentados como herramientas usando los medios cibernéticos. Concluyó que en los conflictos tradicionales existían área de operaciones definidas por limites e impuestas en este medio del ciberespacio ya no existe un área de operaciones definida donde pueda actuar cierta fuerza por lo contrario la tendencia de hoy, que las amenazas actúen y acciones a través de todo el ciberespacio en un entorno global sin límites, entonces un ciberataque realizado por una amenaza es difícil identificar y más aún ubicar, el principio de sorpresa y oportunidad por parte de las fuerzas de ciberdefensa se ven afectadas por que la capacidad de reacción se ven limitadas tanto en acciones propiamente como en tiempo este tipo de fenómeno es nuevo por ellos las fuerzas militares que emplean la capacidad de ciberdefensa deben estar cada día más entrenada para actuar en este nuevo dominio.

Andress Jasson y Wintelferd seteve (2011) en su investigación denominada “Cyber Warfare, Técnica, Tácticas y Herramientas para practicantes de ciberseguridad” menciona que el plan de protección propone evaluar vulnerabilidades implementando programas proactivos, mejorando los protocolos de seguridad, e implementando información en tiempo real que comparte y asistiendo con planificación de contingencia y recuperación. Las infraestructuras criticas están identificadas por el gobierno de EE.UU. son aplicables a cada país, algunos de estos más directamente a comunicaciones, transporte, departamento de defensa , la base industrial defensiva, la mayoría de canales de comunicación militar a través de circuitos comerciales, así que cualquier compromiso de la infraestructura comercial será eficazmente cortada fuera de todas las comunicaciones para las instalaciones militares, mucho soporte material el ejército requiere este entregado sobre la infraestructura comercial, así que para poder tener suministros, podría causar retrasos significativos en las operaciones. Finalmente, el departamento de defensa depende de los contratistas para todo soporte de personal de desarrollo de equipamiento y operación, si otra nación quiso saber cómo para defender contra el sistema de armas tardío o lo quiso clonar, intentarían robar información de diseño del sistema. El método tradicional seria para infiltrar un espía o compromiso a alguien que trabaja. Hoy es más fácil ingresar a los servidores que tiene la información hay dos ubicaciones para ir después de aquella información, el departamento de defensa programa que los controles el desarrollo o el contratista que diseño y lo construye. La infraestructura que habilita nuestra fuerza y nuestra debilidad.

2.2 Bases teóricas

El estudio se sustenta en la teoría basada en el empleo de la capacidad militar de ciberdefensa y su implementación en diferentes fuerzas militares y como esta capacidad emergente se viene empleando dentro del Ejército del Perú y su concepción propia de las operaciones en el ciberespacio y como está vinculada a la seguridad nacional.

Debemos tener presente que las ciberamenazas son cada vez más avanzadas, la valoración que tengamos de las diferentes amenazas es una parte importante para dar una respuesta, con medidas de seguridad acordes a través de una prevención, detección, respuesta, mitigación y recuperación, son pautas que debemos tener en cuenta para las operaciones en ciberdefensa.

Estos elementos que se han establecido en estos últimos años vienen creciendo en medida que los países se industrializan y tecnifican y directamente proporcional a la seguridad que se establece. Es por ello que muchos ejércitos han adoptado esta nueva capacidad ante una nueva amenaza y los nuevos escenarios en el cual se podrían desarrollar una ciberguerra. cuyo estudio es la base para nuestra investigación. Al respecto menciona Rexton (2014):

> El ciberespacio y la ciberguerra son los cinco debates distintos y constantes sobre este nuevo dominio y cómo actuar en el mismo, los debates incluyen quien establece los limites en el ciberespacio y cuál es la diferencia en guerra y delito en el ciberespacio. (p. 30)

Las amenazas en el ciberespacio son cada día más avanzadas y sofisticadas para realizar diferentes actividades y causar efectos sobre sus objetivos, el Instituto Español de Estudios Estratégicos (2010) nos menciona que “las características únicas de la ciberamenazas, su evolución continuada y las implicancias potenciales de un ataque, hacen que lo que se lleva años, ahora se pueda realizar en meses y hasta en días, horas” (p. 79). Podemos mencionar que la respuesta a ciberataque respondes a planes de respuesta cibernética acordes a oportunidad y procesos óptimos, las ciberarmas empleadas tanto por la capacidad de ciberdefensa como por las amenazas, han evolucionado de una exponencial debido a las vulnerabilidades propias de las plataformas tecnológicas de cada organización gubernamental o corporativa.

2.3 Categorías, Sub Categorías Apriorísticas

En este sentido el empleo de la capacidad de ciberdefensa que se ha dado en diferentes ejércitos establece conceptos cada vez más innovadores y cambiantes en vista

que el entorno es cambiante, las amenazas en el ciberespacio varían de acuerdo a las vulnerabilidades y tecnologías.

2.3.1 Capacidad Militar de Ciberdefensa

La Ley N° 30999 establece parámetros “Ciberdefensa es una capacidad de tipo militar el cual actúa frente a ciberamenazas empleando como medio el ciberespacio” (Congreso de la República de Perú, 1993, Artículo 4). Pero debemos de saber que esta ley no nació sola, que sus antecesores fueron una serie de esfuerzos, políticas, lineamientos, planes, entre otras, que dieron soporte legal para que la Ciberdefensa se encuentre enmarcada a la seguridad Nacional.

Asimismo, como obligaciones del Estado define “el estado tiene como deber primordial proteger a la población de las amenazas que afecten la seguridad” (Congreso de la República de Perú, 1993, Artículo 15).

2.3.1.1 Capacidades operativas

Procesos propiamente, denominados: la capacidad de respuesta, defensa y explotación cada una de ellas enfocadas propiamente a una misión específica, sin embargo, todas ellas se interrelacionan para poder realizar operaciones militares en el ciberespacio. La capacidad operativa que posee Ciberdefensa del Ejército se circunscribe a tres:

Capacidad respuesta

Realizar operaciones militares ofensivas en el ciberespacio de forma legítima, oportuna y proporcionada con la finalidad de tener como efecto la degradación y destrucción de infraestructuras cibernéticas del adversario en el Ciberespacio. El uso de la fuerza bajo un contexto internacional sea un mandato (ONU entre otras) teniendo en consideración las reglas de enfrentamiento. Para ello se deberá analizar la efectividad de los efectos, eficiencia, daños colaterales, y el riesgo.

El proceso de operaciones militares de respuesta a un nivel táctico, se lleva bajo la conducción del comandante del Departamento de respuesta (ofensivo), quien, apoyado en sus secciones y en coordinación con los Departamentos de Protección y Exploración, ejecutará operaciones de Ciberdefensa ofensiva.

Se inicia con la recepción de disposiciones del jefe del CECIBER en cumplimiento al orden/plan de operaciones Ciberdefensa emanadas por el escalón superior y finaliza con la misión cumplida, asignada en dicho plan/orden de operaciones.

- Respuesta oportuna
- Respuesta Legitima
- Respuesta proporcionada

Capacidad explotación

Realizar operaciones militares de explotación en el ciberespacio de forma legítima, oportuna y proporcionada. El proceso de operaciones militares de respuesta, se lleva bajo la dirección del comandante del departamento de explotación, quien, apoyado en sus secciones y en coordinación con los Departamentos de Protección, ejecuta operaciones de Ciberdefensa.

Se inicia con la recepción de disposiciones del jefe del CECIBER en cumplimiento al orden/plan de operaciones Ciberdefensa emanadas por el escalón superior y finaliza con el cumplimiento de la misión asignada en dicho plan/orden de operaciones.

- Inteligencia de ciberamenazas (OSINT)
- Alerta temprana
- Caza de amezanas (theart huntings)

Capacidad defensiva

Realizar operaciones defensivas y acciones de protección preventivas, proactivas y reactivas en el ciberespacio, para proteger los ACN asignados, así como también a la infraestructura cibernética institucional que emplean las fuerzas terrestres en el ciberespacio.

El proceso de operaciones militares de protección, se lleva bajo la conducción del comandante del Departamento de Protección, quien, apoyado en sus secciones y en coordinación con los Departamentos de Respuesta y Exploración, ejecuta operaciones de Ciberdefensa.

Se inicia con la recepción de la misión del jefe del CECIBER en cumplimiento al orden/plan de operaciones Ciberdefensa emanadas por el escalón superior y finaliza con el cumplimiento de la misión asignada en dicho plan/orden de operaciones.

Defensa preventiva

- Seguridad física
- Control de accesos
- Securización
- Análisis de vulnerabilidades
- Alertas
- Normativa
- Concienciación

Defensa Proactiva

- Auditorias
- Monitoreo de eventos
- Test pentester

Defensa reactiva

- Gestión de incidentes
- Análisis forense
- Ingeniería inversa

Tecnología Militar de Ciberdefensa

Las tecnologías en temas militares han sido fundamentales a lo largo del espectro de los diferentes conflictos en el mundo, el actor militar que ha poseído una tecnología desarrollada, casi siempre ha obtenido una ventaja sobre su adversario.

Es por ello que las fuerzas militares buscan desarrollar y adquirir tecnología para sus diferentes operaciones militares, el desarrollo de armas es un proceso constructivo del hombre y de las sociedades por defenderse y realizar actividades ofensivas si están se requieren.

dentro de su funcionamiento de los diferentes sistemas militares propio son cada vez más complejos algoritmos digitales para su operatividad y eficacia en el entorno de su objetivo.

Es por ello en actividades propias de la Ciberdefensa a tecnologías son complejas una dinámica cambiante dentro de su estructura propia, en vista que el medio de empleabilidad es el medio digital o ciberespacio, que es la congruencia de un entorno físico y digital, a ello debemos establecer que las tecnologías de conectividad, los lenguajes de programación empleados, plataformas de desarrollo, tengan una funcionabilidad automática, para la actividad propia de Ciberdefensa.

Defensiva

Las tecnologías para tareas defensivas deberán pasar por una estrategia y análisis en base a lo que se desea proteger y cuanta tecnología se pretende emplear para dicho propósito. Realizar un apreciación de Ciberdefensa empleando para ello la capacidad operativa defensiva estableciendo niveles de seguridad, nos facilite que podamos tomar las decisiones para el planeamiento y preparación y así poder implementar los diferentes componente que brinde una securización de la parte física de la infraestructura cibernética como de la lógica en dicha infraestructura y así poder proteger la data que se maneja en los

datacenter, esta tarea táctica tendrá como objetivo principal establecer una defensa del perímetro de red, empezando desde un punto externo de la infraestructura hasta llegar a los datacenter, donde se almacena la información, ambas puntos críticos deben ser protegidos frente a la conexión de redes sospechosas y ajenas.

Asimismo, se debe plantear un enfoque de protección basada en anillos establecido alrededor del datacenter, resaltando las políticas y procedimientos de una defensa red que facilite protección de la información, pasando por la defensa desde el host de datos, la capa de aplicación y finalizar con la defensa de datos, estableciendo como guía el modelo OSI convencional y las directrices planteadas en las normas ISO 27002 de TI, técnicas de seguridad.

- Defensa de datos: se refiere a determinar la seguridad de los datos almacenados de forma lógica de la infraestructura TI.

- Defensa de aplicación: establecer la seguridad en la operatividad de las aplicaciones de las plataformas del C2 dentro de la infraestructura TI.

- Defensa de host: para establecer este tipo de defensa debemos establecer un diseño basado en un sistema de pasarela ubicado en los servidores, que facilite la protección de la red interna de la infraestructura TI teniendo en previsión un servicio que pueda ser permeable a los ciberataques, un ejemplo de ello puede ser un firewall de una infraestructura.

- Defensa de red: el propósito de esta defensa es configurar la red interna y externa de la infraestructura TI, como también sus diferentes puntos de separación que establezcan conexión con otras redes de usuarios o cuando estos se encuentren fuera, antes esta situación se tomara como referencia el modelo OSI, que facilita poder aplicar capas de protección en la red, iniciando en la parte física, hasta el nivel de aplicación, lo que permitirá que se inicie una protección lógica.

Seguridad perimetral cibernética

Son todas las tecnologías de seguridad que tiene por finalidad la de dar protección ante ciberataques e intrusos de perímetro de la infraestructura cibernética de la organización. La tarea táctica consiste en proteger las redes y sus diferentes plataformas.

es una primera línea de defensa, este sistema nos permite reducir el riesgo a que se ex filtren información o realicen un ciberespionaje.

Funciones de la seguridad perimetral

La seguridad perimetral nos brinda una protección de las redes y esta tiene que cumplir cuatro funciones:

- Resistir a ciberataques externos.
- Identificar ciberataques ocurridos y dar una alerta oportuna.
- Segmentar servicios y sistemas y aislarlos en función del ciberataque producido.
- Bloquear el tráfico y filtrarlo, si este es necesario frente a los ciberataques.

Herramientas de seguridad perimetral

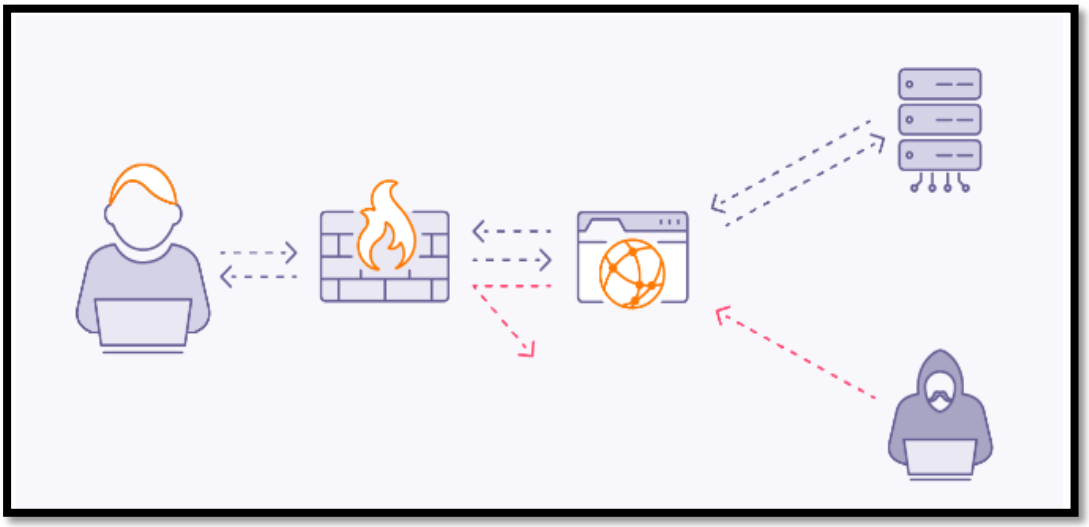
Cortafuegos

Sistema de seguridad digital que analiza el tráfico de la red. Por consiguiente, tiene como efecto mantener fuera todo el tráfico de red no autorizado y solamente permite ingresar las conexiones que son establecidas como seguras. Esta tecnología nos permite garantizar conexiones seguras al conectarse a Internet. tipos de cortafuegos:

- Cortafuego de filtrado de paquetes
- Cortafuego proxy

Figura 1

Empleo de Cortafuegos



NOTA. *Filtran el tráfico entrante de red y poder bloquear las ciberamenazas a la red amiga. De "Cortafuegos", por Avast, 2022 (https://www.avast.com/es-es/c-what-is-a-firewall)*

:

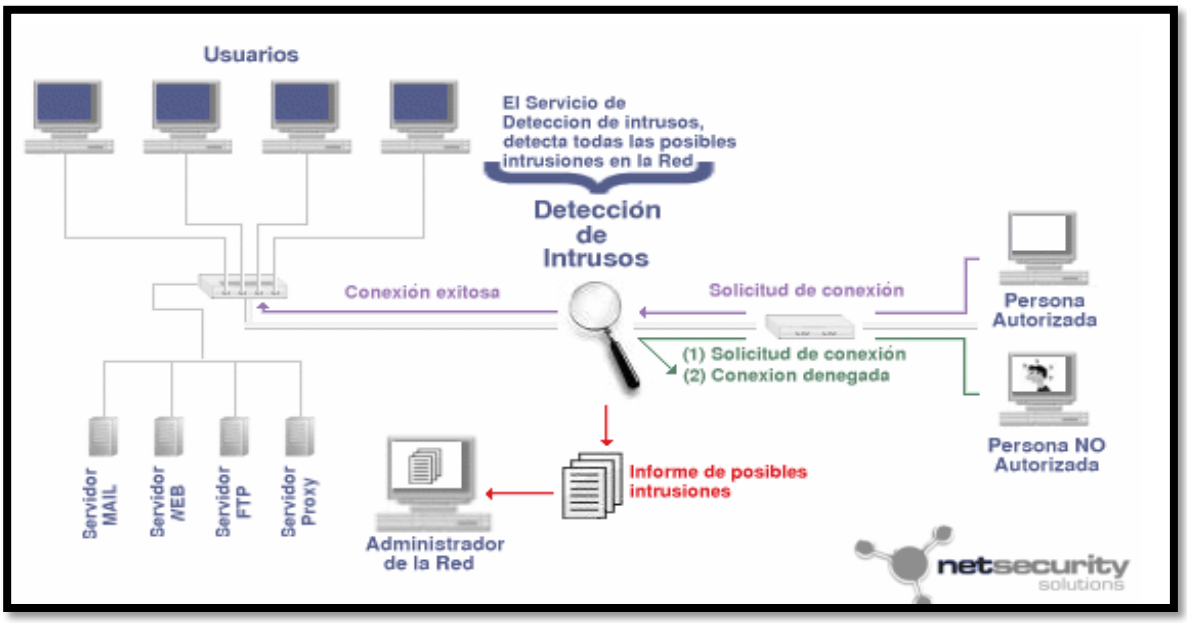
Sistemas de Detección de Intrusos

IDS permite detectar accesos no autorizados a una infraestructura de red dichos sistemas realizan actividades de monitoreo del tráfico red entrante y este permite comparar con una base de datos actualizada con firmas de ciberataques conocidas. Asimismo, ante cualquier acción sospechosa, emite alertas a los administradores de la infraestructura de red, y estos deberán tomar acciones o medidas oportunas antes estas situaciones sospechosas. Estos accesos pueden reflejar ciberataques realizados por agentes hostiles o repetidos con un rango de tiempo, también pueden ser ejecutados con sistemas automáticas. Sus acciones son reactivas. su proceso es el siguiente:

- Registro de evento
- Bloqueo de ataques
- Identificación de posible ataque

Figura 2

Sistema detección de intrusos



NOTA. Permite detectar accesos no autorizados a una infraestructura de red. De “Acceso no autorizado”, por Ecured, 2022 (https://www.ecured.cu/Archivo:Deteccion_intrusos_550x310.gif)

Honeypots

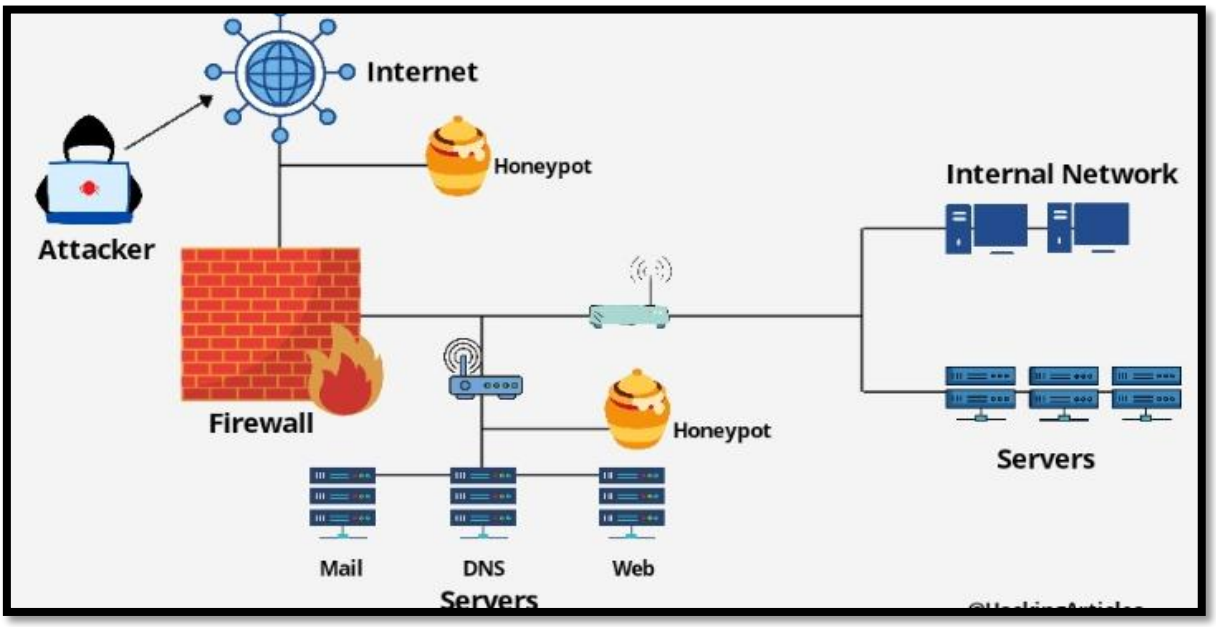
Un honeypot es un sistema conectado a la red que se configura como un señuelo para atraer a los adversarios y poder detectar, desviar e investigar los intentos de ciberataque para obtener acceso no autorizado a los sistemas de información. Los sistemas Honeypot a menudo usan sistemas operativos mejorados en los que se han tomado medidas de seguridad adicionales para reducir su exposición a las amenazas. A menudo se configuran para proporcionar a los atacantes vulnerabilidades explotables. Por ejemplo, podría parecer que un sistema que responde a las solicitudes del protocolo Bloque de mensajes del servidor (SMB) utilizado por el ataque del ransomware, WannaCry y se hace pasar por un servidor de base de datos corporativo.

Basado en su tecnología de engaño

- Honeypot para malware
- Honeypot para email
- Honeypot base de datos
- Honeypot para spam

Figura 3

Empleo de honeypots



NOTA: configura como un señuelo para atraer a los atacantes cibernéticos. De "Honeypots", por Hackingarticles, 2020 (https://www.hackingarticles.in/comprehensive-guide-on-honeypots/)

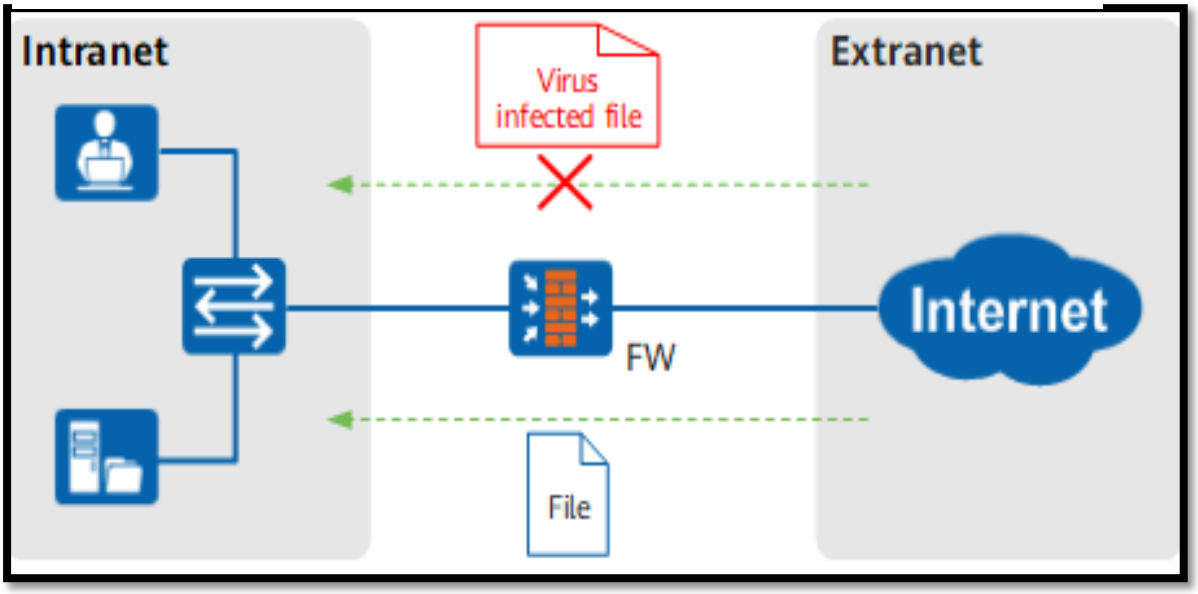
Antivirus y antispam

Estos son sistemas intermediarios que filtran contenido malicioso para que estos no puedan infiltrarse en la red de la infraestructura de la fuerza amiga. Estos malware son detectados en portales web y servidores de correo, evitando que afecte e infecte a los sistemas de la infraestructura de la organización, para poder obtener una óptima protección con estas herramientas se debe de implementar tecnología de seguridad perimetral es administrar y diseñar acorde a la organización de acuerdo a lo siguiente:

- Una topología red adecuada.
- Alternativa de soluciones eficientes.
- configuración de elementos red e Instalación que sean prioritarios.
- proporcionar soporte para el seguimiento, administración de la red.

Figura 4

Escenario de aplicación de Antivirus



NOTA: La función antivirus es proteger la red y los datos del sistema. De “Antivirus”, por Huawei, 2022 (https://forum.huawei.com/enterprise/es/modulo-contenido-de-seguridad-la-funci%C3%B3n-antivirus-para-un-firewall-serie-usg6000e/thread/671009-100233)

Seguridad perimetral empleando SIEM

La seguridad se ha configurado como prioridad y responsabilidad dentro de las organizaciones orientadas a tecnología y aún más en las organizaciones militares.
La necesidad de depender de tecnologías y emplear el internet para realizar actividades propias de los procesos militares durante las operaciones, como sistema encriptados, aplicaciones cloud y almacenamiento en la nube, hace que exista un riesgo en las infraestructuras cibernéticas de las organizaciones militares frente a ataques externos.

Sistema Security Information and Event Management SIEM

Es un sistema de seguridad que busca que las diferentes organizaciones obtengan una respuesta oportuna para poder detectar de manera eficiente y poder responder ante cual ciberamenaza o incidente informático sobre las infraestructuras cibernéticas.

Los SIEM poseen un dominio sobre lo eventos dentro de una plataforma, dichos eventos sedan dentro de una organización, este nos brinda un control para poder detectar

alguna tendencia o patrón y así poder actuar de forma oportuna frente a estos eventos. SIEM es la una tecnología que ha evolucionado dentro de los sistemas de seguridad tecnológicos.

Los SIEM están estructurados para elevar y empoderar los niveles de seguridad de las diferentes organizaciones dentro de ellas de las organizaciones militares.

Funciones de un SIEM

La función de los SIEM es la de almacenar los diferentes registros y analizar, estos diferentes procesos se realizan en tiempo real lo que permite tener visión clara frente a una reacción oportuna, lo que permite estar alerta ante cualquier incidente cibernético en impedir cualquier intromisión y dar solución a los incidentes relacionados a seguridad informática.

Los SIEM almacenan de manera centralizada en una base de datos y así poder analizar de manera exhaustiva y poder identificar patrones y futuros tendencias de comportamientos anómalos.

Las características que poseen los sistemas SIEM implementadas para seguridad y respuesta oportuna dentro de la infraestructura cibernéticas del Ejercito son:

- Identificar ciberamenazas reales, falsos incidentes.
- Monitorear centralizadamente ciberamenazas potenciales.
- Reorientar la actividad del personal especialista para dar solución.
- Otorgar conocimiento en incidentes informáticos y su resolución.
- Documentar los diferentes procesos de seguridad informática detección, actuación y resolución.

Los SIEM son una tecnología orientada a la seguridad informática la cual no permite que las infraestructuras cibernéticas de una organización militar estén protegidas de manera oportuna de cualquier ciberamenaza externo e interno. Con el empleo de los SIEM el CECIBER estará en condiciones para responder de forma manera cualquier ciberamenaza sobre sus infraestructuras TI, garantizando que el incidente tendrá una resolución oportuna en el tiempo,

Los SIEM como tecnología de la Ciberdefensa evita o minimiza los efectos de un ciberataque y realizan una evaluación continua de las infraestructuras de la red militar en tiempo real y un escaneo continuo, un monitoreo pasivo, inventariado de activos y gestión de software. Lo que permite identificar vulnerabilidades, comportamientos anómalos y permitir acciones en tiempo real e impedir que se realice un ciberataque o incidente informático
Si el problema ocurre, será detectado de forma oportuna para solucionar y analizar los efectos ocasionados.

. SIEM focaliza la respuesta rápida en base a un monitoreo en tiempo real de los diferentes procesos identificando comportamientos anómalos, Para obtener la respuesta en tiempo real se debe de automatizar diferentes procesos tales escaneos, monitoreo o alertas generadas.

SIEM como base de conocimiento

SIEM es su registro y documentación constante de incidentes, actividades y medidas. Tomando como referencia la base de conocimiento unificada que sirve para dar solución a futuros incidentes de forma mucho más eficiente y oportuna

SIEM toma como referencia la automatización de procesos facilitando la optimización del personal dentro de la organización. no teniendo que realizar actividades repetitivas de monitoreo, escaneo y otros, que son automatizadas de forma inteligente por el SIEM.
Un SIEM otorga una gestión de los recursos orientados a seguridad lo que aporta en una economía de medios y presupuesto de la organización

Herramientas SIEM más utilizadas

Dentro de los diferentes sistemas basados en seguridad tenemos diferentes tecnologías teniendo como variables el tiempo identificación y de respuesta oportuna, tenemos los siguientes:

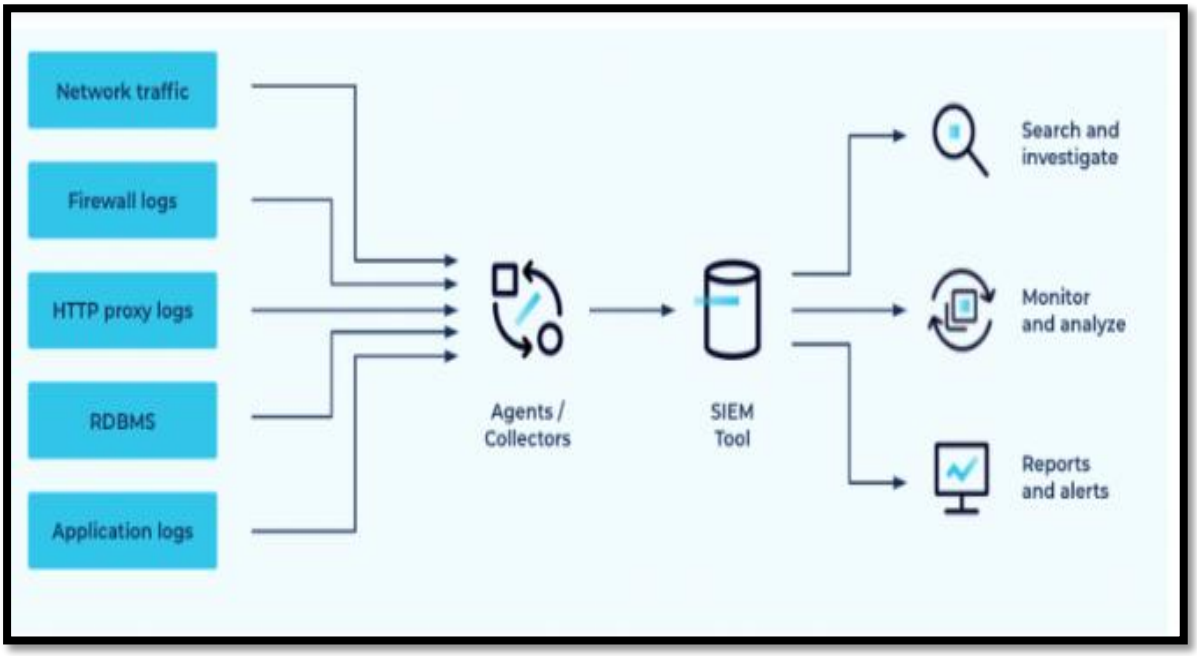
- IBM Security QRadar. capaces de soportar grandes cargas, que pueden manejar millones de eventos por día.

- McAfee Enterprise Security Manager. SIEM permite monitorear sistemas para recopilar, analizar y comparar incidentes de seguridad con una gran base de datos de registros y así detectar amenazas inteligentes.

- LogRhythm. Esta es una solución SIEM dirigida a organizaciones más pequeñas que no pueden permitirse herramientas más avanzadas.

Figura 5

Empleo de un SIEM



NOTA: Arquitectura de una plataforma SIEM. De “SIEM”, por “Confluent”, 2021 (https://www.confluent.io/blog/siem-optimization-for-better-cyber-security/)

Seguridad empleando WAF

Firewall para aplicaciones web que protege aplicaciones web de ciberataques y bots que normalmente afectan las infraestructuras TI de las organizaciones, dichos ataques ponen en riesgo la seguridad. A través del WAF se puede tener el control del tráfico sobre las aplicaciones, permite establecer reglas de seguridad que controlan el tráfico de bots, cabe mencionar a través del WAF se pueden bloquear diferentes patrones de ciberataques, tales como SQL injections o scripting en web. Asimismo, se puede establecer reglas que filtran patrones de tráfico específicos. un preconfigurado de reglas de las WAF que nos permite identificar dentro de ello los 10 riesgos de seguridad principales de OWASP y los bots automatizados que consumen recursos en exceso, las reglas se actualizan constantemente en base a una programación establecida a medida que surgen nuevos problemas. Un firewall establece una protección de diferentes ciberataques al servidor de aplicaciones web llamado backend.

WAF es monitorear, bloquear o limitar la velocidad de los bots

WAF Bot Control, establece un monitoreo de tráfico bots, en la consola WAF, se puede monitorear bots comunes, como monitores de estado y motores de búsqueda, a través de escáneres y rastreadores, también podemos implementar reglas administradas de Bot Control con diferentes WAF que se pueda disponer eso dependerá de la tecnología que dispongamos en la organización.

Protección oportuna ante ataques en la web

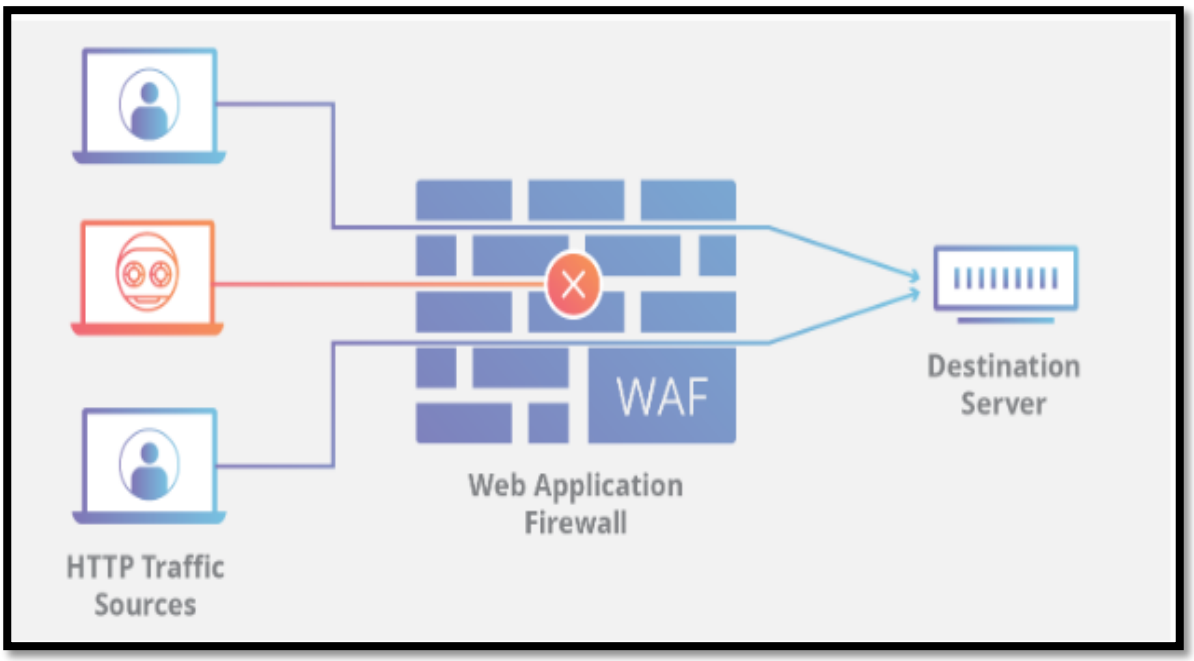
Una variable importante son las actualizaciones de las reglas de WAF, lo que permite actualizar rápidamente la seguridad cuando se identifican incidentes sobre la infraestructura. Los WAF también protege las aplicaciones web de los diferentes ciberataques a través del filtrado del tráfico con referencias a las reglas que se establezcan.

A través de los WAF podemos filtrar diferentes partes de la solicitud web, tales como IP V4 y IP V6, encabezados HTTP, cuerpo HTTP o cadenas de URI. Lo cual nos facilita neutralizar los diferentes patrones y ciberataques más comunes del medio, ataques a base de datos de inyección SQL o ejecución de Scripts. El WAF analizan las diferentes peticiones que se envían al servidor.

Las seguridades de las aplicaciones web también están orientadas en la nube. Configurado por medio de un proxy inverso, los WAF monitorean e identifican todo el tráfico orientado hacia la aplicación web la cual bloquea cualquier tráfico sospechoso y malintencionado. La solución está configurada para los POPs y así poder asegurar una latencia mínima y una cobertura máxima. Una vez protegida, su aplicación web sólo aceptará tráfico de nodos WAF.

Figura 6

Empleo o de una Web Aplication firewall



NOTA. Arquitectura de una WAF, De "WAF", por Cloudflare, 2021(https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/)

Seguridad empleando ANTI - DDOS

Los DDoS Ataque de denegación de servicio distribuido consisten en actividades maliciosas con la finalidad de irrumpir el tráfico de un servidor, servicio, red con el objetivo saturar la infraestructura con una intensidad de tráfico de Internet.

Los tipos de ataques DDoS se pueden dar:

Ataques a la capa de red

Este tipo de ciberataque se dan con la amplificación UDP, como los ataques de saturación NTP. Estos ataques envían una intensidad de tráfico a una red. Esta cantidad volumétrica de tráfico satura la red y la congestiona.

Ataques a la capa de transporte

Consiste que estos ciberataques tienen como propósito la inundación SYN y los ciberataques de inundación de conexión se incluyen en esta categoría. Estos ciberataques

consumen los diferentes recursos de las diferentes conexiones de un servidor para lograr la disrupción de servicio (DoS).

Ataques a la capa de sesión

Estos ciberataques consumen los recursos de sesión SSL de un servidor para lograr la denegación de los servicios.

Ataques a la capa de aplicación

Ataques que están dirigidos a la capa de aplicación incluyen la saturación de DNS e inundación de HTTP. Estos ataques usan los recursos de procesamiento de aplicaciones y utilizan los diferentes recursos de procesamiento de un servidor para lograr denegación de servicio.

Una solución anti-DDoS tiene los siguientes procesos: filtración, análisis, detección y desviación,

SERVICIO ANTI-DDOS

Identificar el tráfico que estaría alertando un ciberataque del tipo DDoS. La Una sistema anti-DDoS establece una detección eficiente, debe estar en condiciones de reconocer un ciberataque de manera oportuna en el tiempo que permita una reacción, descartando falsos positivos.

Asimismo, orientar el tráfico a su descarte, ya sea para neutralizarlo o filtrarlo. Al realizar la actividad de filtrar, buscamos como efecto queremos neutralizar el ciberataque de tipo DDoS como también poderlo identificar como malicioso. Una sistema anti-DDoS eficiente no afectaría a los usuarios legítimos de cada organización.

Debemos tener en cuenta que el análisis consiste en la evaluación de los registros de tráfico y poder realizar optima recopilación sobre los ciberataques y su respectiva información, como también poder identificar al agente hostil y poder mejorar las acciones de futuros ciberataques referente a este vector de ataque.

Una solución anti-DDoS orientada a la nube normalmente brinda una capacidad de red en terabits por segundo. Establece más de lo que requiere cualquier sitio web.

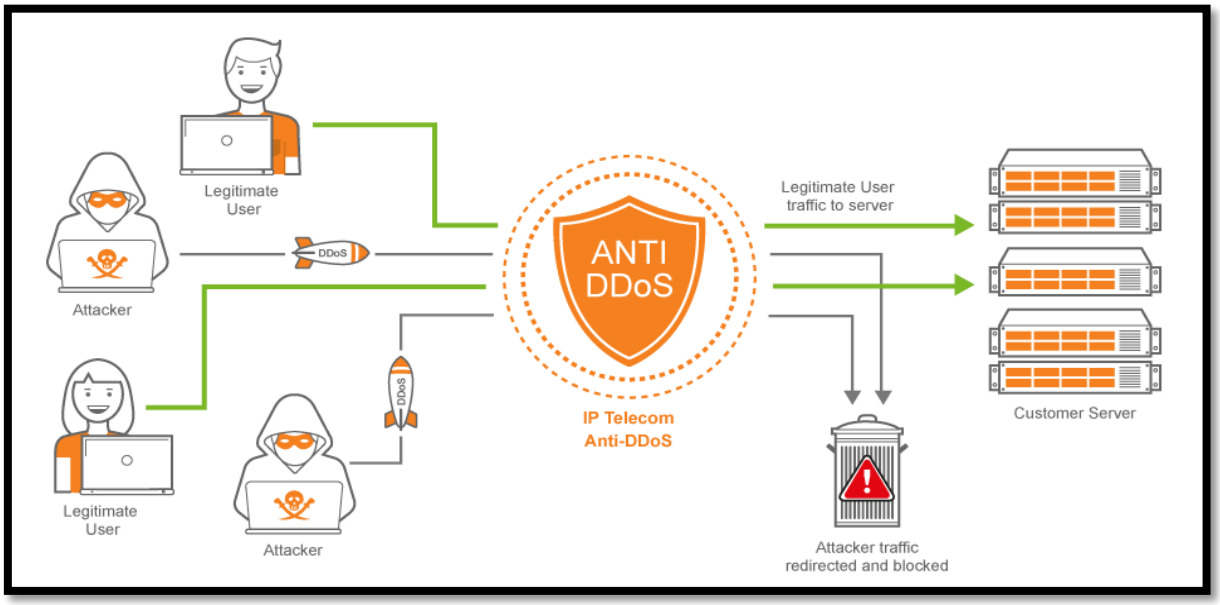
Una de las consideraciones a tener a nivel de servicio, es la cantidad de envío y entrega. Los ciberataques suelen alcanzar de 300 a 500 Gbit/s, y otros ciberataques alcanzan

1 Tbit/s. La capacidad de procesar de una tecnología anti-DDoS debe superar todo ello, para ser efectiva.

La mitigación dependerá de acuerdo al método que emplee la tecnología para identificar un ciberataque. Una solución activa constantemente y con una detección preventiva debe brindar mitigación casi instantánea. Pero esta situación deberá darse en un escenario de condiciones de la vida real.

Figura 7

Empleo de un anti DDOS



NOTA: Arquitectura de un AntiDDOS protege de los ataques volumetricos. de “Antiddos”, por Iptelecom, 2020 (http://www.iptelecom.asia/index.php/ddos-attack-protection/)

2.3.1.2.2 Ofensiva. Las operaciones ofensivas se basan Acciones realizadas en el ciberespacio para degradar, interrumpir, denegar o destruir sistema de comando y control sistemas de armas, comunicaciones, sistemas industriales (SCADA), sistemas ciberarmas del adversario.

Para ello se emplean una serie de capacidades tecnológicas ofensivas o denominadas también ciberarmas y habilidades propias de los operadores cibernéticos.

Tecnologías ofensivas

Las infraestructuras cibernéticas han ido evolucionando en el tiempo, simultáneamente los agentes hostiles (estados, organizaciones, hackers) buscan identificar

vulnerabilidades y para ello realizan muchas acciones ofensivas con la finalidad de causar algún efecto sobre la infraestructura de la fuerza amiga, así pues, ante acciones del adversario. La fuerza amiga debe realizar múltiples acciones ofensivas enmarcadas en la Ley de Ciberdefensa.

Tenemos las siguientes plataformas ofensivas:

Kali Linux. Es una distribución de Linux basada en debían de código abierto destinada a pruebas de penetración avanzadas, cuenta con más de 600 herramientas**.**

BlackArch. Es una distribución basada en arch linux diseñada para investigadores, cuenta con 3000 herramientas lo cual permite realizar diferentes operaciones de respuesta ofensiva.

Parrot security. Distribución de Linux basada en Debian utilizado dentro del mundo de la ciberseguridad y análisis forense, además de la comunidad de los Hackers y Crackers.

Sin embargo, para operaciones ofensivas, el operador puede desarrollar sus distribuciones a la medida de sus requerimientos implementado dentro de dichas distribuciones diferentes herramientas opensource y/o licenciadas

Herramientas opensource

Son aquellas que son libres y que pueden ser manipuladas, modificadas con la finalidad de explotar vulnerabilidades sobre sus objetivos, dichas herramientas opensource pueden ser desarrolladas a través de diferentes scripts empleando para ellos lenguajes de programación tales como PHP, Python, Javascript, C#, C++, entre otras, asimismo el empleo de inteligencia artificial permite que los ataques cibernéticos sean más avanzados y persistentes, por cuanto los operadores que realizan operaciones ofensivas deben de tener esa destreza de emplear dichas herramientas, configurarlas de acuerdo a sus requerimientos, existen una cantidad innumerable de herramientas para poder ser empleadas en diferentes repositorios tales como github o disponibles también en la darkweb.

Técnicas ofensivas

Para operaciones ofensivas sobre objetivos concretos (infraestructuras TI, Sistemas C2, Sistemas de armas, etc.) se establece las siguientes:

- **Reconocimiento**

  Consiste en una técnica que se estructura en la recopilación de información de los objetivos sea esta de forma pasiva o activa y a través de ella establecer la mejor selección de objetivos. Dentro de la información obtenida indica detalles de la infraestructura TI de las organizaciones o de los sistemas de armas, comando u control etc., a través del reconocimiento se obtiene información que puede ser utilizada en las diferentes fases de las operaciones ofensivas como para realizar el acceso inicial o para poder determinar objetivos y realizar posteriores compromisos.

- **Desarrollo de recursos**

  A través del desarrollo de recursos se tiene como finalidad el de ser usadas como apoyo a las operaciones en las diferentes fases, esta técnica consiste en que también se pueda crear, comprar, comprometer y ser soporte para la selección de objetivos, estos recursos pueden ser infraestructuras emergentes, diversas cuentas como también capacidades, a través de estos recursos podemos emplearla en otras fases, como adquirir diversos dominios para poder establecer el C2, cuentas para realizar un pishing como primer paso del acceso inicial así como comprometer certificados de firma.

- **Acceso inicial**

  Esta técnica consiste en emplear diferentes vectores de ataque para poder obtener un punto de inicio de una red, las técnicas normalmente son el phishing dirigidos, así como poder explotar las debilidades de servidores web públicos, estos puntos de acceso inicial pueden establecer un acceso continuo a través de cuentas operativas, servicios remotos externos.

- **Ejecución**

  Esta técnica consiste en la ejecución de código malicioso que tiene como objeto un código controlado desde un entorno local o remoto, la ejecución de códigos malicioso implica la aplicación combinada de diferentes técnicas para poder objetivos amplificados que permita explorar una red y exfiltrar datos, un ejemplo claro es el de emplear a través de herramientas remotas que permitan el acceso ejecutar scripts de powershell y poder obtener un control remoto del sistema.

- **Persistencia**

  Esta técnica radica en mantener nuestro punto de apoyo que obtuvimos a través de nuestro acceso inicial, ante reinicios que se den a los sistemas, cambios de credenciales y las diversas disrupciones que puedan interferir en el acceso, para poder mantener la persistencia se pueden emplear las técnicas de cambios de acceso, así como configuraciones en los sistemas que permita la persistencia a través del punto de apoyo obtenido, reemplazar código o establecer código de inicio

- **Escalada de privilegios**

  Consiste en establecer que se pueda obtener permisos del más alto nivel dentro de los sistemas y red comprometidas. Los operadores pueden accesar y explorar una red sin privilegios en su acceso, pero estas necesitan de permisos elevados y poder cumplir con sus objetivos. Un punto importante es aprovechar las vulnerabilidades del sistema, las configuraciones incorrectas. Ejemplos de acceso elevado incluyen poder tener permisos como nivel raí, administrador local, cuenta con acceso de administrador

- **Evasión de defensa**

  Se busca no ser detectado. esta técnica se para evitar la detección en el compromiso de los sistemas, Las técnicas utilizadas pueden ser la desinstalación/desactivación del software de seguridad, ofuscación de datos y secuencias de comandos. Los también se busca ocultar y camuflar los malware.

- **Acceso a credenciales**

  Obtener cuenta y contraseñas de diferentes sistemas. para obtener credenciales se realizan a través de registro de teclas o el volcado de credenciales.

- **Descubrimiento**

  técnica para poder establecer nuestro ambiente operacional dentro de los sistemas. Asimismo, y poder establecer que entorno dentro de la red o sistemas se pueden controlar y establecer como beneficia a la ofensiva.

- **Movimiento lateral**

  Consiste en una técnica que tiene por objeto ingresar y controlar sistema remoto en una red determinada, su objeto fundamental es explorar el entorno comprometido para encontrar su objetivo para ello debe de pasar por diferentes sistemas de red, cuentas, para la acción ofensiva se pueden emplear diferentes soluciones de acceso remoto y poder obtener el movimiento lateral o también operar con credenciales legítimas y se pueda llevar de manera más sigilosa.

- **Recopilación**

  La técnica de recopilación de información y las fuentes son importantes para cumplir con los objetivos Con frecuencia, el recopilar datos es extraer (exfiltrar) los datos. Las fuentes normalmente son navegadores, audio, video, correo electrónico, la recopilación incluye capturas de pantalla y entrada de teclado.

- **Comando y control**

  Es una técnica que se usa para enlazarse con los sistemas y establecer un control dentro de la red comprometida. Normalmente se usa el tráfico normal esperado para evitar la detección. todo dependerá de la infraestructura de la red y las defensas de la infraestructura atacadas

- **Exfiltración**

  técnicas en la cual se puede usar para extraer datos de su red. Extraído los datos los normalmente se empaquetan con la finalidad de ser detectados. Pueden llevarse a través de compresión y encriptación. Las transferencias se realizan a través de su enlace de C2, influye también los límites de tamaño en la transmisión.

- **Impacto**

  La técnica de impacto incluye los efectos de la destrucción o manipulación de datos, el flujo de trabajo se ve bien, pero es posible que se haya cambiado para ayudar a la causa. Los adversarios pueden usar estos métodos para lograr sus objetivos finales o para ocultar violaciones de privacidad.

técnicas preparatorias

- **Reconocimiento**

  Escaneo activo

  Los atacantes pueden realizar escaneos de reconocimiento activos con la finalidad de recopilar información para ser usado durante la selección de objetivos. El escaneo activo es donde los adversarios analizan la estructura de la víctima a través de la red,

  La información de estos escaneos puede revelar oportunidades para otras formas de reconocimiento (sitios web, dominios y bases de datos técnicas abiertas), establecer recursos operativos (desarrollar capacidades y obtener capacidades) y/o acceso (servicios remotos externos o aprovechar la aplicación pública).

  Escaneo activo: escaneo de bloques IP

  Se puede escanear bloques de IP para recopilar información de la red de la víctima, así como información más detallada sobre los hosts asignados a estas direcciones. Los escaneos pueden variar desde simples pings (solicitudes y respuestas ICMP) hasta escaneos más matizados que pueden revelar versiones/software del host a través de banners de servidor u otros artefactos de red. La información de estos escaneos puede revelar oportunidades para otras formas de reconocimiento (buscar sitios web, dominios abiertos y buscar bases de datos técnicas abiertas), establecer recursos operativos (desarrollar capacidades y obtener capacidades) y/o acceso inicial (servicios remotos externos).

  Escaneo activo: Escaneo de vulnerabilidades

  Los escaneos de vulnerabilidad identifican si la configuración de un host/aplicación de destino es vulnerable al objetivo de un exploit que el atacante puede usar.

  Estos escaneos también pueden incluir intentos más amplios de obtención de información del host víctima que se puede usar para identificar vulnerabilidades explotables más conocidas. Los escaneos de vulnerabilidades generalmente recolectan software en ejecución y números de versión a través de banners de servidor, puertos de escucha u otros artefactos de red. La información de estos escaneos puede revelar oportunidades para otras formas de reconocimiento (p. ej., Buscar sitios web/dominios abiertos o Buscar bases de datos técnicas abiertas),

establecer recursos operativos (desarrollar capacidades y obtener capacidades) y/o acceso inicial (aprovechar la aplicación orientada al público).

Escaneo activo. Escaneo listo de palabras

Los adversarios pueden usar herramientas de descubrimiento de contenido web como Dirb, DirBuster y GoBuster y listas de palabras genéricas o personalizadas para enumerar las páginas y los directorios de un sitio web. Esto puede ayudarlos a descubrir páginas antiguas y vulnerables o portales administrativos ocultos que podrían convertirse en el objetivo de otras operaciones (aprovechar la aplicación pública o la fuerza bruta).

Recopilar información sobre el anfitrión de la víctima

Los adversarios pueden obtener información de varias maneras, como acciones de recopilación directa a través de escaneo activo o Phishing. también puede comprometer los sitios e incluir contenido malicioso diseñado para recopilar información del host de los visitantes. La información sobre los anfitriones también puede estar expuesta a los adversarios a través de conjuntos de datos accesibles en línea u otros (por ejemplo, redes sociales o sitios web propiedad de víctimas de búsqueda). La recopilación de esta información puede revelar oportunidades para otras formas de reconocimiento (buscar sitios web/dominios, base de datos), establecer recursos operativos (desarrollar capacidades y obtener capacidades) y/o acceso inicial desde servicios remotos externos.

Recopilar información de identidad de la víctima

Los atacantes pueden obtener esta información de varias maneras, como la obtención directa a través de Phishing para Información. La información sobre los usuarios también podría enumerarse a través de otros medios activos (es decir, escaneo activo), como sondear y analizar las respuestas de los servicios de autenticación que pueden revelar nombres de usuario válidos en un sistema. La información sobre las víctimas también puede estar expuesta a los adversarios a través de conjuntos de datos accesibles en línea u otros (por ejemplo, redes sociales).

La recopilación de esta información puede revelar oportunidades para otras formas de reconocimiento (p. ej., búsqueda de sitios web/dominios abiertos o suplantación de

identidad para obtener información), establecimiento de recursos operativos (cuentas comprometidas) y/o acceso inicial (suplantación de identidad o cuentas válidas).

Recopilar información de la red de víctimas

Los atacantes pueden obtener esta información de varias maneras, como acciones de recopilación directa a través de Active Scanning o Phishing for Information . La información sobre las redes también puede estar expuesta a los adversarios a través de conjuntos de datos accesibles en línea u otros (buscar bases de datos técnicas abiertas). La recopilación de esta información puede revelar oportunidades para otras formas de reconocimiento (escaneo activo o búsqueda de sitios web/dominios abiertos), establecimiento de recursos operativos (p. ej., adquisición de infraestructura o compromiso de infraestructura) y/o acceso (por ejemplo: relación de confianza).

Recopilar información de la organización de la víctima

Los atacantes pueden obtener esta información de varias maneras, como la obtención directa a través de Phishing for Information. La información sobre una organización también puede estar expuesta a adversarios a través de conjuntos de datos en línea u otros accesibles (por ejemplo, redes sociales o sitios web propiedad de víctimas de búsqueda). La recopilación de esta información puede revelar oportunidades para otras formas de reconocimiento (phishing para obtener información o buscar sitios web/dominios abiertos), establecer recursos operativos (establecer cuentas o cuentas comprometidas) y/o acceso inicial (suplantación de identidad o relación de confianza).

Phishing para obtener información

Todas las formas de phishing son ingeniería social entregada electrónicamente. Los adversarios también pueden tratar de obtener información directamente a través del intercambio de correos electrónicos, mensajes instantáneos u otros medios de conversación electrónica. El phishing para obtener información implica con frecuencia técnicas de ingeniería social, como hacerse pasar por una fuente con un motivo para recopilar información (por ejemplo, establecer cuentas o comprometer cuentas) y/o enviar múltiples, mensajes aparentemente urgentes.

Buscar fuentes cerradas

Los atacantes buscan recopilar información de las víctimas de fuentes cerradas La información de las víctimas se puede adquirir a través de la compra en fuentes y bases

de datos privadas acreditadas, como suscripciones pagas a fuentes de datos de inteligencia técnica/amenazas. Los adversarios también pueden comprar información de fuentes de menor reputación, como la web oscura o los mercados negros de ciberdelincuencia.

Los adversarios pueden buscar en diferentes bases de datos cerradas según la información que busquen recopilar. La información de estas fuentes puede revelar oportunidades para otras formas de reconocimiento (phishing para obtener información o buscar sitios web/dominios abiertos), establecer recursos operativos (desarrollar capacidades u obtener capacidades) y/o acceso inicial (servicios remotos externos o cuentas válidas).

Buscar bases de datos técnicas abiertas

Los adversarios pueden buscar en las bases de datos técnicas que se puede utilizar durante la selección. La información de las víctimas puede estar disponible en bases de datos y repositorios en línea, como registros de dominios/certificados, así como colecciones públicas de datos/artefactos de red recopilados a partir del tráfico y/o escaneos. Los adversarios pueden buscar en diferentes bases de datos abiertas según la información que busquen recopilar. La información de estas fuentes puede revelar oportunidades para otras formas de reconocimiento (phishing para obtener información o buscar sitios web/dominios abiertos), establecer recursos operativos (adquirir infraestructura o comprometer infraestructura) y/o acceso inicial (servicios remotos externos o relación de confianza).

Buscar sitios web/dominios abiertos

Los atacantes pueden buscar en diferentes sitios en línea según la información que buscan recopilar. La información de estas fuentes puede revelar oportunidades para otras formas de reconocimiento (phishing para obtener información o buscar bases de datos técnicas abiertas), establecer recursos operativos (establecer cuentas o cuentas comprometidas) y/o acceso inicial (servicios remotos externos o suplantación de identidad).

Buscar sitios web propiedad de las víctimas

Los atacantes buscan sitios web propiedad de las víctimas para recopilar información procesable. La información de estas fuentes puede revelar oportunidades para otras

formas de reconocimiento (phishing para obtener información o buscar bases de datos técnicas abiertas), establecer recursos operativos (establecer cuentas o cuentas comprometidas) y/o acceso inicial (relación de confianza o suplantación de identidad).

- **Desarrollo de recursos**

Adquirir Infraestructura

El uso de estas soluciones de infraestructura permite que un adversario escenifique, lance y ejecute una operación. Las soluciones pueden ayudar a que las operaciones adversarias se mezclen con el tráfico que se considera normal, como el contacto con servicios web de terceros. Dependiendo de la implementación, los adversarios pueden usar una infraestructura sean estos servidores físicos, nube, dominios, servicios web de terceros, botnets, así como utilizar una infraestructura que se puede aprovisionar, modificar y cerrar rápidamente a través del alquiler o comprar.

Cuentas de compromiso

Existe una variedad de métodos para comprometer las cuentas, como la recopilación de credenciales a través de Phishing for Information, la compra de credenciales de sitios de terceros o la fuerza bruta de las credenciales (por ejemplo, la reutilización de contraseñas de volcados de credenciales de incumplimiento). Antes de comprometer las cuentas, los adversarios pueden realizar Reconocimiento para informar las decisiones sobre qué cuentas comprometer para promover su operación. Las personas pueden existir en un solo sitio o en varios sitios (por ejemplo, Facebook, LinkedIn, Twitter, Google, etc.). Las cuentas comprometidas pueden requerir un desarrollo adicional, esto podría incluir completar o modificar la información del perfil, desarrollar aún más las redes sociales o incorporar fotos. Los adversarios pueden aprovechar directamente las cuentas de correo electrónico comprometidas para Phishing.

Infraestructura comprometida

El uso de una infraestructura comprometida permite que un adversario escenifique, lance y ejecute una operación. La infraestructura comprometida puede ayudar a que las operaciones adversarias se mezclen con el tráfico que se considera normal, como el contacto con sitios confiables o de alta reputación. Por ejemplo, los adversarios pueden aprovechar la infraestructura comprometida (potencialmente también junto

con los certificados digitales) para integrarse aún más y respaldar la recopilación de información por etapas y/o las campañas de phishing.

Desarrollar capacidades

Se pueden requerir diferentes conjuntos de habilidades para desarrollar capacidades de acuerdo a la selección de los objetivos. Las habilidades necesarias pueden ubicarse internamente o pueden necesitar ser subcontratadas. El uso de un contratista puede considerarse una extensión de las capacidades de desarrollo de ese adversario, siempre que el adversario desempeñe un papel en la configuración de los requisitos y mantenga un grado de exclusividad de la capacidad.

Capacidades de desarrollo: Malware

La creación de software malicioso puede incluir el desarrollo de malware, payloads, droppers, herramientas posteriores al compromiso, backdoors Al igual que con los esfuerzos de desarrollo legítimos, es posible que se requieran diferentes conjuntos de habilidades para desarrollar malware. Las habilidades necesarias pueden ubicarse internamente o pueden necesitar ser subcontratadas. El uso de un contratista puede considerarse una extensión de las capacidades de desarrollo de malware de ese adversario, siempre que el adversario desempeñe un papel en la configuración de los requisitos y mantenga un grado de exclusividad para el malware. Algunos aspectos del desarrollo de malware, como el desarrollo del protocolo C2, pueden requerir que los adversarios obtengan infraestructura adicional. Por ejemplo, el malware desarrollado que se comunicará con Twitter para C2 puede requerir el uso de servicios web. Al utilizar una infraestructura comprometida, los adversarios pueden dificultar vincular sus acciones con ellos. Antes de apuntar, los atacantes pueden comprometer la infraestructura de otros adversarios.

Establecer cuentas

Los atacantes pueden crear cuentas que se pueden usar para crear una identidad para otras operaciones. Estas personas pueden ser ficticias o hacerse pasar por personas reales. La persona puede existir en un solo sitio o en varios sitios (por ejemplo, Facebook, LinkedIn, Twitter, Google, GitHub, Docker Hub, etc.). Establecer una persona puede requerir el desarrollo de documentación adicional para que parezca real. Esto podría incluir completar la información del perfil, desarrollar redes sociales o incorporar fotos. El establecimiento de cuentas también puede incluir la

creación de cuentas con proveedores de correo electrónico, que pueden aprovecharse directamente para Phishing.

Obtener capacidades

Los atacantes pueden comprar y/o robar capacidades que pueden usarse durante la orientación. En lugar de desarrollar sus propias capacidades internamente, los adversarios pueden comprarlas, descargarlas gratuitamente o robarlas. Las actividades pueden incluir la adquisición de malware, software (incluidas las licencias), exploits, vulnerabilidades que se encuentran en la darkweb. Además de descargar malware, software y exploits gratuitos de Internet, los adversarios pueden comprar estas capacidades de entidades de terceros. Las entidades de terceros pueden incluir compañías de tecnología que se especializan en malware y exploits, mercados criminales o de individuos. Además de las capacidades de compra, los adversarios pueden robar capacidades de entidades de terceros (incluidos otros adversarios). Esto puede incluir el robo de licencias de software, malware, SSL/TLS y certificados de firma de código, o la incursión en bases de datos cerradas de vulnerabilidades o exploits.

Capacidades de escenario

Los adversarios pueden cargar, instalar o configurar capacidades que se pueden usar durante la selección de objetivos. Para respaldar sus operaciones, es posible que un adversario deba tomar las capacidades que desarrolló (desarrollar capacidades) u obtuvo (obtener capacidades) y colocarlas en la infraestructura bajo su control. Estas capacidades pueden organizarse en infraestructura que el adversario compró o alquiló previamente (adquirir infraestructura) o que de otro modo se vio comprometida por ellos (comprometer infraestructura). Las capacidades también se pueden organizar en servicios web, como GitHub o Pastebin.

La puesta en escena de las capacidades puede ayudar al adversario en una serie de comportamientos de acceso inicial y posteriores al compromiso, que incluyen (pero no se limitan a):

- Puesta en escena de recursos web para un objetivo de enlace que se utilizará con spearphishing.
- Cargar malware o herramientas en una ubicación accesible para la red de una víctima.

- Instalar un certificado SSL/TLS previamente adquirido para cifrar el comando y controlar el tráfico (criptografía asimétrica con protocolos web).

Acceso inicial

Compromiso de conducción

A menudo, el sitio web utilizado por un adversario es visitado por una comunidad específica, como el gobierno, una industria en particular o una región, donde el objetivo es comprometer a un usuario o conjunto de usuarios específicos en función de un interés compartido. Este tipo de campaña es un compromiso web estratégico

Aprovechar la aplicación orientada al público

Los adversarios pueden intentar aprovechar una debilidad en una computadora o programa con acceso a Internet utilizando software, datos o comandos para provocar un comportamiento no deseado.

Servicios Remotos Externos

Se pueden aprovechar los servicios remotos externos para acceder inicialmente y/o persistir dentro de una red, el acceso a cuentas válidas para usar el servicio suele ser un requisito, que se puede obtener a través del pharming de credenciales o al obtener las credenciales de los usuarios después de comprometer la red empresarial. El acceso a servicios remotos puede utilizarse como mecanismo de acceso redundante o persistente durante una operación.

Suplantación de identidad

Los operadores pueden enviar mensajes de phishing para tener acceso a los sistemas de las víctimas. Todas las formas de phishing se aplica la ingeniería social.

Los operadores pueden enviar correos electrónicos a las víctimas que contienen archivos adjuntos o enlaces maliciosos, generalmente para ejecutar código malicioso en los sistemas de las víctimas.

Ejecución

Intérprete de comandos y secuencias de comandos

Los operadores pueden usar los intérpretes de comandos y scripts para ejecutar comandos, scripts o archivos binarios a través terminales/shells interactivos, así como utilizar varios Servicios Remotos para lograr la Ejecución remota.

Intérprete de comandos y secuencias de comandos: PowerShell

Los operadores usan scripts de PowerShell para su ejecución. PowerShell también se puede usar para descargar y ejecutar ejecutables desde Internet, que se pueden ejecutar desde el disco o en la memoria sin tocar el disco. Hay disponibles varias herramientas de prueba ofensivas basadas en PowerShell, incluidas Empire , PowerSploit, PoshC2 y PSAttack

Intérprete de comandos y secuencias de comandos: AppleScript

Los operadores pueden abusar de AppleScript para ejecutar varios comportamientos, como interactuar con una conexión SSH abierta, moverse a máquinas remotas e incluso presentar a los usuarios cuadros de diálogo falsos.

Intérprete de comandos y secuencias de comandos: Consola de comandos de Windows

Los adversarios pueden abusar del shell de comandos de Windows para su ejecución. pueden aprovechar cmd para ejecutar varios comandos y cargas útiles. Los usos comunes incluyen cmd para ejecutar un solo comando, o abusar de cmd de forma interactiva con entrada y salida reenviadas a través de un canal de comando y control.

Intérprete de comandos y secuencias de comandos: Python

Los operadores pueden abusar de los comandos y scripts de Python para su ejecución. Python viene con muchos paquetes integrados para interactuar con el sistema subyacente, como operaciones de archivos y E/S de dispositivos. Los adversarios pueden usar estas bibliotecas para descargar y ejecutar comandos u otros scripts, así como para realizar varios comportamientos maliciosos.

Intérprete de comandos y secuencias de comandos: JavaScript

Los operadores pueden abusar de varias implementaciones de JavaScript para su ejecución. Los usos comunes incluyen hospedar scripts maliciosos en sitios web como parte de un Compromiso Drive-by o descargar y ejecutar estos archivos de script como cargas útiles secundarias. Dado que estas cargas útiles se basan en texto, también es muy común que los adversarios ofusquen su contenido como parte de archivos o información ofuscados.

Explotación para la ejecución del cliente

Los adversarios pueden aprovechar las vulnerabilidades del software en las aplicaciones de los clientes para ejecutar código. Pueden existir vulnerabilidades en el software debido a prácticas de codificación no seguras que pueden conducir a un comportamiento inesperado.

Ejecución de usuario

Los operadores pueden engañar a los usuarios para que realicen acciones como habilitar el software de acceso remoto y permitir el control directo del sistema al adversario o descargar y ejecutar malware para la ejecución del usuario. Por ejemplo, las estafas de soporte técnico se pueden facilitar a través de phishing, vishing o varias formas de interacción con el usuario. Los adversarios pueden utilizar una combinación de estos métodos, como la suplantación de identidad y la promoción de números gratuitos o centros de llamadas que se utilizan para dirigir a las víctimas a sitios web maliciosos, para entregar y ejecutar cargas útiles que contienen malware o software de acceso remoto.

Persistencia

Manipulación de cuenta

Los operadores. para crear o manipular cuentas, el adversario ya debe tener suficientes permisos en los sistemas o el dominio. Sin embargo, la manipulación de cuentas también puede dar lugar a una escalada de privilegios en la que las modificaciones otorgan acceso a funciones adicionales, permisos o cuentas válidas con privilegios superiores.

Ejecución de inicio automático de inicio o inicio de sesión

Los adversarios pueden configurar los ajustes del sistema para ejecutar automáticamente un programa durante el inicio o el inicio de sesión del sistema para mantener la persistencia u obtener privilegios de mayor nivel en los sistemas comprometidos. Dado que algunos programas de inicio o inicio de sesión automáticos se ejecutan con mayores privilegios, un adversario puede aprovecharlos para elevar los privilegios.

Scripts de inicialización de arranque o inicio de sesión

os adversarios pueden usar secuencias de comandos que se ejecutan automáticamente en el arranque o en la inicialización del inicio de sesión para establecer la persistencia. Los adversarios pueden usar estos scripts para mantener la persistencia en un solo sistema. Según la configuración de acceso de los scripts de inicio de sesión, es posible que se necesiten credenciales locales o una cuenta de administrador.

Crear o modificar el proceso del sistema

Los operadores pueden crear o modificar procesos a nivel del sistema para ejecutar repetidamente cargas útiles maliciosas como parte de la persistencia. Los servicios, demonios o agentes pueden crearse con privilegios de administrador, pero ejecutarse con privilegios de root/SYSTEM. Los adversarios pueden aprovechar esta funcionalidad para crear o modificar procesos del sistema con el fin de aumentar los privilegios.

Servicios Remotos Externos

Los operadores pueden aprovechar los servicios remotos externos para acceder inicialmente y/o persistir dentro de una red. El acceso también se puede obtener a través de un servicio expuesto que no requiere autenticación. En entornos en contenedores, esto puede incluir una API de Docker expuesta, un servidor de API de Kubernetes, kubelet o una aplicación web como el panel de control de Kubernetes.

Componente de software de servidor

Las aplicaciones de servidor de las organizaciones pueden incluir funciones que permiten a los desarrolladores escribir e instalar software o scripts para ampliar la funcionalidad de la aplicación principal. Los adversarios pueden instalar componentes maliciosos para extender y abusar de las aplicaciones del servidor.

Escalada de privilegios

Mecanismo de Control de Elevación de Abuso

Los operadores pueden eludir los mecanismos diseñados para controlar los privilegios elevados. La mayoría de los sistemas modernos contienen mecanismos de control de elevación nativos destinados a limitar los privilegios que un usuario puede realizar en una máquina.

Manipulación de tokens de acceso

Los operadores pueden modificar los tokens de acceso para operar bajo un contexto de seguridad de usuario o sistema diferente para realizar acciones y eludir los controles de acceso. También existen otros mecanismos, como los campos de Active Directory, que se pueden utilizar para modificar los tokens de acceso.

Scripts de inicialización de arranque o inicio de sesión

Los adversarios pueden usar secuencias de comandos que se ejecutan automáticamente en el arranque o en la inicialización del inicio de sesión para establecer la persistencia. Los adversarios pueden usar estos scripts para mantener la persistencia en un solo sistema. Según la configuración de acceso de los scripts de inicio de sesión, es posible que se necesiten credenciales locales o una cuenta de administrador.

Crear o modificar el proceso del sistema

Los operadores pueden instalar nuevos servicios, demonios o agentes que pueden configurarse para ejecutarse al inicio o en un intervalo repetible para establecer la persistencia. De manera similar, los adversarios pueden modificar servicios, demonios o agentes existentes para lograr el mismo efecto.

Explotación para la escalada de privilegios

Los operadores pueden explotar las vulnerabilidades del software, cuando obtiene acceso inicialmente a un sistema, un adversario puede estar operando dentro de un proceso con menos privilegios que le impedirá acceder a ciertos recursos en el sistema. Pueden existir vulnerabilidades, generalmente en los componentes del sistema operativo y el software que normalmente se ejecuta con permisos más altos, que pueden explotarse para obtener niveles más altos de acceso al sistema. Esto podría permitir que alguien pase de permisos sin privilegios o de nivel de usuario a permisos de SISTEMA o raíz, según el componente que sea vulnerable. Esto también podría permitir que un adversario pase de un entorno virtualizado, como dentro de una máquina o contenedor virtual, al host subyacente. Este puede ser un paso necesario para que un adversario comprometa un sistema de punto final que se ha configurado correctamente y limita otros métodos de escalada de privilegios.

Flujo de ejecución de secuestro

Los operadores pueden ejecutar sus propias cargas maliciosas Hay muchas formas en que un adversario puede secuestrar el flujo de ejecución, incluso manipulando cómo el sistema operativo ubica los programas para ejecutar. También se puede interceptar cómo el sistema operativo localiza las bibliotecas que utilizará un programa. Las ubicaciones en las que el sistema operativo busca programas/recursos, como directorios de archivos y, en el caso de Windows, el Registro, también podrían envenenarse para incluir cargas maliciosas.

Evasión de defensa

Mecanismo de Control de Elevación de Abuso

Los operadores pueden eludir los mecanismos diseñados para controlar los privilegios elevados. La mayoría de los sistemas modernos contienen mecanismos de control de elevación nativos destinados a limitar los privilegios que un usuario puede realizar en una máquina.

Manipulación de tokens de acceso

Un operador puede usar las funciones integradas de la API de Windows para copiar tokens de acceso de los procesos existentes; esto se conoce como robo de fichas. Estos tokens se pueden aplicar a un proceso existente (es decir, suplantación/robo de

tokens) o utilizarse para generar un nuevo proceso (es decir, crear un proceso con token).

Crear imagen en el host

Los adversarios pueden crear una imagen de contenedor directamente en un host para eludir las defensas que monitorean la recuperación de imágenes maliciosas de un registro público. Se puede enviar una solicitud remota para la API de Docker que incluye un Dockerfile que extrae una imagen de base estándar, como alpine, de un registro público o local y luego crea una imagen personalizada a partir de ella.

Explotación para Evasión de Defensa

Los operadores pueden tener conocimiento previo a través del reconocimiento de que existe software de seguridad dentro de un entorno o pueden realizar comprobaciones durante o poco después de que el sistema se vea comprometido por Security Software Discovery. Es probable que el software de seguridad sea objeto directo de explotación. Hay ejemplos de software antivirus que están siendo atacados por grupos de amenazas persistentes para evitar la detección.

Inyección de proceso

Los operadores pueden inyectar código en los procesos para evadir las defensas basadas en procesos y posiblemente elevar los privilegios. Hay muchas formas diferentes de inyectar código en un proceso, muchas de las cuales abusan de funcionalidades legítimas.

Rootkit

Los adversarios pueden usar rootkits para ocultar la presencia de programas, archivos, conexiones de red, servicios, controladores y otros componentes del sistema. Los rootkits son programas que ocultan la existencia de malware interceptando/enganchando y modificando las llamadas API del sistema operativo que proporcionan información del sistema.

Evasión de Virtualización/Sandbox

Los adversarios pueden emplear varios medios para detectar y evitar entornos de virtualización y análisis. Esto puede incluir comportamientos cambiantes en función

de los resultados de las comprobaciones de la presencia de artefactos indicativos de un entorno de máquina virtual (VME) o sandbox. Los adversarios pueden usar varios métodos para lograr la evasión de virtualización/sandbox, como buscar herramientas de monitoreo de seguridad (por ejemplo, Sysinternals, Wireshark, etc.) u otros artefactos del sistema asociados con el análisis o la virtualización. Los adversarios también pueden verificar la actividad legítima del usuario para ayudar a determinar si se encuentra en un entorno de análisis. Los métodos adicionales incluyen el uso de temporizadores de suspensión o bucles dentro del código de malware para evitar operar dentro de una zona de pruebas temporal.

Acceso a credenciales

Adversario-en-el-medio

Los adversarios pueden intentar posicionarse entre dos o más dispositivos en red utilizando una técnica de adversario en el medio, para respaldar comportamientos de seguimiento como Network Sniffing o transmisión de data.

Fuerza bruta

Los operadores pueden usar técnicas de fuerza bruta para obtener acceso a las cuentas cuando se desconocen las contraseñas o cuando se obtienen hashes de contraseñas. Las credenciales de fuerza bruta pueden tener lugar en varios puntos durante una infracción. Por ejemplo, los adversarios pueden intentar acceder por fuerza bruta a cuentas válidas dentro de un entorno de víctima aprovechando el conocimiento recopilado de otros comportamientos posteriores al compromiso, como el volcado de credenciales del sistema operativo, el descubrimiento de cuentas o el descubrimiento de políticas de contraseñas. Los adversarios también pueden combinar actividades de fuerza bruta con comportamientos como servicios remotos externos como parte del acceso Inicial.

Autenticación forzada

Los operadores pueden recopilar credenciales invocando u obligando a un usuario a proporcionar automáticamente información de autenticación a través de un mecanismo en el que pueden interceptar. Los sistemas Windows también suelen utilizar la creación y el control de versiones distribuidos en la web (WebDAV) como

protocolo de copia de seguridad cuando SMB está bloqueado o falla. WebDAV es una extensión de HTTP y normalmente funcionará en los puertos TCP 80 y 443.

Robar token de acceso a la aplicación

El robo de tokens también puede ocurrir a través de la ingeniería social, en cuyo caso se puede requerir la acción del usuario para otorgar acceso. Una aplicación que desee acceder a servicios basados en la nube o API protegidas puede ingresar usando OAuth 2.0 a través de una variedad de protocolos de autorización. Un ejemplo de secuencia de uso común es el flujo de concesión de código de autorización de Microsoft. Un token de acceso de OAuth permite que una aplicación de terceros interactúe con recursos que contienen datos de usuario en las formas solicitadas por la aplicación sin obtener credenciales de usuario.

Descubrimiento

Descubrimiento de cuenta

Los adversarios pueden intentar obtener una lista de cuentas en un sistema o dentro de un entorno. Esta información puede ayudar a los adversarios a determinar qué cuentas existen para ayudar en el comportamiento de seguimiento

Descubrimiento de cuenta: cuenta de dominio

Los operadores pueden intentar obtener una lista de cuentas de dominio. Comandos como net user /domainy net group /domain de la utilidad Netdscache util -q group, en macOS y ldapsearchen Linux pueden listar usuarios y grupos de dominio

Descubrimiento de cuenta: cuenta de correo electrónico

Los operadores pueden intentar obtener una lista de direcciones de correo electrónico y cuentas. En Exchange local y Exchange Online, el Get-GlobalAddressListcmdlet de PowerShell se puede usar para obtener direcciones de correo electrónico y cuentas de un dominio mediante una sesión autenticada.

Descubrimiento de cuenta: cuenta en la nube

Los adversarios pueden intentar obtener una lista de cuentas en la nube. Con acceso autenticado, hay varias herramientas que se pueden usar para encontrar cuentas. El Get-MsolRoleMembercmdlet de PowerShell se puede usar para obtener nombres de

cuenta con un rol o un grupo de permisos en Office 365. La CLI de Azure (AZ CLI) también proporciona una interfaz para obtener cuentas de usuario con acceso autenticado a un dominio. El comando az ad user list mostrará una lista de todos los usuarios dentro de un dominio.

Movimiento lateral

Explotación de Servicios Remotos

Los adversarios pueden explotar los servicios remotos para obtener acceso no autorizado a los sistemas internos una vez dentro de una red. Es posible que un adversario deba determinar si el sistema remoto se encuentra en un estado vulnerable, lo que puede hacerse a través de network service discovery u otros métodos de discovery en busca de software vulnerable común que pueda implementarse en la red, la falta de ciertos parches que pueden indicar vulnerabilidades o software de seguridad que puede usarse para detectar o contener la explotación remota. Es probable que los servidores sean un objetivo de alto valor para la explotación del movimiento lateral, pero los sistemas de terminales también pueden estar en riesgo si brindan una ventaja o acceso a recursos adicionales. Hay varias vulnerabilidades bien conocidas que existen en servicios comunes como SMB y RDP, así como en aplicaciones que pueden usarse dentro de redes internas como MySQL y servicios de servidor web. Dependiendo del nivel de permisos del servicio remoto vulnerable, un adversario puede lograr la Explotación para la Escalada de Privilegios como resultado de la explotación del movimiento lateral también.

Transferencia lateral de herramientas

Los operadores pueden transferir herramientas u otros archivos entre sistemas en un entorno comprometido. Una vez llevados al entorno de la víctima (es decir, Ingress Tool Transfer), los archivos se pueden copiar de un sistema a otro para organizar las herramientas del adversario u otros archivos en el transcurso de una operación.

Secuestro de sesión de servicio remoto

Los operadores pueden tomar el control de sesiones preexistentes con servicios remotos para moverse lateralmente en un entorno. Los operadores pueden requisar estas sesiones para llevar a cabo acciones en sistemas remotos. El secuestro de

sesión de servicio remoto difiere del uso de servicios remotos porque secuestra una sesión existente en lugar de crear una nueva sesión utilizando cuentas válidas.

Replicación a través de medios extraíbles

En el caso del movimiento lateral, esto puede ocurrir a través de la modificación de archivos ejecutables almacenados en medios extraíbles o copiando malware y renombrándolo para que parezca un archivo legítimo para engañar a los usuarios para que lo ejecuten en un sistema separado.

Servicios Remotos

Las aplicaciones legítimas (como las Herramientas de implementación de software y otros programas administrativos) pueden utilizar Servicios remotos para acceder a hosts remotos. Por ejemplo, Apple Remote Desktop (ARD) en macOS es un software nativo que se utiliza para la administración remota. ARD aprovecha una combinación de protocolos, incluido VNC para enviar la pantalla y los búferes de control y SSH para la transferencia segura de archivos. Los operadores usan aplicaciones como ARD para obtener la ejecución remota de código y realizar movimientos laterales.

Recopilación

Datos de la unidad compartida de red

Los operadores pueden buscar recursos compartidos de red en computadoras que han comprometido para encontrar archivos de interés.

Comando y control

Los operadores pueden utilizar muchos protocolos diferentes, incluidos los que se utilizan para la navegación web, la transferencia de archivos, el correo electrónico o el DNS. Para las conexiones que ocurren internamente dentro de un enclave (como aquellas entre un proxy o un nodo pivote y otros nodos), los protocolos comúnmente usados son SMB, SSH o RDP.

Canal encriptado

Los adversarios pueden emplear un algoritmo de cifrado conocido para ocultar el tráfico de comando y control en lugar de confiar en las protecciones inherentes proporcionadas por un protocolo de comunicación.

Túnel de protocolo

Hay varios medios para encapsular un protocolo dentro de otro protocolo. Por ejemplo, los adversarios pueden realizar túneles SSH (también conocido como reenvío de puertos SSH), lo que implica el reenvío de datos arbitrarios a través de un túnel SSH cifrado. Los adversarios también pueden abusar del túnel de protocolo durante la resolución dinámica. Conocido como DNS sobre HTTPS (DoH), las consultas para resolver la infraestructura C2 pueden encapsularse dentro de paquetes HTTPS cifrados.

Exfiltración

Exfiltración automatizada

Los adversarios pueden exfiltrar datos, como documentos confidenciales, mediante el uso de procesamiento automatizado después de recopilarlos durante la Recopilación. Cuando se utiliza la exfiltración automatizada, es probable que también se apliquen otras técnicas de exfiltración para transferir la información fuera de la red, como Exfiltración sobre el canal C2 y Exfiltración sobre el protocolo alternativo.

Exfiltración sobre el canal C2

Los adversarios pueden robar datos exfiltrándolos a través de un canal de C2 existente. Los datos robados se codifican en el canal de comunicaciones normal usando el mismo protocolo que las comunicaciones de comando y control.

Exfiltración sobre medio físico

Dichos medios podrían ser un disco duro externo, una unidad USB, celular u otro dispositivo extraíble de procesamiento y almacenamiento. El medio o dispositivo físico podría usarse como el punto de exfiltración final o para saltar entre sistemas que de otro modo estarían desconectados.

Exfiltración a través del servicio web

Los servicios web populares que actúan como un mecanismo de exfiltración pueden brindar una cantidad significativa de cobertura debido a la probabilidad de que los hosts dentro de una red ya se estén comunicando con ellos antes del compromiso. Es posible que ya existan reglas de firewall para permitir el tráfico a estos servicios. Los

proveedores de servicios web también suelen utilizar el cifrado SSL/TLS, lo que brinda a los adversarios un nivel adicional de protección.

Transferencia programada

Los adversarios pueden programar la exfiltración de datos para que se realice solo en ciertos momentos del día o en ciertos intervalos. Esto podría hacerse para combinar los patrones de tráfico con la actividad o disponibilidad normal. Cuando se usa la exfiltración programada, es probable que también se apliquen otras técnicas de exfiltración para transferir la información fuera de la red, como Exfiltración a través del canal C2 o Exfiltración a través del protocolo alternativo.

Ciberarmas

La tecnología a emplear son diferentes y basadas en tareas que puedan realizar y los efectos que se deseen obtener, empleando para ello plataformas con herramientas ofensivas desarrolladas por lo mismo operadores cibernéticos, opensource, o adquiridas.

Dentro de las ciberarmas desarrolladas a medida podemos mencionar que estas serán diseñadas de acuerdo al objetivo que se desee neutralizar o irrumpir, para esta solución el operador desarrollara empleando diversos lenguajes de programación y plataformas digitales acorde a sus requerimientos operacionales, por ejemplo si nuestro objetivo es un sistema de armas y de comando y control que ha sido desarrollado en lenguaje de programación java, el operador deberá dominar el lenguaje java y sus ciberarmas deberán ser diseñadas para afectar el sistema de armas así como el de comando y control.

Los lenguajes de programación son fundamentales, el dominio que tengan los operadores el conocimiento de las diferentes tecnologías, el conocimiento de plataformas ofensivas, como Linux, Blackarch, Parrot security, o las que se puedan desarrollar, el desarrollo de troyanos, malware, botnet, rasonware, etc, es fundamental para los propósitos, o el de disrumpir un sistema SCADA.

El conocimiento de ciberarmas opensource que se encuentra en la internet también es fundamental porque permite la optimización de tiempo y costo, en vista que dichas ciberarmas pueden ser modificadas para nuestros propósitos.

La adquisición de ciberarmas también es fundamental, otros países han desarrollados tecnologías eficaces que permiten vulnerar sistemas de armas, comando y control, de comunicaciones de tipo móvil 4G. siendo estas oportunas en tiempo y espacio.

Debemos tener en cuenta que el empleo de las ciberarmas no solo se operativiza dentro de un área de operaciones, sino que esta abarca de manera global, al buscar ser anónima para su empleo, necesariamente será dinámica.

2.3.2 Operaciones Militares de Ciberdefensa

Serán ejecutadas por dependencias ejecutoras del MINDEF, la Resolución Ministerial N° 1490-2016-DE/CCFFAA a través de la Capacidades Militares estableciendo también que el área de Capacidad de “Protección y Supervivencia” contiene la Capacidad Militar “Ciberdefensa”: Que permite impedir, contener y neutralizar ataques realizados en el ciberespacio contra nuestros sistemas de redes de comunicaciones e informática, para permitir el cumplimiento de los roles estratégicos.

Asimismo, la planificación y ejecución de las operaciones en el ciberespacio están a cargo del Comando Conjunto de las Fuerzas Armadas, cabe mencionar que en la Resolución Ministerial N° 388-2019-DE/CCFFAA. CO Y CE DEL CCFFAA establece que dentro de los Comandos Operacionales (CO) de tipo funcional se encuentra el Comando Operacional de Ciberdefensa, asignándole como misión planear, organizar, dirigir y conducir operaciones especiales conjuntas en el Ciberespacio, con el fin de neutralizar ciberataques sobre nuestras fuerzas y medios de alto valor militar y activos críticos.

El Manual del Ejército del Perú ME 1-13 establece operaciones terrestres según el Ejército del Perú (2015) “el conjunto de encuentros terrestres; decisivos, de relativa o de poca importancia para el desarrollo de la guerra, comprende la Maniobra, el Apoyo de Combate y el Servicio de Combate como un Sistema” (p. 13). Teniendo el concepto de ciberespacio como un ámbito digital y físico interconectado por redes y sistemas, dicho ámbito se contempla actividades, se concentra información, se dan comunicaciones no solo de tipo militar sino de un entorno global, es por ello que las operaciones militares no solo se deben enfocar a un ámbito terrestre, la Ciberdefensa puede dar un soporte a las operaciones para que se lleven a cabo operaciones terrestres. La Ciberdefensa puede realizar operaciones militares en este medio del tipo ofensivas y defensivas, a través de un proceso adecuado de las operaciones, un buen planeamiento que se enfoque la conjugación de operaciones terrestres como en el ciberespacio, se ha explicado que las amenazas son cada vez más avanzadas, las operaciones deben ser acorde a ello, el proceso de las operaciones implica un ciclo en el cual se debe evaluar constantemente las operaciones por medio del ciberespacio a fin que se regulen dichas operaciones en vista que tenemos una amenaza no identificada, así como no ubicada, esta capacidad y empleo no solo es exclusivo del Ejército del Perú, sino que es una capacidad que engranda la sinergia de las fuerzas marítimas como aéreas, y sus

capacidades de Ciberdefensa. Asimismo, debemos comprender que las Operaciones ofensivas en el ciberespacio son acciones destinadas a crear efectos de denegación, degradación o interrupción del uso del ciberespacio de los adversarios, mediante el empleo de ciberarmas. Y las operaciones defensivas en el ciberespacio son acciones de defensa protección del ciberespacio propio y ajeno asignado, con la finalidad de brindar protección ante Actos Hostiles o Intenciones Hostiles, para asegurar su disponibilidad, confidencialidad e integridad, mediante la aplicación de medidas preventivas, proactivas, reactivas y de recuperación.

De los órganos ejecutores y las capacidades de Ciberdefensa del Ministerio de Defensa

Los órganos ejecutores del Ministerio de Defensa en sus respectivos ámbitos de competencia y con arreglo a ley deberán dirigir las operaciones con la finalidad de defender sus redes de información y las designadas, preparar el espectro de las posibles operaciones y garantizar libertad de acción de sus componentes en el ciberespacio.

Las capacidades de Ciberdefensa de los órganos ejecutores del Ministerio de Defensa son las siguientes:

- **Capacidad de Defensa**: Consiste en la defensa protección de las diferentes plataformas tecnológicas o sistemas de información ante ataques y su recuperación en caso de fallo o inutilización total o parcial.
- **Capacidad de Explotación**: Consiste en la búsqueda y detección de amenazas en el ciberespacio.
- **Capacidad de Respuesta**: Es negar o alterar el uso del ciberespacio al adversario.

Intervención del CCFFAA y sus componentes de Ciberdefensa

La intervención del Comando Conjunto de las Fuerzas Armadas y sus componentes de Ciberdefensa para realizar operaciones conjuntas, se da dentro del territorio nacional y donde los intereses nacionales lo demanden, con la finalidad de hacer frente a amenazas en el ciberespacio.

el Comando Operacional de Ciberdefensa del Comando Conjunto de las Fuerzas Armadas es el responsable de realizar el planeamiento, organización y conducción de las operaciones militares conjuntas en el ciberespacio, protección de sus sistemas de información, garantizando el libre acceso, la libertad de acción y maniobra de las fuerzas asignadas, empleando los componentes de Ciberdefensa de las Fuerzas Armadas.

Los componentes de Ciberdefensa de las Fuerzas Armadas son los siguientes:

- Componente de Ciberdefensa del Ejército del Perú.
- Componente de Ciberdefensa de la Marina de Guerra del Perú.
- Componente de Ciberdefensa de la Fuerza Aérea del Perú

2.3.2.1 Ambiente Operacional

Las operaciones se realizan en ambientes operacionales complejos, cambiantes e inciertos, un ambiente operacional es la combinación de las condiciones, que afectan el empleo de las capacidades de ciberdefensa

Ambiente digital "ciberespacio"

En todo este tiempo que entró en vigencia el quinto dominio denominado "ciberespacio", varias comunidades internacionales también han dado diferentes definiciones de Ciberespacio como Information Systems Audit and Control Association (ISACA) una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información. National Institute of Standards and Technology (NIST), este marco ayuda a mejorar la seguridad cibernética de la infraestructura crítica y se enfoca la seguridad cibernética, la gestión de riesgos y la resistencia de sus sistemas. En el Perú a la ciberseguridad se le denomina Seguridad Digital y se encuentra plasmado en la D.L N° 1412, cuyo objeto menciona:

> Que es 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 los tres niveles de gobierno define como entorno digital como el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, infraestructuras y la interacción entre personas (Congreso de la República de Perú, Artículo 1).

Dicha D.L N°1412 va enfocado a un entorno civil del estado y entidades privadas, no vinculando aun a la Fuerzas Armadas, este fue un esfuerzo en la cual se reconocía la existencia de un entorno digital y que este demandaba seguridad no solo física, sino lógico. Para España "es el nombre que se designa al dominio global y dinámico compuesto por infraestructuras de tecnología de la información, incluida internet, redes y los sistemas de información y de telecomunicaciones" un concepto en la región como es el caso de Brasil

establece “el ciberespacio es una de las cinco áreas operacionales que penetra las demás como son. Tierra, mar, aire y espacio que son interdependientes”.

Definiendo el ciberespacio

En base de las diferentes y variadas definiciones de ciberespacio, podemos establecer que existen características comunes de carácter global, que resulta de la interacción de elementos, físicos (hardware, espacio geográfico), lógicos (conectividad, software, servicios), personales, sociales por medio del cual se obtiene, procesa y difunde información información teniendo como característica relevante el desarrollo en tiempo real influenciado en el comportamiento, convivencia propia del hombre y su entorno, mientras más sofisticados sean los elementos físicos y lógicos las personas podrán establecer un ciclo de información más oportuno.

El ciberespacio posee también brechas de seguridad que la hacen más vulnerable al ataque cibernético, en la actualidad en el ciberespacio posee múltiples propietarios siendo estas personas u organizaciones teniendo estas diferentes intenciones y con un dominio de seguridad segmentado de acuerdo a la prioridad y manejo de su información.

El ciberespacio concepto militar

Dominio compuesto por elementos físicos (sistemas C2, Armas, sistemas informáticos militares, ambiente operacional, etc.), lógicos (interconectividad, softwares militares, etc.), combatientes y no combatientes por medio de su interacción el comandante busca obtener superioridad y supremacía en el ciberespacio.

2.3.2.2 Planeamiento Operaciones Ciberdefensa

Entendiendo que la operaciones cibernéticas se establecerán en dos escenarios, el primero en la ejecución de operaciones militares llevados a cabo en el ciberespacio, el segundo a través de acciones militares, como proteger los ACN y recursos claves, en vista que el poderío terrestre normalmente solidifica el resultado, el poderío terrestre es la capacidad que por medio de amenazas, fuerza u ocupación puede obtener, sostener y explotar el control sobre el terreno, los recursos y las personas, un escenario en el cual las operaciones militares cibernéticas actúan de manera independientes en un entorno virtual denominado “cyber guerra” algunos expertos señalan que la guerra cibernética incluye la destrucción de objetivos físicos y para ser considerado como un acto de guerra cibernética pudiéndose identificar tareas tácticas a fin a la capacidad de Ciberdefensa.

Principios de la Ciberdefensa

Según la guía de ciberdefensa de la Junta Interamericana de Defensa (JID) establece ciertos principios como:

- **Flexibilidad**
  Es poder adoptar nuevas medidas defensivas, ofensivas o de explotación referente a las Técnicas, Tácticas y procedimientos de los ciberataques.

- **Economía de medios**
  Eficiente empleo de los recursos de ciberdefensa, en vista que su empleo es costoso costosos frente al de realizar un ciberataque y su desarrollo demanda de tiempo extendido.

- **Concentración de esfuerzos**
  Establecerlas capacidades ventajosas de ciberdefensa en el momento y lugar oportuno para poder obtener los efectos deseados.

- **Unidad de mando**
  Disponer un único líder para cada misión, operación en los niveles determinados de las operaciones de ciberdefensa.

- **Seguridad**
  Capacidad de establecer medidas de prevención y reacción en contra de ciberataques.

- **Sorpresa**
  Es realizar acciones de ciberdefensa en un momento, lugar empleando para ello técnicas, tácticas y procedimientos sobre el adversario que no está preparado.

- **Masa**
  Se aplica a la capacidad operativa de respuesta cuando se ejecutan ataques de denegación de servicio (DOS).

- **Maniobra**

  Son operaciones de ciberdefensa con el fin de lograr una posición ventajosa respecto a los adversarios empleando para ello todas sus capacidades relacionadas a tecnología y el personal con sus habilidades.

Arte y diseño operacional

En los manuales de operaciones militares establecen conceptos de arte y diseño operacional, pero según el Ejército del Perú (2015) afirma “que el arte es inherente al comandante y dentro de ella el diseño como metodología que emplea el pensamiento crítico y creativo para desarrollar una comprensión del ambiente operacional” (p. 3). Los comandantes utilizan el arte para idear y definir un estado final deseado y asi poder llegar a la esencia de una gran operación aquí el comandante establece y traduce el concepto de las operaciones en un diseño, y por ende en tareas tacticas de ciberdefensa.

Se puede establecer que le diseño se utiliza para comprender el ambiente operacional.

Elementos del diseño

- **Estado final deseado**

  Condiciones necesarias que define el logro de un objetivo militar, En el ambiente del ciberespacio, los límites no podrán ser definidos con claridad, por lo tanto, el estado final deseado operacional será afectado sin dudas por las acciones de la guerra cibernética.

- **Líneas operacionales**

  las líneas de operaciones inician del centro de gravedad cibernético propio para alcanzar el centro de gravedad cibernético adversario y así contribuir con el disloque del centro de gravedad del oponente. Asimismo, no permitirá alcanzar puntos decisivos que a la ve nos dará acceso al centro de gravedad

  Estas líneas de operaciones serán tipo mixtas: físicas porque parten desde un hardware y se unirán a otros (Puntos Decisivos) en forma lógica. En las operaciones las líneas de operaciones cibernéticas serán los comandantes de ciberdefensas quienes la diseñen y conduzcan**.**

- **Objetivo**

  operación militar que conlleva una meta clara, una vez que el estado final deseado ha sido entendido con claridad, los objetivos y efectos establecen identificación de tareas a realizarse.

- **Efectos**

  Es un comportamiento operacional producto de una acción o acciones. Los efectos deseados también son considerados condiciones para consecución de objetivos y los efectos no deseados puede inhibir el progreso hacia un objetivo. Los efectos pueden ser medibles y se pueden vincular directamente a uno o más objetivos.

- **Puntos decisivos**

  Es un espacio lógico o físico, un factor crítico que permite tener una ventaja táctica sobre el adversario, también se puede denominar PD como eventos claves tales como disrupción de un servicio de una infraestructura TI del adversario

- **Centro de gravedad**

  La identificación y análisis de los centros de gravedad en el ámbito de la ciberdefensa constituyen una tarea importante para los comandantes que conducen operaciones, un CG es una fuente de energía, pudiendo ser esta física o digital. Los CG físicos pueden ser objetivos materiales como datacenter, plantas nucleares, plantas industriales etc. Sin embargo, CG digital pueden ser los sistemas de redes, software, diferentes sistemas de armas y de C2.

  Los comandantes de ciberdefensa deben identificar los CG propios como los del enemigo. Una vez identificados debe determinar la forma como atacarlos y como proteger los propios.

Metodología para determinar CG

Figura 8

Metodología determinación Centros de gravedad

OBJETIVO OPERACIONAL ENEMIGO: OBTENER LA SUPREMACÍA EN EL CIBERESPACIO.	
CoG Operacional: **Comando de ciberdefensa del Ejército**	**Capacidades Criticas:** ✓ Capaz de realizar ataques cibernéticos a gran escala ✓ Capaz de impulsar actividades de ciberespionaje ✓ Capaz de ejercer el hacktivismo en TO
Vulnerabilidades Criticas ✓ Escaneo de redes y sistemas ✓ Infección de malware ✓ Movimientos laterales por malware ✓ Infección y malware tome C2 ✓ Exfiltración de información	**Requerimientos Críticos** ✓ Sistemas del adversario vulnerables ✓ Disponibilidad de spyware ✓ Disponer de redes sociales hacktivistas

Capacidades Criticas

Habilidades de ciberdefensa que permiten al centro de gravedad realizar acciones en un determinado escenario, situación, y poder cumplir con su misión teniendo como medio el ciberespacio.

Requerimientos Críticos

Condición, recurso o medio necesario e indispensable para que la capacidad crítica determinada sea plenamente operativa.

Vulnerabilidades Criticas

Se derivan de los requisitos críticos, o componentes que son identificados vulnerables a la destrucción, neutralización, degradación.

Diseño de la operación

- **Aproximación directa**

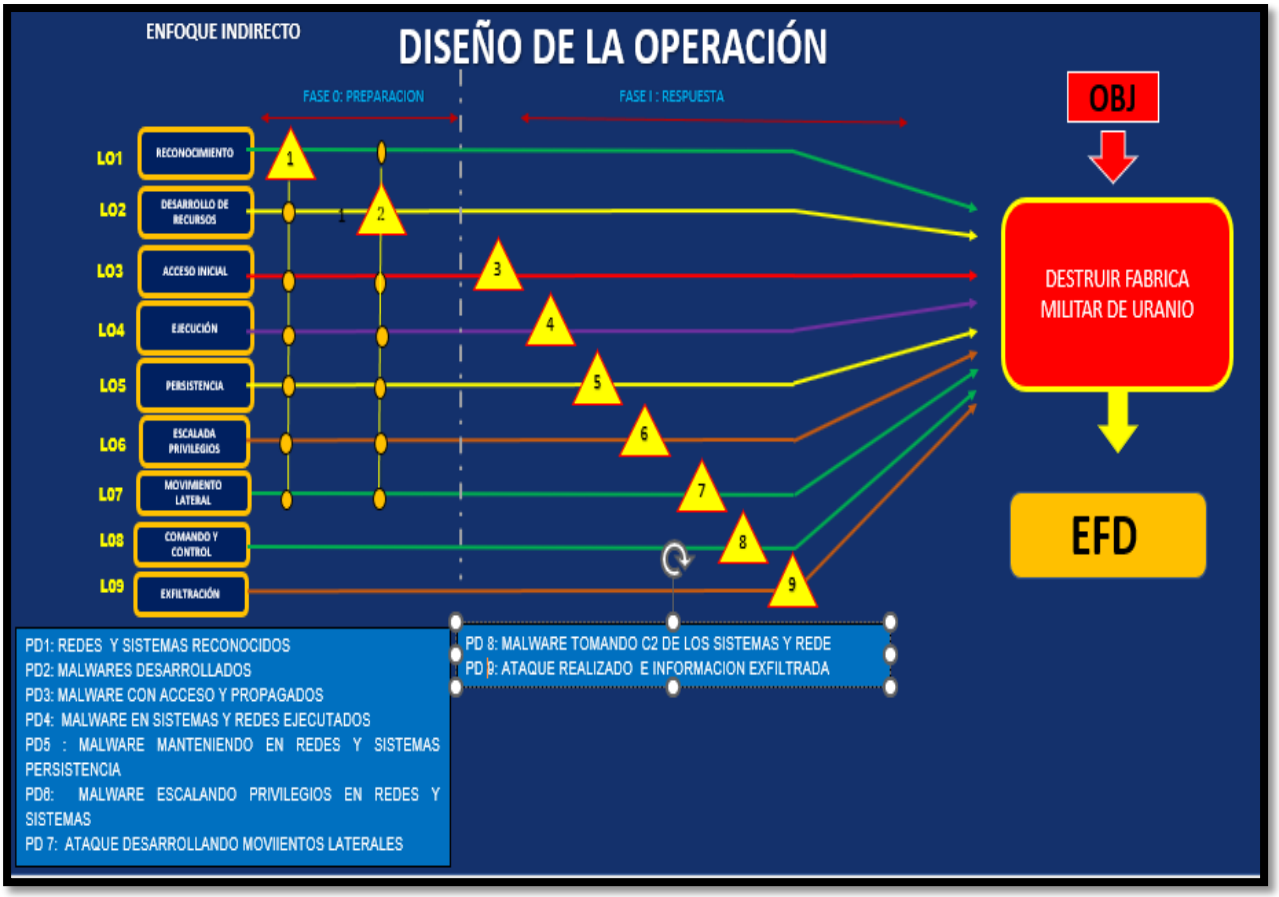
  Hace referencia que el CG en el ámbito de ciberdefensa obedece a un planeamiento lineal ininterrumpible.

- **Aproximación indirecta**

  Se busca aprovechar sus vulnerabilidades para ello empleamos una serie de puntos decisivos dispondremos de tiempo el adversario es superior en su infraestructura de seguridad perimetral.

Figura 9

Diseño de la operación



Tareas tácticas de las capacidades operativas

Capacidad de protección

- **Sostener (mantener)**
  La fuerza amiga asegura que una característica del ciberespacio físico y digital (comando y control, sistema informático, entre otros). que está bajo control de la fuerza amiga permanezca libre de dominio o del uso de la fuerza enemiga.

- **Impedir (bloquear)**
  Negar al enemigo el acceso a un área en el ciberespacio o impedirle el avance en el dominio de la fuerza amiga, una tarea de impedir generalmente requiere que la fuerza amiga bloquee a la fuerza enemiga por cierto periodo de tiempo y con diferentes acciones en el ciberespacio.

- **Proteger**
  Tarea táctica cuya finalidad es proteger ante una acción enemiga que perjudique o destruya el ciberespacio de dominio de la fuerza amiga (comando y control, sistema informático, entre otros). en esta tarea generalmente se conducen actividades de protección del ciberespacio de dominio de la fuerza amiga.

Capacidad de explotación

- **Descubrir**
  Una fuerza amiga adquiere conocimientos sobre el sistema y la red interna de las fuerzas enemigas. estas tareas ayudan a las fuerzas amigas a observar el entorno y a orientarse antes de decidir cómo actuar. también permiten que las fuerzas amigas exploren qué pueden controlar y qué hay alrededor de su punto de entrada para descubrir cómo podría beneficiar a su misión.

- **Recopilar**
  Fuerza amiga pueden realizar recopilación de información utilizando las fuentes de internet a través de motores de búsqueda sobre sistema de combate, sistema de comando y control, sistema informático, entre otros) de la la fuerza enemiga. que son relevantes para cumplir con los objetivos.

- **Explorar**
  Se usa para obtener información de las amenazas cibernéticas a través del ciberespacio a fin de conocer sus intenciones generalmente requiere que la fuerza

amiga identifique las amenazas cibernéticas, para que la fuerza amigas adopte medidas de Ciberdefensa pasivas, activas o de engaño.

Capacidad respuesta

- **Destruir (destruir)**
  Dejar a la fuerza enemiga físicamente y digitalmente fuera de combate en/y mediante el ciberespacio, así mismo destruir un sistema de combate (comando y control, sistema informático entre otros) es dañarlo a tal punto que no pueda desempeñar ninguna función o que, para repararlo y usarlo de nuevo, se tenga que reconstruir por completo.

- **Accesar**
  Consiste en utilizar varios vectores de entrada para ganar su punto de apoyo inicial dentro de una red. las técnicas utilizadas para afianzarse incluyen el reconocimiento dirigido y la explotación de las debilidades en los sistemas de combate (comando y control, sistema informático entre otros). los puntos de apoyo obtenidos a través del acceso pueden permitir el acceso continuo, como cuentas válidas y el uso de servicios remotos externos.

- **Explotar**
  La fuerza amiga ejecuta tareas que resultan en código controlado por la fuerza amiga que se ejecuta en un sistema local o remoto sistema de combate, sistema de comando y control, sistemas informáticos, entre otros. las técnicas que ejecutan código malicioso a menudo se combinan con técnicas de todas las demás tácticas para lograr objetivos más amplios, como explorar una red y obtener datos.

- **Persistir**
  Las fuerzas amigas mantienen el acceso a los sistemas de combate (comando y control, sistemas informáticos entre otros). de la fuerza enemiga, se mantienen durante los reinicios, las credenciales cambiadas y otras interrupciones que podrían cortar su acceso. las técnicas utilizadas para la persistencia incluyen cualquier cambio de acceso, acción o configuración que les permita mantener su posición en los sistemas.

- **Escalar privilegios**
  El escalamiento de privilegios la utilizan las fuerzas amigas sobre fuerzas enemigas para obtener permisos de nivel superior en un sistema o red. los adversarios a menudo pueden ingresar y explorar una red con acceso sin privilegios, pero requieren permisos

elevados para cumplir con sus objetivos. los enfoques habituales son aprovechar las debilidades del sistema, las configuraciones incorrectas y las vulnerabilidades.

- **Evadir la defensa**

  La evasión de defensa consiste en técnicas que utilizan las fuerza amigas para evitar ser detectados por las fuerzas enemigas durante su compromiso al sistema de combate (comando y control, sistemas informáticos entre otros).

- **Movimiento lateral**

  El movimiento lateral es una tarea que utilizan las fuerzas amigas para ingresar y controlar sistemas remotos en una red (sistema de combate, comando y control, sistemas informáticos, entre otros). su objetivo principal a menudo requiere explorar la red para encontrar su objetivo y, posteriormente, obtener acceso a él. alcanzar su objetivo a menudo implica girar a través de múltiples sistemas y cuentas para ganar acceso. las fuerzas amigas pueden instalar sus propias herramientas de acceso remoto para lograr el movimiento lateral o utilizar credenciales legítimas con herramientas nativas de red y sistema operativo, que pueden ser más sigilosas.

- **Controlar**

  Las fuerzas amigas comunica con los sistemas comprometidos para controlarlos. esta tarea consiste en que las fuerzas amigas pueden comunicarse con los sistemas bajo su control dentro de una red comprometida (comando y control, sistemas informáticos, internet entre otros). las actividades fuerzas amigas comúnmente intentan imitar el tráfico normal esperado para evitar ser detectados. hay muchas formas que las fuerzas amigas puede establecer el control con varios niveles de compromiso dependiendo de la estructura de red y las defensas de las fuerzas enemigas.

- **Exfiltrar (exfiltrar)**

  La exfiltración es una tarea que las fuerzas amigas pueden utilizar para extraer datos de interés de su red comprometida (sistema de combate, comando y control, sistemas informáticos, entre otros). una vez que han recopilado los datos de interés, las fuerzas amigas a menudo los empaquetan para evitar la detección mientras los eliminan. esto puede incluir compresión y cifrado. las técnicas para obtener datos de una red comprometida de destino generalmente incluyen transferirlos a través de su canal de comando y control o un canal alternativo y también pueden incluir poner límites de tamaño a la transmisión.

2.3.2.2.1 Planeamiento Operaciones Ciberdefensa Defensivas

Marco NIST

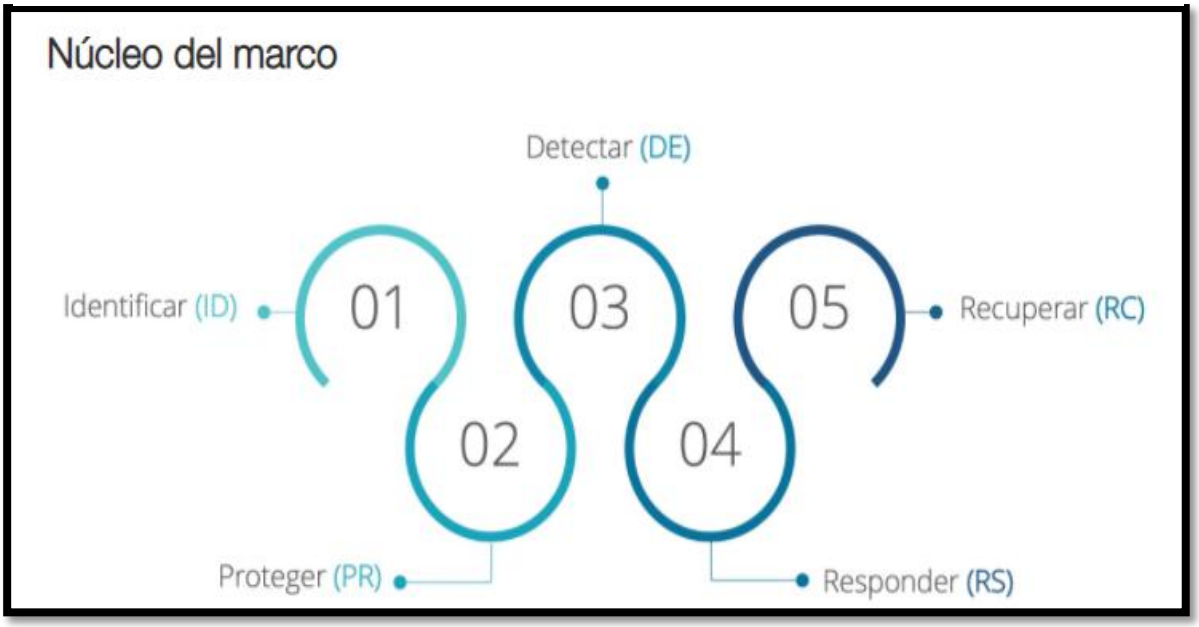
El Marco de Ciberseguridad del NIST se enfoca a las organizaciones a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Orientado a los riesgos cibernéticos un nuevo enfoque si necesitamos realizar una propuesta de empleo de la Ciberdefensa en el Perú es necesario adoptar un marco y tomar un enfoque holístico de la seguridad en un entorno cibernético. NIST nos enfoque de ciberseguridad adoptando dos capacidades de Ciberdefensa la de exploración, protección estas capacidades debe llevar procedimientos puestos de manifiesto en planes de operaciones, NIST nos da ese aporte necesario para un manejo acorde de un incidente cibernético, debemos entender que un incidente es producto de un riesgo materializado por ello el Framework Core comprende un conjunto de actividades de ciberseguridad, resultados y referencias informativas que son comunes a través de los sectores de infraestructura crítica. Así, proporciona la orientación detallada para el desarrollo de perfiles individuales de la compañía. Mediante el uso de los perfiles, el marco ayudará a la organización a alinear sus actividades de ciberseguridad con sus requisitos de negocio, tolerancias de riesgo y recursos. Por su parte, los niveles de implementación del marco *(*tiers*)* proporcionan un mecanismo para que las entidades puedan ver y comprender las características de su enfoque para la gestión del riesgo de ciberseguridad.

- Núcleo del marco

El núcleo proporciona cinco funciones continuas, la identificación de nuestros activos que poseemos en nuestra organización, la protección que debemos llevar a cabo con ellas, la detección de anomalías que puedan ocurrir dentro de nuestra organización esto consta de un monitoreo continuo, la respuesta ante los diferentes incidentes cibernéticos ejecutando nuestros planes de respuesta y por último la recuperación de nuestros servicios.

Figura 10

Funciones NIST



NOTA: El núcleo establece cinco funciones, obtener resultados ciberseguridad, De “Núcleo del marco”, por Nist, 2019 (https://www.nist.gov/)

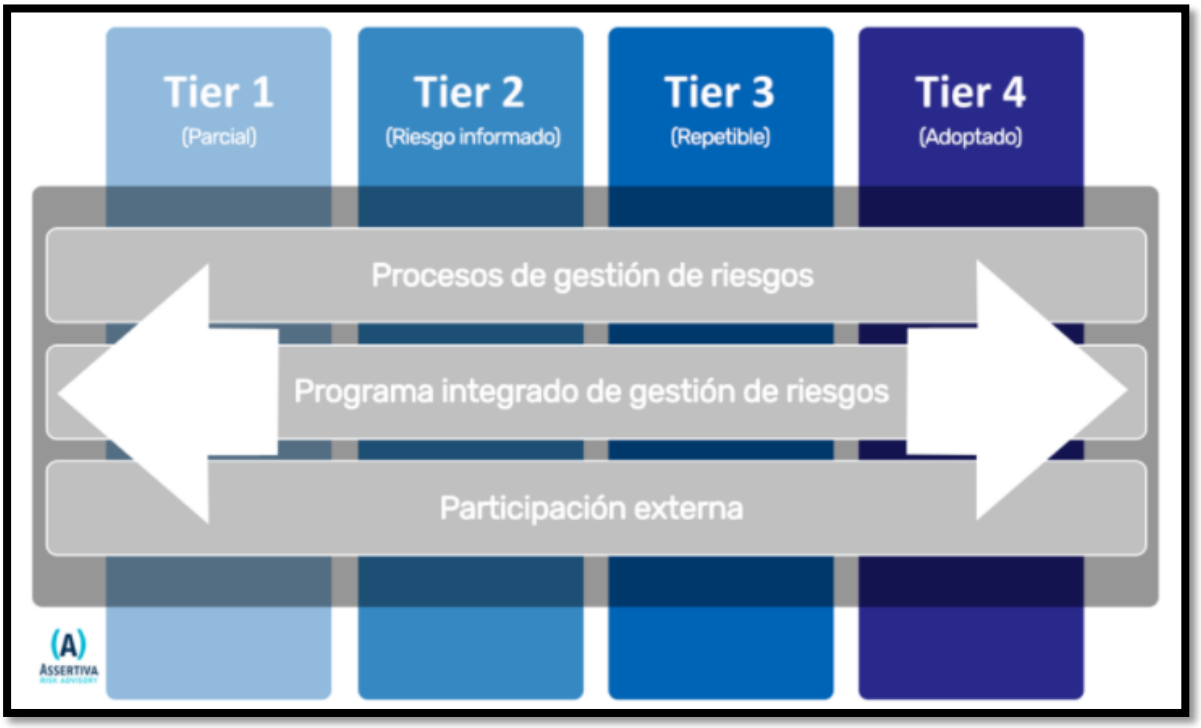
- Niveles de implementación

Los niveles proporcionan un contexto sobre cómo una organización ve el riesgo cibernético y su tratamiento para ello establecen un avance desde respuestas informales y reactivas hasta soluciones que sean ágiles y que se encuentren informados oportunamente en base al riesgo. Estos cuatro niveles establecen la implementación de este marco desde su inicio como tratamos el riesgo esto depender mucho de cada organización como se encuentra en procesos, tecnología y personas. Según Urrutia (2019) menciona:

> Los niveles describen el grado en que las prácticas de gestión de riesgos de ciberseguridad de una organización exhiben las características definidas en el Marco. Los niveles van desde Parcial (Nivel 1) a Adaptativo (Nivel 4) y describen un grado cada vez mayor de rigor, y qué tan bien integradas están las decisiones de riesgo de ciberseguridad en decisiones de riesgo más amplias, y el grado en que la organización comparte y recibe información de ciberseguridad de fuentes externas. (p. 4).

Figura 11

Niveles NIST



Nota: Los Niveles definen cuál es el grado de rigor con el que las organizaciones adhieren al Framework NIST. De “Los niveles” por Nist, 2019 (https://www.nist.gov/)

La propuesta para realizar el empleo de la capacidad de Ciberdefensa está enfocada en base NIST en vista que es un marco orientado al ciberriesgo, pero debemos tener en cuenta que la diferencia entre ambos enfoques, que Ciberdefensa posee una capacidad que puede ser empleada solo con orden, esta capacidad es la capacidad de Respuesta viéndolo desde un enfoque ofensivo como operaciones militares en el ciberespacio. El marco NIST nos establecerá poder fortalecer las otras capacidades de Ciberdefensa.

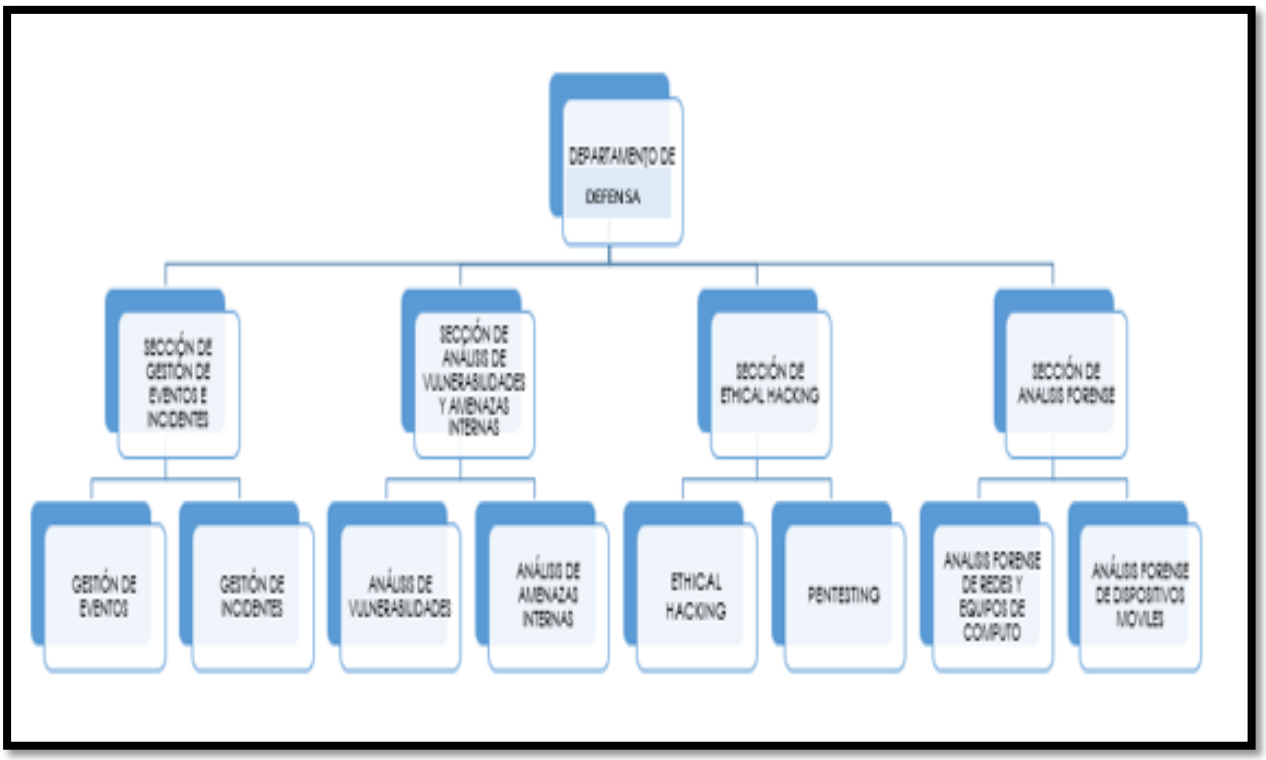
Asimismo, debemos tener en claro que en el ciberespacio es un dominio que puede ser empleado y tener efectos en los tres niveles de la guerra Estratégico, Operacional y en el Táctico. En el ciberespacio se converge distintas organizaciones de tipo estatales como privadas son estas las que van a influir en las operaciones en ciberespacio. El empleo técnicas y diferentes de vectores de ataque que se dan en el ciberespacio es cada vez más rápido siendo un ambiente donde los efectos pueden ser devastadores. En el ciberespacio es representado tres capas: la capa física, Capa lógica, la capa social.

Articulación Departamento de defensa CECIBER

La articulación dentro del departamento de defensa se llevará a cabo de la siguiente manera, definiendo la estructura organizacional:

Figura 12

Estructura organización Departamento defensa ciberdefensa



Gestión de eventos e incidentes.

Supervisar la gestión de eventos e incidentes de los sistemas de información a fin de ejecutar operaciones militares de defensa oportunas. Determinar, identificar y analizar los eventos e incidentes a fin de ejecutar operaciones militares. El proceso de la sección de gestión de eventos e incidentes, se realiza bajo la dirección del jefe del departamento de protección, quien formula e identifica las brechas entre lo planificado y ejecutado, sus principales causas y posibles acciones correctivas, así como proponer e impulsar el correcto proceso de gestión de eventos e incidentes.

Análisis de vulnerabilidades y amenazas internas

Diagnosticar, identificar y analizar las amenazas y vulnerabilidades a fin de ejecutar operaciones militares designados por el escalón superior. El proceso de la sección de análisis de vulnerabilidades se lleva bajo la dirección del jefe Departamento de Protección, quien apoyado de su sección de gestión de eventos e incidentes realizan la identificación, priorización y defensa de las vulnerabilidades y amenazas a los objetivos designados por el Escalón Superior.

Ethical hacking y pentesting

Búsqueda y explotación de vulnerabilidades de seguridad en sistemas y redes lo más importante es remarcar que el hacking consiste tanto en la búsqueda como en la explotación de esas vulnerabilidades. pentesting sería el testing de un sistema, red o aplicación web con el objetivo de encontrar vulnerabilidades de seguridad que un atacante podría explotar.

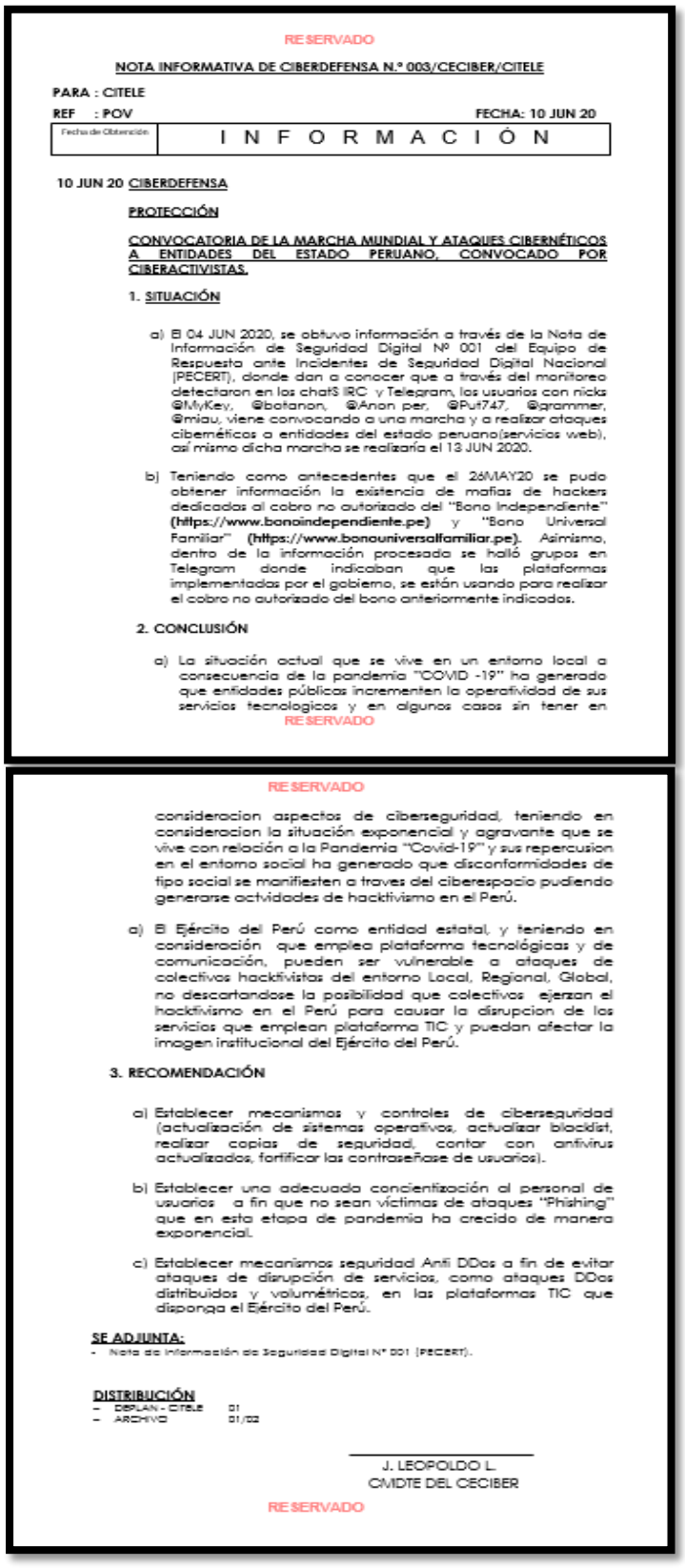
Análisis forense

Se centra más en encontrar, aislar y buscar los motivos que llevaron al atacante a elegir ese objetivo, El principal objetivo de la metodología militar es aislar la causa del incidente, recuperar el sistema y establecer las medidas oportunas para que dicho incidente no se pueda repetir, revisando las directivas de respuesta y actuación.

Para la articulación de la información de ciberdefensa procesada se llevará a cabo del siguiente documento denominado Nota Informativa de Ciberdefensa (NIC) de acuerdo al siguiente detalle:

Figura 13

Nota informativa de Ciberdefensa



RESERVADO

NOTA INFORMATIVA DE CIBERDEFENSA N.° 003/CECIBER/CITELE

PARA : CITELE

REF : POV FECHA: 10 JUN 20

Fecha de Obtención	I N F O R M A C I Ó N

10 JUN 20 CIBERDEFENSA

PROTECCIÓN

CONVOCATORIA DE LA MARCHA MUNDIAL Y ATAQUES CIBERNÉTICOS A ENTIDADES DEL ESTADO PERUANO, CONVOCADO POR CIBERACTIVISTAS.

1. SITUACIÓN

a) El 04 JUN 2020, se obtuvo información a través de la Nota de Información de Seguridad Digital Nº 001 del Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional (PECERT), donde dan a conocer que a través del monitoreo detectaron en los chat$ IRC y Telegram, los usuarios con nicks @MyKey, @botanon, @Anon per, @Put747, @grammer, @miau, viene convocando a una marcha y a realizar ataques cibernéticos a entidades del estado peruano(servicios web), así mismo dicha marcha se realizaría el 13 JUN 2020.

b) Teniendo como antecedentes que el 26MAY20 se pudo obtener información la existencia de mafias de hackers dedicados al cobro no autorizado del "Bono Independiente" **(https://www.bonoindependiente.pe)** y "Bono Universal Familiar" **(https://www.bonauniversalfamiliar.pe)**. Asimismo, dentro de la información procesada se halló grupos en Telegram donde indicaban que las plataformas implementadas por el gobierno, se están usando para realizar el cobro no autorizado del bono anteriormente indicados.

2. CONCLUSIÓN

a) La situación actual que se vive en un entorno local a consecuencia de la pandemia "COVID -19" ha generado que entidades públicas incrementen la operatividad de sus servicios tecnologicos y en algunos casos sin tener en

RESERVADO

RESERVADO

consideracion aspectos de ciberseguridad, teniendo en consideracion la situación exponencial y agravante que se vive con relación a la Pandemia "Covid-19" y sus repercusion en el entorno social ha generado que disconformidades de tipo social se manifiesten a traves del ciberespacio pudiendo generarse actvidades de hacktivismo en el Perú.

a) El Ejército del Perú como entidad estatal, y teniendo en consideración que emplea plataforma tecnológicas y de comunicación, pueden ser vulnerable a ataques de colectivos hacktivistas del entorno Local, Regional, Global, no descartandose la posibilidad que colectivos ejerzan el hacktivismo en el Perú para causar la disrupcion de los servicios que emplean plataforma TIC y puedan afectar la imagen institucional del Ejército del Perú.

3. RECOMENDACIÓN

a) Establecer mecanismos y controles de ciberseguridad (actualización de sistemas operativos, actualizar blacklist, realizar copias de seguridad, contar con antivirus actualizados, fortificar las contraseñase de usuarios).

b) Establecer una adecuada concientización al personal de usuarios a fin que no sean victimas de ataques "Phishing" que en esta etapa de pandemia ha crecido de manera exponencial.

c) Establecer mecanismos seguridad Anti DDos a fin de evitar ataques de disrupción de servicios, como ataques DDos distribuidos y volumétricos, en las plataformas TIC que disponga el Ejército del Perú.

SE ADJUNTA:
- Nota de Información de Seguridad Digital N° 001 (PECERT).

DISTRIBUCIÓN
- DIPLAN - CITELE 01
- ARCHIVO 01/02

J. LEOPOLDO L.
CMDTE DEL CECIBER

RESERVADO

2.3.2.2.2 Planeamiento operaciones Ciberdefensa Ofensivas

Referente a las operaciones ofensivas, serán conducidas a través del COCID y ejecutadas por sus fuerzas, debemos tener en claro que las operaciones ofensivas solo se ejecutaran con orden, debiendo entenderse que para ello que los efectos serán sobre (sistemas de armas, C2, sistemas de comunicaciones, etc.) sin embargo las experiencias recientes han establecido un enfoque de guerra de nueva generación donde el empleo de la cibernética cobra relevancia, realizándose a través de ella acciones de ciberespionaje, cibersabotaje, desinformación y propaganda en un escenario de lo que sería una guerra híbrida. Esta guerra de nueva generación no solo va enfocado a objetivos militares sino también a civiles (infraestructuras críticas, servicios informáticos privados).

Como antecedentes tenemos ataques masivos de denegación de servicio, en simultaneidad campañas de desinformación que Rusia empleo contra Estonia en el año 2007 así como Georgia y Kirguistán en los siguientes años.

En lo que refiere a una ofensiva en el ciberespacio, se pueden llevar las siguientes acciones:

- Activación de malware, para ello como un requerimiento primordial se debe realizar una ciberinteligencia sobre los objetivos establecidos a fin identificar sus vulnerabilidades, explotar tener un C2 posicionarlo en la infraestructura objetivo hasta la realización de acción ofensiva pudiendo ser cibersabotaje, ciberespionaje.

- Empleo ciberataques masivos DDoS contra sitios web, con la finalidad de neutralizar los servicios de un objetivo. El realizar este tipo de ataque ocasiona que tanto usuarios y operadores no puedas utilizar los servicios tecnológicos y/o esenciales y traer consigo un efecto de caos y afectación moral de los integrantes de los objetivos.

- Ciberataques masivos en infraestructuras críticas y servicios esenciales, el empleo de diferentes malware, rasonware, botnet con la finalidad de destruir, neutralizar las infraestructuras y con ello traer un ambiente caótico sobre el adversario que será beneficio para las operaciones militares terrestres.

- Defacements masivos en sitios oficiales del objetivo. El realizar este ataque sobre sitios oficiales coloca de manifiesto la inseguridad que se tiene, así como la afectación a la reputación, siendo esto apreciado por diferentes usuarios, personas externas e internas al objetivo.

- Campañas de phishing, Tienen la finalidad de establecer sobre los usuarios de diferentes entidades el engaño, para así obtener credenciales de servicios bancarios, sociales y de diferentes instituciones, a través de estas campañas se puede realizar el ciberespionaje.

- Campañas de suplantación de identidad en redes sociales, tienen como objetivo desinformar sobre las intenciones del objetivo, así como manipular a los espectadores internos y externos, sabiendo que las redes sociales tienen un alcance global.

- Distribución de malware altamente sofisticado, la distribución de estos malware (rasomware, exploit, troyanos) tienen el propósito de infectar toda infraestructura tecnología de un objetivo, para así neutralizarlo y/o destruirlo y establecer una siguiente fase operaciones militares terrestre.

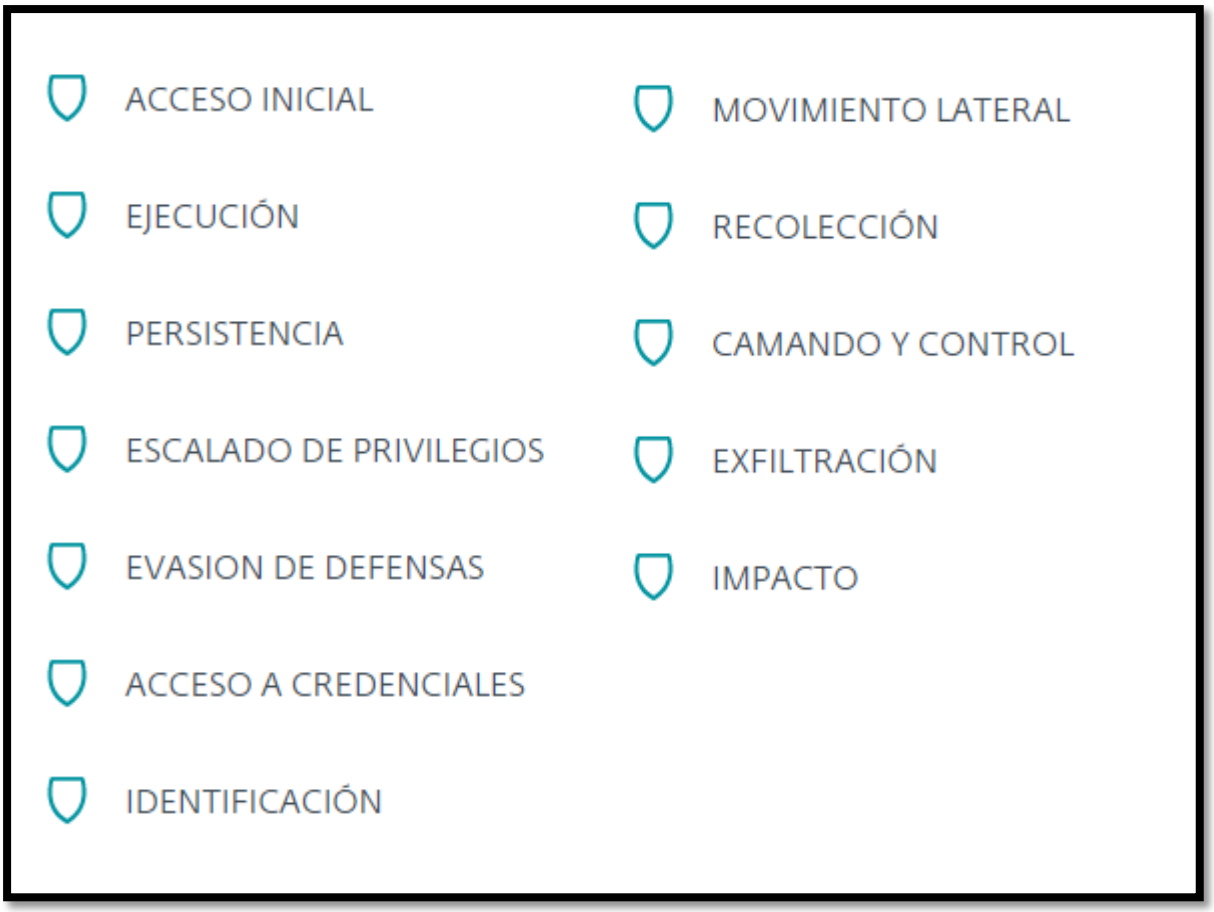
- Campañas de desinformación y propaganda, el realizar estas acciones debe conllevar a que sean potentes y que tengan un impacto sobre los usuarios, personas, entorno del ambiente operacional y que se generan a través de estas las condiciones necesarias para operaciones militares posteriores.

Podemos establecer condiciones necesarias que conlleven a obtener una supremacía en el ciberespacio con la consideración que las ciberoperaciones ofensivas se ejecután con la finalidad de comprometer la confidencialidad, integridad y disponibilidad de la información y operaciones del adversario. obteniendo efectos temporales o permanentes, para facilitar las operaciones militares ha ejecutarse en el teatro de operaciones. El manual de operaciones ciberneticas de Estados Unidos (2018) “Los ataques al ciberespacio son acciones de ataque en el ciberespacio crean efectos de negación notables (es decir, degradación, interrupción o destrucción) en el ciberespacio o manipulación que conduce ha efectos de negación en los dominios físicos” (p. 67).

Para la ejecucion de estas operaciones se llevan acabo a traves de las siguientes fases:

Figura 14

Etapas ofensiva ciberdefensa



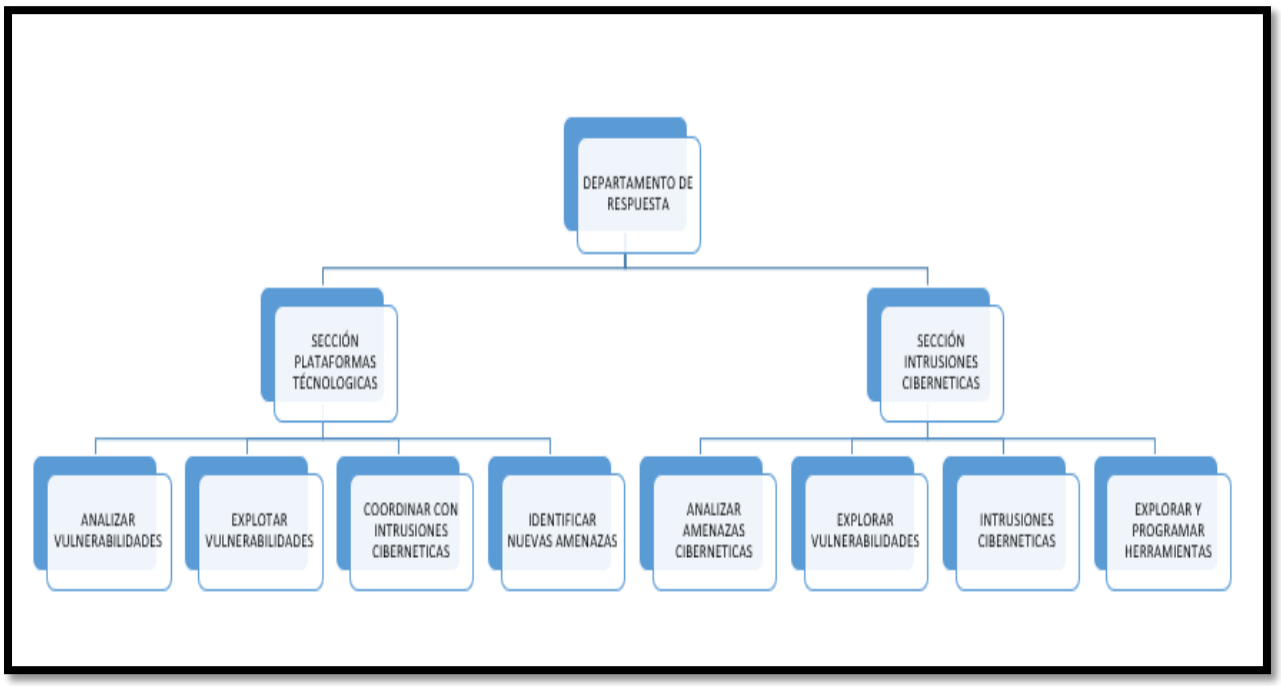
Nota: Etapas de la ofensiva investigación realizada Mitre Att&ck. De “Mitre”, por Welivesecurity, 2019 (https://www.welivesecurity.com/la-es/2019/06/06/como-utilizar-mitre-attck-repositorio-tecnicas-procedimientos-ataques-defensas/)

En el CECIBER en el departamento de respuesta, reflejado en la parte ofensiva de la ciberdefensa carece de un procedimiento para realizar estas acciones a través de las diferentes tareas tácticas, en base a la investigación realizada sea podido diseñar el siguiente procedimiento:

Figura 15

Estructura organización Departamento respuesta ciberdefensa

La figura N° 15 refleja que para ejecución de operaciones de respuesta sea



establecido dentro del departamento de respuesta dos (02) secciones la primera; plataformas tecnológicas que hacer referencia al análisis de vulnerabilidades, empleando para ello diferentes herramientas de análisis como Nmap, Acunetix, Greenbon, etc. Asimismo, dentro de la sección de intrusiones cibernéticas realizaría actividades de analizar amenazas cibernéticas, explorar vulnerabilidades, realizar intrusiones cibernéticas y explorar y desarrollar herramientas. Debiéndose articular de la siguiente manera:

Plataforma Tecnológica

Analizar, explotar e identificar las amenazas, vulnerabilidades e intrusiones. Coordinar con la sección de intrusiones cibernéticas a fin de ejecutar operaciones militares de respuesta oportunas. El proceso de la sección de plataforma tecnológica, se realiza bajo la dirección del jefe del departamento de respuesta, quien formula e identifica las brechas entre lo planificado y ejecutado, sus principales causas y posibles acciones correctivas, así como proponer e impulsar el correcto proceso de plataforma tecnológica.

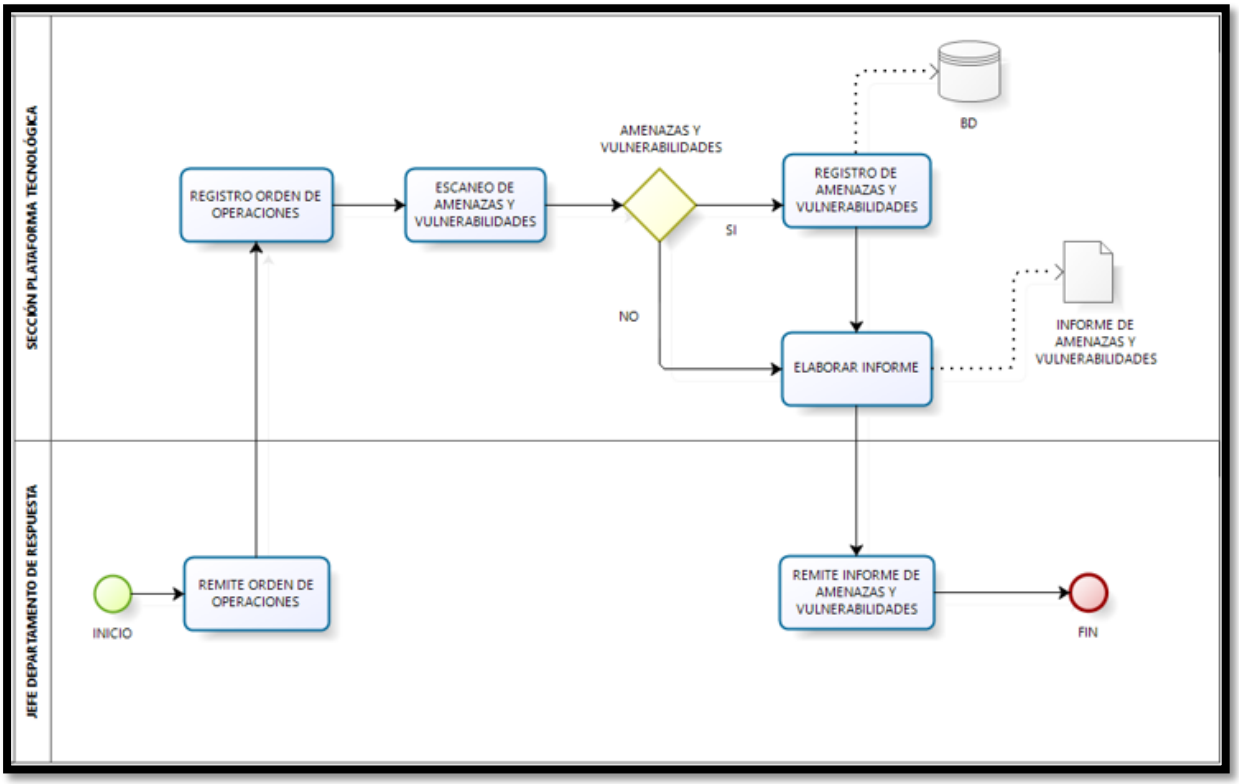
- **Analizar vulnerabilidades y amenazas de las plataformas tecnológicas (SCADA, PLC's, S.O)**

  Analizar los sistemas tecnológicos a fin determinar las vulnerabilidades que posea dichas plataformas tecnológicas. Corresponde al proceso de Analizar

Vulnerabilidades de las Plataformas Tecnológicas (SCADA, PLC's, S.O), llevado a cabo por la sección de plataformas tecnológicas, que inicia con una orden de operaciones de ciberdefensa y culmina con la remisión del informe de operaciones de ciberdefensa.

Figura 16

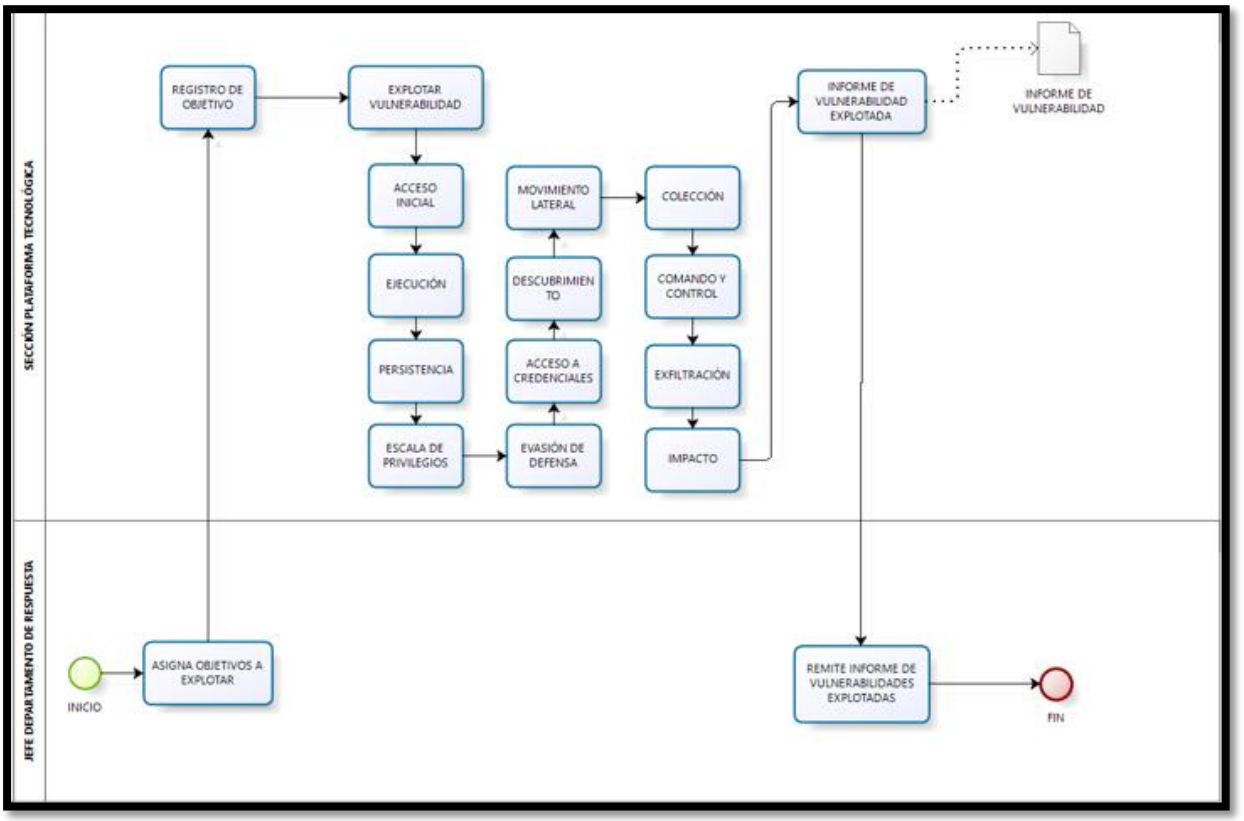
Procedimiento Analizar vulnerabilidades y amenazas



- **Explotar las vulnerabilidades de los dispositivos de seguridad perimetral de red**
  Dirigir, realizar y coordinar el proceso de explotación de las vulnerabilidades de los dispositivos de seguridad perimetral de red corresponde al proceso de explotar vulnerabilidades de los dispositivos de seguridad perimetral de red, llevado a cabo por la sección de plataforma tecnológica, inicia con el jefe del departamento de respuesta asignado el objetivo a explotar y termina con la remisión del informe de vulnerabilidades explotadas.

Figura 17

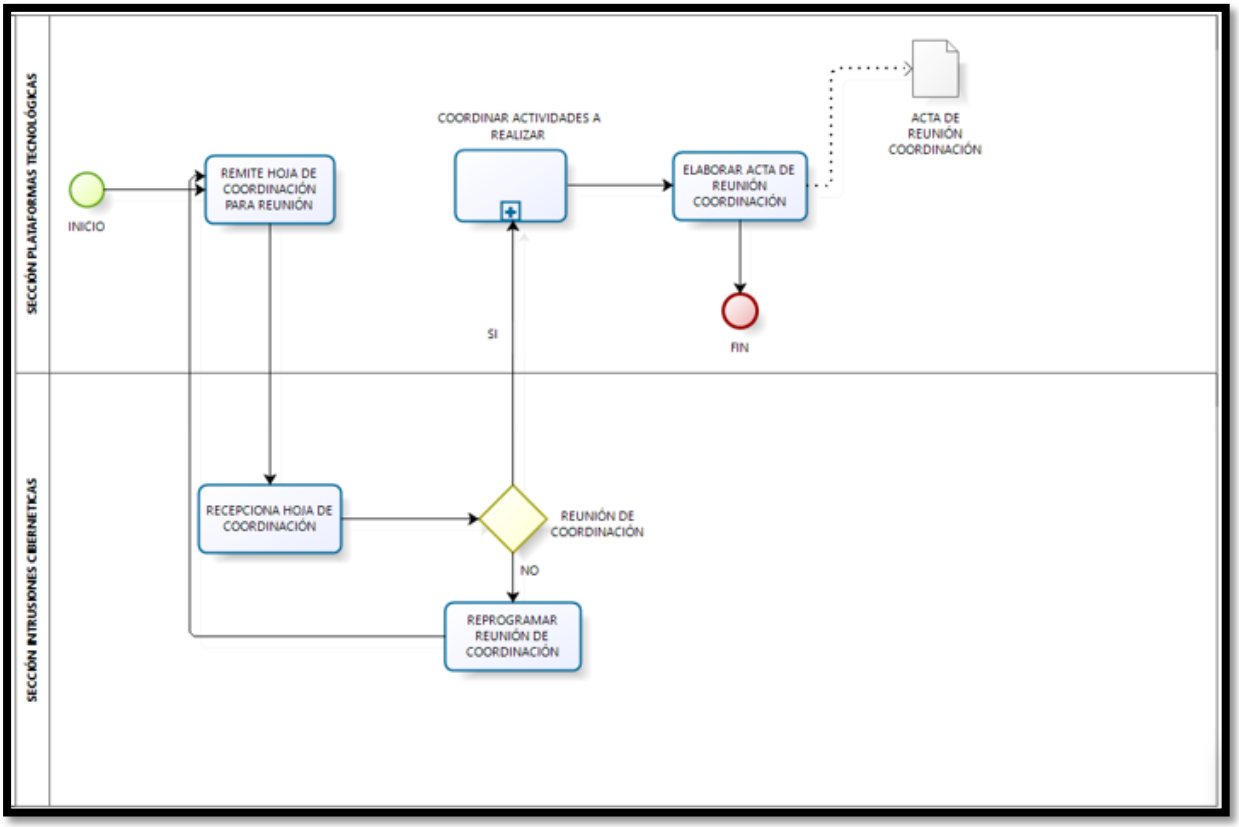
Explotar las vulnerabilidades de los dispositivos



-
- **Coordinar con la sección de intrusiones cibernéticas a fin de ejecutar operaciones militares de respuesta oportunas.**
  Corresponde al proceso de coordinación con la sección de intrusión para realizar operaciones militares de respuesta, llevado a cabo por la sección de plataformas tecnológicas, inicia con la remisión de la hoja de coordinación para realizar la reunión de coordinación con la sección de intrusiones cibernéticas y culmina con el acta de las actividades a realizar.

Figura 18

Coordinar con la sección de intrusiones cibernética

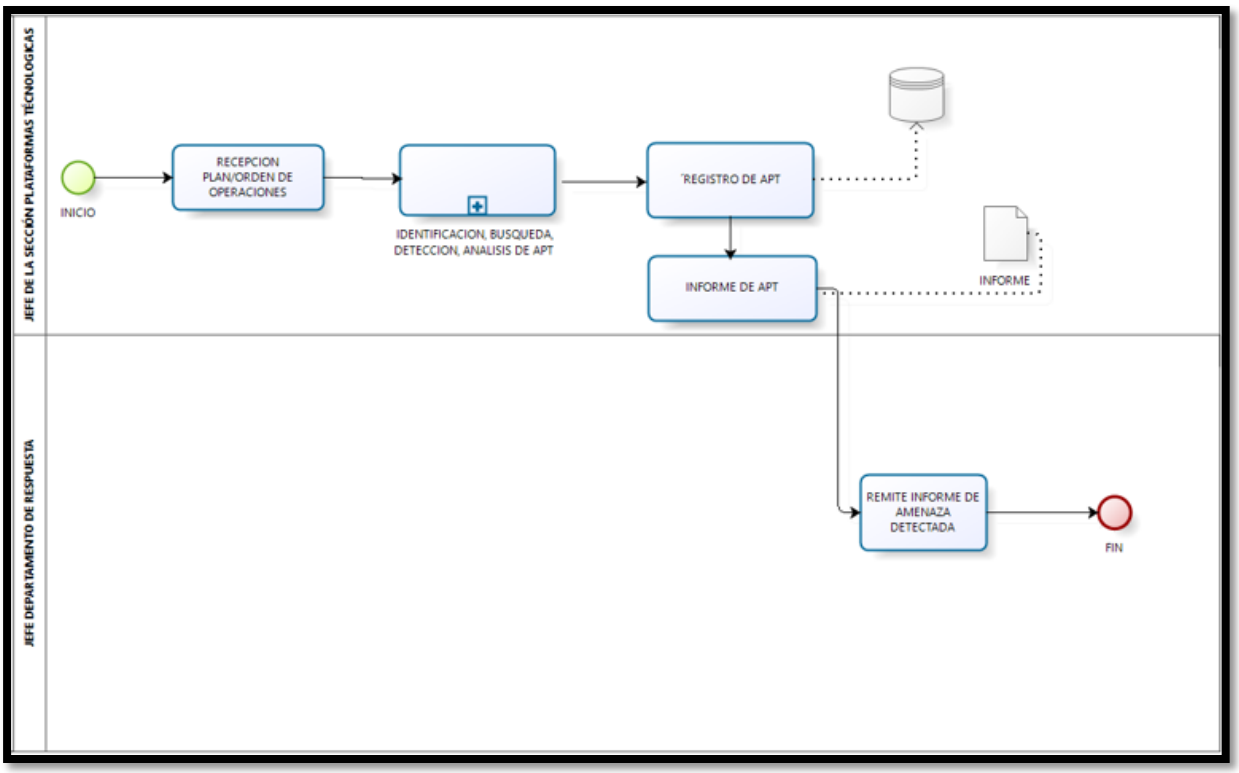


- **Identificar nuevas amenazas avanzadas persistentes en el ciberespacio sobre plataformas tecnológicas**.

  Dirigir y realizar el proceso de identificación de nuevas amenazas en el ciberespacio sobre plataformas tecnológicas. Corresponde al proceso de identificar nuevas amenazas avanzadas en el ciberespacio que afecten las plataformas tecnológicas, este procedimiento es llevado a cabo por la sección de plataforma tecnológica, que inicia con la recepción del plan/orden de operaciones y termina remitiendo el informe de operaciones de amenazas avanzadas detectadas al jefe del departamento de respuesta.

Figura 19

Identificar nuevas amenazas avanzadas persistentes (APT)



Intrusiones Cibernéticas

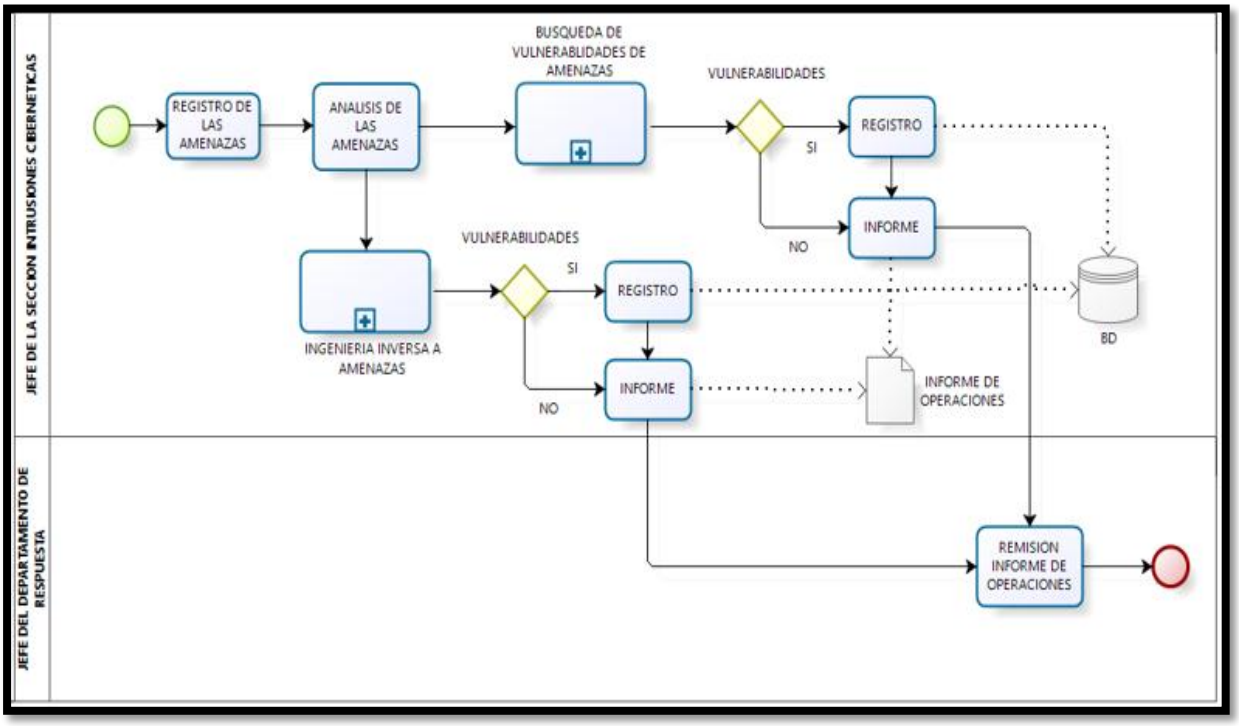
Explorar, analizar y explotar las vulnerabilidades de objetivos designados por el escalón superior**.** El proceso de conducción de la sección de intrusiones cibernéticas se encuentra bajo la dirección del jefe departamento de respuesta, quien apoyado de su sección de intrusiones cibernéticas realiza la intrusión a los objetivos designados por el Escalón Superior.

- **Analizar las amenazas cibernéticas**

  Es el estudio y estrategia de seguridad para destruir y degradar las amenazas cibernéticas, las plataformas digitales y objetivos designados por el comando, inicia con la identificación de las amenazas y culmina con la elaboración del informe de operaciones de ciberdefensa.

Figura 20

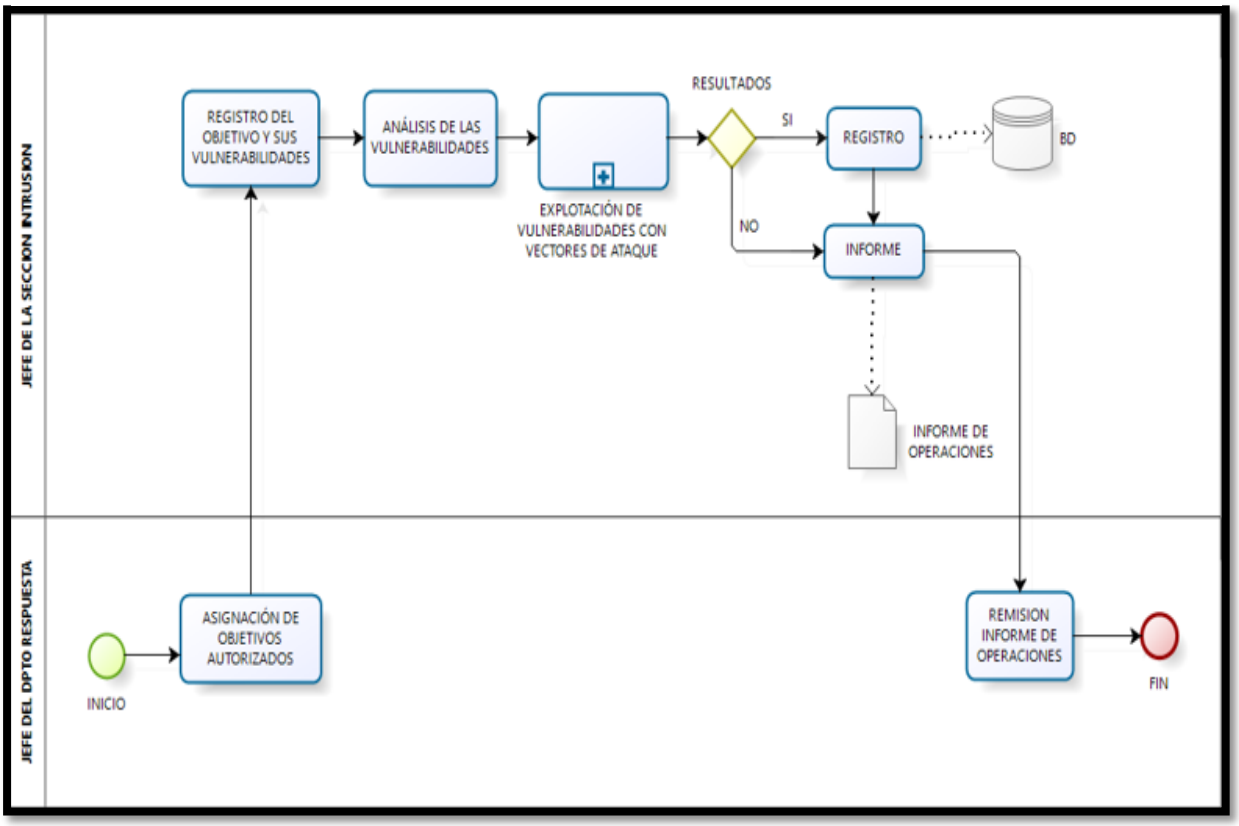
Analizar las amenazas cibernéticas



- **Explotar las vulnerabilidades sobre los objetivos autorizados**
  Explotar vulnerabilidades de los objetivos autorizados con la finalidad de cumplir con la misión asignada. Asimismo, el software y/o hardware que utilizan los objetivos autorizados por el Escalón Superior.

Figura 21

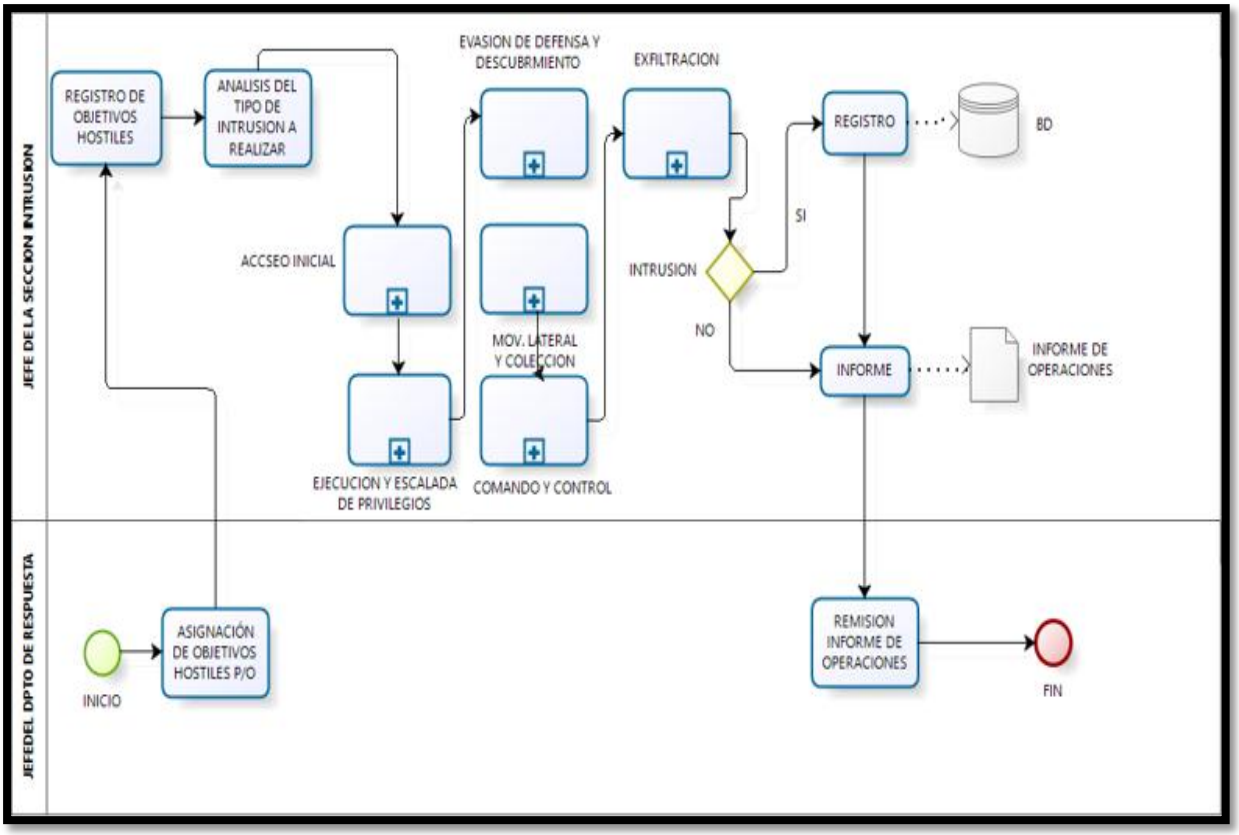
Explotar las vulnerabilidades sobre los objetivos autorizado



- **Realizar intrusiones cibernéticas para degradar o destruir objetivos hostiles**
  Destruir o neutralizar sistemas informáticos de los objetivos designados por el escalón superior, Denegar o suspender los servicios de las plataformas digitales del enemigo.

Figura 22

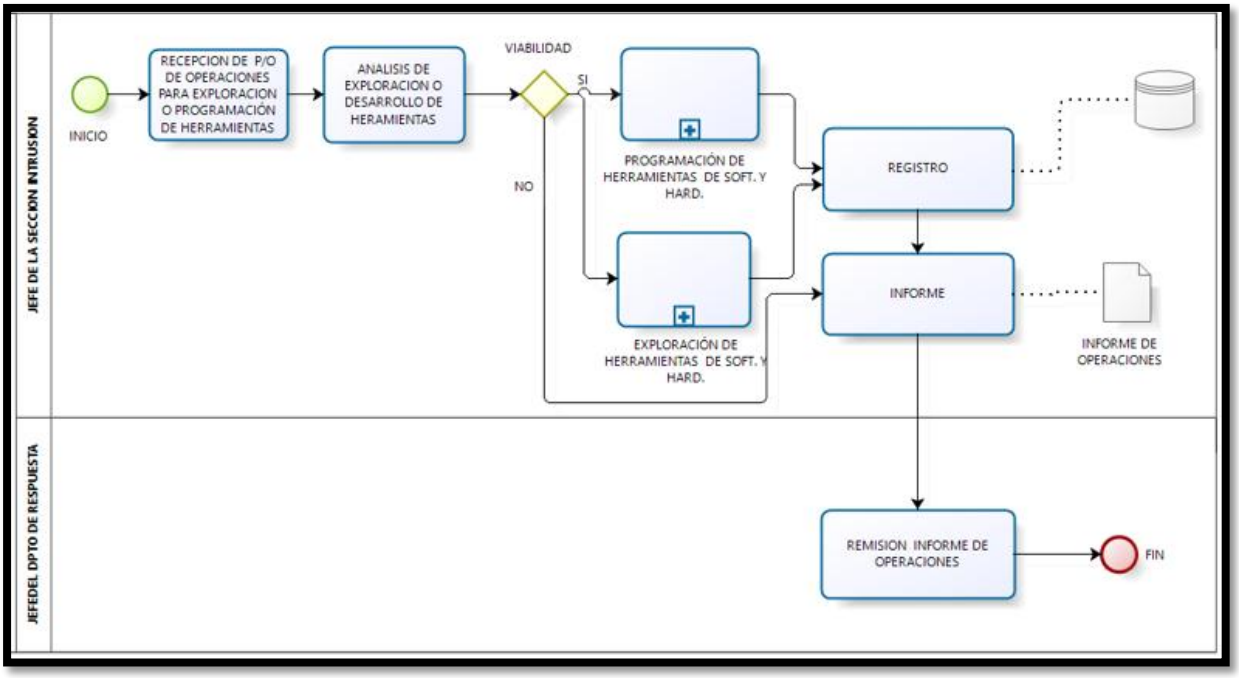
Realizar intrusiones cibernética



- **Explorar y desarrollar herramientas de software y hardware ofensivas**
  Investigar para el desarrollo de hardware y software como vectores de ataque, se debe tener el conocimiento y potencial para el desarrollo nuevas tecnologías.

Figura 23

Explorar y desarrollar herramientas de software y hardware ofensivas



Empleo de la capacidad de Ciberdefensa en el Ejército del Perú

En el Perú y específicamente en las fuerzas armadas se vienen realizando los esfuerzos para sacar adelante un empleo adecuado de la ciberdefensa en operaciones militares teniendo como marcos legal D.L N° 30999 para ello se crea el Comando Operacional de Ciberdefensa con Resolución Ministerial N° 0388-2019 DE/CCFFAA de fecha 25 de marzo del 2019, el cual tiene como misión: “Planear, organizar, dirigir y conducir operaciones militares conjuntas de ciberdefensa en el ciberespacio, ejerciendo el comando y control de las operaciones de ciberdefensa”. Alineado a fortalecer la capacidad de ciberdefensa el 30 de octubre del 2018 se crea el Comando de Ciberdefensa del Ejército (COCIBER) dentro del Ejército del Perú, siendo a partir de la fecha una preocupación para el comando del Ejército del Perú establecer nuevos lineamientos en esta nueva capacidad de ámbito global, la problemática que enfrenta la capacidad de ciberdefensa es la carencia de una doctrina, su empleo limitado es debido a la falta de personal, tecnología y procedimientos adecuados, sin embargo el CECIBER se empleado en actividades de ciberseguridad frente a los juegos panamericanos Lima 2019 teniendo como misión un monitoreo continuo de amenazas que afecten a dichos juegos, en el año 2020 se estable el CSIRT del Ejército del Perú que tienes como responsabilidad de establecer un equipo para respuesta ante incidentes informáticos, participando de manera efectiva durante las Elecciones Congresales del año 2019, las

capacidades que posee el CECIBER son limitados, esta investigación va reflejado a ello el poder establecer una propuesta del empleo de las capacidades alineados a buenas prácticas de marcos de trabajo como es el caso de NIST. Asimismo, como entidad militar debemos conocer nuestras amenazas cibernéticas entendiendo que el Perú recibe ataques cibernéticos sean estos a través de diferentes vectores de ataques malware, rasonware, pishing explotación de diferentes vulnerabilidades con zero-day, que se expenden en la Dark Web para ello la hemos establecido en las siguientes categorías:

Las amenazas cibernéticas

Hoy en día, nos encontramos en una articulación de sistemas tecnológicos sinérgicos de manera global. Las amenazas cibernéticas han aumentado a un ritmo exponencial e increíble. En este contexto, la ciberdefensa juega un papel prioritario frente a los distintos actores, creando un eje básico del poder militar, proponiendo una visión que garantice las capacidades de ciberdefensa del país, y la quinta guerra. En este contexto, la convergencia tecnológica ha incrementado, entre otras cosas, el nivel nacional de riesgo cibernético. En este contexto, nos enfrentamos a una serie de desafíos que requieren una fuerte dependencia técnica. Esto abre escenarios oportunistas, pero se vuelve complejo y difícil frente al rápido crecimiento exponencial de las amenazas cibernéticas y las vulnerabilidades.

Amenazas estatales

Como amenazas estatales tenemos a las actividades que realizan los estados a través de sus fuerzas militares o grupos anónimos avalados por los estados empleando personal especialista en ofensiva de seguridad para irrumpir sistemas, sabotear, así como realizar espionaje por organismos de inteligencia los estados hoy en día acrecientan sus capacidades de ciberdefensa empleando software avanzados, así como hacker una de las características de estas amenazas es que son anónimas, en vista que no se pueden identificar la ubicación. Son muchas las motivaciones para este tipo de amenazas pueden ser sus intereses nacionales, o convicciones policías en una región para ello emplean gran cantidad de presupuesto.

Amenazas ciberterrorismo

Las amenazas terroristas emplean softwares especiales, malwares, redes botnet, firmas irreconocibles, para cumplir con sus terroristas por ello las agencias de inteligencia coloca al terrorismo cibernético como el delito más poderoso para el año 2030;

Amenazas hacktivismo

Es una amenaza que se viene llevando potencialmente empleando las redes sociales, donde se comparte información de hacking para compartir conocimiento y generar una tendencia y su accionar sea puesta de manifiesto empleando el ciberespacio.

Amenazas ciberdelincuencia

Constituye actualidad una amenaza, y cada vez más usuarios están conectados a Internet a través de equipos portátiles, smartphones y tablets. El ciberdelito ve ello como algo rentable para sus propósitos.

2.3.2.3 Acciones militares de Ciberdefensa en los Activos Críticos Nacionales

Están a cargo del CCFFAA, cuando la capacidad de protección de sus operadores y/o del sector responsable y de la DINI sea sobrepasada, teniendo como base legal DS N° 007-2019 Directiva Nacional de Seguridad y Defensa Nacional para la Protección de los ACN, estableciendo que el MINDEF es el responsable de la protección de los ACN a partir de un tercer momento, a través del CCFFAA y de las IIAA teniendo en consideración que los ACN son aquellos que son el soporte de una nación ya que de ser afectados pondrían en peligro la estabilidad de dicho estado según el D.S N° 106-2017 menciona que son todos aquellos recursos, infraestructuras y sistemas que son importantes e imprescindibles para desarrollar, mantener y continuar con las capacidades que cuenta un estado (Presidencia de Consejo de Ministros, 2017). Asimismo, las siguientes consideraciones son importantes:

- Entiéndase por Ciberdefensa a la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional. Asimismo, la Ciberdefensa es el uso de conocimiento, habilidades y medios para realizar operaciones en y mediante el ciberespacio a fin de asegurar su empleo por las fuerzas propias.

- Entiéndase como seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

- En la R.M N° 360-2009-PCM - Art N° 04, establece que:
  Cada Ministerio a través de su unidad de seguridad de la información, creará una coordinadora de respuestas a emergencias en redes informáticas la cual coordinará con la PECERT (Presidencia de Consejo de Ministros, 2009).

- El CCFFAA dispone la creación del CSIRT en el Ejército del Perú, para promover la coordinación entre las FF. AA de prevención, detección, manejo, recopilación de información y desarrollo de soluciones para los incidentes de ciberseguridad.

- El CITELE, por ser la unidad rectora de Ciberdefensa dentro del Ejército del Perú, dispone de las capacidades humanas y tecnológicas en ciberdefensa y ciberseguridad para cumplir con el misionamiento asignado por el Escalón Superior.

- El CSIRT CITELE EP, realizará operaciones en el ciberespacio para cumplir con su misionamiento, operando con su personal durante las 24 horas del día, el periodo que dure las operaciones.

para ello el Ejército del Perú dispondrá de un CSIRT permanente para dar una respuesta oportuna ante cualquier incidente que deberá estar integrado al PCERT del Perú para tener una articulación óptima frente a incidentes o ciberataques que ocasione disrupción de los servicios de los ACN, recursos claves u otras entidades que el COCIBER – CCFFAA establezca.

CSIRT – EP

La misión del CSIRT CITELE es:

Proporcionar una respuesta oportuna ante los incidentes de Seguridad Digital y Ciberdefensa apoyando a entidades del Estado, entidades consideradas activos críticos nacionales y recursos claves.

Alcance

CSIRT CITELE es una entidad que provee servicios de respuesta a incidentes de manera preventiva, proactiva y reactiva, los mismos que son proporcionados a los ACN o que el escalón superior establezca.

Miembros

Los miembros del CSIRT CITELE, tenemos miembros internos: Ciberdefensa y Telemática del Ejército (CITELE) y sus centros, miembros externos: CSIRT- CCFFAA, CSIRT- MGP, CSIRT – FAP) considere debe ser atendida por los servicios que ofrece CSIRT CITELE.

Cooperación

El CSIRT CITELE es autorizado por el Ejército del Perú y está afiliado a entidades del sector defensa a través del CSIRT - CCFFAA con el objetivo de colaborar y apoyar en Ciberdefensa y seguridad digital.

Políticas

- **Tipos de incidentes y niveles de soporte**

  CSIRT CITELE se ocupa de recibir, atender y procesar los eventos de seguridad cibernética, que ocurran en las entidades nacionales consideradas activos críticos nacionales o aquellas consideradas de interés nacional siendo la prioridad alta, ataques a infraestructuras de activos críticos nacionales, ataques al sector financiero, ataque de DDOS, en una prioridad intermedia tenemos, ataques cuentas de usuario, compromiso sistemas de escritorio y por último, suplantación de identidades y negación de servicio a cuentas individuales.

  El CSIRT CITELE comprende que existen diferencias en las experiencias en las entidades – ACN y mientras el CSIRT CITELE presente la información necesaria, proveerá asistencia a un nivel apropiado para cada entidad-ACN, el CSIRT CITELE realizará acciones bajo el alcance de situaciones escaladas.

  El CSIRT CITELE busca mantener informada de vulnerabilidades potenciales a los diferentes CSIRT de las FF. AA

Servicios

- **Evento e incidente**

  Se realiza la gestión de eventos e incidentes considerando la definición de evento e incidente según lo descrito:

Respuesta a incidentes

CSIRT CITELE apoyará a las entidades - ACN en el manejo de aspectos técnicos y organizacionales de los incidentes reportados a través de un formulario de incidentes.

Servicios Proactivos

- Auditorias
- Detección de intrusos

Servicios Reactivos

- Alertas
- Análisis de incidentes
- Análisis de vulnerabilidad
- Análisis forense

Investigación inicial de incidentes

- Investigar el incidente ocurrido
- Establecer alcance de incidente

Coordinación de incidentes

- Causas del incidente (vulnerabilidad)
- Analizar involucrados
- Reportes CSIRT

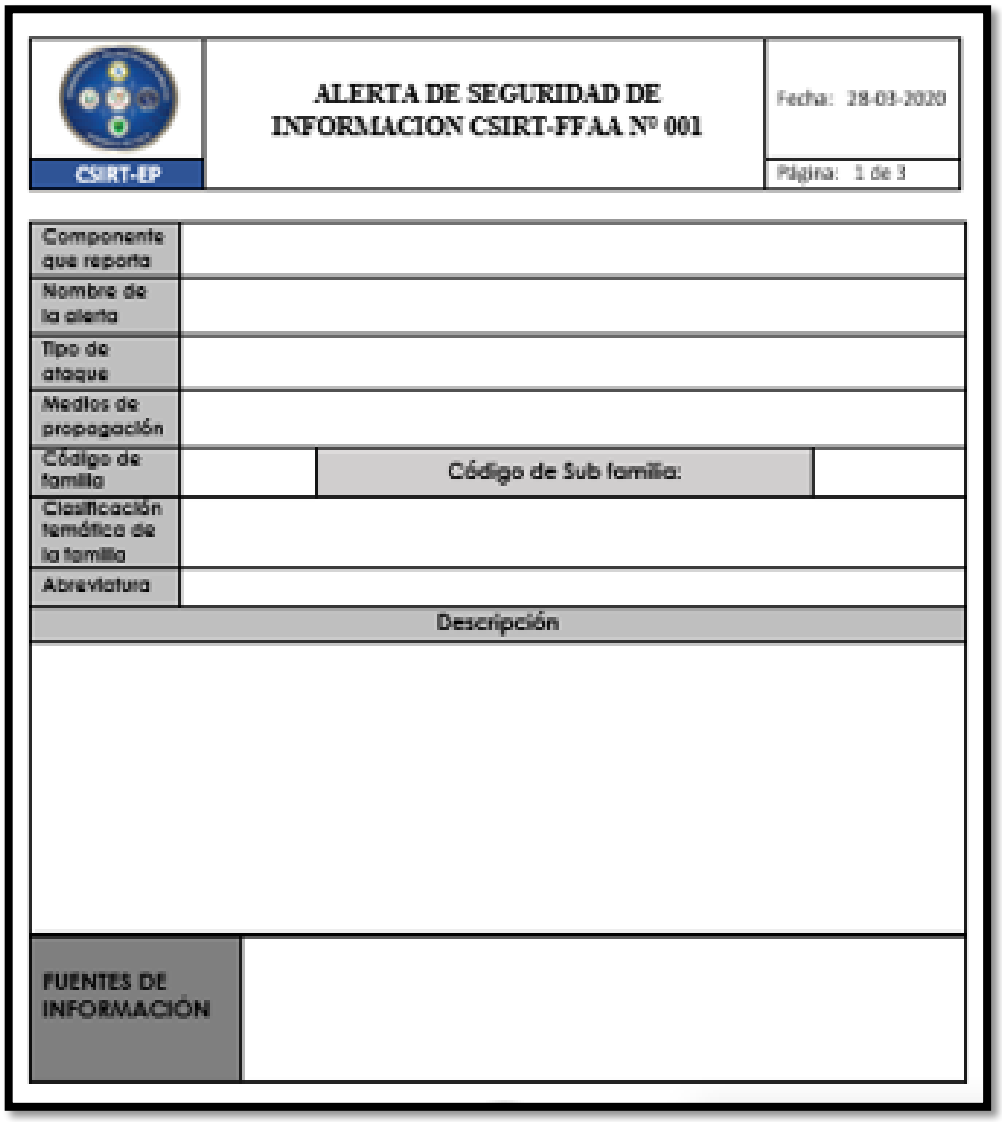
Resolución de incidentes

- Eliminar la vulnerabilidad
- Apoyo en el aseguramiento de sistemas derivados de lo aprendido en el incidente.
- Recolección de evidencias luego del hecho, observación de un incidente en progreso, plantando trampas al intruso, etc.
- Recolectar evidencia cuando se contemplen acciones judiciales, policiales, o acción disciplinaria dentro de la organización donde ocurre el evento.

Formulario de reporte de incidentes

Figura 24

Reporte de alertas



CSIRT-EP	ALERTA DE SEGURIDAD DE INFORMACION CSIRT-FFAA Nº 001	Fecha: 28-03-2020 Página: 1 de 3

Componente que reporta			
Nombre de la alerta			
Tipo de ataque			
Medios de propagación			
Código de familia		Código de Sub familia:	
Clasificación temática de la familia			
Abreviatura			
Descripción			
FUENTES DE INFORMACIÓN			

Nota: Alertas de seguridad de información CSIRT – FF. AA. De “Alertas de ciberdefensa”, por CSIRT - EP, 2019 CSIRT-EP

Catálogo de servicios del CSIRT CITELE

servicio reactivo y proactivo

- **Alertas, avisos y anuncios**

  Este servicio implica la difusión de información que describe un ataque de intrusos, vulnerabilidad de seguridad, alerta de intrusión, virus informático o engaño, y

proporciona cualquier curso de acción recomendado a corto plazo para tratar el problema resultante.

Proceso básico para alertas, avisos y anuncios.

Proceso siguiente para ser tenido en cuenta cuándo evaluamos alertas, avisos y anuncios:

- Colección de información: qué fuentes de información son utilizadas y evaluadas.
- Valoración de riesgo: información y su necesidad de fuentes para ser evaluado antes de que pueda ser enviado fuera dicha alerta u aviso o anuncio. El riesgo percibido a receptores será esencial en este proceso.
- Diseminación: la información importante necesitará ser diseminada a los receptores, utilizando un mecanismo de comunicación eficaz.
- Retroalimentación: los receptores que hacen con la información que reciben, ¿Qué tan eficaz es? ¿Qué lecciones pueden ser aprendidas?

Tipos

Pueden ser encontrados on-line:

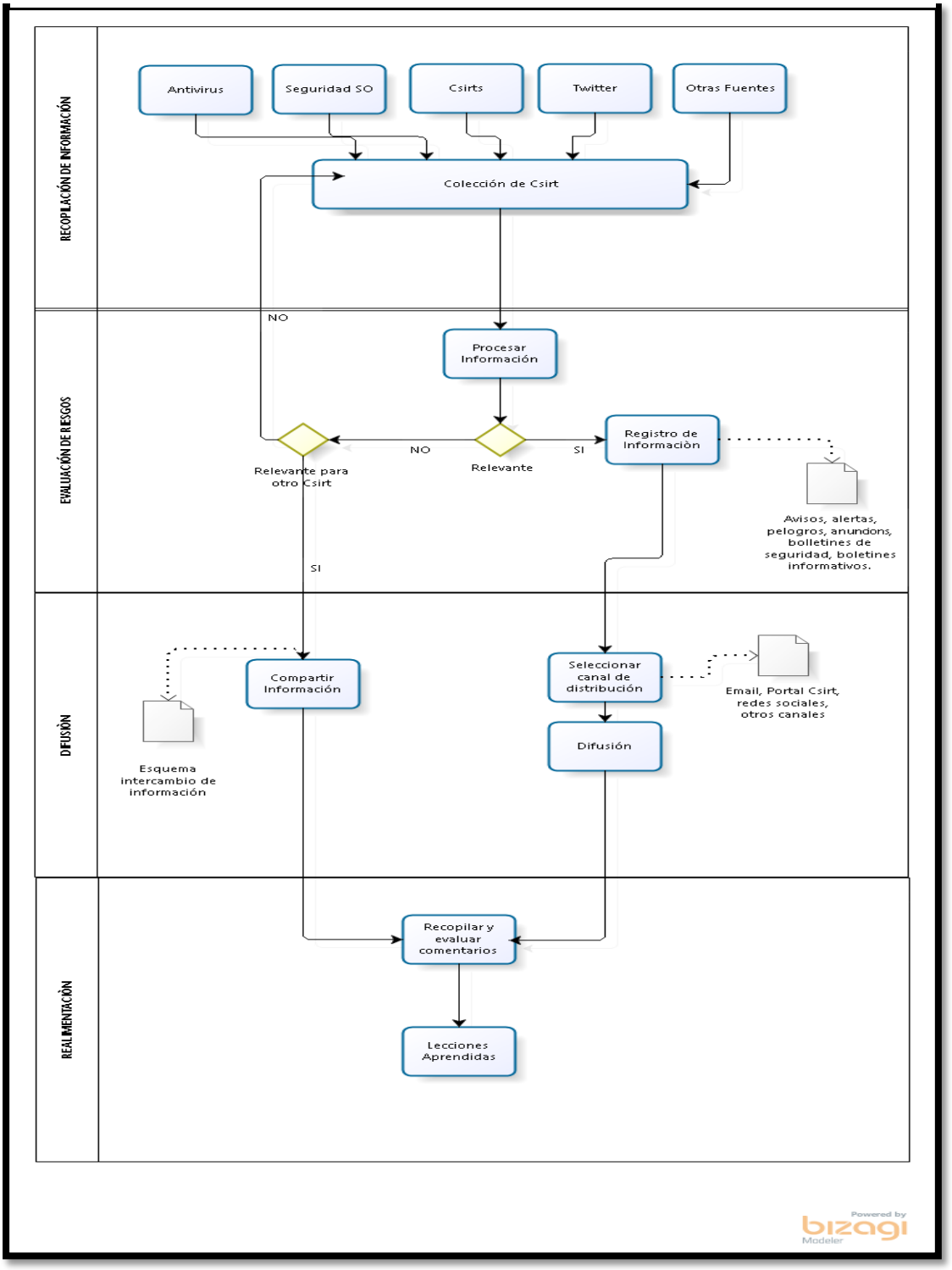
- Recomendaciones.
- Avisos.
- Alertas.
- Anuncios.
- Boletines de seguridad.

Los tipos son utilizados en ambos servicios tanto proactivos y reactivo. Por lo tanto, la clasificación a un proactivo o el servicio reactivo no es útil de identificar el tipo de alerta.

Proceso de alertas, avisos y anuncios

Figura 25

Proceso de alertas



Colección de la información

Alertas, avisos y anuncios todos dependen completamente en la colección de información útil de información buena y fuentes fiables. Cada CSIRT tiene la necesidad de escoger el tipo de información para recoger y las fuentes de aquella información.

Figura 26

Colección de la información

a. Escoger los tipos de canales de información: el CSIRT tiene que tener en cuenta que hay muchos canales electrónicos (incluyendo la web, email, twitter y otro on-line noticioso) pero también diarios, revistas y otros medios de comunicación como televisivos.

b. Listar todas las fuentes que se necesitan de los canales de información escogidos. Una lista parcial de fuentes incluye:

- Otro CSIRT boletines;
- Mailing Lista/foros (p. ej. fulldisclosure, bugtraq);
- Portales de seguridad (p. ej. thehackernews.com)

c. Evaluar las varias fuentes de información:

- Verifica identidad;
- Importancia de la fuente;
- Fiabilidad de la fuente;
- Uso de estándares/de formato de la comunicación;
- Uso de canales seguros.

El control que emerge fuentes de información

Otras fuentes emergentes de información incluyen twitter, redes sociales, IRC, pastebin, foros de Internet, etc. Estas fuentes han devenido muy populares.

Valoración del riesgo

Una vez las fuentes de información han sido listadas y valoradas, la información necesita ser individualmente evaluada para descubrir la pertinencia para el CSIRT, la importancia de informe si es urgente para actuar. Esta valoración es generalmente basada en los factores siguientes:

- La fuente del informe.
- La urgencia del informe.
- La valoración de riesgo inicial.
- La severidad en plazos de impacto potencial directo.
- La amenaza en plazos de la pérdida de reputación.

Estos factores se pueden tener en cuenta por introducir el concepto de valoración de riesgo. El riesgo es generalmente definido “la probabilidad multiplicada por el impacto”. Esto significa que el riesgo implicado con un acontecimiento seguro es la posibilidad que aquel acontecimiento ocurrirá, multiplicado por el impacto de aquel acontecimiento cuándo ocurre.

Diseminación

El paso final en crear alertas, avisos y los anuncios es para enviarles fuera a los receptores. Este proceso se denomina diseminación.

Potenciales receptores:

- CSIRT (CCFFAA, MGP, FAP)
- El mundo (CSIRT escoge hacer sus informes disponibles al público).

Para todos receptores, hay la necesidad de canales de diseminación eficaz para ser identificado. Esto puede variar de email y web-editoriales, a Twitter u otras redes sociales, RSS, pero también radiofónico, televisión o diarios.

Cada canal de diseminación tiene sus demandas propias.

Retroalimentación

Si la información ha sido compartida con un CSIRT es importante de pedir retroalimentación cuándo sea posible. Los trabajos de retroalimentación son para establecer las lecciones aprendidas y para implementar recomendaciones.

Criterios de retroalimentación:

- Tiempo de reacción a la información.
- Velocidad de diseminación.
- Relevancia para el receptor.
- Contenido de los informes (claridad, estructura, valoración de riesgo).
- Relevancia de la valoración de riesgo.

2.4 Definición de términos

Amenaza

Situación perjudicial que puede ocurrir y una vez ocurrida tiene consecuencias negativas. Si esta circunstancia se pueden dar factores externos al explotar una vulnerabilidad o debilidad de los sistemas informáticos de una organización afectando desde un impacto leve hasta muy alto y puede derivar en un incidente de seguridad.

Amenaza avanzada persistente (APT)

Es un tipo de ataque informático es una amenaza avanzada que utiliza técnicas de hackeo continuas, clandestinas y avanzadas para acceder a un sistema y permanecer allí durante un tiempo prolongado, con consecuencias potencialmente destructivas. (Karpesky, 2021)

Análisis de riesgos

Proceso que implica identificar los activos cibernéticos, sus vulnerabilidades, las amenazas tanto internas como externas las que están expuestos y el análisis de su potencial impacto para poder así determinar los controles adecuados para abordar el riesgo.

Ciberataque

Utilizan diversos vectores de ataque y vulnerabilidades de seguridad para realizar acciones con fines maliciosos, robar información, extorsionar al propietario o simplemente sabotear un sistema.

Ciberdelincuente

Personas que comprometen sistemas informáticos con la finalidad de robar, manipular o irrumpir dichos sistemas cibernéticos, poseen amplio conocimiento informáticos para alterar sistemas gubernamentales, corporativos teniendo efectos grave consecuencia para las organizaciones tanto en reputación como activos propios.

Acto Hostil

Ataque en o a través del ciberespacio contra la soberanía, los intereses nacionales, los activos críticos nacionales, recursos claves, así como contra los sistemas de información digital de los órganos ejecutores del Ministerio de Defensa, que da derecho a utilizar la fuerza en autodefensa, y demanda la formulación, aprobación e implementación de las reglas de enfrentamiento correspondientes.

Ciberarma

Toda capacidad, dispositivo o técnicas empleadas para afectar la infraestructura informática en el ámbito del ciberespacio, a la integridad, confidencialidad o disponibilidad de datos, y que su empleo puede generar perjuicio o daño de carácter personal o material.

Intención Hostil

Es la amenaza de un ataque en o a través del ciberespacio contra la soberanía, los intereses nacionales, los activos críticos nacionales, recursos claves, así como contra los sistemas de información digital de los órganos ejecutores del Ministerio de Defensa.

Uso de la Fuerza en Legítima Defensa

Es aquel que se produce sólo cuando los medios, recursos, o procedimientos que pueden ser empleados para prevenir o evitar un ataque se han agotado, no se encuentran disponibles, o se consideran insuficientes para defender la soberanía nacional, intereses nacionales y recursos claves, ante dichas circunstancias.

CSIRT

Un CSIRT o “Equipo de respuesta de incidentes de Seguridad Informática” es un equipo que ejecuta, coordina y apoya la respuesta a incidentes de seguridad cibernética que afectan a organizaciones gubernamentales. (Lanfranco, 2021)

Ciberguerra

Una guerra cibernética o guerra tecnológica es cuando un país utiliza un ataque digital para dañar el sistema informático más importante de otro país. Puede utilizar software malicioso avanzados cuya característica fundamental es de ser anónimos dichos ataques.

Operaciones militares

Comprenden Operaciones Ofensivas que se orientan a destruir o derrotar al enemigo y las Operaciones Defensivas ganar tiempo, economizan Fuerzas o desarrollan condiciones favorables para pasar a las Operaciones Ofensivas. (Ejército del Perú, 2015)

Acto Hostil

Ataques empleando el ciberespacio dirigido a violar la soberanía, los intereses nacionales, los recursos críticos, así como plataformas digitales de las entidades públicas del estado.

Ciberarma

Toda capacidad, dispositivo o técnicas empleadas para afectar la infraestructura informática en el ámbito del ciberespacio, a la integridad, confidencialidad o disponibilidad de datos, y que su empleo puede generar perjuicio o daño de carácter personal o material.

Ciberdefensa

Capacidad militar que permite actuar frente amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten a la seguridad nacional. (Congreso de la República del Perú, Ley 30999 de 2019. Por lo cual se expide Ley de Ciberdefensa, 2019)

Ciberespacio

El ciberespacio es un dominio nuevo con características propias basados en tecnologías cada día emergentes donde la información es una variable importante y que a diferencia de los demás dominios éste ha sido diseñado por el hombre. (Congreso de la República del Perú, Ley 30999 de 2019. Por lo cual se expide Ley de Ciberdefensa, 2019)

Intención Hostil

Es la amenaza de un ataque en o a través del ciberespacio.

Operaciones Militares en el ciberespacio:

Es una operación en la que se emplean capacidades militares ofensivas y defensivas y de explotación, mediante el ciberespacio con el objetivo principal de alcanzar objetivos militares. El Ejército a través de ciberdefensa y telemática del Ejercito del Perú opera con su centro de ciberdefensa y realiza dichas operaciones a través de un proceso de operaciones cibernéticas enmarcado en sus cuatro fases de preparación, planeamiento, ejecución y evaluación, la compresión del ambiente operacional es muy importante para el comándate de Ciberdefensa, porque permite establecer la situación actual y los diferentes actores que intervienen y afectaran las operaciones, a través de las capacidades operativas se ejecutaran operaciones de ciberdefensa, cada una de ellas se enmarcara en base al escenario respectivo sea este de ciberguerra, apoyo a las operaciones militares terrestres y protección de ACN.

2.5 Hipótesis

La eficiencia en el empleo de la capacidad militar de ciberdefensa influenciará en el desarrollo de operaciones militares en el ciberespacio.

CAPITULO III: METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Enfoque de investigación

La investigación corresponde a un cualitativo porque tiene como propósito conocer el empleo de ciberdefensa en las operaciones militares en el ciberespacio, donde se analizaron las capacidades de Ciberdefensa, y su comprensión como operaciones militares a través del ciberespacio, de acuerdo con Vargas (2011) señala: “la metodología cualitativa es aquella cuyos métodos, observables, técnicas, estrategias e instrumentos concretos seencuentran en lógica de observar necesariamente de manera subjetiva algún aspectode la realidad” (p. 21).

3.2 Tipo de investigación

El tipo de la investigación que se empleo es un tipo de investigación teórico- empírica porque en esta investigación se analiza el empleo de la Capacidad militar de Ciberdefensa en el Ejército del Perú. De acuerdo con Vargas (2011) afirma: “nombramos investigación teórico-empírica a aquellos trabajos que encuentran primero la estructura empírica y categorial de alguna realidad concreta para luego ponerla a dialogar con distintos autores teóricos” (p. 78).

3.3 Método de investigación

El método que se utilizó en la presente investigación ha sido el método hermenéutico porque se ha realizado análisis e interpretación de la información que se encuentra en una realidad concreta del empleo de la capacidad militar de ciberdefensa a la fecha del Ejército del Perú, asimismo, realizar una propuesta de diseño de la capacidad militar de ciberdefensa indagando a través de este método contribuir con verdades subjetivas Al respecto Vargas (2011) afirma: “la realidad no está fuera de manera objetiva todo lo contrario, constituye subjetivamente lo que sucede en el interior de las personas como consecuencia del vivir y al margen de toda teoría” (p. 33).

3.4 Objeto de estudio

En la presente investigación el objeto de estudio es el empleo de la capacidad militar de Ciberdefensa, es conceptual porque se analizó las capacidades que esta posee y poder establecer su empleo vinculado a la protección de activos críticos nacionales como en la de operaciones militares propias, siendo este de carácter teórico. Al respecto Vargas (2011) señala: “en la etapa I: Planteamiento, lo más importantes durante este momento es la identificación del objeto de estudio dentro de este ámbito o circunstancia por el cual nos interesamos” (p. 56).

Tabla 1

Observables apriorísticas

CATEGORÍAS	SUBCATEGORÍAS	OBSERVABLES
Capacidad militar de Ciberdefensa	- Capacidades operativas	• Equipamiento de las capacidades • Procedimientos • Tipo de medios
	- Tecnología militar ciberdefensa	• Tipo de tecnología. • Empleo
Operaciones militares en el ciberespacio	- Ambiente operacional	• Ambiente Digital
	- Planeamiento operaciones ciberdefensa	• Plan operaciones ofensivas • Plan operaciones defensivas
	- Acciones Militares ciberdefensa en ACN	• Empleo CSIRT – EP. • Procesos

3.5 Muestra de estudio

El tipo de muestra que emplearemos en este trabajo de investigación será la muestra de expertos, lo cual es necesario en vista que existen personas que han destinado importante parte de su tiempo en estudiar el empleo de la capacidad militar de ciberdefensa en las operaciones de militares en el ciberespacio, para ello se tiene previsto recurrir 05 oficiales quienes poseen conocimiento y experiencia en el tema en mención, esta muestra de expertos ayudará a complementar el análisis y estudio de teórico sobre el tema.

3.6 Técnicas e instrumentos de recolección de datos

3.6.1 Técnica

En el presente estudio las técnicas a emplearse en el desarrollo serán en primer lugar la técnica de la entrevista para lo cual se empleará el instrumento de guía de entrevista semiestructurada, observación directa y por último se empleará la técnica del análisis documental empleando para ello la ficha de análisis documental como instrumento de recolección. Al respecto Vargas (2011) señala: “es recomendable elegir al menos dos técnicas a fin de poder triangular la información recabada” (p. 45).

Asimismo, los instrumentos de recolección de información fueron: preguntas por realizar, grabadoras de voz y video, dirección de sitios virtuales o físicos donde pueden ser encontrados, porque estos instrumentos han sido los materiales con el cual se ha realizado las técnicas.

3.7 Rigor científico

En relación al rigor científico para metodología cualitativa es necesario tener en consideración los siguientes factores:

Validez: se basa a que los instrumentos empleados tengan la consistencia interna en las guias de entrevista, observacion y análisis documental que permitan establecer con exactitud las categorias y sub categorias y asi instrumentos de investigacion validos (Hernández-Sampieri y Mendoza, 2018).

Triangulación: Permite cotejar y analizar información gracias a la triangulación de técnicas: entrevista, observación y análisis documental, lo que permite estudiar de forma más cercana, compleja y coherente los datos y la información.

Objetividad. En investigaciones cualitativas es limitado que posean una objetividad como lo sería en investigaciones cuantitativas, concibe como el grado en que este es o no permeable

a la influencia de los sesgos y tendencias del investigador o investigadores que lo administran, califican e interpretan (Hernández - Sampieri y Mendoza, 2018)

3.8 Técnica de procesamiento y análisis de datos

Teniendo en cuenta Para el procesamiento y análisis de datos, la selección de la herramienta más adecuada que se utiliza para completar la técnica elegida, como la entrevista, es una guía de entrevista semiestructurada, que permite a los encuestados responder a las preguntas con total libertad. y amplitud donde se realizará la reflexión crítica y la reflexión al momento de analizar los datos, esto facilita la adquisición de contenidos que sean esclarecedores y beneficiosos para la audiencia objeto de estudio; lo que señala Hernández (2013) afirmando que:

> Como guía de entrevista, cabe señalar que el número de preguntas está relacionado con la cantidad de tiempo que una persona busca durante la entrevista. Solo se incluyen las preguntas necesarias, y debe escribir varias formas de hacer las mismas preguntas, para reemplazarlas en caso de que no entienda. (p. 407).

CAPITULO IV: ANÁLISIS Y SÍNTESIS

4.1 Recolección de datos

Después de ser validados los instrumentos de recolección de datos y siendo aprobada la autorización de acceso al campo de estudio, la misma que se gestionó por intermedio de la Dirección de la Escuela Superior de Guerra – EPG, se procedió con la recolección de datos para conocer la capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio centro de Ciberdefensa del ejército, 2021

La muestra que se realizó en la investigación a través del tipo intencional, del tipo de expertos en Capacidad militar de Ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio. Al respecto Izcara (2014) sostiene que:

Durante la construcción de muestras, es informal, sigue una lógica estricta. El tipo de muestreo utilizado en la investigación cualitativa es intencional, es decir, es el investigador quien decide qué actores del contexto social formarán parte de la muestra.

En una investigación cualitativa se definen datos a un conjunto de informaciones derivadas de las interacciones entre sujetos e investigadores, las actividades realizadas, así como los contextos que las crean, a través de documentos u objetos físicos, determinada la muestra la cual fue de 05 oficiales conocedores de la capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio, procediendo a la recolección de los datos con información fehaciente y necesarios para el análisis, obteniéndose la información de fuentes humanas y documentos.

4.2 Organización de los datos

Los datos fueron organizados de manera ordenada por cada instrumento, según los datos recabados, transcritos en un documento de texto para explicar información relevante sobre la capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio, 2021.

Guía de Entrevista

Teniendo presente las medidas de salud por emergencia sanitaria de virus denominado covid 19, se efectuaron 05 entrevistas, utilizando la plataforma virtual meet y zoom para agilizar su realización, las mismas que fueron convertidas a un formado de documento word para una mejor interpretación, facilitando la compresión de la muestra, siendo guardada en la carpeta denominada entrevistas.

Guía de observación

Los datos obtenidos por la observación directa no participante mediante la bitácora de campo se transcribieron observando aquellas informaciones esenciales con respecto a la capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio, 2021.

Indagación documental

De la misma forma de resto de los anteriores instrumentos, se seleccionó la información obtenida en la ficha de investigación, la información destacada siendo fue transcrita al formato Word, para su correspondiente análisis.

Al respecto Hernández y Mendoza (2018) sostiene que:

Según el volumen recaudado de la información, la misma debe de ser bien organizada de acuerdo a los datos, siendo si fuese necesario el empleo de herramientas auxiliares para la realización del análisis.

Habiéndose organizado respectiva los datos respectivamente por instrumentos, y convertidos al formato de Word, la cual facilitó el análisis del material, para ello se empleó el método de la Hermenéutica.

Tabla 2

Organización de los datos obtenidos

	Guía de entrevista	**Guía de observación**	**Ficha de investigación**
Guía de entrevista	Entrevistado 1 Entrevistado 2 Entrevistado 3 Entrevistado 4 Entrevistado 5		
Guía de Observación		Bitácora de campo con todas las anotaciones de la observación	

	directa no participante en las instalaciones del centro de ciberdefensa del Ejército.	
Ficha de Investigación		• Manual de ciberdefensa JID • Concepción de las operaciones militares. • Operaciones y acciones terrestres unificadas. • Manual de ciberdefensa OTAN • Normas legales vigentes

4.3 Definición de categorías.

Por medio de un óptimo estudio del material documental consintió la conceptualización de las unidades de análisis, esta que eran parágrafo con datos fundamentales, accedió entender el problema sobre la capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio.

Con respecto a la categorización de la información importante en un estudio cualitativo, eligen algunos fragmentos que brotan de la deducción de la investigación. La clasificación permitirá dar inicio a elaborar las ideas y dejar ver los significados, entendiendo el contexto de la información, formando entendimiento y sentido cuando se plantea el problema. las codificaciones son como protocolos que logran nivelar las clases, consintiendo poseer un significado de las imágenes, segmentos y materiales (Hernández y Mendoza, 2018)

4.3.1 Definición de temas (grupos de categorías) de las entrevistas

Tabla 3

Definición de los temas de las guías de entrevista

tema (codificación axial)	Categoría (Codificación abierta)	Abrev	Frec	Síntesis
Capacidad militar de ciberdefensa	Capacidades operativas ciberdefensa	CO	6	La capacidad militar de ciberdefensa se implementó de manera parcial en el Ejército del Perú, en octubre del 2018, para lo cual se creó el Centro de Ciberdefensa del Ejercito, posterior a ello se aprobó la creación de Ciberdefensa Telemática del Ejercito, dentro de la estructura del Ejército del Perú, siendo la capacidad de Ciberdefensa una sinergia de capacidades operativas, tecnológicas y de recursos humanos. En lo que refiere a las capacidades operativas reúne a ofensivas, explotación y defensivas, todas estas serán las que ejecutarán las operaciones militares en y por medio del ciberespacio. Asimismo, en lo que refiere a tecnología militar para Ciberdefensa esta requiere tecnologías acordes a las operaciones en y mediante el ciberespacio, para lo cual se deberá adquirir herramientas cibernéticas de acuerdo a los
	Tecnología ciberdefensa	TMC	5	

				requerimientos operacionales propios de las tareas como también desarrollar herramientas o ciberarmas a medida de las operaciones. Respecto a los operadores cibernéticos, es personal especialista que reúne habilidades propias en el uso y desarrollo de ciberamas, estos deberán poseer un perfil adecuado en diversas actividades a realizar dentro de la capacidad de ciberdefensa.
Operaciones militares ciberdefensa	Ámbito operacional	AO	7	La ciberdefensa en el Ejército del Perú opera en un ámbito operacional que engranan el físico y el digital, el primero de ellos se debe a que las tecnologías denominadas hardware requieren de una implementación física sea esta ubicación en el terreno de Datacenter en sus diferentes niveles o sean redundantes, las conexiones para el empleo de internet satelital o través de un proveedor de servicios cableado, así también proveer un sistema de alimentación eléctrica que se debe tener y protección física perimetral que debe poseer esta implementación para que pueda responder a los requerimientos operacionales cibernéticos militares. Un ámbito a analizar es el digital, por este medio se realizará

	Planeamiento operaciones militares ciberdefensa	POMC	6
	Preparación de los operadores conjuntos	POC	4
Capacidad de interoperabilidad			

todas tareas tácticas a realizar a través del empleo de software apropiados, sistemas operáticos, canales de comunicación virtualizados. Todo el empleo de tanto de software y hardware debe de estar enmarcado a un planeamiento de operaciones y que se pueda realizar un proceso propio de ello en sus diferentes fases, que permita cumplir con los objetivos tácticos y con el estado final del comandante.

La ciberdefensa al ser una actividad militar según la Ley N° 30999, donde especifica que esta responsabilidad recae en la fuerzas armadas y sus órganos ejecutores son Ejército, Marina y Aviación, hace necesario que entre las tres lleven a cabo una sinergia, en primer lugar que los operadores cibernéticos a nivel de las tres fuerzas mantenga entre ellas un nivel de preparación y entrenamiento acorde a los requerimientos operacionales en vista que el Comando Conjunto de las Fuerzas armadas a través del componente de ciberdefensa será la que conduzca las operaciones de ciberdefensa en un teatro de

				operaciones, por ello se requiere de una preparación óptima para los operadores, asimismo dentro de la ejecución propia de las operaciones se debe establecer una taxonomía unificada entre las fuerzas a fin que se pueda realizar un análisis del ambiente operacional identificar centros de gravedad, objetivos y tener un entendimiento de la misión óptima.
	Taxonomía ciberdefensa	TC	4	
Doctrina de ciberdefensa	Manuales ciberdefensa	MC	6	La doctrina siendo un pilar fundamental para la preparación y entrenamiento de la fuerza y su empleo en un ambiente se carece de manuales desarrollados que sirvan para el empleo propio de la ciberdefensa en un entorno operacional real, asimismo se ha identificado solo dos ejercicios tácticos en ciberdefensa para el empleo de doctrina, lo que conlleva a que la fuerza no esté a un nivel óptimo para la conducción y ejecución de operaciones cibernéticas.
	Ejercicios tácticos de ciberdefensa	ETC	6	

4.3.2 Definición de temas (grupo de categorías) de la observación directa

Tabla 4

Observación directa

tema (codificación axial)	Categoría (Codificación abierta)	Abrev	Frec	Síntesis
Capacidad militar de ciberdefensa	Capacidades operativas ciberdefensa	COC	6	Se evidencia que si bien se ha creado en el 2018 el Centro de ciberdefensa del Ejército y posterior ciberdefensa y telemática del Ejército como dentro de la estructura orgánica del Ejército del Perú la capacidad militar de Ciberdefensa no ha sido implementada, conllevando esto que las capacidades operativas de Ciberdefensa no se han implementadas o desarrolladas, con referente a la tecnología se evidencio que dentro del CECIBER, se instaló computadoras, de gama baja no siendo estas las óptimas para realizar operaciones cibernéticas, asimismo que labora en CITELE, no es el acorde en vista que no son especialistas ni calificados en ciberdefensa, y en su gran mayoría no reúnen el perfil que se requiere para realizar operaciones militares en y mediante el ciberespacio.
	Tecnología Militar ciberdefensa	TMC	5	

Operaciones militares ciberdefensa	Ámbito operacional	EO	5	Se evidencio que la capacidad militar de ciberdefensa en el Ejercito del Perú, carece de experiencia en operaciones cibernéticas militares, debido a que no posee la infraestructura física ni digital es decir, en el ámbito físico, no posee un datacenter exclusivo, no posee un sistema de conectividad a internet de proveedores locales o regionales, en lo referente al ámbito digital carece de software que permitan realizar operaciones de ciberdefensa en un ámbito operacional identificado, dentro del ámbito del planeamiento carece de una metodología que permita analizar el ambiente operacional y realizar un buen diseño de las operaciones para poder cumplir con estado final deseado del comandante.
	Planeamiento operaciones militares ciberdefensa	POMC	5	

Capacidad de interoperabilidad	Preparación de los operadores conjuntos	POC	3	Se evidenció que la capacidad de interoperabilidad del centro de ciberdefensa del Ejército se encuentra en un nivel no interoperable la integración es aún nula, en vista que la preparación de los operadores cibernéticos a nivel fuerzas armadas está en una fase inicial, no se ha establecido un taxonomía unificada en el ámbito de ciberdefensa, asimismo los procesos de operaciones son iniciales, lo que no permite un proceso de las operaciones interoperable, lo que dificulta que exista un comando y control en ciberdefensa adecuado del componente de ciberdefensa con su órgano de ejecución que viene a ser ciberdefensa y telemática del Ejército del Perú.
	taxonomia ciberdefensa	TC	4	
		MC	6	Se evidenció que la doctrina en operaciones de ciberdefensa es carente, lo que limita el conocimiento de los avances tecnológicos y as metodologías a emplear, además se

Doctrina de ciberdefensa	Manuales ciberdefensa Ejercicios tácticos de ciberdefensa	ETC	3	observó, que no se tiene boletines de Ciberdefensa que colaboren en la generación de doctrina, si bien existe un programa de ciberdefensa denominado operaciones cibernéticas desde el 2015, a la fecha no se ha desarrollado un manual acorde a los avances tecnológico, asimismo el Programa de operaciones cibernéticas es dictado a oficiales de diferentes armas que al término de ello, no realizan investigaciones, conllevando a la carente generación de doctrina en esta capacidad, asimismo en el año 2020 se llevó a cabo el primer Ejercicio de ciberdefensa denominado CIBERDEP 1.0 ejercito táctico que reunió a participar a diferentes dependencias orientadas a tecnología conducido por el centro de ciberdefensa del Ejercito, en el año 2021 se realizó CIBERDEP 2.0 ejercicio táctico en ciberdefensa.

4.3.3 Definición de temas (grupo de categorías) de la indagación documental

Tabla 5

Definición de los temas de indagación documental

tema (codificación)	Categoría (Codificación abierta)	Abrev	Frec	Síntesis
Capacidad militar de ciberdefensa	Capacidades operativas cibernéticas	COC	6	La Capacidad militar de Ciberdefensa consiste y se basa en el proceso de las operaciones cibernéticas en cuanto demanda que exista un planeamiento, preparación, ejecución y constante evaluación de las operaciones, el comandante de ciberdefensa debe tener claro en ambiente operacional cibernético, y poder identificar que actores pueden afectar nuestra operación asimismo se debe permitir la libertad de maniobra para con ello alcanzar los objetivos militares. Podemos categorizar en cuatro capacidades operativas defensiva, explotación y respuesta, esta última será con orden de acuerdo a ley en todo ello también establecemos unas operaciones de sostenimiento tecnológico operacional que serían el desarrollo, investigación e innovación considerando que la tecnología es cambiante, dinámica.
	Tecnología militar ciberdefensa	TMC	5	
				La capacidad operativa ofensiva o llamada de respuesta son

				actividades que establecen la determinación para alcanzar objetivos militares en o a través del ciberespacio, asimismo establece efectos temporales o permanentes. La capacidad defensiva o de protección son medidas pasivas, activas con la finalidad que la fuerza amiga mantenga el dominio del ciberespacio, así como proteger las infraestructuras cibernéticas de la fuerza amiga durante la operación
Operaciones cibernéticas militares	Ámbito operacional	EO	5	El ámbito operacional cibernético es importante dentro de las operaciones por que permite tener un panorama claro de los factores que influyen en operaciones militares cibernéticas ello será de acuerdo al escenario en el cual se encuentre la fuerza: ciberguerra, protección de Activos Críticos Nacionales, o en apoyo a operaciones militares. La ciberguerra es una confrontación de las fuerzas empleando como medio el ciberespacio aquí ambas fuerzas despliegan todas sus capacidades, existe una reglamentación materializada en un documento denominado manual de Tallin 2.0 donde establece reglas del conflicto pero que aún nada está claro en vista

				que el ciberespacio es un dominio que aún falta investigar.
	Planeamiento operaciones militares ciberdefensa	POMC	6	Las operaciones cibernéticas referente a la protección de activos críticos nacionales es por mandato de acuerdo a Ley. Por ende, se requiere que las capacidades operativas cibernéticas se encuentren acordes a las diferentes tecnologías que poseen dichos ACN, y esta protección y respuesta sea lo más oportuno.
	Preparación de los operadores conjuntos			La interoperabilidad agrega una complejidad al proceso de operaciones que el comandante y el estado mayor deben abordar e integrar en las actividades asociadas con la planeación, preparación, ejecución y evaluación de una misión u operación determinada, Las soluciones técnicas emergentes permiten un mejor intercambio de información y una mejor comprensión de la situación entre los socios de la misión. Para lograr los niveles deseados de interoperabilidad entre los socios de la misión, las unidades deben aplicar los procedimientos adecuados y establecer las organizaciones y estructuras necesarias en función de los requisitos de interoperabilidad. Esto debe hacerse teniendo en cuenta las
Capacidad de interoperabilidad				

	Taxonomía ciberdefensa	TC	4	soluciones técnicas disponibles y depender de las especificaciones de la misión, como los socios de la misión, el tiempo disponible, los activos orgánicos, los recursos externos disponibles, las prioridades del Ejército.
Doctrina de ciberdefensa	Manuales ciberdefensa	MC	6	La doctrina de ciberdefensa, se enfoca en establecer y elaborar manuales del empleo de la ciberdefensa en un teatro de operaciones, así como la de realizar ejercicios tácticos el cual generen en los operadores un nivel de adiestramiento que permita ello un empleo de las diferentes capacidades operativas de ciberdefensa de la forma más óptima.
	Ejercicios tácticos de ciberdefensa	ETC	3	

4.4 Soporte de Categorías

Tabla 6

Soporte de Categorías

tema (codificación axial)	Categoría (Codificación abierta)	Abrev	Frec	Síntesis
Capacidad militar de ciberdefensa	Capacidades operativas ciberdefensa	COC	6	La capacidad militar de ciberdefensa del Ejército del Perú cuenta con capacidades operativas, que son ofensiva, defensiva y explotación, a través de ellas se realizan operaciones militares en y mediante el ciberespacio.
	Tecnología militar ciberdefensa	TMC	5	La tecnología cibernética empleada para realizar operaciones militares en y mediante el ciberespacio, debe ser la más óptima y acorde a los avances tecnológicos globales, sin embargo, en el centro de ciberdefensa del Ejercito no se evidencio medios tecnológicos acordes a los requerimientos propias de las operaciones.
				Los operadores cibernéticos están comprendidos por el personal especialista en temas de ciberdefensa, comprender el proceso de las operaciones militares, así como

				la ejecución al nivel más técnico, este personal obedece a un adecuado perfil tanto en habilidades y destrezas que debe poseer, en el Centro de Ciberdefensa del Ejército del Perú no se puedo evidenciar personal especialista.
Operaciones militares ciberdefensa	Ámbito operacional	AO	5	Las operaciones se realizan en ambientes operacionales complejos, cambiantes e inciertos, un ambiente operacional es una combinación de las condiciones, circunstancias e influencias que afectan el empleo de capacidades y dan resultados en las decisiones del comandante, este abarca informaciones de sistemas de los adversarios, amigos y neutrales, que son relevantes para las operaciones cibernéticas.
				El planeamiento es el arte y la ciencia de comprender la situación, visualizar un futuro deseado y trazar un enfoque

	Planeamiento operaciones militares ciberdefensa	POMC	6	operacional para alcanzar ese futuro el planeamiento visualiza el desarrollo de una operación, es una actividad continua dentro del proceso de las operaciones, ello no termina con la elaboración de un plan u orden, el plan se perfecciona continuamente a medida que se mejora el entendimiento de la situación.
	Operadores cibernéticos conjuntos	*OCO*	5	son los que integran la capacidad de ciberdefensa en el componente de ciberdefensa (COCID) dichos operadores están integrados por las tres fuerzas Ejército, Marina, Fuerza Aérea, todos con sus respectivos comandos de ciberdefensa, los operadores cibernéticos conjuntos deben estar en la capacidad de operar de manera conjunta y sinérgica.
Capacidad de interoperabilidad	Taxonomía ciberdefensa	TC	4	La taxonomía de ciberdefensa va dirigida hacia una nueva etapa de amenazas y vulnerabilidades en el ciberespacio, es por ello, que conlleva una actualización de la clasificación de las categorías y subcategorías actuales.

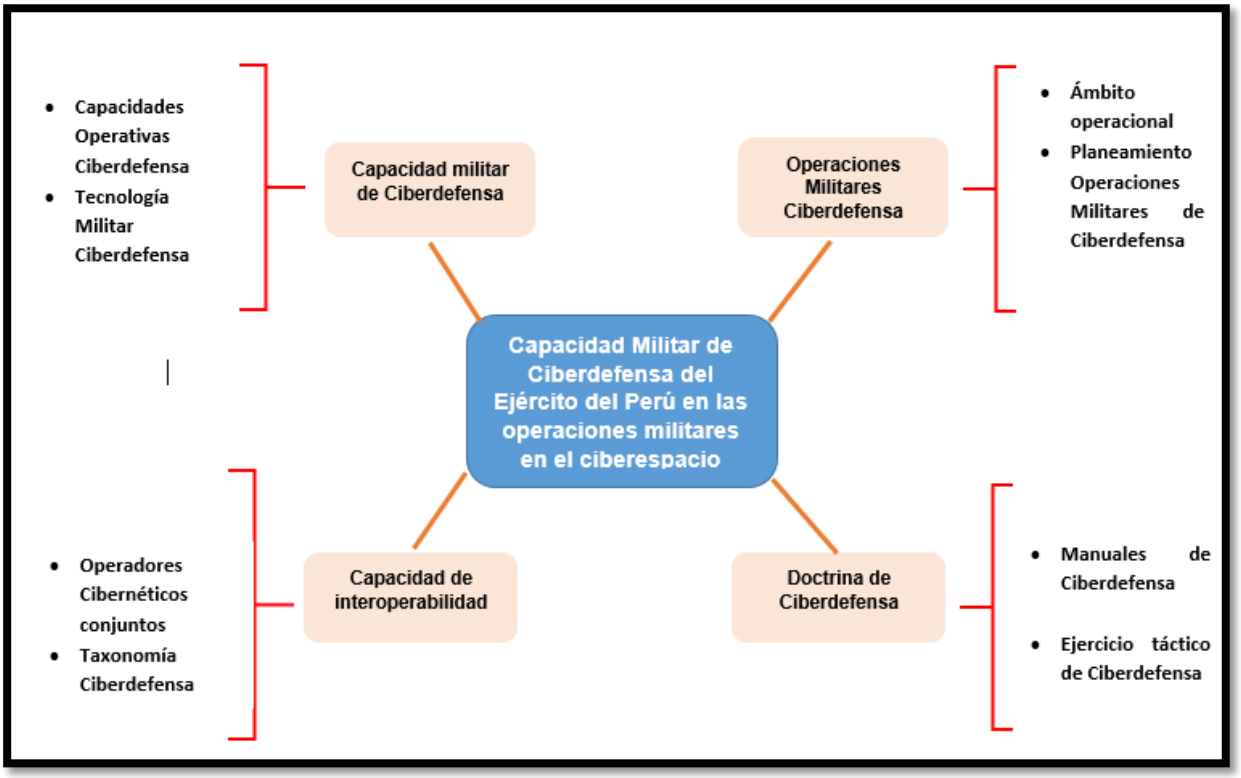
	Manuales ciberdefensa	MC	6	Los manuales son una guía de instrucciones de todos los procedimientos de las actividades que las personas realizan en las operaciones cibernéticas servir base de adiestramiento, comprender el proceso de las operaciones.
Doctrina de ciberdefensa	Ejercicios tácticos de ciberdefensa	ETC	3	Los ejercicios tácticos permiten fortalecer e incrementar las habilidades y destrezas de los operadores cibernéticos, a través de ejercicios, empleando técnicas cibernéticas que permitan explotar vulnerabilidades, así como la defensa de ataques de agentes hostiles.

4.5 Red Semántica

Establece los problemas que existen en capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio, 2021, con respecto al cumplimiento de su misión asignada. Además, se analizó la capacidades militares operativas, como medio para realizar operaciones cibernéticas militares teniendo en consideración que la interoperabilidad cibernética es un factor crítico durante el proceso de las operaciones integrado al componente de ciberdefensa, incluyendo que la doctrina de ciberdefensa es necesario con la finalidad de mantener actualizada en base a la tecnología emergente como requerimiento necesario para la realización de operaciones militares en y mediante el ciberespacio.

Figura 27

Red semántica de la investigación



4.6 Triangulación

En el enfoque cualitativo es la triangulación sostiene Cervantes (2017) "la que se entiende como la convergencia de distintas perspectivas y métodos en el estudio de un mismo objeto, asegurando así una aproximación más comprensiva del problema investigado (mayor validación)" (p. 120). Mediante la triangulación se establece una mayor validez y rigurosidad a la investigación científica, por lo que, se contrastó por temas de los resultados obtenidos en las entrevistas, la indagación documental y la observación directa, permitiendo la construcción de la realidad través del material textual producto del trabajo de campo.

Tabla 7

Triangulación de técnicas cualitativas

Categorías	Entrevistas	Observación directa	Indagación documental	Síntesis integrada
Capacidad militar de ciberdefensa	La capacidad militar de ciberdefensa se implementó en el Ejército del Perú, en el año 2018, para lo cual se creó el Centro de Ciberdefensa del Ejercito, posterior a ello se aprobó la creación de ciberdefensa telemática del Ejército, dentro de la estructura orgánica del Ejército del Perú, siendo la capacidad de Ciberdefensa una sinergia de capacidades operativas, tecnológicas y de recursos humanos. En lo que refiere a las capacidades operativas	Se evidencia que si bien se ha creado en el 2018 el centro de ciberdefensa del Ejército y posterior ciberdefensa y telemática del Ejército dentro de la estructura orgánica del Ejército del Perú la capacidad militar de ciberdefensa no ha sido implementada, conllevando esto que las capacidades operativas de Ciberdefensa no se han implementadas o desarrolladas, con referente a la tecnología se evidencio que dentro del CECIBER, se instaló computadoras, de	La capacidad militar de ciberdefensa podemos categorizar en cuatro capacidades operativas defensiva, explotación y respuesta, esta última será con orden de acuerdo a ley en todo ello también establecemos unas operaciones de sostenimiento tecnológico operacional que serían el desarrollo, investigación e innovación considerando que la tecnología es cambiante y dinámica y en algunos casos compleja la capacidad operativa	Podemos sintetizar que, en esta categoría, la capacidad militar de ciberdefensa, en el Ejército se implementó en el año 2018, creándose en Centro de ciberdefensa del Ejército, sin embargo, tenemos que mencionar solo se llevó a cabo de manera administrativa, cediéndose una infraestructura en el en sótano del Cuartel General del Ejército, sin embargo, operativamente no cuenta con la infraestructura tecnológica adecuada para la realización de

reúne a ofensivas, explotación y defensivas, todas estas serán las que ejecutarán las operaciones militares en y por medio del ciberespacio. Asimismo, en lo que refiere a tecnología militar para ciberdefensa esta requiere tecnologías acordes a las operaciones en y mediante el ciberespacio, para lo cual se deberá adquirir herramientas cibernéticas de acuerdo a los requerimientos operacionales propios de las tareas como también desarrollar herramientas o ciberarmas a medida de las operaciones. respecto a los operadores cibernéticos, es personal especialista que gama baja no siendo estas las óptimas para realizar operaciones cibernéticas, asimismo que labora en CITELE, no es el acorde en vista que no son especialistas ni calificados en ciberdefensa, y en su gran mayoría no reúnen el perfil que se requiere para realizar operaciones militares en y mediante el ciberespacio.

ofensiva o llamada de respuesta son actividades que establecen la determinación para alcanzar objetivos militares en o a través del ciberespacio asimismo establece efectos temporales o permanentes.

La capacidad defensiva o de protección son medidas que pasivas activas que tienen como finalidad que la fuerza amiga mantenga el dominio del ciberespacio asimismo también la de proteger las infraestructuras cibernéticas de la fuerza amiga durante las operaciones

La capacidad operativa de explotación permite realizar actividades de monitorio e

operaciones cibernéticas militares y su empleabilidad de las capacidades operativas, ofensivas, defensivas y de explotación, si bien en el año 2019 participaron en acciones militares durante los juegos panamericanos Lima 2019, ello no implico a que se llevara a cabo la empleo de la capacidades operativas debido a una limitada infraestructura tecnológica, personal especialista y de procedimientos en ciberdefensa contra agentes hostiles, debemos de entender que en el ciberespacio se puede llevar acabo la maniobra ya que estará radicara en la

	reúne habilidades propias en el uso y desarrollo de ciberarmas, estos deberán poseer un perfil adecuado en diversas actividades a realizar dentro de la capacidad de ciberdefensa.		identificación de ciberamenazas vulnerabilidades que puedan afectar la infraestructura cibernética de la propia fuerza por cuanto mantiene una coordinación constante con la capacidad operativa de protección	diferentes tareas tácticas que puedan emplearse.
Operaciones militares ciberdefensa	La ciberdefensa en el Ejército del Perú opera en un ámbito operacional que engranan el físico y el digital, el primero de ellos se debe a que las tecnologías denominadas hardware requieren de una implementación física sea esta ubicación en el terreno de datacenter en sus diferentes niveles o sean	Se evidenció que la capacidad militar de ciberdefensa en el Ejército del Perú, carece de experiencia en operaciones cibernéticas militares, debido a que no posee la infraestructura física ni digital es decir, en el ámbito físico, no posee un datacenter exclusivo, no posee un sistema de conectividad a internet de	Las operaciones se basan en el proceso de las operaciones cibernéticas en cuanto demanda que exista un planeamiento, preparación, ejecución y constante evaluación de las operaciones, el comandante de ciberdefensa debe tener claro en ambiente operacional cibernético, y poder identificar que actores pueden afectar nuestra	La capacidad de ciberdefensa no es exclusivamente del Ejército, sino que es la sinergia de los órganos ejecutores de ministerio de defensa por cuanto se realizan operaciones cibernéticas la responsabilidad de la ejecución recae en el comando operacional de ciberdefensa a la que a través de las tres fuerzas

redundantes, las conexiones para el empleo de internet satelital o través de un proveedor de servicios cableado, así también proveer un sistema de alimentación eléctrica que se debe tener y protección física perimetral que debe poseer esta implementación para que pueda responder a los requerimientos operacionales cibernéticos militares. Un ámbito a analizar es el digital, por este medio se realizará todas tareas tácticas a realizar a través del empleo de software apropiados, sistemas operáticos, canales de proveedores locales o regionales, en lo referente al ámbito digital carece de software que permitan realizar operaciones de ciberdefensa en un ámbito operacional identificado, dentro del ámbito del planeamiento carece de una metodología que permita analizar el ambiente operacional y realizar un buen diseño de las operaciones para poder cumplir con estado final deseado del Comandante. operación asimismo se debe permitir la libertad de maniobra para con ello alcanzar los objetivos militares. El ámbito operacional cibernético es importante dentro de las operaciones por que permite tener un panorama claro de los factores que influyen en operaciones militares cibernéticas ello será de acuerdo al escenario en el cual se encuentre la fuerza: ciberguerra, protección de activos críticos nacionales, o en apoyo a operaciones militares. La ciberguerra es una confrontación de las fuerzas empleando como medio el ciberespacio aquí ambas fuerzas despliegan todas sus capacidades, existe armadas ejecutara las operaciones, lo que conlleva a que entre dichas fuerzas exista un lenguaje en común que predomine entre las fuerzas y durante las operaciones

comunicación virtualizados. Todo el empleo de tanto de software y hardware debe de estar enmarcado a un planeamiento de operaciones y que se pueda realizar un proceso propio de ello en sus diferentes fases, que permita cumplir con los objetivos tácticos y con el estado final del comandante.		una reglamentación materializada en un documento denominado manual de Tallin 2.0 donde establece reglas del conflicto pero que aún nada está claro en vista que el ciberespacio es un dominio que aún falta investigar.	
La ciberdefensa al ser una actividad militar según la Ley N°30999, donde especifica que esta responsabilidad recae en la fuerzas armadas y sus órganos ejecutores son Ejército, Marina y Aviación, hace necesario que entre	Se evidenció que la capacidad de interoperabilidad del centro de ciberdefensa del Ejército se encuentra en un nivel no interoperable la integración es aún nula, en vista que la preparación de los operadores cibernéticos a	La interoperabilidad agrega una complejidad al proceso de operaciones que el comandante y el estado mayor deben abordar e integrar en las actividades asociadas con la planeación, preparación, ejecución y	La interoperabilidad de la capacidad de ciberdefensa es el proceso por el cual se deben integrar las actividades asociadas a la planeación, preparación, ejecución y evaluación de las operaciones entre las fuerzas que son actores en

Capacidad de interoperabilidad	las tres lleven a cabo una sinergia, en primer lugar que los operadores cibernéticos a nivel de las tres fuerzas mantenga entre ellas un nivel de preparación y entrenamiento acorde a los requerimientos operacionales en vista que el comando conjunto de las fuerzas armadas a través del componente de ciberdefensa será la que conduzca las operaciones de ciberdefensa en un teatro de operaciones, por ello se requiere de una preparación óptima para los operadores, asimismo dentro de la ejecución propia de las operaciones se debe establecer una taxonomía unificada entre las fuerzas a	nivel Fuerzas armadas está en una fase inicial, no se ha establecido un taxonomía unificada en el ámbito de ciberdefensa, asimismo los procesos de operaciones son iniciales, lo que no permite un proceso de las operaciones interoperable, lo que dificulta que exista un comando y control en ciberdefensa adecuado del componente de ciberdefensa con su órgano de ejecución que viene a ser ciberdefensa y telemática del Ejercito.	evaluación de una misión u operación determinada, Las soluciones técnicas emergentes permiten un mejor intercambio de información y una mejor comprensión de la situación entre los socios de la misión. Para lograr los niveles deseados de interoperabilidad entre los socios de la misión, las unidades deben aplicar los procedimientos adecuados y establecer las organizaciones y estructuras necesarias en función de los requisitos de interoperabilidad. Esto debe hacerse teniendo en cuenta las soluciones técnicas disponibles y depender de las especificaciones de la	el ámbito del ciberespacio, teniendo en consideración que el COCID es el conduce las operaciones cibernéticas por ende las tres fuerzas deben ser interoperables en un nivel de integración para que las operaciones puedan cumplir con la misión asignada. La capacidad de ciberdefensa del Ejército no mantiene un nivel de interoperabilidad en vista que no se encuentra integrada a una infraestructura tecnológica podamos decir en el caso de capacidad operativa de defensa, la integración a un SIEM o Firewall interinstitucional donde se

	fin que se pueda realizar un análisis del ambiente operacional identificar centros de gravedad, objetivos y tener un entendimiento de la misión óptima.		misión, como los socios de la misión, el tiempo disponible, los activos orgánicos, los recursos externos disponibles, las prioridades del Ejército.	puedan detectar comportamientos anómalos y que las tres fuerzas puedan actuar de manera oportuna ante cualquier intrusión detectada.
Doctrina de ciberdefensa	La doctrina siendo un pilar fundamental para la preparación y entrenamiento de la fuerza y su empleo en un ambiente se carece de manuales desarrollados que sirvan para el empleo propio de la ciberdefensa en un entorno operacional real, asimismo se ha identificado solo dos ejercicios tácticos en ciberdefensa para el empleo de doctrina, lo que conlleva a que la fuerza no esté a un nivel óptimo para la	Se evidenció que la doctrina en operaciones de Ciberdefensa es carente, si bien existe un programa de ciberdefensa denominado operaciones cibernéticas desde el 2015, a la fecha no se ha desarrollado un manual acorde a los avances tecnológico, asimismo el programa de operaciones cibernéticas es dictado a oficiales de diferentes armas que al término de ello, no realizan investigaciones,	La doctrina de ciberdefensa, se enfoca en establecer y elaborar manuales del empleo de la ciberdefensa en un teatro de operaciones, así como la de realizar ejercicios tácticos el cual generen en los operadores un nivel de adiestramiento que permita ello un empleo de las diferentes capacidades operativas de Ciberdefensa de la forma más óptima.	En esta categoría de la doctrina en Ciberdefensa es un pilar fundamental ya que encuadra los procedimientos, investigaciones, buenas prácticas que enmarcan en documentación que permitirá un óptimo empleo de las capacidades operativas de Ciberdefensa en el ciberespacio, conllevando ello como soporte para la toma de decisiones, por cuanto la aplicación de juicios

conducción y ejecución de operaciones cibernéticas. Siendo ambas necesarias en vista que en proceso de las operaciones de preparación es una fase importante en el desarrollo de operaciones militares.	conllevando a la carente generación de doctrina en esta capacidad, asimismo en el año 2020 se llevó a cabo el primer Ejercicio de ciberdefensa denominado CIBERDEP 1.0 Ejército táctico que reunió a participar a diferentes dependencias orientadas a tecnología conducido por el centro de ciberdefensa del Ejército, en el año 2021 se realizó CIBERDEP 2.0.	teniendo como base la información y conocimientos encaminará a una toma de decisiones oportuna. Asimismo, la doctrina apoyara a que el operador cibernético obtenga un pensamiento crítico, permitiendo el desarrollo de habilidades que permitan analizar y argumentar ideas dentro de la actividad propia del ciberespacio.

CAPITULO V. DIALOGO TEÓRICO – EMPÍRICO

En el presente capitulo se mencionarán diversos artículos, tanto estudios e investigaciones realizadas por autores con la finalidad de realizar una confrontación con los hallazgos determinados en la presente investigación.

Iniciamos citando lo manifestado por la Junta Interamericana de Defensa (2020):

> El ciberespacio ya no es un dominio emergente, sino un potencial escenario de colaboración en el que todas las naciones soberanas podrían participar de manera activa y diaria. En todo el mundo, los actores gubernamentales y no gubernamentales han desarrollado capacidades cibernéticas, que han desencadenado una reexaminación de las nociones tradicionales del poder global, así como, las prioridades dentro de las naciones. (p. 2)

En base a lo antes mencionado, la preocupación de las naciones ante una nueva amenaza emergente, como son las ciberamenazas (virus, malware, agente hostiles) que tienen como características, el ser anónimas y de no poseer una magnitud de fuerza definida para realizar un ciberataque, asimismo los estados también sean convertido en ciberamenazas debido a sus múltiples interés nacionales por cuanto, en su intención de obtener información oportuna realizan diversas actividades de inteligencia como espionaje, siendo esta también considerada una ciberamenaza, los estados han optado también por un nuevo método y que consiste en el de obtener información a través del ciberespacio, optando por contratar a grupos de hacker, para no tener un vínculo directo hacia las actividades ilegales que se realiza, estos grupos son denominados APT (Amenazas Avanzadas Persistentes) cuya peculiaridad es la de emplear vectores de ataques sofisticados sobre infraestructura estatales vulnerables y carentes de una seguridad sobre su infraestructura de tecnología de información y operaciones. Ante esta nueva amenaza los estados en la región han establecido la creación de cibercomandos con la finalidad de proteger sus infraestructuras de tecnología de la información y operaciones, dichas entidades en un proceso de creación y de implementación que demanda recursos económico, personales y de infraestructura se han visto limitado en su avance y en la de poder cumplir con su misión asignada, aunado a ello que algunos países de la región no dispone de la legalidad correspondiente para realizar sus actividades generando una problemática para sus operaciones.

Es por ello que según Centro de Estudios Estratégicos de Chile (2017) “el ciberespacio es el quinto dominio, junto con lo terrestre, marítimo, aéreo y el espacio, por esta razón debe existir especial preocupación acerca del concepto de ciberguerra” (p. 38).

Los Estados a través de sus diferentes entidades vinculadas a la ciberseguridad y ciberdefensa, realizan esfuerzos para mitigar los ciberataques a las infraestructura de

tecnologías de la Información estatales, asimismo los ciberataques que se llevan a cabo durante todo el año, muchas organizaciones estatales son hackeadas sin saberlo otras están informadas que están siendo hackeadas sin embargo por el tema de reputación nunca denuncian, el Estado del Perú ha creado el Centro Nacional de Seguridad Digital (CNSD) en el año 2020 con la finalidad de garantizar la seguridad del ciberespacio frente a su uso ilícito o malicioso por cuanto promueve la coordinación entre las entidades de la administración de redes informáticas de la administración pública nacional, para la prevención, detección, manejo, recopilación de información y desarrollo de soluciones para los incidentes de seguridad. Sin embargo, todo ello es una medida en el entorno de la seguridad digital. Pero cuando es rebasada la seguridad digital de las entidades del estado, asume la responsabilidad el comando conjunto de la fuerzas armadas a través del comando operacional de ciberdefensa (COCID) creado en el año 2020 con la finalidad de defender, explotar y responder ante amenazas y ataques realizados a través del ciberespacio que afecten la seguridad digital de las redes, sistemas de información, telecomunicaciones y activos críticos de nuestras fuerzas y medios de alto valor militar, teniendo como órganos ejecutores a las tres fuerzas armadas, sin embargo el centro de ciberdefensa del Ejército se había creado con anterioridad en el año 2018, pero afrontando la misma problemática de algunos cibercomandos de la región, el tema presupuestal, pese a su creación y sin tener un respaldo presupuestal, pese a ello se realizaron esfuerzos limitados por sacar adelante la capacidad de ciberdefensa en el Ejército, ya teniendo una apreciación de una situación actual de la ciberdefensa debemos establecer como esta se relaciona con la defensa nacional y el SEDENA (Secretaria de Defensa Nacional) nos menciona un concepto de seguridad Nacional en la cual define: “Como el conjunto de Previsiones y acciones que el estado genera y ejecuta permanentemente para garantizar la soberanía, independencia, integridad territorial y la protección de los intereses nacionales“ (SEDENA, 2014). Por cuanto al tener claro que las operaciones de ciberdefensa garantizar la protección de los intereses nacionales. Un aspecto importante dentro de la ley de ciberdefensa N° 30999 viene a ser el uso de la fuerza en y mediante el ciberespacio, estableciendo que toda amenaza o ataque en y mediante el ciberespacio que ponga en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales, da lugar al ejercicio del derecho de legítima defensa. Y se encuentran enmarcados en los principios de legalidad, necesidad y oportunidad por cuanto podemos establecer claramente que la capacidad operativa ofensiva solo estará autorizada de acuerdo a los protocolos establecidos de acuerdo a ley. podemos establecer tres escenarios para el empleo de la capacidad de Ciberdefensa del Ejercito, el primero de ello es dentro de una ciberguerra cuya definición ya la hemos establecido en presente investigación, sin embargo, al respeto Schmitt (2013):

> No hay disposiciones de tratados que se ocupen directamente de la "guerra" cibernética. Del mismo modo, dado que la práctica cibernética de los Estados y las expresiones de opinio juris disponibles al público son escasas, a veces es difícil concluir definitivamente que exista alguna norma de derecho internacional consuetudinario específica para el ciberespacio. (p. 19)

El escenario de una ciberguerra aun es incierto inclusive para la OTAN, al no tener reglas claras del empleo del ciberespacio, sin embargo el hecho de poder llevar operaciones ciberneticas, ententiendose como el empleo de las capacidades ciberneticas con el fin de lograr objetivos teniendo como medio el ciberespacio, los estados tienen responsabilidad sobre la conduccion de las operaciones ciberneticas que realizan sus diferentes entidades, por cuanto ningun estado puede reclamar sobre el ciberespacio, sin embargo puede establecer soberania sobre la infraestructuras ciberneticas ubicadas dentro de su territorio y que estas vinculan. Asimismo, debemos de comprender que estado ejerce sobre la infraestructura cibernetica un control regulatorio legal, asi la de protección de ello sea publico o privado. Del empleo de la capacidad operativa ofensiva de una fuerza que representa un estado podemos establecer que cuando un Estado ataca la infraestructura cibernetica de otro estado trangrede la soberania del estado ultimo, pero aun no se podido determinar si la colocación de malware que no causa daños físicos utilizado para vigilar, constituye una violación de la soberanía.

De realizar una ofensiva cibernética califica como un "ataque armado" activa el derecho de legítima defensa individual o colectiva.

Los organos ejecutores del comando operacional de ciberdefensa (CCFFAA) en esta investigacion referida al Ejército del Perú a traves del centro de ciberdefensa, ejecutará las diferentes tareas tacticas con la unica finalidad de cumplir con los objetivos militares en el ciberespacio. Y estas deben llevarse de la manera mas sinergica e interoperable entre todas las fuerzas armadas. Para ello debera contar con tres pilares fundamentales: procesos, tecnologia y operadores, estos tres aspectos son fundamentales y concatenadas para un optimo desarrollo del proceso de operaciones cibernéticas, el planeamiento cibernético debe llevarse a cabo de para entender la situación actual del ambiente operacional para asi poder visualizar un futuro deseado, este planeamiento debe ser sistemico en vista que se debe analizar las infraestructuras ciberneticas del adversario para realizar un ofensiva cibernética oportuna, y tambien una defensa de nuestra infraestructura propia acorde a neutralizar los vectores de ataque adversarios. Asimismo, se debe realizar un exploración del ciberespacio con la finalidad de identificar ciberamemazas y se genere informacion procesada con la finalidad de mitigar la vulnerabilidades de nuestra infraestructura cibernética asi como identificar agente hostiles (Estados, organizaciones criminales, personas) que permita

monitorearlo a fin de establecer sus vectores de ataque comunmente empleados durantes sus ciberataques.

Otro de los escenarios determinados es en apoyo a las operaciones militares dentro de un teatro de operaciones, la forma de apoyo establecida es la de emplear las capacidades operativas de protección y explotación, en vista que la primera se enmarca a proteger la infraestructura tecnológica de la GUB y GUC dentro de un teatro de operaciones, la protección radica en la ejecución de la tarea táctica de neutralizar los ciberataques con el empleo de tecnologías apropiadas como firewall, IDS, sistemas de encriptación de información que permita establecer una protección a la redes de internet y que se emplean en el área de operación de las diferentes unidades de maniobra y de apoyo, se posea un comando y control adecuado durante las operaciones militares. La capacidad operativa de explotación ejecuta la tarea táctica de explorar en el ciberespacio cuya finalidad radica en identificar vulnerabilidades de nuestra infraestructura tecnológica a fin de poder ser actualizados a últimas versiones nuestros sistemas, también se explora para identificar ciberamenazas (malware, vectores de ataque, agentes hostiles). En el teatro de operaciones se debe disponer de los requerimientos cibernéticos apropiados para sostenimiento a las operaciones, con tecnologías apropiadas, procesos claramente bien estructurados, y operadores especializados de acuerdo a los últimos avances tecnológicos.

Un escenario importante en la protección de los activos críticos nacionales, radíca en el apoyo a las operaciones militares dentro de un teatro de operaciones teniendo en consideración que son aquellos recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales de un estado, ante esta situación el centro de ciberdefensa del Ejército deberá actuar como CSIRT para respuesta ante incidentes cibernéticos deberá actuar de forma integrada con todos los órganos estatales que colaboran y cooperan en materia de seguridad digital a nivel nacional.

La capacidad militar de ciberdefensa está enmarcada en un proceso de operaciones donde la evaluación es una etapa importante, envista que permite realizar una continua supervisión de progreso de las operaciones en el ámbito cibernético, teniendo en consideración que el ciberespacio será cambiante en base a su infraestructura tecnológica dinámica por las nuevas investigaciones y desarrollo de nuevas tecnologías siendo todo ello un desafío para la ciberdefensa.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Del Objetivo N° 01

La capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio, como parte de la ciberdefensa del estado deberá estar en condiciones de neutralizar los ataques del adversario empleando para ello a tecnología más adecuada, teniendo en consideración que la tecnología no es una infraestructura estática y que no basta con adquirir una tecnología y prolongarla en el tiempo, siendo esta una problemática identificada dentro del ejército, la tecnología es una infraestructura dinámica, cambiante. el hombre diseña tecnologías con la finalidad de mejorar y facilitar la vida de las personas a nivel mundial, pero debemos tener en cuenta que estas tecnologías son diseñadas y programadas por personas por cuanto presentan errores de programación por desconocimiento u omisión, estableciendo una vulnerabilidad en dicha tecnología, asimismo será vulnerable con el pasar del tiempo debido a que existirá agentes hostiles que intenten explotar dichas vulnerabilidades por falta de actualizaciones o por una deficiente diseño y programación al no establecer los parámetros de seguridad que son normados.

Del Objetivo N° 02

La capacidad militar de ciberdefensa del Ejército del Perú en la protección de los Activos Críticos Nacionales requiere de una articulación adecuada con los órganos de protección del 1er nivel (entidades público y privadas) y 2do nivel (DINI) en vista que al participar en un tercer momento, se debe de estar en condiciones de dar una respuesta optima de continuidad a los servicios que ofrecen los ACN frente a los incidentes cibernéticos, para ello el CSIRT EP, estará en condiciones de actuar empleando para ello todos sus medios disponibles, en este aspecto las tecnologías SIEM son necesarias para poder realizar una identificación de los comportamientos anómalos a través de los logs almacenados y poder analizar dentro de la infraestructura TI y OT (redes, sistemas, aplicaciones) evidencias claras de ciberamenazas, siendo el operador cibernético el que debe poseer un amplio conocimiento de las diferentes tecnologías emergentes, los ataques cibernéticos no obedecen a un solo patrón, por el contrario es la aglomeración de diferentes tecnologías ofensivas y esto es lo que hace diferente a cualquier tipo de ataque de carácter militar, el operador cibernético debe poseer esa destreza de identificar qué tipo de ataque y así poder establecer las medidas preventivas y reactivas frente a este, cuando mencionamos tecnologías emergente nos referimos a lenguajes de programación, sistemas operativos (servidores, SCADA, usuarios) y cualquier tecnología que en el devenir del tiempo emerja.

Del Objetivo N° 03

El diseño del empleo de la capacidad militar de Ciberdefensa del Ejército del Perú como apoyo a las operaciones militares obedece aun de proceso de operaciones cibernéticas donde los comandantes y sus estados mayores lo utilizan para integrar diferentes procesos y actividades que permiten dar un dinamismo a las operaciones, también permite que el comandante ejerza el ejercicio de comando y control dentro de las operaciones, enfocándose en un planeamiento que sea el diseño de la operación. La preparación que permita la mejora de las capacidades puesta de manifiesto durante la ejecución de la operación y así poner en acción un plan u orden de operaciones, donde la evaluación es continua frente a las tres fases, llevar un proceso de las operaciones es fundamental porque nos permite cumplir con los objetivos establecidos, de una manera pormenorizada y ejerza el comandante una compresión, visualización, descripción y dirección propia las operaciones cibernéticas. Debemos de tener claro que el ciberespacio es el quinto dominio aún muy poco estudiado e incierto, donde la comprensión situacional de comandante es fundamental, así como el dominio técnico necesario para dicha comprensión, sumado a que los ciberataques son sofisticados y cambiantes en el tiempo. Por cuanto las exigencias para las fuerzas de nivel táctico en Ciberdefensa son cada vez mayores.

6.2 Recomendaciones

Para determinar el empleo de la capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio es muy importante tener claro el ambiente operacional y la comprensión de que actuamos como parte de la ciberdefensa que lidera el comando operacional de ciberdefensa y realizamos operaciones cibernéticas de manera conjunta en vista que necesitamos integrarnos a diferentes cibercomandos con la finalidad de poder identificar ciberamenazas y vulnerabilidades de las infraestructuras cibernéticas a la cual protegemos, por cuanto se recomienda que las capacidades operativas ofensiva, defensiva y explotación requieren ser implementadas óptimamente con infraestructura tecnológica (datacenter, simuladores, computadoras potentes, entornos controlados, etc.) sin ello poco se hará en poder cumplir con la misión asignada de protección hacia nuestras fuerzas y hacia los activo críticos nacionales que por ley se ha sido consignado.

Referente a la capacidad operativa ofensiva, se recomienda dotar de operadores especializados, en base a personal de nuestra fuerza identificados y evaluados en base perfiles establecidos, o reclutar especialistas del entorno civil. Dicho personal debe ser consecuente que la ciberdefensa es una capacidad militar que requiere de personal investigador y de dominio de diferentes tecnologías. En la capacidad operativa explotación se

requiere de sistemas OSINT, basabas en tecnología de inteligencia artificial, Big data para el tratamiento de amplia información, y tecnología emergente que nos permita explorar e identificar ciberamenazas y vulnerabilidades en el ciberespacio.

Con respecto La capacidad militar de ciberdefensa del Ejército del Perú en la protección de los activos críticos nacionales que es muy importante la articulación con los niveles de seguridad de los ACN, se recomienda identificar los procesos adecuados que conlleve a una articulación entre las entidades protegidas, DINI y COCIBER, en lo que refiere al Ejército del Perú el CECIBER se recomienda que establezca sus planes procedimentales en lo que refiere a respuesta a incidentes a través de su CSIRT EP, asimismo implementar tecnologías de monitoreo de log a través de un SIEM colector articulado con los ACN, con la finalidad de poder identificar ciberamenazas, en lo que refiere a operadores cibernéticos deben de tener un perfil adecuado, se recomienda que el Comando de Educación y doctrina del Ejército (COEDE) implemente la capacidad de ciberdefensa como un programa educacional en las escuelas de formación Escuela Militar, Escuela Técnica, Escuela de Inteligencia. Un programa de nivel básico hasta el avanzado que permita despertar el interés del personal militar en sus niveles de formación y poder identificar personal con el perfil más adecuado para esta capacidad, sin embargo esto llevaría algunos años, y teniendo en consideración esta capacidad debe ser potenciada de manera oportuna en el tiempo, se recomienda realizar una captación a nivel nacional a través de la gestión del talento humano y poder identificar el personal más adecuado sin circunscribirnos a un arma o especialidad y poderlo promover con puntajes adecuados para mejorar las aspiraciones dentro de la institución, asimismo a través de la Dirección de Personal del Ejército (DIPERE) realice la captación de personal de procedencia universitaria y técnica con el perfil adecuado para esta capacidad y así poder tener operadores cibernéticos acordes a los requerimientos operacionales.

En referencia al diseño del empleo de la capacidad militar de ciberdefensa del Ejército del Perú como apoyo a las operaciones militares se recomienda que el CITELE como órgano rector al ciberdefensa dentro del ejército, pueda establecer los procesos adecuados a la empleabilidad de la ciberdefensa del ejército, en base a los escenarios de ciberguerra, en apoyo a las operaciones militares , siendo este muy importante la ejecución de las operaciones y como en el proceso propio de las operaciones cibernéticas, cabe de detallar que el análisis del ambiente operacional en el ámbito de la ciberdefensa es complejo y dinámico por su naturaleza propia en vista que la tecnología emerge y con ella las ciberamenazas y la diferentes vulnerabilidades, por cuanto los procesos adecuados a las

capacidades operativas como conducción y ejecución requieren que estos seas establecidos. Con respecto a las tecnologías que forman parte de la ciberdefensa dentro del ejercito del Perú se recomienda ciberdefensa y telemática del Ejército, centro de ciberdefensa, y la Dirección de Ciencia y Tecnología del Ejército, establezcan una sinergia investigativa, con la finalidad de poder realizar una campaña agresiva a nivel nacional, que promueva la Investigación, desarrollo e innovación en tecnología para la ciberdefensa, asimismo a través de la Dirección de Planeamiento del Ejército poder establecer como una prioridad el contar con una ciberdefensa institucional y que se encuentre entre una de las mejores de la región, que este cuente con el presupuesto adecuado para su implementación de infraestructura física.

Referencias bibliográficas

Consejo de Ministros. (2017). Decreto Supremo Nº106-2017-PCM. *Identificación de activos críticos nacionales*. Lima.

Ministerio de Defensa. (2005). *Libro Blanco.* MINDEF.

Andress, J., & Wintelferd, s. (2011). *Cyber Warfare técnicas, tácticas y herramientas para practicantes de seguridad.* Warfare.

Avast. (2002). *Cortafuegos*. .https://www.avast.com/es-es/c-what-is-a-firewall

CEEAG. (2017). *La ciberguerra: sus impactos y desafíos. Chile.* Andros.

Cloudflare. (2021). *WAF.* https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

Comando Conjunto. (2016). *R.M N° 1490.* MINDEF.

Comando Conjunto. (2016). *Resolución Ministerial 1490 de 2016. Aprueba la definición de los factores que conforman una capacidad militar y la tipología de las capacidades militares de las Fuerzas Armadas.*

Comando Operacional de Ciberdefensa. (2020). *Ministro de Defensa inauguró instalaciones del Comando Operacional de Ciberdefensa. Gob.pe. Recuperado el 24 de setiembre 2021.* https://www.gob.pe/busquedas?term=cocid&institucion=ccffaa&topic_id

Confluent. (2021). *SIEM*. https://www.confluent.io/blog/siem-optimization-for-better-cyber-security/

Congreso Constituyente Demócratico. (1993). *Constitución Política del Perú de 1993.*

Congreso de la República del Perú. (2018). *Decreto Legislativo N° 1412. Por lo cual se expide Ley de Seguridad Digital.*

Congreso de la República del Perú. (2019). *Ley 30999 de 2019. Por lo cual se expide Ley de Ciberdefensa.*

Consejo de Ministros. (2017). *Decreto supremo N° 106 de 2017. Por lo cual se expide la Identificación de Activos Criticos Nacionales.* PCM.

Ecured. (2022). *Acceso no autorizado.* https://www.ecured.cu/Archivo:Detección_intrusos_550x310.gif

Ejército de Estados Unidos. (2018). *Operaciones cibernéticas JP 3-12.* US ARMY.

Ejército del Perú. (2015). *Manual de operaciones M 1-13.* EP.

Emanuel. (2019). *Capacidad de respuesta del centro de ciberdefensa en las operaciones y acciones militares. Lima [Tesis de Maestria, Escuela de Guerra del Perú].* http://repositorio.esge.edu.pe/handle/20.500.14141/251

Hackingarticles. (2020). *Honeypots.* https://www.hackingarticles.in/comprehensive-guide-on-honeypots/

Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación las rutas cuantitativa, cualitativa y mixta.* McGRAW-HILL Interamericana.

Huawei. (2022). *Antivirus.* https://forum.huawei.com/enterprise/es/modulo-contenido-de-seguridad-la-funci%C3%B3n-antivirus-para-un-firewall-serie-sg6000e/thread/671009-100233

Instituto de Estudios Estratégico. (2010). *Ciberseguridad, retos y amenazas. Ministerio de Defensa.*

Iptelecom. (2020). *Antiddos.* http://www.iptelecom.asia/index.php/ddos-attack-protection/

JID. (2020). II Conferencia de Ciberdefensa 2020. Bogotá, Colombia. https://www.iadfoundation.org/es/2020/05/28/ii-conferencia-de-ciberdefensa-2020/

Karpesky. (2021). *Las amenazas avanzadas persistentes. Recuperado el 05 enero 2022.* https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Lanfranco, E. (2021). *Computer emergency response team.* UNLP.

NIST. (2019). *Núcleo del marco.* https://www.nist.gov/

Rexton, P. (2014). *Como analizar la guerra en WIFI de ciberguerra a wikiguerra: la lucha por el ciberespacio.Recuperado el 25 octubre 2022.* REX. https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20141231_art007SPA.pdf.

Rochina, P. (3 de julio de 2022). *Hacktivismo: Qué hay detrás de este movimiento activista? Retrieved from INESEM, Recuperado el 24 de junito 2021*. https://www.inesem.es/revistadigital/informatica-y-tics/hacktivismo/

Saenz, C. C. (2020). *La Ciberdefensa en el sistema de mando y control en la 9na Brigada Blindada. Lima. [Tesis de Maestria, Escuela de guerra del Perú].* Lima. http://repositorio.esge.edu.pe/handle/20.500.14141/246

Salcedo, C. A. (2017). *Un ensayo sobre la seguridad y la defensa en el Perú, nuevas amenazas, nuevos roles. CCFFAA.* MINDEF. https://www.esffaa.edu.pe/wp-content/uploads/2020/10/libro-ensayo-seguridad-defensa.pdf.

Schmitt, M. N. (2013). *Manual de Tallin 2.0.*

SEDENA. (2014). *Seguridad y Defensa Nacional.*

Urrutia, F. D. (2019). *Ciberseguridad marco NIST, un abordaje integral a la ciberseguridad. OEA.* https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Vergara, E., & Trama, G. (2017). *Operaciones militares ciberneticas.* Vertra.

Vilcarromero Zubiate, L. L., & Vilchez Linares, E. (06 de Agosto de 2018). *Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de.* Lima, Perú: UPC.

ANEXOS

ANEXO 1

1. Matriz de consistencia

MATRIZ DE CONSISTENCIA

TITULO: CAPACIDAD MILITAR DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ EN LAS OPERACIONES MILITARES EN EL CIBERESPACIO, 2021

Preguntas de Investigación	Objetivos	Teorías	Categorías	Subcategorías	Metodología	Análisis de datos
¿Cómo se emplea la capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio? ¿Cómo se relaciona la capacidad militar de ciberdefensa del Ejército del Perú en la protección de los Activos Críticos Nacionales? ¿Cuál es el enfoque de diseño para el empleo de la capacidad militar de ciberdefensa del Ejército del Perú en apoyo a las operaciones militares?	Analizar la capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio. . Analizar la capacidad militar de ciberdefensa del Ejército del Perú en la protección de los Activos Críticos Nacionales. Proponer un enfoque de diseño a través de buenas prácticas para el empleo de la capacidad militar de ciberdefensa del Ejército del Perú en apoyo a las operaciones militares.	La presente investigación se sustenta en la teoría basada en el enfoque del diseño de la capacidad militar de ciberdefensa y su implementación a través de buenas prácticas en las diferentes entidades militares y como esta capacidad se ha empleado en el Ejército del Perú y su concepción propia de las operaciones en el ciberespacio y como está vinculada a la seguridad nacional.	Capacidad militar de ciberdefensa Operaciones militares de ciberdefensa Capacidad de interoperabilidad . Doctrina de ciberdefensa	• Capacidades operativas. • Tecnología militar de ciberdefensa • Ambiente operacional • Planeamiento operaciones de ciberdefensa. • Operadores cibernéticos conjuntos • Taxonomía ciberdefensa • Manuales de ciberdefensa • Ejercicio táctico de ciberdefensa	**Enfoque:** Cualitativo **Tipo:** teórico- empírica **Método:** Hermenéutico **Muestra**: Muestra de expertos, teniendo previsto la entrevista a 05 oficiales con amplios conocimientos del tema.	**Técnicas:** Entrevista Observación Análisis documental **Instrumentos:** Guía de entrevistas Guía de observación Ficha documental **Técnica de análisis de datos:** Se desarrollará de manera artesanal

ANEXO 2

2. Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

Buenos días/tardes, expreso mi agradecimiento por el tiempo y la atención prestada para poder realizar esta entrevista, cuya información y comentarios proporcionados serán muy valiosos para profundizar la presente investigación.

Entrevistado: Grado Académico: DNI: Lugar – fecha : Experiencia alcanzada:	
Título de la investigación: Capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio, 2021	
N°	GUÍA DE ENTREVISTA
01	Conociendo el avance de la tecnología en los últimos años y con ella las amenazas a la Seguridad Nacional, ¿Qué opina de la capacidad militar de ciberdefensa en el Ejército del Perú frente a las ciberamenazas?
	Rpta
02	¿Cómo considera usted, que debería emplearse la capacidad militar de ciberdefensa para realizar maniobras en el ciberespacio?
	Rpta
03	¿Cómo establecería la relación entre el factor humano y los procesos propios de la ciberdefensa?
	Rpta
04	Dentro de las operaciones de ciberdefensa, ¿Qué procedimientos se emplean actualmente en el Ejército del Perú para identificar a los agentes hostiles, teniendo en cuenta que las ciberamenazas son anónimas
	Rpta
05	Sabiendo que la doctrina en ciberdefensa en el Ejército del Perú es limitada, ¿Qué esfuerzos se están realizando y que herramientas emplean para el planeamiento y ejecución de las operaciones de ciberdefensa?
	Rpta
06	En base a los pilares de tecnología, procesos y personas dentro de la capacidad militar de ciberdefensa ,¿Qué opinión tiene referente a que los 3 estén al mismo nivel para la realización optima de operaciones?
	Rpta
07	¿Cómo definiría usted el ciberespacio desde un nuevo enfoque militar teniendo en cuenta la relación a las operaciones de ciberdefensa?
	Rpta
08	¿Cómo sería la integración de la ciberdefensa del Ejercito del Perú dentro del Comando Operacional de Ciberdefensa?
	Rpta

FICHA DE ANÁLISIS DOCUMENTAL

Se seleccionó los documentos que contenían información que está relacionada a capacidad militar de Ciberdefensa del ejército del Perú en las operaciones militares en el ciberespacio centro de Ciberdefensa del Ejército

TIPO DE DOCUMENTO	PAIS	REFERENCIA	TEMAS
Ley	Perú	*Ley de Ciberdefensa Ley N° 30999.*	Capacidad de Ciberdefensa de las FF. AA
Ley	Perú	Decreto Legislativo N° 1412. *Ley de Gobieno Digital*.	Normativa de la Seguridad Digital
Libro	Chile	*La Ciberguerra: sus impactos y desafíos*	Ciberguerra
Informe	EE. UU	*II Conferencia de Ciberdefensa*	Operaciones de Ciberdefensa
Manual	Estonia	*Manual de Tallin 2.0.*	Parámetros de la ciberguerra
Libro	Perú	*Seguridad y Defensa Nacional.*	Principios de la Seguridad Nacional
Libro	EE. UU	*Ciberseguridad Marco NIST.*	Marco de trabajo
Libro	Argentina	*Operaciones militares ciberneticas*	Capacidades de ciberdefensa

ANEXO 3

3. Validación de instrumentos

HOJA DE VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA INVESTIGACIÓN: Capacidad militar de Ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio, 2021

I. DATOS DEL EXPERTO:

a. Apellidos y nombres : CAMACHO SORIANO Adrian Victor
b. Grado académico-profesión : Magister en Ciencias Militares
c. D.N.I. : 42835847
d. N° de teléfono : 976694234
e. Lugar y fecha : Chorrillos, 05 Octubre 2021

II. DATOS DEL INSTRUMENTO DE EVALUACIÓN

a. Autor del Instrumento : Bach. Alexander Bladimir Pampa Urieta
b. Método de Investigación : Hermenéutico
c. Tipo de entrevista : Semi- Estructurada

III. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	SI	No	Observaciones
1	CONSISTENCIA	Las preguntas de la entrevista son congruentes a los objetivos de la investigación	X		
2	CLARIDAD	Está formulada con una sintaxis y semántica que permita la comprensión adecuada	X		
3	ORGANIZACION	Existe una organización lógica en el instrumento	X		
4	SUFICIENCIA	Contiene preguntas necesarias para recabar información suficiente	X		
5	RELEVANCIA	Las preguntas se orientan a la obtencion de informacion trascendente y substancial.	X		
Sugerencias y/o Recomendaciones		El suscrito es de opinión que el presente instrumento es aplicable.			

.....

Firma y Post firma del Validador

HOJA DE VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA INVESTIGACIÓN: Capacidad militar de Ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio, 2021

I. DATOS DEL EXPERTO:

a. Apellidos y nombres : CANAVAL RAMÍREZ Fernando Javier
b. Grado académico-profesión : Mg. Crl EP (r)
c. DNI : 43662341
d. N° de teléfono : 943271321
e. Lugar y fecha : Chorrillos, 29 noviembre 2021

II. DATOS DEL INSTRUMENTO DE EVALUACIÓN

a. Autor del instrumento : Bach. PAMPA URIETA Alexander Bladimir
b. Método de investigación : Hermenéutico
c. Tipo de entrevista : Semi- Estructurada

III. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	SI	No	Observaciones
1	CONSISTENCIA	Las preguntas de la entrevista son congruentes a los objetivos de la investigación	X		
2	CLARIDAD	Está formulada con una sintaxis y semántica que permita la comprensión adecuada	X		
3	ORGANIZACIÓN	Existe una organización lógica en el instrumento	X		
4	SUFICIENCIA	Contiene preguntas necesarias para recabar información suficente	X		
5	RELEVANCIA	Las preguntas se orientan a la obtencion de informacion trascendente y substancial	X		
Sugerencias y/o Recomendaciones		El instrumento es aplicable			

FERNANDO JAVIER CANAVAL RAMÍREZ
Mg. Crl EP (r)
Asesor Metodológico

ANEXO 4

4. Autorización para recolección de datos

PERÚ | Ministerio de Defensa | Ejército del Perú | COEDE Escuela Superior de Guerra del Ejército Escuela de Postgrado

"Año del Bicentenario del Perú: 200 años de Independencia"

Chorrillos, 10 de setiembre del 2021

Oficio Nº 145/U-8.g.1/DGI/27.00

Señor Gral Brig Cmdte Gral de Ciberdefensa y Telemática del Ejército.–**SAN BORJA**

Asunto : Solicita brindar facilidades a personal que se indica

Ref. : a. Reglamento para la obtención del grado académico de Maestro en Ciencias Militares
b. Reglamento de Investigaciones de la ESGE-EPG

Tengo el agrado de dirigirme a Ud., en relación a los documentos de la referencia para solicitarle se sirva brindar las facilidades para el levantamiento de datos e informaciones al **My Art PAMPA URIETA Alexander Bladimir**, estudiante de la X Maestría en Ciencias Militares de esta casa de estudios, que está realizando la investigación titulada: **Capacidad militar de Ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio, 2021.**

Agradeciendo de antemano por las facilidades brindadas, en espera del acuse de recibo correspondiente, es propicia la oportunidad para expresarle mis consideraciones y deferente estima.

Dios guarde a Ud.

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO ESCUELA DE POST GRADO DIRECCIÓN

O – 0214452666 – A+
LUIS ALBERTO ROJO ALZAMORA
General de Brigada
Director de la Escuela Superior de Guerra
Escuela de Postgrado

Distribución:
CITELE.....01
Archivo.....01/02

COMANDO DE EDUCACION Y DOCTRINA DEL EJERCITO
DEPARTAMENTO DE PERSONAL
OFICINA POSTAL DEL COEDE
SECCION RECEPCION
Fecha Hora 23 SEP 2021
Firma.....
ALZAPATA T
SGTO 1 REE 14:41

ANEXO 5

5. Compromiso ético

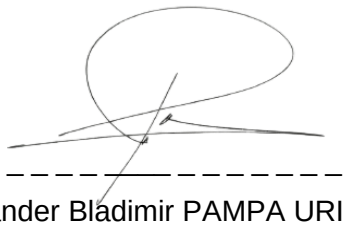
Declaración de Compromiso Ético

El presente trabajo de investigación titulado: **Capacidad militar de ciberdefensa del Ejército del Perú en las operaciones militares en el ciberespacio, 2021**, se ha realizado en estricto apego a la metodología de la investigación y a las normas éticas para investigación en Ciencias Militares promulgadas por el Departamento de Gestión de la Investigación de la Escuela Superior de Guerra del Ejército-Escuela de Postgrado.

En vista de lo anterior:

Yo Bach Alexander Bladimir PAMPA URIETA, egresado de la X Maestría en Ciencias Militares de la Escuela Superior de Guerra del Ejército-Escuela de Postgrado (ESGE-EPG), declaro bajo juramento que he desarrollado esta investigación siguiendo las instrucciones brindadas por el Departamento de Gestión de la Investigación, desde la elaboración del marco referencial y recolección de la información, hasta el análisis de datos y elaboración del informe final.

En tal sentido la información contenida en el presente documento es producto de mi trabajo personal, apegándome a la legislación sobre propiedad intelectual, sin haber incurrido en falsificación de la información o cualquier tipo de fraude, por lo cual me someto al marco legal y normativo vigente relacionado a dicha responsabilidad, así como a las normas disciplinarias establecidas en la ESGE-EPG.



Alexander Bladimir PAMPA URIETA

DNI N° 42194606

ANEXO 6

6. Hoja de datos personales

HOJA DE DATOS PERSONALES

GRADO MY EP

NOMBRES ALEXANDER BLADIMIR

APELLIDOS PAMPA URIETA

EMAIL DUBOA_2003@HOTMAIL.COM

DIRECCIÓN RESIDENCIAL TORRES DE MATELLINI

SECTOR A BLOCK 14 DEP 104

TELEFONO +51 950492910

FIRMA

ANEXO 7

7. Aporte a la investigación

7.1 Título del aporte a la investigación

Propuesta de empleo de la Capacidad de Ciberdefensa del Ejército del Perú en operaciones y acciones militares en/y mediante el ciberespacio

7.2 Objetivos del aporte de investigación

Este manual ha sido desarrollado con el propósito de establecer el empleo de la capacidad de Ciberdefensa teniendo como capacidades operativas: defensa, explotación y respuesta todo ello estipulado de manera normativa en la Ley de Ciberdefensa, teniendo en consideración que solo la capacidad de respuesta será con orden del escalón superior, asimismo el CCFFAA es la responsable de conducir y ejecutar operaciones de Ciberdefensa a través de su Comando Operacional (COCIBER) articulando esta con las IIAA. Este manual señala como se articulan las capacidades operativas con las tecnologías, procesos y operadores, el empleo de la capacidad de Ciberdefensa, también visualizará una metodología sobre el proceso de las operaciones teniendo como medio el ciberespacio de acuerdo al siguiente detalle:

- Operaciones de Ciberdefensa en operaciones militares.
- Operaciones de Ciberdefensa en acciones militares.

7.3 Justificación del aporte de investigación

El empleo de la capacidad de Ciberdefensa en las operaciones militares justifica su necesidad por cuanto el Ejército del Perú al implementar dicha capacidad dentro de su organización estructural esgrimió la compresión de un ambiente global vigente de tecnologías emergentes a gran escala en un aspecto militar y civil, como también de ciberamenzas existentes, comprendiendo que las infraestructuras cibernéticas disponibles del estado sean estos públicos o privados, requieren para su funcionamiento y sostenimiento dentro de aparato productor de estado se le brinde protección frente los diferentes incidentes cibernéticos.

Asimismo, un estado de ciberguerra, que demandaría la realización de operaciones militares, requiere que las capacidades operativas de Ciberdefensa sean las más optimas, en vista que una de las características fundamentales de las ciberamenazas en el ciberespacio es el anonimato, lo que dificulta identificar al agente hostil que ha vulnerado o intenta vulnerar la infraestructura cibernética, otra dificultad identificada es poder determinar la magnitud de la agente hostil pudiendo ser un Estado, organización, persona, para poder determinar dicha magnitud resultará de un análisis profundo, empleando capacidades operativas lo que demandaría tiempo esfuerzo y recursos para que estos sean lo más oportuno posibles.

ANEXO 8

8. CD conteniendo la tesis en pdf

ESCUELA SUPERIOR DE GUERRA
DEL EJÉRCITO

ESCUELA DE POSTGRADO

TESIS

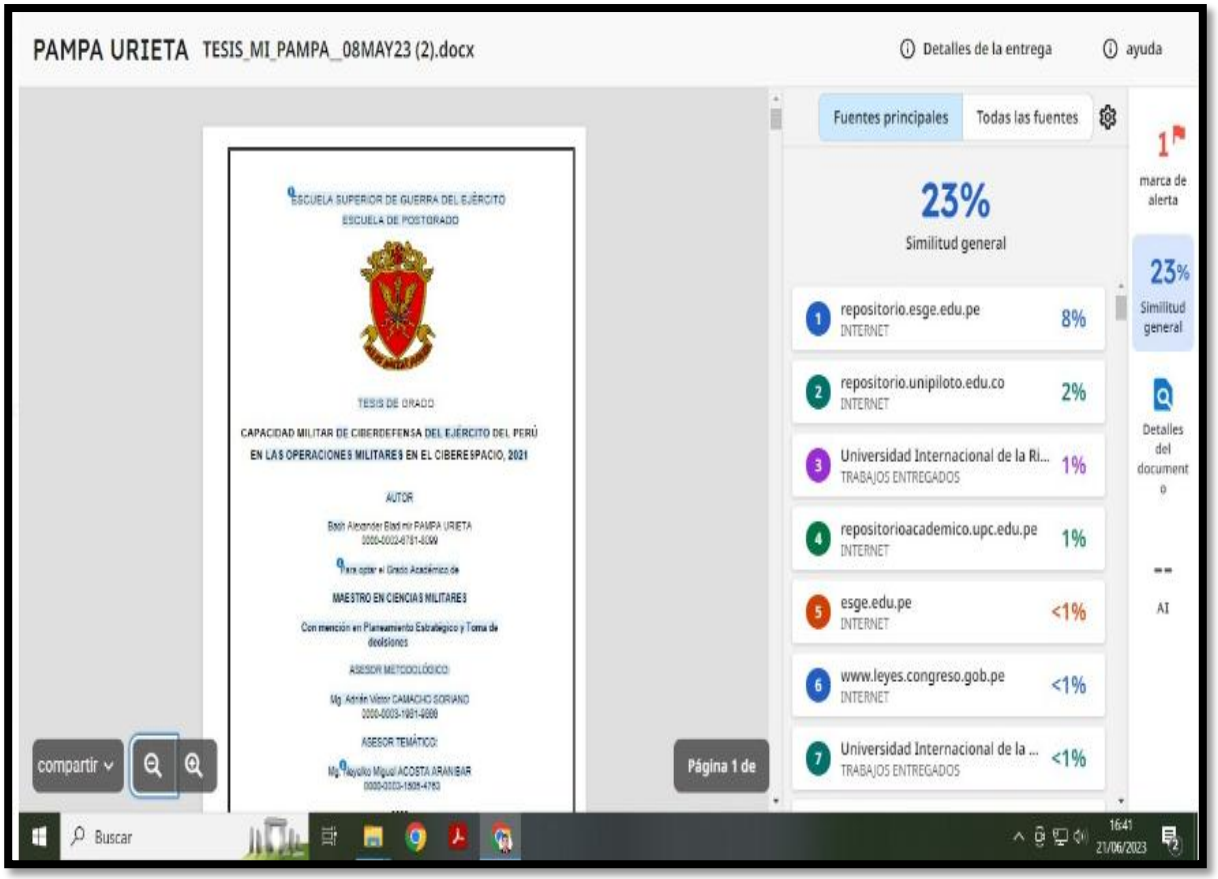
CAPACIDAD MILITAR DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ EN LAS OPERACIONES MILITARES EN EL CIBERESPACIO, 2021

AUTOR:
Bach. Alexander Bladimir PAMPA URIETA

2023

ANEXO 9

9. Reporte de similitud turnitin


PAMPA URIETA TESIS_MI_PAMPA_08MAY23 (2).docx
Detalles de la entrega
ayuda
ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO
TESIS DE GRADO
CAPACIDAD MILITAR DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ EN LAS OPERACIONES MILITARES EN EL CIBERESPACIO, 2021
AUTOR
Bach Alexander Elad mir PAMPA URIETA
0000-0002-6781-8099
Para optar el Grado Académico de
MAESTRO EN CIENCIAS MILITARES
Con mención en Planeamiento Estratégico y Toma de decisiones
ASESOR METODOLÓGICO:
Mg. Arnán Víctor CAMACHO SORIANO
0000-0003-1981-9088
ASESOR TEMÁTICO:
Mg. Rayuko Miguel ACOSTA ARANIBAR
0000-0003-1905-4783
Fuentes principales
Todas las fuentes
23%
Similitud general
1 repositorio.esge.edu.pe INTERNET 8%
2 repositorio.unipiloto.edu.co INTERNET 2%
3 Universidad Internacional de la Ri... TRABAJOS ENTREGADOS 1%
4 repositorioacademico.upc.edu.pe INTERNET 1%
5 esge.edu.pe INTERNET <1%
6 www.leyes.congreso.gob.pe INTERNET <1%
7 Universidad Internacional de la ... TRABAJOS ENTREGADOS <1%
1 marca de alerta
23% Similitud general
Detalles del documento
-- AI
compartir
Página 1 de
Buscar
16:41
21/06/2023