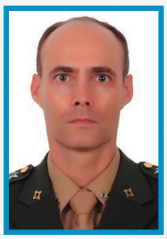
El presente artículo propone una perspectiva amplia y general de algunos conceptos, lineamientos y propuestas de desarrollo de doctrina para ser considerado como posible alternativa por nuestro Comando Conjunto de las Fuerzas Armadas, desarrollado como resultado de seis meses de estudio e investigación en el Programa de Operaciones Cibernéticas de la Escuela de Comunicaciones del Ejercito (ECOME).

PROPUESTA ALTERNATIVA DE DOCTRINA CIBERNÉTICA

COMO REFERENCIA EN EL EJÉRCITO DEL PERÚ

This article proposes a broad and general perspective of some concepts, guidelines and doctrine development proposals to be considered as a possible alternative by our Joint Command of the Armed Forces, developed as a result of six months of study and research in the Cybernetics Operations Program, which may serve as a guide and consultation to soon develop a doctrine of our own Army of Peru.



Teniente Coronel
Ejército de Brasil
André Ferreira Alves Machado

Licenciado en Ciencias Militares en la Academia Militar de las Agulhas Negras (AMAN), Rio de Janeiro, Brasil. Licenciado en Matemáticas en la Universidad Regional Integrada (URI), Rio Grande do Sul, Brasil. Diplomado en Tecnología de la Información y Comunicación en Curitiba, Brasil. Diplomado en Redes de Computadoras en Brasilia, Brasil. Magister en Comunicaciones Militares, Rio de Janeiro, Brasil. Magister en Computación, en el Instituto Tecnológico de Aeronáutica (ITA), São Paulo, Brasil. Profesor de la Escuela de Comunicaciones del Ejercito (ECOME) del curso de Defensa Cibernética.

INTRODUCCIÓN

Con la evolución de las Tecnologías de la Información y Comunicaciones (TIC´s) se está creando un nuevo escenario donde se vienen desarrollando diversas actividades, tanto lícitas como ilícitas, en el ciberespacio. El principal problema que tenemos como Nación es la falta de conciencia y de desarrollo de la capacidad para poder enfrentar estos nuevos cambios en el escenario mundial, particularmente el sector Defensa, en el cuál involucra al Comando Conjunto de las Fuerzas Armadas y, en especial, el Ejército del Perú. Pero ¿Qué hacer si no tenemos una guía?, ¿Necesitamos una guía?, a base de estas dos preguntas se formula el presente artículo.

Es cierto que tenemos mucha referencia extranjera sobre el actuar en estos nuevos escenarios los cuales son ya tipificados en muchos manuales y libros como: marítimo, terrestre, aéreo, espacial, espacio electromagnético y ciberespacio. El espacio cibernético tiene la característica especial de involucrar a todos los demás. Así, para poder adecuar estos escenarios a nuestra realidad, deberíamos primero desarrollar capacidades en cada uno, lo cual es todavía poco probable debido a los múltiples problemas sociales y económicos por el cual estamos atravesando como Nación.

El presente artículo solo tomará conceptos y propuestas comunes, porque todo lo que enmarca la cibernética es un tema muy amplio y extenso. Lo que se quiere plantear es una forma de visualizar todo este nuevo escenario, definiendo algunos conceptos, desarrollando algunas conceptualizaciones del problema y como tal tratar de brindar esa guía que tanto necesitamos para posteriormente crear una Doctrina que parta primero del Ministerio de Defensa para luego ser referencia en los siguientes niveles hasta tener la que

PALABRAS CLAVE: CIBERNÉTICA, DOCTRINA, EJÉRCITO, PERÚ.
KEYWORDS: CYBERNETIC, DOCTRINE, ARMY, PERU.

necesitamos: una doctrina de operaciones y acciones en el ciberespacio del Ejército del Perú.

PROPUESTA DE DOCTRINA CIBERNÉTICA

En el presente artículo, brindamos un enfoque en todos los niveles en los que se está trabajando o implementando esta nueva área común, tanto para la sociedad civil como para las Fuerzas Armadas, denominada comúnmente como cibernética. Es a partir del enfoque que tengamos, ayudado por los niveles de planeamiento, de donde se va a poder dictar los lineamientos, procedimientos y guías para la creación de una futura Doctrina Cibernética Nacional, como base y referencia para un empleo a posteriori en el Comando Conjunto de las Fuerzas Armadas, y también una viable posibilidad de doctrina para uso de nuestro Ejército.

Para ello creemos que los siguientes conceptos deberían de estar inmersos en la propuesta de doctrina cibernética elaborada por la más alta organización respecto a Seguridad Cibernética Militar que existe en el Perú. Además, esta documentación debe estar alineada, relacionada y amparada con normas y procedimientos de la Secretaria de Gobierno Digital y demás órganos civiles responsables por la Seguridad Cibernética en nuestro País.

1. CONCEPTOS CIBERNÉTICOS

La definición de ciberespacio varía notablemente dependiendo del país y de los intereses y necesidades que se tengan. Del manual militar estadunidense tenemos que: “Es un dominio global dentro del entorno de la información, compuesto por una red de infraestructuras de tecnologías de la Información interdependientes; que incluye el internet, las redes de telecomunicaciones, los sistemas de información y los controladores y procesadores integrados junto con sus usuarios y operadores” (EUA, 2013)

Esta definición de ciberespacio se escogió porque justamente abarca en un concepto simple toda esta información descrita. Decimos que es un dominio total en el entorno de la información y, al referirnos al dominio, explicamos el espacio en sí, en el que se encuentra toda esta nueva dimensión; se trata de independizar un nuevo escenario, el ciberespacio. Formando también parte de este espacio el internet, las redes, que pueden ser alámbricas o inalámbricas, los sistemas de información, tanto de organismos privados como públicos, y hasta los mismos usuarios y operadores que ejecutan comandos en esta nueva dimensión.

Siguiendo la estructura presentada por Martín Libicki, en el Centro Superior de la Defensa Nacional de España (CESEDEN, 2012), dividimos el ciberespacio en tres capas: Capa sintáctica, capa semántica y la capa física.

Capitán EP
Ddedwin Galindo Gonzales

Licenciado en Ciencias Militares en la Escuela Militar de Chorrillos “Crl Francisco Bolognesi”. Licenciatura en Administración en la Universidad Señor de Sipan. Magister en Docencia Universitaria con Mención en Gestión Educativa en la Universidad San Pedro de Chimbote. Programa básico en Blindados en la Escuela de Blindados, Locumba. Especialización en Operaciones Cibernéticas, en la Escuela de Comunicaciones del Ejercito (ECOME), Lima – Perú.

Teniente EP
Eloy Robles Gayoso

Licenciado en Ciencias Militares y diplomado en gestión del escuadrón de caballería blindado, en la Escuela Militar de Chorrillos "Crl Francisco Bolognesi". Especialización en Operaciones Cibernéticas, en la Escuela de Comunicaciones del Ejercito (ECOME), Lima – Perú.

1. Capa sintáctica: La constituyen los datos, los programas que introducimos para gestionar el conocimiento almacenado en los discos y servidores. Abarca en si toda la información por procesar o transmitir. Es una capa lógica.
2. Capa semántica: Contiene las instrucciones que los diseñadores y usuarios introducen en los sistemas como protocolos, lenguajes y sistemas operativos. Se puede deducir que también es una capa lógica y que almacena todos los procedimientos, funciones algorítmicas que son necesarias para poder procesar y transmitir la información.
3. Capa física: Es todo aquello que podemos ver y tocar en nuestro ordenador, servidores ubicados en otros países, cables submarinos y satélites. Específicamente nos estamos refiriendo a todo el hardware.

Una vez definido el concepto y la división del ciberespacio, podemos tener ya un entendimiento común de donde se van a realizar tanto acciones como operaciones militares. Pero no todo se va a actuar simultáneamente, existe una diferencia de niveles de planeamiento y una específica tarea para cada nivel. Para tener un mejor entendimiento de los niveles de planeamiento de una nación, particularmente del Perú, hemos tomado como referencia el Manual de doctrina del proceso de planeamiento conjunto (PERÚ, 2010) que tipifica estos niveles de la siguiente manera:

1. Nivel Político / Estratégico Nacional: Nivel donde se desarrolla el Planeamiento Estratégico nacional y se determinan objetivos de la Seguridad y Defensa Nacional, emplean todos los poderes del Estado y se establece cómo deben actuar en el ámbito Político, Económico, Psicosocial, Científico, Tecnológico y Militar. Por ser un nivel de ámbito nacional, tiene responsabilidad directa de esta Seguridad la Presidencia del Consejo de Ministros, la Secretaría de Gobierno Digital, todos los Ministerios, en especial el Ministerio de Defensa.
2. Nivel Estratégico Operacional: Nivel donde se relaciona la Política de Seguridad y Defensa Nacional con las actividades operacionales, siendo responsable el Jefe del Comando Conjunto de las Fuerzas Armadas (CCFFAA). En este nivel también tienen responsabilidad los Institutos Armados de la Nación (Ejército, Marina y Fuerza Aérea), amparados en los artículos 163, 164 y 165 de nuestra Constitución Política vigente, donde se define claramente el grado de responsabilidad para la Defensa Nacional.
3. Nivel Operacional: Nivel donde se desarrollan las Maniobras Estratégicas Operacionales, administra el Teatro de Operaciones (Área de responsabilidad), siendo responsable el Comandante del

Comando Operacional. Debido al auge de acciones y operaciones en el ciberespacio, el CCFFAA ha creado el Comando Operacional de Ciberdefensa (COCID); que es el órgano responsable de la Defensa Cibernética frente a ataques cibernéticos y protección de nuestros activos críticos; constituyéndose también con componentes de los tres Institutos Armados.

4. Nivel Táctico: Nivel donde se conducen Grandes Unidades de Combate o fuerzas de tarea en el campo de batalla. Aquí es donde se desarrollaría las actividades tácticas dentro de un Instituto Armado, pero dependiendo directamente del COCID.

Dentro del contexto de los Niveles de Planeamiento, tenemos que definir qué responsabilidad cibernética se le va a otorgar a cada uno, sabiendo que en cada Nivel de Planeamiento la visualización y ejecución de la acción u operación en el ciberespacio cambia de noción considerablemente. Teniendo como referencia el Manual de Doctrina cibernética de Brasil (BRASIL, 2014), se sugiere las siguientes definiciones:

1. Seguridad Cibernética: "Capacidad de asegurar la existencia y la continuidad de la sociedad de la información de una nación, garantizando y protegiendo, en el ciberespacio, sus activos de información y sus infraestructuras críticas". Con esta definición, se está planteando una capacidad de carácter y ámbito nacional.

TABLA 1: NIVELES DE PLANEAMIENTO Y SU RELACIÓN CON LOS RESPONSABLES

Niveles de Planeamiento	Acciones	Responsables
Político / Estratégico Nacional	Seguridad Cibernética	Presidencia del Consejo de Ministros
		Secretaria de Gobierno Digital
		Ministerios (1)
Estratégico Operacional	Defensa Cibernética	Jefe de CCFFAA (2)
		Comando Operacional de Ciberdefensa
		Ejercito del Perú (EP)
		Marina de Guerra del Perú (MGP)
		Fuerza Aérea del Perú (FAP)
Operacional	Guerra Cibernética	Cibercomando EP (3)
		Cibercomando MGP (3)
		Cibercomando FAP (3)
Táctico	Guerra Cibernética	STGC - Grandes Unidades de Combate (4)
		STGC - Zonas Navales (4)
		STGC - Alas Aéreas (4)

Fuente: Elaboración propia

1) Cada Ministerio debe de tener sus medios para hacer la seguridad cibernética. Puede ser coordinada por la Secretaria de Gobierno Digital u otro órgano de nivel Nacional;
2) Coordina las acciones del Comando Operacional de Ciberdefensa;
3) Cuando activo, coordinado por el Comando Operacional de Ciberdefensa;
4) Sección Táctica de Guerra Cibernética (STGC). Cuando activa, coordinada por el Cibercomando correspondiente (EP, MGP, FAP).

2. Defensa Cibernética: "Conjunto de acciones ofensivas, defensivas y exploratorias realizadas en el ciberespacio, en el contexto de un planeamiento nacional de nivel estratégico operacional, coordinado e integrado por el Ministerio de Defensa y el Comando Conjunto de las Fuerzas Armadas". En esta, identificamos la responsabilidad de los poderes militares.
3. Guerra Cibernética: "Corresponde al uso ofensivo y defensivo de la información para negar, corromper, explorar, degradar o destruir capacidades de Comando y Control del adversario, en el contexto de un planeamiento militar de nivel operacional, táctico o de una operación militar. Abarca esencialmente las capacidades cibernéticas…".

Las definiciones presentadas corresponden a cada nivel de planeamiento, así mismo debe de tener sus propios organismos e instituciones responsables, como lo indica la tabla 1.

La nueva era de las Tecnologías de la Información sugieren nuevos principios, los cuales guían toda acción u operación militar en el ciberespacio. Basándonos en el Manual de Doctrina cibernética de Brasil (BRASIL, 2014), se han considerado los siguientes principios:

1. Principio de Disimulo: Son todas las medidas activas que deben ser adoptadas en el ciberespacio, dificultando el rastreo y trazabilidad de las acciones cibernéticas ofensivas y de exploración contra los Sistemas de Información del enemigo. Disimulando la autoría y el punto de origen de estas acciones.
2. Principio de trazabilidad: Se deben adoptar medidas efectivas para detectar acciones cibernéticas ofensivas y de exploración contra nuestros Sistemas de Información. Casi siempre las acciones en el ciberespacio involucran movimiento y manipulación de datos, los cuales pueden ser registrados.

Otros principios son relacionados en dicho manual, pero estos son los más significativos para nuestra actual situación (propuesta inicial de doctrina). No obstante que, con el pasar de los estudios y principalmente con el empleo real de la cibernética en nuestras fuerzas militares, nuevos principios deberán ser relacionados como primordiales.

Además de los principios que son vitales para la formulación y guía de esta propuesta de doctrina, necesitamos también definir las características, las cuales son cualidades o propiedades que permiten distinguir algo. Refiriéndonos a esto, se sabe que el ciberespacio tiene sus propias características, las cuales son tomadas también como referencia del Manual de Doctrina Cibernética de Brasil (BRASIL, 2014).

1. Inseguridad Latente: Ningún sistema informático es totalmente seguro, teniendo en cuenta que las vulnerabilidades (puntos débiles) en los activos de información[1] serán siempre objeto de exploración por amenazas cibernéticas.
2. Alcance Global: las Operaciones Cibernéticas posibilitan la conducción de acciones a escala global, simultáneamente y en diferentes frentes. Las limitaciones físicas de distancia y espacio no se aplican al ciberespacio. En conformidad con esta característica, la falta de fronteras geográficas para las acciones cibernéticas es otra característica especial del ciberespacio.
3. Mutabilidad: No existen leyes de comportamiento inmutables en el ciberespacio, pues pueden adaptarse a las condiciones ambientales y de creatividad.
4. Incertidumbre: Las acciones en el ciberespacio pueden no generar los efectos deseados como consecuencia de las diversas variables que afectan el comportamiento de los sistemas de información. Así, un ataque en un sistema enemigo pude generar efectos en otros, o puede afectar hasta nuestros sistemas.
5. Dualidad: En las Operaciones Cibernéticas, las mismas herramientas pueden

ser usadas por atacantes y administradores de sistemas con finalidades distintas. Una herramienta que busque las vulnerabilidades del sistema, con el objetivo de arreglarlo, puede también ser usada por atacantes para encontrar puntos que representen oportunidades de ataque.

6. Paradoja Tecnológica: Cuanto más tecnológicamente desarrollado esté un sistema dependiente de la TI, este podrá ser más vulnerable a las acciones cibernéticas. Sin embargo, paradójicamente, este mismo oponente tendrá más condiciones para defenderse de los ataques cibernéticos, en virtud de su alto grado de desarrollo tecnológico.
7. Función Asesoría: Las Operaciones Cibernéticas no son un fin en sí mismas, siendo generalmente empleadas para apoyar la conducción de otros tipos de operación o viceversa.
8. Asimetría: Basada en la desproporción de fuerzas, causada por la introducción de uno o más elementos de ruptura tecnológicos, metodológicos o procedimentales que pueden causar daños tan perjudiciales como aquellos perpetrados por Estados u organizaciones con mayores condiciones económicas.

Algunas características cibernéticas, del manual de referencia, no fueron presentadas porque identificamos que dejaron de tener valor. En cibernética, las cosas cambian rápido debido a las nuevas tecnologías, tendencias, comercio, interés. Pero esto no es una característica solamente de la cibernética; es una característica de las personas, sociedad y gobiernos.

CAPACIDAD DEFENSIVA:

El Estado en su conjunto deberá de buscar la supremacía en el ciberespacio. Deberá buscar un dominio total y completo de este, para poder desarrollar e implementar su propia seguridad, siendo menos vulnerable a posibles amenazas por parte del enemigo, garantizando el desarrollo nacional y la protección de las Infraestructuras Críticas[2] y activos de la información. A manera general las capacidades que cualquier Nación debe desarrollar como necesidad son las capacidades defensivas y ofensivas, tomado del CESEDEN (2012).

Se dice que el ciberespacio es difícil de delimitar, no tiene límites geográficos establecidos ni nada, pero posiblemente en un futuro se tratará de delimitar este nuevo escenario, porque en la actualidad es como tratar de defender una casa con infinitas puertas, tarea casi imposible. Además, debemos de distinguir dos tipos distintos de defensa: Una en el ámbito nacional y la otra en el ámbito privado, cada uno desarrolla su propia defensa, pero estas deberían estar integradas y buscar un fin común: salvaguardar su sistema de información.

Los tipos de defensa que se deben de desarrollar o implementar son (TURIBIO; SANCHEZ, 2012):

a. Defensa pre activa: Son las que se ejecutan antes que se sufra el ataque. Entre las medidas a realizar tenemos la concientización y formación de usuarios y técnicos; definición de normas y procedimientos; y las acciones de disuasión.

b. Defensa proactiva: Son las que se ejecutan en el momento que se detecta el ataque cibernético. Se pueden distinguir tres tipos de reacciones:
   - Reacciones pasivas: Son aquellas donde solo se colocan defensas, sin tomar ninguna otra acción.
   - Reacciones semi activas: Son aquellas donde las defensas establecidas toman pequeñas acciones no agresivas como cortar comunicaciones, bloquear direcciones IP,[3] etc.
   - Reacciones activas: Son los contraataques, en los que se toman acciones contra los agresores.

c. Defensa reactiva: Son las que se deberán de ejecutar una vez que se haya identificado el ataque cibernético. Objetivan la recuperación del sistema, averiguar donde se produjo el daño o robo de la información y colocar medios para evitar una posible repetición del ataque.

TABLA Nº 2: RELACIÓN ENTRE CAPACIDADES Y ACCIONES CIBERNÉTICAS

Capacidades	Tipos	Acciones Cibernéticas
Defensiva	Defensa preactiva	Protección cibernética
	Defensa proactiva	
	Defensa reactiva	Ataque cibernético
Ofensiva	Ciberataque	
	Ciberespionaje	Exploración cibernética

Fuente: Adaptado de MD31-M-07 y CESEDEN

La tabla Nº 2, presenta la relación entre capacidades, tipos de acción cibernética sugerida y acciones cibernéticas relacionadas.

CAPACIDAD OFENSIVA:

Tener capacidad ofensiva implica varios aspectos, como conocer al enemigo, tomar la iniciativa cuando sea necesario y tener la posibilidad de contraatacar después de un ataque. Es responsabilidad directa de la Presidencia del Consejo de Ministros si se quiere emplear esta capacidad o no, pero es necesario reunir ciertas características para su uso eficaz como son el acceso a un sistema que permita explotar una vulnerabilidad e inocular una carga dañina.

Algunos tipos de ataques cibernéticos son, por ejemplo, el ciberespionaje y ciberataque.

En ambos, la diferencia radica en el tipo de carga inoculada, el primero tendrá la misión de sustracción y envío de información, mientras que el segundo será la destrucción de datos, o degradación e inutilización de algún sistema. Los pasos posibles que siguen un ataque son (CEH, 2014):

- Obtención de información: por intermedio de técnicas conocidas por reconocimiento (footprinting) y escaneo de red. En esta fase es común el empleo de la Inteligencia Cibernética.
- Acceso a un sistema: Este podrá ser remoto (internet, red) o local (computadoras, USB, cables, acceso directo a la red, etc.);
- Explotación de vulnerabilidades: Estas pueden ser en cualquiera de las tres capas del ciberespacio (semántica, sintáctica o física), esto es comunicaciones, software o hardware;
- Inoculación de carga dañina: La carga define realmente lo que se va a hacer una vez que la vulnerabilidad haya sido explotada: ocultarse, reproducirse, retransmitir datos, bloquear un sistema, borrar datos, encriptar datos, lograr acceso de administrador, controlar equipos, etc.
- Borrar rastros: después de lograr éxito del ataque, el atacante busca borrar todas las "huellas" digitales para evitar su identificación o identificación del ataque.

Hasta el momento ya hemos definido algunos conceptos que nos dan una orientación para poder proponer una Doctrina cibernética del Ejército, también con la tabla 2 se está relacionando los tipos de capacidades cibernéticas propuestas y desarrolladas en los párrafos anteriores con las acciones cibernéticas (modelo actual del Ejército de Brasil). Así mismo a continuación vamos a mencionar las formas de actuación, debido a que no siempre se va a emplear una responsabilidad cibernética. Esto dependerá del tiempo, el momento y las circunstancias particulares específicas. Tomando como referencia el Manual de Doctrina Cibernética de Brasil (BRASIL, 2014) las formas de actuación cibernética pueden variar de acuerdo con el nivel de Planeamiento (Estratégico nacional, estratégico operacional, operacional o táctico), responsabilidad por cada nivel, contexto de empleo, nivel tecnológico empleado, sincronización y tiempo de preparación, como será presentado a continuación.

1. Actuación Cibernética Estratégica Nacional / Estratégica Operacional: Esta ocurre desde el tiempo de paz, para alcanzar un objetivo político o estratégico definido al más alto nivel, planteado como Política de Defensa. Tiene las siguientes características: Obtención de inteligencia cibernética, es multisectorial, uso alto de la tecnología, duración prolongada y es parte de una Operación de Inteligencia.

2. Actuación Cibernética Operacional / Táctica: Es típicamente empleada en el contexto de una Operación u acción Militar, contribuyendo a la obtención de un efecto deseado. Planeado previamente en una Directiva emitida probablemente (no caso de la cibernética) por el CCFFAA. Sus características son: Preparación del campo de batalla (ciberespacio), dentro del marco del Ministerio de Defensa, uso medio de la tecnología, duración limitada y es parte de una Operación Militar sincronizado con la maniobra.

CONCLUSIONES

Antes de tener una doctrina cibernética, será necesario e importante la creación de una Política de Seguridad Cibernética en el más alto nivel de Planeamiento de la Nación, como lo es el nivel Estratégico Nacional; con la finalidad de dictar las normas, las directrices y algunas definiciones a fin de regular los demás tratados o manuales de niveles inferiores. Entre ellos el que pertenece el Ejército del Perú, antes de definir acciones u operaciones cibernéticas, se debe de tener clara la definición del entorno en donde se van a desarrollar dichas acciones u operaciones cibernéticas, en vista que es un espacio amplio y todavía sin límites (ciberespacio).

Con el presente artículo, identificamos que necesitamos una guía de conceptos y algunos lineamientos de doctrina cibernética para el CCFFAA y, consecuentemente, para el Ejército del Perú. En vista que se trata de dar una propuesta de lineamiento o guía común para poder desarrollar una doctrina propia como Institución, esta guía puede abarcar todas las responsabilidades, conceptos y características cibernéticas tratadas en el presente trabajo.

Es responsabilidad de la autoridad competente, Presidencia del Consejo de Ministros (Secretaría de Gobierno Digital) desarrollar la(s) capacidad(es) que crea conveniente(s) para garantizar la seguridad de los activos críticos de la Nación, en trabajo coordinado con el Comando Conjunto de las Fuerzas Armadas (Comando Operacional de Ciberdefensa), cuando definamos nuestras responsabilidades cibernéticas en cada nivel de planeamiento, vamos a poder determinar qué tipo de capacidad desarrollar, y poder conocer y designar a su responsable directo para esta ejecución.

Como trabajos futuros, destacamos la importancia del estudio respecto a cuáles son las capacidades especificas (ejemplo: encriptación, simulación, etc) que nuestro País necesita para garantizar la seguridad y defensa cibernética, así como tener un poderío militar para desarrollar acciones ofensivas cibernéticas. De igual manera, estudios al respecto de la formación, constitución y forma de empleo de la Sección Táctica de Guerra Cibernética (STGC), necesitan ser desarrollados.

El presente artículo trata de enmarcar una parte específica sobre la cibernética, en el nivel planeamiento doctrinario. También se trata de dar la posible alternativa de solución a lo que nos hace falta, es cuestión de nosotros mismos como institución, tomar o dejar esta propuesta, pero sabemos que esta realidad del ciberespacio no nos es ajeno, es parte de nuestra realidad y se sugiere realizar trabajos propios de misionamiento, organización, empleo y maniobra en el ciberespacio, pero definiendo claramente las responsabilidades, objetivos y metas futuras.

REFERENCIAS BIBLIOGRÁFICAS

1. Los activos de información son los recursos del Sistema de Seguridad de la Información, necesarios para que la empresa o institución funciones y consiga los objetivos que se ha propuesto. (ISO 27001, 2013).
2. "…servicios tales como el sistema de transportes, el agua, la electricidad, las telecomunica-

ciones, etc. ... servicios básicos imprescindibles, junto a la necesidad de su protección" (BEJARANO, 2011).

3. Internet Protocol (IP) es un estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes conmutados. (TANENBAUM, 2011).

BIBLIOGRAFÍA

1. BEJARANO, María José Caro. (2011). La Protección De Las Infraestructuras Críticas. Instituto Español de Estudios Estratégicos. 2017. Sitio web: <http://www.ieee.es/Galerias/fichero/docs_analisis/2011/DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf>. Acceso en: 20/02/18.
2. BRASIL. Doutrina militar da defesa cibernética (MD31 - M – 07). Estado maior conjunto das forças armadas. Ministério da Defesa. Brasil, 2014.
3. CESEDEN. Centro Superior de la Defensa Nacional. El ciberespacio, nuevo escenario de confrontación. Ministerio de Defensa de España, 2012.
4. CEH - Certified Ethical Hacker. Introduction to Ethical Hacking. EC-Council, module 01, v8. 2014.
5. EUA. Cyberspace Operations. Joint Chiefs of Staff (JP 3 – 12 R). Department of Defense (2013).
6. ISO 27001. Tecnología de la Información, técnicas de seguridad, sistemas de gestión de la seguridad de la información. Norma, 2013.
7. PERÚ. Manual de doctrina del proceso de planeamiento conjunto (MFA – CD – 05 -02). Comando Conjunto de las Fuerzas Armadas. Ministerio de Defensa, 2010.
8. PERÚ. Reglamento del Decreto Legislativo N° 1129, que regula el sistema de Defensa Nacional, Decreto Supremo 037. Presidencia del Consejo de Ministros, 2013.
9. PERÚ. Proyecto de Política Nacional de Ciberseguridad. Secretaría de Gobierno Digital. Presidencia del Consejo de Ministros, 2017.
10. TANENBAUM, A. S., Wetherall, D. Redes de Computadores. Editora Campus, 582 pp. (Sexta Edição), 2011.
11. TURIBIO, Lopez; JAVIER, Sanchez. La evolución del conflicto hacia un nuevo escenario bélico, Centro Superior de la Defensa Nacional (CESEDEN). Ministerio de Defensa de España, 2012.