# Estrategia efectiva para el desarrollo sostenido de capacidades cibernéticas de la Armada Nacional.

**Francisco José Jaraba Hadechiny**

Trabajo de grado para optar al título profesional:

**Maestría en Ciberseguridad y Ciberdefensa**

**Escuela Superior de Guerra "General Rafael Reyes Prieto"**
Bogotá D.C., Colombia

2020

Ministerio de Defensa Nacional
Comando General de las Fuerzas militares
Escuela Superior de Guerra
Maestría en Ciberseguridad y Ciberdefensa



# "Estrategia efectiva para el desarrollo sostenido de capacidades cibernéticas de la Armada Nacional."

Francisco José Jaraba Hadechiny

Director
Manuel Ignacio Santander Peláez

Políticas y Modelos en Seguridad y Defensa

Maestría en Ciberseguridad y Ciberdefensa
Trabajo de Grado
Bogotá D.C. – Colombia
2020

# Página de Aceptación

## Página Dedicatoria

**A mi esposa Andrea y a mis hijas Sara y Sofia.**

## Página de agradecimientos

**Resumen**

Desde el año 1997 la Armada de la Republica de Colombia vio como oportunidad el acceso al ciberespacio con el fin de desempeñarse como un actor en el entorno evolutivo de la guerra electrónica, tema en el cual poseía gran conocimiento por la naturaleza de su doctrina naval, en este nuevo escenario buscaba obtener de cierta forma el control del entorno virtual y negárselo al enemigo, desde esa fecha hasta ahora se han encontrado toda clase de experiencias, retos y oportunidades que fueron tomados sin la obtención de un fin claro hacía el estado deseado, por lo cual, surge la necesidad del desarrollo de una estrategia que sea propia a nuestras características, capacidades y limitaciones.

Por tal razón se efectuó una búsqueda en información documentada que contara la experiencia de otros países con similares características, los cuales han desarrollado avances en el entorno cibernético, encontrando que en este ámbito virtual las leyes físicas actúan de forma diferente pero que aún es dependiente de sus componentes físico y lógico, lo cual deja como evidencia que el estudio de una estrategia cibernética debía hacerse desde una perspectiva multipolar que permita identificar todas las variables disponibles para que esta sea efectiva y útil, entre estas variables se pueden nombrar los aspectos militares, sociales, económicos, otros poco conocidos como las bases doctrinales, el psicológico, la prospectiva, que permita emplear de una manera efectiva la organización actual de la fuerza, encontrar lineamientos que coadyuve al cumplimiento de sus actividades misionales, teniendo como parámetro estrategia de nivel superior de la Armada Nacional al 2030 .

Con el propósito de realizar un diagnóstico que permitirá formular una estrategia, se hizo necesario la realización de un conjunto de metodologías que nos pudiesen dar un panorama en

profundidad, primero se realizó metodología de análisis comparado[1] de estudios de casos, avances teóricos, y una encuesta cualitativa basada en los test de *Blockmon* sobre conocimientos en *ethical hackig*, ingeniera forense y capacidades de administración de la seguridad, con el fin de identificar el impacto del nivel de capacitación del talento humano en ciberdefensa de la Armada Nacional, en forma posterior para identificar un estado de madurez, se desarrolla una metodología sobre la administración de capacidades, empleada en las fuerzas militares de Estados Unidos, donde a través, de la evaluación DOMPIS[2] (CAMERA, 2014) y finalmente con el fin de implementar una estrategia, se realiza un análisis diagnóstico de la metodología DOFA.

El resultado obtenido resalta la importancia del ciberespacio como dominio para el sostenimiento y desarrollo de un estado, así como de sus fuerzas militares y la necesidad de su protección, requiere una estrategia que permita elevar conocimientos y capacidades, potencializando el talento humano.

**Palabras Claves:**

Ciberguerra; Ciberseguridad; Ciberdefensa; Seguridad informática; Ciberinteligencia; Ciberterrorismo; Ciberpoder.

**Abstract**

Since 1997, the Colombian Navy has seen the opportunity represented by cyberspace as an evolution of electronic warfare, a subject in which it possessed great knowledge due to its own nature of naval doctrine. In this new scenario, it sought to obtain control in a certain way of

[1] Método Comparativo, procedimiento de la comparación sistemática de casos de análisis que en su mayoría se aplica con fines de generalización empírica y de la verificación de hipótesis. Cuenta con una larga tradición en la metodología de las ciencias sociales; aunque también se encuentra en otras disciplinas, puede decirse que en grado especial es propia de la →Ciencia Política.

[2] DOMPIS (Doctrina, Organización, Material, Personal, Infraestructura, Servicios).

the virtual environment and deny it to the enemy, from that date until now have been found all kinds of experiences, challenges and opportunities that were taken without a clear vision to the desired state, for which arises the need to develop an effective strategy that is own to our characteristics, capacities and limitations.

For that reason a search was made on documented information that counted on the experience of other countries with similar characteristics which have developed advances of the cybernetic environment, finding that the cybernetic sphere, where the physical laws act in different form but still is dependent on its physical and logical components, which leaves as evidence that the study of a cybernetic strategy had to be done from a multipolar perspective that allows to identify all the available variables so that it is effective and useful, among these variables can be named military, social, economic, other little known as the doctrinal bases, the psychological, the prospective, that allows to use in an effective way the current organization of the force, to find guidelines that contribute to the fulfillment of its missionary activities, having as parameter strategy of superior level of the National Armada to 2030.

With the purpose of making a diagnosis that will allow and formulate a strategy, it was necessary to carry out a set of methodologies that could give us an in-depth picture. First, we performed a methodology of comparative analysis of case studies, theoretical advances, and qualitative survey based on the Blackmon test of knowledge in ethical hacking, forensic engineering, and security management skills, in order to identify the impact of the training level of human talent in cyberese's, in a later way to identify a state of maturity a methodology is developed on capacity management, used in the United States military, where, through the DOMPIS evaluation, and finally in order to implement a strategy, a diagnostic analysis of the DOFA methodology is carried out.

The result obtained highlights the importance of cyberspace as a domain for the support and development of a state, as well as its military forces and the need for its protection requires a strategy that allows to raise knowledge and capabilities, enhancing human talent.

## Tabla de Contenido

## Tabla de Abreviaturas

| | |
|---|---|
| • Armada Nacional Republica de Colombia | ARC |
| • Fuerzas Militares de Colombia | FFMM |
| • Organización del Tratado del Atlántico Norte | OTAN |
| • National Security Agency | NSA |
| • Security Operation Center | SOC |
| • Tecnologías de la información y las comunicaciones | TIC´s |
| • Tecnologías información | TI |
| • Organización para la Cooperación y el Desarrollo Económicos | OCDE |

## Introducción

Entre el periodo que comprende la aparición de la internet como una súper autopista de la información, hasta el momento en el que algunos países suscribieron en sus leyes que el acceso internet fuese considerado como un derecho inalienable para sus ciudadanos, las grandes potencias han tenido intereses sobre el deseo de ejercer un control sobre el ciberespacio; para este caso hablaremos de un control militar relacionado al concepto de defensa de la Nación, teniendo en cuenta que diferencia de los otros cuatro dominios este escenario no corresponde a un desarrollo natural, ya que fue creado por el hombre y en su explotación ha demostrado que es casi imposible de ejercer un control real, pareciera que como los otros dominios contuviese fuerzas invisibles que han trazado su propia naturaleza única, aunque en este particular en el quinto escenario las leyes físicas son distintas y la asimetría de los factores no son determinantes en el teatro de operaciones, las acciones que se realicen en este pueden tener un impacto de afectación global.

Aunque existen muchas definiciones sobre el ciberespacio, todas poseen como común denominador que se caracteriza porque en su descripción siempre deambulan en tres activos fundamentales la lógica, física y lo virtual (Definición, 2013), por lo cual no es extraño que las políticas, estrategias o sistemas de defensa y seguridad que buscan ejercer un control sobre el ciberespacio intenten explotar uno o todos los activos mencionados, para lo cual se requiere una visión multidimensional y cuya probabilidad de éxito está ligada al conocimiento real de los riesgos, amenazas, así mismo del como solventarlo de acuerdo a las capacidades propias de cada institución o país. (Kesan & Hayes, 2011)

Con base en lo anterior se destaca que el objetivo de la presente investigación busca establecer un proceso metodológico para construir bases sólidas en conocimiento, identificar con

rigor académico los factores que pueden influir en la formulación de una estrategia para el desarrollo de capacidades cibernéticas al interior de la Armada Nacional de la República de Colombia, mediante un estudio de caso con el propósito de analizar la experiencia de otros países con similares características socioculturales y económicas, e identificando los factores que pueden interferir de manera directa o en el entorno de la estrategia.

La relevancia del ciberespacio, la cotidianidad de su empleo y la dependencia de los estados sobre el mismo, ha llevado a la aparición de nuevos adversarios en la batalla por la información, los cuales emplean técnicas avanzadas para explotar vulnerabilidades de los subsistemas que componen el escenario cibernético, contiene una capa social la cual ha sido expuesta con las vulnerabilidades psicológicas y sociales del ser humano, la capa lógica de los sistemas queda en evidencia mediante metodologías que buscan explotar la información, la cual se convierte en activo importante para algún actor, y que es accesible de alguna forma a través del ciberespacio, por lo anterior y teniendo en cuenta la existencia de un punto de convergencia entre las actividades políticas, económicas y militares, visualizamos la información como ese activo estratégico que las soporta, por lo cual las infraestructuras críticas que a sus ves son redes de información para prestar un servicio, se convierten en un objetivo de gran valor en la ciberguerra.

## 1. Hitos o puntos de interés para el inicio de una estrategia cibernética.

Para el desarrollo de toda estrategia se requiere la identificación de bases fuertes o pilares que permitan establecer un punto de partida, para el caso de consolidar una estrategia efectiva en cibernética para uso militar y en particular de la Armada Nacional es necesario focalizar la búsqueda de información e identificar que puede ser la materia prima documentada que ayude a obtener el resultado deseado, se establece el punto de partida, los conceptos del empleo de las fuerzas del estado frente a la amenaza cibernética, el autor Bejarano; M. J. C. en su artículo "Alcance y ámbito de la seguridad nacional en el ciberespacio". describe su postura frente a la militarización del internet como un campo de batalla con condiciones deferentes a los teatros de guerra comunes, como la asimetría , la inexistencia de fronteras definidas, así mismo describe las iniciativas de países como España, Estados Unidos y otros miembros de la Organización del Tratado del Atlántico Norte (en adelante: OTAN) en formalizar algún tipo de doctrina para la realización de operaciones en el ciberespacio, estandarizar cuales son los tipos de ataques cibernéticos que se puede enfrentar una fuerza regular, así como los arquetipos de atacantes que pueden encontrar en este entorno virtual, manifiesta que en este campo de batalla la estrategia que se tome debe tener únicamente dos posibles posturas: la defensiva o la ofensiva. (Bejarano, 2011)

No obstante es de importancia indicar porqué las fuerzas militares y en este caso la Armada Nacional tiene el interés de participar en la llamada militarización del internet, estando fundamentado en la responsabilidad de las fuerzas militares sobre la defensa nacional, los

intereses nacionales y la protección o recuperación de los sistemas de infraestructuras críticas cuando estos se vean en riesgo, igualmente aunque son claras las responsabilidades del poder militar, ellas deben estar articuladas a los otros organismos del estado, por tal razón es oportuno generar conciencia en los decisores políticos para adaptarse a los nuevos riesgos, amenazas de la soberanía digital en un entorno poco explotado en nuestro país; es responsabilidad de los actores políticos proyectar el planeamiento estratégico de la ciberseguridad y la creación de estructuras organizativas de carácter técnico en el uso del ciberespacio en lo relacionado a la seguridad nacional. (Marcuello, S. C., & Chaime, A., 2006), la denominada militarización del internet ha llevado a la necesidad de idear proyectos colaborativos entre naciones con el propósito de lograr cooperación internacional en temas de seguridad y defensa que se relacionen con el ciberespacio, un ejemplo en particular aborda las políticas de seguridad y defensa de México y Argentina con el fin de evaluar sus prioridades y puntos en común, implementando un marco de acercamiento entre las dos naciones geográfica mente alejadas pero unidas en un entorno virtual que buscan la obtención de poder correlacionado en forma estratégica, así aprovechar las ventajas del ciberespacio donde la geoestratégica permite que sea maleable más allá del plano físico, esto le permita proyectar en el horizonte futuro algunas áreas en las cuales ambos países pueden confluir en proyectos cooperativos (Daponte & Moreno, 2016).

El caso anterior demuestra que la unión de países o alianzas multilaterales pueden ser viables en el ciberespacio, sin embargo, el análisis de la posibilidad y evolución de la intensidad de la amenaza hasta llegar a una ciberguerra no es inalcanzable, por lo cual, las unidades militares deben estar preparadas para ello. Según el autor del texto "La ciberguerra una realidad contemplada desde la prospectiva", la probabilidad de la ocurrencia de grandes guerras en el

futuro serán más factibles, esté será un escenario donde las potencias mundiales tomaran diferentes posiciones, integrando en su estrategia de campos convencionales al ciberespacio como un activo cada vez de mayor valor dentro de los teatros de operaciones, ya que por sus características dinámicas permite el desarrollo de operaciones que impacten en el mundo físico y el virtual, los cuales mediante el empleo de códigos afecten el funcionamiento de infraestructuras críticas o sistemas de soporte de las sociedades como la banca o las telecomunicaciones; la materialización de esta amenaza genera una notable preocupación en los países desarrollados, que cuentan con extensas y sólidas estructuras e infraestructuras, considerado como posibles objetivos de una guerra convencional y de una guerra en el ciberespacio.

Los Estados han de adoptar medidas y constituir organismos para la defensa ante ciberataques. En algunos casos más allá del punto de defender sus necesidades particulares pueden requerir con capacidad para atacar, por tal motivo la comunidad internacional ha de plantearse una ética que rija en este campo (León, 2016). Los estados como garantes de la seguridad y tranquilidad de sus ciudadanos han debido adaptar sus estructuras y marcos normativos para prevenir y enfrentar las nuevas amenazas de origen cibernético, sin embargo surgen oportunidades para que las amenazas también evolucionen, permitiendo a los agresores muchas formas de acercase a su víctima de tal manera que minimize el riesgo y aumentando su anonimato, por lo cual los estados deben adoptar medidas más fuertes para garantizar la seguridad de sus ciudadanos, para lo cual las estructuras y la normativa deben adaptase para prevenir y enfrentar la posibilidad de la materialización de estas amenazas, por otro lado se hace de importancia alinear la estrategia nacional de un país para prevenir y repeler cualquier ataque

de naturaleza cibernética. (Mariña, 2002), la implantación de políticas de ciberseguridad en países en desarrollo, la aparición de las tecnología de la información y las comunicaciones, así como que la dependencia de los países sobre el ciberespacio abraza los aspectos sociales, económicos y políticos, los cuales son primordiales para garantizar la gobernanza, por lo cual, es importante desde las iniciativas del estado abordar los temas de seguridad de lo que se podría denominar el patrimonio digital y cultural de los individuos, organizaciones y países; de manera que se hace imperante la generación de estrategias en todos sus alcances, ya sea en seguridad de la informática y de las telecomunicaciones o ciberseguridad, que permita mantener un nivel de seguridad informática suficiente para prevenir los riesgos tecnológicos que afecten los servicios esenciales para el adecuado funcionamiento de los Estados y de las organizaciones, pero para alcanzar y mantener este nivel de seguridad se debe ser objetivo en el sentido de partir por unas buenas bases, afrontando un planteamiento global, multidisciplinario y exhaustivo. («Guía de ciberseguridad para los países en desarrollo», s. f.)

Sin embargo, a diferencia de este punto de vista militar existen otras posturas, como la planteada en política Económica y Social por el Consejo Nacional, quienes a través del Departamento Nacional de Planeación han publicado dos documentos CONPES el 3701 de 2011 y el 3854 de 2016, en estos documentos se encuentra plasmada la evolución temporal de los enfoques y lineamientos de ciberseguridad y ciberdefensa en Colombia, se considera de importancia traerlos a colación por su carácter complementario, en primera instancia el CONPES 3701 generó lineamientos de política en ciberseguridad y ciberdefensa en la búsqueda de encontrar una estrategia nacional que brindara los mecanismos para contrarrestar el incremento de las amenazas informáticas, tomando las lecciones aprendidas de los incidentes

nacionales e internacionales y asumiendo la normativa internacional existente, para la aplicabilidad de la estrategia se crean tres instancias: el COLCERT como el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, el Comando Conjunto Cibernético CCOC y el Centro Cibernético Policial. CCP (MIN TICS, 2011).

La política presentada en el 2016 como el CONPES 3854, sigue los lineamientos generales de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) frente a la afectación del sector económico mundial cara a las actividades criminales que utilizan el ciberespacio con incidencia en el desarrollo comercial, por tal motivo, esta segunda fase se concentra en contrarrestar el incremento de las amenazas relacionadas con la defensa del país y la lucha contra el cibercrimen con un enfoque de la evaluación de la amenaza en relación a la gestión del riesgo en el entorno digital, teniendo en cuenta el creciente uso de las tecnologías de la información y las comunicaciones (en adelante TICS) en las actividades relacionadas con el desarrollo económico, tomando relevancia la implantación de procesos de planificación, prevención, e intención de contrarrestar cualquier afectación negativa, para esto se hace necesario un marco de implementación claro en seguridad digital, donde el objetivo es el desarrollo de las capacidades los sectores públicos y privados con la finalidad de obtener una capacidad a nivel país para identificar, gestionar, tratar y mitigar los riesgos, generándo confianza en el uso del entorno digital se multiplique la participación activa y permanente, trayendo como fin último fortalecer la defensa y seguridad nacional en el entorno digital.(MIN TICS, 2011) (MIN TICS, 2016).

Tomando como bases los marcos en materia de ciberseguridad de las políticas CONPES descritas, se resalta la iniciativa de varios autores por formalizarlas, como la Autora María Constanza Bermúdez Arciniegas. (2014), quien posterior al lanzamiento del CONPES 3701,

plantea en su tesis "Estrategia para la creación de una unidad cibernética". (Universidad Sergio Arboleda), en mencionado artículo resalta la importancia de diseñar de una estructura jerarquizada de carácter militar que aunque en un principio fue diseñada para la Armada Nacional puede ser aplicada a cualquier Fuerza del Orden, y fortalecimiento de la gestión del talento humano mediante el cumpliendo un plan de carrera que permita la adquisición de conocimientos de forma escalada, de igual forma, el autor Julián David Aponte Díaz, en su trabajo de final de maestría "Proyecto para la creación del Comando de Ciberseguridad y Ciberdefensa de la Armada Nacional de la República de Colombia". Universidad Politécnica de Madrid, plantea que en el ámbito militar el uso de las tecnologías de la información y las comunicaciones juegan un papel fundamental en el desarrollo de operaciones, afirmando que es prácticamente imposible desarrollar cualquier tipo de misión sin el apoyo de estas tecnologías, esta apreciación es recogida de los manuales de operaciones cibernéticas de los Estados Unidos, empleando el concepto de operaciones centradas en la red, las cuales se caracterizan por emplear TIC'S para conseguir una superioridad informativa, que se traduzca en superioridad en el campo de batalla, (Julián David Aponte Díaz, 2015; Maria Cosntanza bermudez Arciniegas, 2014)

Posteriormente al observar los puntos de vista de distintos países que pueden ser tenidos en cuenta al momento de formular una estrategia propia, es claro que la amenaza de origen cibernético corresponde a una problemática global, por lo cual se hace necesario observarla como un teatro de operaciones global, así lo plantea el articulo EL CIBERESPACIO: EL NUEVO TEATRO DE GUERRA GLOBAL del Autor Recalde, publicado en la Revista de Ciencias de Seguridad y Defensa, en este el autor expone que en el concepto de ciberespacio se aleja de la definición tradicional de teatro de operaciones terrestres de fronteras definidas se

minimiza, por lo cual, las fuerzas del orden deben adaptarse a la nueva condición del espacio virtual como un teatro de guerra mundial, en el que se relaciona los otros espacios naturales, terrestres, marítimos, aéreos y espacial; el autor manifiesta que el estudio de las guerras no se basa únicamente sobre el enfrentamiento de los adversarios, sino también en el empleo de la táctica y la estrategia, así mismo que la guerra es una condición humana del pensamiento de la conducción militar en sus niveles estratégico, operacional y táctico, por lo tanto, el ciberespacio es nuevo teatro de guerra que conlleva el desarrollo de las TIC´S, y origina un espacio intangible para realizar operaciones militares en los niveles operacionales y estratégicos, lo que corresponde a una nueva oportunidad para el empleo de sistemas electrónicos, redes e infraestructura en operaciones militares. necesario por lo cual, la aparición del ciberespacio como un teatro de operaciones ha requerido la adaptación de nuevas disciplinas; la inteligencia no es la excepción sea visto desde el enfoque militar, comercial y hasta personal, la relación de obtener y entender la información es clave para alcanzar y mantener una posición privilegiada, por lo cual, la rama de la ciberinteligencia ha debido evolucionar en su concepto en razón a un entorno dinámico en el cual se debe tener una visión integral para poder afrontar el cambio de un enfoque reactivo a uno proactivo, que permita obtener, analizar y elaborar información con una evaluación de amenazas completas, precisas, en forma oportuna y relevante, para la toma de decisiones. (IBÁÑEZ, s. f.)

### 1.1. ¿Cómo está la situación actual de la organización frente al problema de nuestra investigación?

Se puede observar que en un relativo corto tiempo se han logrado grandes avances en los marcos del ejercicio del cumplimiento de las políticas de ciberseguridad dentro de un marco

doctrinal, sin embargo es notorio que existe desigualdad en el grado de madurez de la Armada Nacional la cual ha crecido a necesidad y prioridad de los lineamientos estado, desde un ambiente de desarrollo en la cibernética han surgido varias unidades subordinadas con funciones y responsabilidades similares, las cuales oscilan entre la conectividad, el soporte, el servicio y la seguridad, pero cada una con una prioridad específica, lo cual afecta directamente las estrategias adoptadas a nivel general sin haber una particular, mientras en nuestro ámbito regional algunos como en el caso de Colombia existen grandes progresos aunque aún se encuentra en una etapa de implementación, los avances de mayor alcance están relacionados con la banca buscando protección de su inversión mas no una fortaleza sectorial, de tal forma que no reflejan una estrategia integral y mucho menos general, sino un sistema de alertas tempranas, en busca de apoyo internacional y dependencia de los sistemas extranjeros; en el entorno mundial es evidente que los estados que son más dependientes en el internet han logrado poner en marcha estrategias más fuertes y claras en donde hay fuerte inversión en el tema, se consolida la seguridad y el servicio como un interés nacional, sus políticas se rigen en el empleo del quinto dominio, proyectando fuertes penas para los delitos informáticos los cuales casi en el contexto mundial se encuentran bien tipificados, así como en las políticas de defensa es más clara en roles y en las funciones que debe tener la ciberdefensa de los Estados.

La doctrina que en la actualidad se maneja en las unidades de ciberdefensa que se encuentran en el territorio nacional están influenciadas por dos grandes sectores: el primero corresponde a países con grandes recursos como Estados Unidos o países de bloque como la Unión Europea, así mismo el posicionamiento geopolítico de estos países hace que el desarrollo de sus operaciones sean demasiados especificas a sus capacidades de infraestructura, es decir a sus necesidades particulares, talento humano, doctrina, organización, material, equipo y

servicios, por lo cual la propuesta de investigación está orientada a focalizar los esfuerzos de inversión y el conocimiento existente para desarrollar una nueva estrategia cibernética naval para la Armada Nacional, que permita desarrollar operaciones con un elevado impacto, que permita la reducción de costos y riesgos, puntualizando en la conciencia situacional, esto permite la construcción de un panorama cibernético entendible para el comandante, buscando tener una mayor apreciación de la realidad coadyuvando al proceso para la toma de decisiones, ya que por sí solo el ciberespacio no será decisivo en las estrategias militares nacionales actuales, pero si serán influyentes en el desarrollo de operaciones cinéticas y no cinéticas.

## 1.2. La real importancia del quinto dominio.

Hoy en día parece que resulta más que obvio o dado por hecho el ciberespacio es considerado como el quinto dominio de la guerra, ¿pero lo es en realidad? ¿en qué consiste este dominio, porque es tan importante?, ¿qué es lo que en si protegemos y queremos arrebatárselo al enemigo?, ¿porque se requieren estrategias de ciberdefensa? y ¿por qué se requiere que las personas estén preparadas para enfrentar amenazas de origen cibernético?

Desde que se presentó la denominada revolución de la información que según Peter Drucker trajo consigo la aparición de la sociedad del conocimiento.

> "Lo que llamamos revolución de la información es de hecho una revolución del conocimiento [...] es la reorganización del trabajo tradicional basado en siglos de experiencia, mediante la aplicación del conocimiento y en especial del análisis sistemático y lógico. La clave no es la electrónica sino la ciencia cognitiva.
>
> Eso significa que la clave para mantener el liderazgo en la economía y en la tecnología que van a surgir estará en la posición social que tengan los profesionales del

conocimiento y la aceptación social de sus valores." (Drucker & Drucker, 1999; Micheli, 2002)

Por lo cual, la mencionada revolución de conocimiento y sumado a la reducción del costo de la transmisión de los datos, permitió el acceso a información en cualquier lugar del mundo desde cualquier lugar de él (Kuehl, 2009), los usuarios del ciberespacio no sólo cuentan con la posibilidad de recibir contenidos, también cuentan con la opción de generar o comunicar contenidos propios, esta tendencia ha direccionado la evolución tecnológica de tener conexión desde nuestras casas y lugares de trabajo, pasando a tenerla mediante elementos portables, hasta convertimos en pequeños sistemas interconectados con la aparición y empleo del internet de las cosas, llegando al desarrollo social y cultural de la necesidad de estar conectados (Kuehl, 2009).

Por lo anterior, inferimos que el desarrollo va involucrando cada vez más el factor humano dentro de la definición de ciberespacio, al comparar varias de las definiciones que se encuentran en este espacio virtual se podría afirmar que es el resultado de pequeñas redes que conectadas entre sí brindan distintos servicios, lo cuales pueden ser sencillos, como la aplicación que usas para optimizar como conduces de un lugar "A" hasta un destino "B", hasta complejos sistemas de control que permiten el monitoreo y control de infraestructura crítica, entre las que pueden estar el control de las telecomunicaciones o algún otro servicio esencial; al unirse muchas pequeñas redes conforman un escenario complejo que ha sido capaz de expandirse a todo el mundo haciendo posible compartir información al instante, por tal razón, no es extraño que en la actualidad también los estados requieran de la interconexión digital para la operación de las actividades vitales (Agua, electricidad, banca, sistemas de salud, seguridad, etc.), la continuidad

y disponibilidad de estos servicios se transforman en el centro de gravedad para el desarrollo de un país, y su desplome afectaría los componentes económico, político, social y la defensa, por ende la gobernabilidad del mismo, es por tal motivo que se denominan infraestructuras críticas (Arquilla & Ronfeldt, 1993), la información de estas infraestructuras ya sean propias o de otros, se convierten en un activo de gran valor ya que ser conscientes de sus debilidades y conocer sus vulnerabilidades se convierte en el real botín de la ciberguerra.

Por tal motivo podríamos definir la ciberguerra como aquella lucha desarrollada en el espacio virtual en donde pueden confluir actores estatales y no estatales bajo motivaciones particulares o altruistas, que deja como resultado robo de información, de propiedad intelectual y hasta pérdida económica. El fin último la ciberguerra se convierte en la lucha por obtener información, sobre que actor sabe ¿cuándo?, ¿dónde?, ¿qué?, y ¿por qué?, con respecto a su autoconocimiento y de su adversario (Riascos, 2015).

En la actualidad cualquier país, organización o persona puede ser víctima de un ataque informático, según Amoroso (2011, p5) podemos encontrar cinco posibles razones para el desarrollo de una ataque de naturaleza cibernética, el primero puede ser el interés de un Estado sobre un actor en particular, esté puede invertir los recursos suficientes hasta materializarlo, motivación de un ataque terrorista, obtención de una ventaja comercial, ataque criminal con fines financieros y hacktivismo (Amoroso, 2012). Aunque encontramos muchos vectores de ataque la mayoría se concentra en el eslabón más débil de la cadena de seguridad, el factor humano, según Kevin Mitnick los hackers maliciosos o ciberdelincuentes se centra cuatro pilares psicológicos y sociales que pueden ser las vías de acceso para conseguir información suficiente para explotar las vulnerabilidades de cualquier sistema:

- **Las "ganas"** de ayudar inherentes a al ser humano, en su condición de sentirse noble y solidario con las personas más desfavorecidas
- **El primer movimiento de confianza hacia el otro**, la colaboración es esencial para fomentar las relaciones interpersonales es intrínsecamente gratificante, satisface una necesidad social básica, proporciona la base para la construcción y el mantenimiento de las relaciones e implica asumir un riesgo mutuo respecto a otra persona.
- **El reconocimiento**, es normal dentro del comportamiento humano sentirse alabado, ya que de alguna forma siempre se espera algún tipo de recompensa por las acciones realizadas.
- **No nos gusta decir "NO",** en la mayoría de los casos el deseo de ayudar, el no sentirnos rechazados, temor a los enfrentamientos o simplemente perder una oportunidad, casi que nos obliga a no decir que NO.

A estos pilares se suman las condiciones propias de la naturaleza humana como la curiosidad, el miedo, la codicia, la compasión, motivaciones de tipo sexual permiten un vector de acceso para la obtención de información privilegiada para atacar una persona, una organización o un país (Mitnick & Simon, 2011).

Todo ataque de naturaleza cibernética tiene como objetivo interferir, dañar o manipular la integridad, disponibilidad y confidencialidad de los datos; para defenderse de este tipo de ataques o incluso para emplearlos en forma activa, es posible acceder a metodologías como por ejemplo la doctrina militar de ciberguerra de los Estados Unidos, donde se utiliza terminología como *(information assurance, cyber security, infosec, computer security, computer networks security, computer networks defence, cyber defence, critical information infrastructure protection, etc.),*

también existen tipos de ataque como los de día cero, los de negación de servicio entre otros, sin embargo es de resaltar que antes de generar una estrategia o definir un vector de ataque cibernéticos, se debe recoger información del blanco que se desea, y para esto de acuerdo al producto del análisis comparado pienso que existen tres tipos de técnicas principales para dar inicio a cualquier intención de ataque, las cuales se pueden definir así: ***Spoofing***, consiste en utilizar una dirección ajena para acceder a algún recurso haciéndose pasar por otra entidad o suplantación; *Jamming* a perturbación deliberada de una vía de comunicación, saturación del canal y el *sniffing*, como la captura no autorizada de la información que pasa por el tráfico (Lichtman et al., 2016), robo de datos, estas técnicas pueden definir la evolución de una amenaza a un riesgo en el momento que un adversario tiene el suficiente conocimiento sobre la información de nuestra infraestructura critica, surge la pregunta ¿estamos preparados para identificar y mitigar la materialización de esta amenaza?, lo anterior permite efectuar la necesidad de un diagnóstico, con el propósito de evaluar si nuestra situación actual es suficiente.

## 2. ¿Estamos preparados para la batalla?

Teniendo en cuenta la demostración por análisis de comparación que hasta el momento se ha descrito, se evidencia el desarrollo de conciencia institucional y personal, del porque es importante nuestra información, por lo cual su exposición estará directamente relacionada a la posibilidad de la materialización de un riesgo cibernético, se hizo necesario realizar una prueba de concepto donde se empleó técnicas de muestreo mediante una encuesta cualitativa basada en los test de Raymond Blockmon volumen 9 de certificación en seguridad de la información, con treinta preguntas sobre *ethical hackig*, ingeniera forense, capacidades de administración de la

seguridad (Blockmon, 2016), se realizó una encuesta a personal de funcionarios de la Armada Nacional cuyas funciones principales están relacionadas con la protección de infraestructura críticas e información confidencial en tecnologías de la información y comunicaciones, con el fin de identificar si su grado de conocimiento frente a amenazas de naturaleza cibernética en niveles bajo, medio, y alto, el resultado de la pruebas quedo graficado en la siguiente tabla (Fig.1) .

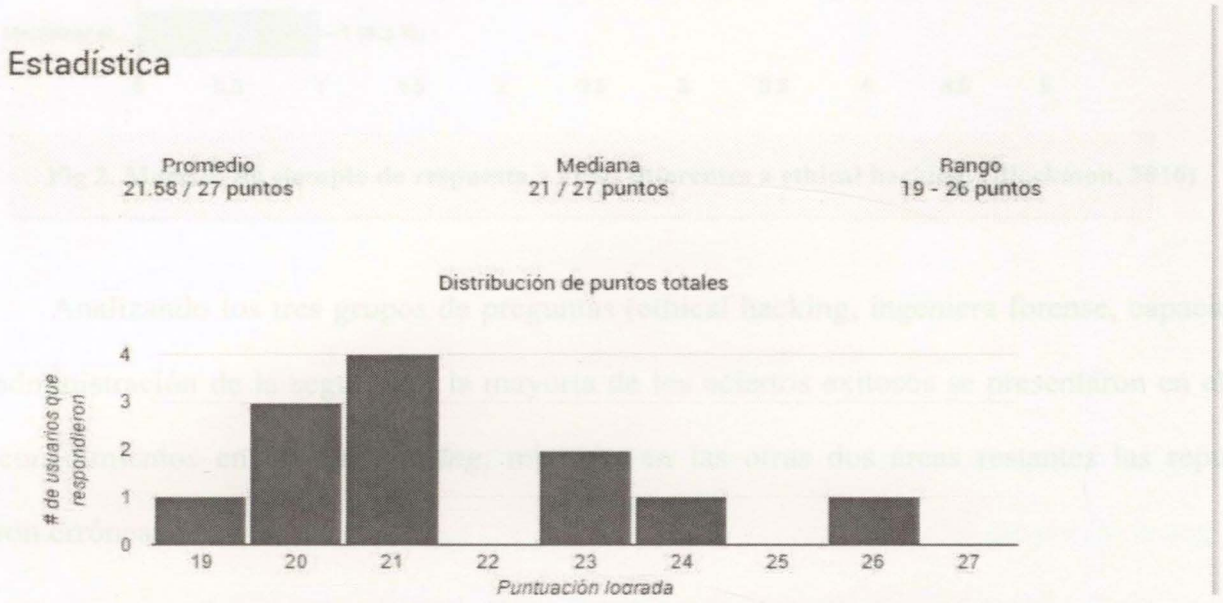


**Fig. 1 Representa estadísticas del total de respuesta de la prueba. (Blockmon, 2016)**

El resultado obtenido demuestra, al momento solo el 1% presenta conocimientos en un nivel Alto, para tener las bases suficientes para identificar y mitigar amenazas, frente a un 21% a una gran mayoría que se encuentra en niveles medio y 78% nivel medio bajo.

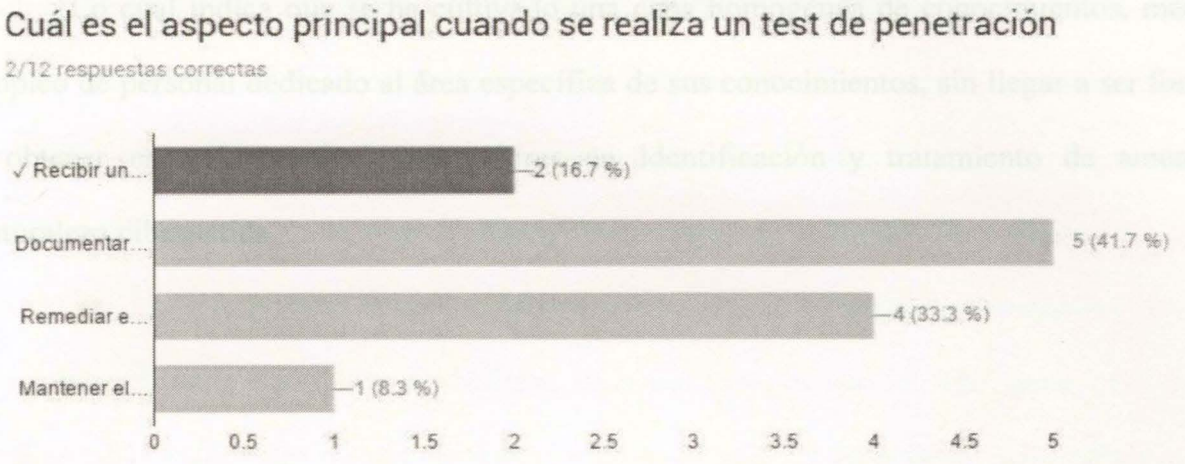


**Fig 2. Muestra de ejemplo de respuesta a áreas diferentes a ethical hacking. (Blockmon, 2016)**

Analizando los tres grupos de preguntas (ethical hacking, ingeniera forense, capacidades de administración de la seguridad) la mayoría de los aciertos exitosos se presentaron en el área de conocimientos en *ethical hacking*, mientras en las otras dos áreas restantes las repuestas fueron erróneas.

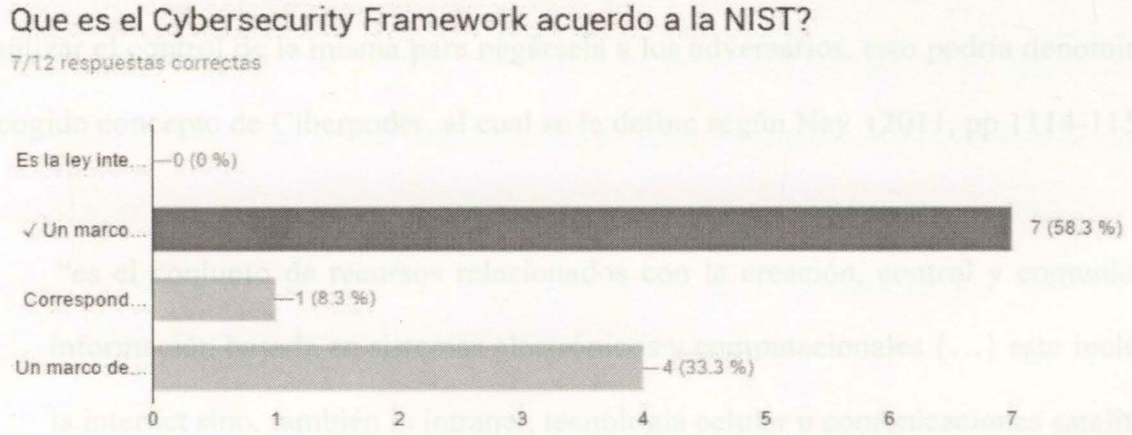


**Fig 3. Muestra de ejemplo de respuesta a área capacidades de administración de la seguridad (NIST 2012)**

Lo cual indica que se ha cultivado una capa homogénea de conocimientos, mediante el empleo de personal dedicado al área específica de sus conocimientos, sin llegar a ser focalizados a obtener específicos niveles superiores en identificación y tratamiento de amenazas de naturaleza cibernética.

### 3. Porque es necesario generar estrategias.

Teniendo en cuenta los resultados obtenidos donde se evidencia que en la actualidad no se cuenta con suficiente personal que posea las condiciones que permitan garantizar la seguridad de nuestra información como fuerza, ante una necesidad tangible de protegerla o por lo menos garantizar el control de la misma para negársela a los adversarios, esto podría denominarse como el acogido concepto de Ciberpoder, al cual se le define según Ney (2011, pp 1114-115)

> "es el conjunto de recursos relacionados con la creación, control y comunicaciones de información basada en sistemas electrónicos y computacionales {...} esto incluye no solo la internet sino, también la intranet, tecnología celular u comunicaciones satelitales"

Por lo cual se hace necesario proyectar la obtención de capacidades incluyendo el conocimiento hacia a la obtención del ciberpoder, ya que toda estrategia debe estar orientada la consecución de un objetivo, si analizamos nuestra necesidad y dependencia como individuos o

como organizaciones e incluso estados sobre las redes de información en el que se basa el sostenimiento, mando y control de las operaciones militares, gobernabilidad y seguridad nacional, aun comparándola con casos como el de los Estados Unidos, se logra observar el posicionamiento de sus unidades de ciberdefensa como el Comando Cibernético, La X (decima) flota naval, la NSA, y todas unidades existentes en forma clandestinas, pero que han demostrado con varios hechos dentro de la historia reciente que poseen un alto grado de conciencia situacional, con grandes vulnerabilidades ante amenazas de naturaleza cibernética, ya que a medida que sus activos estén sujetos a una mayor dependencia de la conectividad para garantizar su funcionamiento, la exposición y el riesgo serán mayores, han adaptado su estrategia a ciberdefensa y adaptarla a la doctrina de seguridad y defensa nacional a la medida de sus necesidades y capacidades. (Trujillo, 2014)

En el caso de américa latina la situación no es distinta, cada uno de los países desde Colombia hasta Chile ha venido incluyendo la amenaza cibernética dentro de sus libros blancos o políticas de defensa y seguridad, ya que en este dominio la posición geográfica y la disposición de sus recursos económicos no son determinantes en el alcance que pude lograr la capacidad cibernética, esta inclusión en sus lineamientos de direccionamiento político está acompañado de la creación de comandos cibernéticos en el campo del sector defensa, centros o grupos de repuestas a incidentes cibernéticos, así como la iniciativa privada de sus propios centros de respuestas a incidentes (Abedrapo, s. f.; MIN TICS, 2016).

## 4. Situación actual de la unidad cibernética.

Hasta este momento hemos comprendido la importancia del quinto dominio, por lo cual se afirma que las TIC's han contribuido de forma decisiva en el desarrollo económico, militar y social del país; sin embargo en la medida en que los diferentes sectores convergen en la dependencia tecnológica, aumenta el nivel de riesgo que representa el ciberespacio para la Seguridad Nacional, por ende como se ha explicado en los capítulos anteriores también es de importancia para la Armada Nacional, y deben ser motivo de evaluación los mecanismos de estudio de la postura de ciberseguridad y ciberdefensa adoptada hasta el momento, evaluar si ha sido eficaz, y si se hace necesario ajustar una estrategia desarrollada de forma conjunta desde su roll misional.

Por lo cual se hace necesario realizar una aproximación al estado de madurez de las capacidades de la Armada Nacional.

Dentro de la metodología planteada mediante entrevistas a doce (12) integrantes de la Armada Nacional de nivel de responsabilidad y dirección que laboran en áreas afines a la ciberdefensa y ciberseguridad, el resultado del análisis a las preguntas sobre ¿cuáles son las principales problemáticas para el desarrollo de actividades de ciberdefensa? evidenciaron problemas u obstáculos para el cumplimiento de su roll, que así mismo impiden el trabajo conjunto, coordinado y unificado que permita la protección del ciberespacio frente a las crecientes amenazas que ponen en riesgo la Seguridad Nacional.

Como resultado se obtiene, evidencia de las situaciones más relevantes que afectan el desarrollo de la capacidad:

- Aunque existe una misión institucional y una visión estratégica para la Armada Nacional, la función de la capacidad cibernética no está orientado a tener un estado deseado de capacidades, por lo cual no se tiene un plan detallado a de consecución y metas intermedias en doctrina, material, personal, infraestructura o servicios.

- Carencia de recursos disponibles para el desarrollo de capacidades que permitan hacer frente a las amenazas cibernéticas en la actualidad.

- Falta de estandarización de capacidades y procedimientos a nivel de las Fuerzas Militares, lo que dificulta la interoperabilidad en el ciberespacio.

- Finalmente, se determinó que uno de los principales objetivos de protección cibernética es la Infraestructura Crítica Cibernética Nacional, en la que actualmente se está trabajando para catalogarla; sin embargo, es importante acelerar dicho proceso y diseñar un plan para su protección y defensa.

## 4.1. Evaluación del estado de madurez

Para evaluar el estado de madurez se describe la observación de una metodología sobre la administración de capacidades, empleada en las fuerzas militares de Estados Unidos, donde a

través de la evaluación DOMPIS[3], el propósito es examinar las características y determinar el estado de madurez de la cibernética naval.

### 4.1.1. Doctrina

En el momento del desarrollo de este trabajo de investigación a nivel de la política pública, no existe una ley o decreto reglamentario que trate de la actuación o la responsabilidad de las actividades cibernéticas. Sin embargo, a nivel de la, existen dos CONPES (Consejo Nacional de Política Económica y Social) que corresponden al 3701 y al 3854.

A pesar de lo anterior, existe la directiva del ministerio de defensa que faculta las actividades de ciberdefensa dentro de las fuerzas militares y en su efecto dentro de la Armada Nacional.

### 4.1.2. Organización.

Existe una unidad cibernética de la Armada Nacional constituida, cuya razón exclusiva asume el rol de las actividades de ciberdefensa, dicha organización está dividida por funciones y responsabilidades, la dirección se formalizo desde el año 2016 por lo cual aún no se cuenta con definiciones específicas que describan las funciones de sus divisiones , la unidad esta formalizada como una dirección y cuatro divisiones de apoyo por áreas misionales, donde de acuerdo valoración de la experiencia del personal que labora en ella se puede definir así :

- **Dirección cibernética naval.**
- **División de ciberseguridad.**

[3] Doctrina, Organización, Material y Equipo, Personal , Infraestructura y Soporte logístico . (CGFM, 2015).

Es la dependencia responsable de proteger las redes de datos de la Armada Nacional, mediante el despliegue de medidas activas y pasivas, al interior de los límites de las redes informáticas de la Institución, que permitan prevenir, detectar y neutralizar ataques o acciones maliciosas contra los sistemas que se encuentran dentro de dichas redes; lo anterior teniendo en cuenta que se requiere de sistemas relacionados a las TIC's que puedan ser utilizados de forma segura para poder desarrollar su misión; lo anterior para entregar elementos a la Dirección Cibernética Naval, que faciliten la toma de decisiones que conlleven a incrementar el nivel de seguridad dentro de la red de datos Institucional.

- **División de ciberdefensa.**

Es la dependencia encargada de defender las redes de datos de la Armada Nacional y contribuir a la defensa de aquellas redes utilizadas dentro del sector marítimo nacional, que hagan parte de la Infraestructura Crítica Cibernética Nacional; mediante el despliegue de medidas activas y pasivas que permitan anticiparse a la amenaza y reaccionar frente a ataques o situaciones maliciosas que se presenten dentro de las redes de datos Institucionales o aquellas utilizadas por el sector marítimo nacional, que se enmarquen dentro de la Infraestructura Crítica Cibernética Nacional; de forma que se entreguen los elementos que le permitan a la Dirección Cibernética Naval tomar decisiones para neutralizar la amenaza, antes que esta pueda actuar contra las redes de datos de la Institución. Lo anterior teniendo en cuenta la necesidad de preservar la capacidad Institucional, así como contribuir a la preservación de del sector marítimo, para hacer uso del ciberespacio en situaciones de paz y guerra.

- **División de desarrollo cibernético.**

Es la dependencia encargada de liderar los procesos de Investigación, desarrollo, experimentación e innovación sobre técnicas y herramientas que permitan la solución de problemas para el desarrollo de operaciones de ciberseguridad y de ciberdefensa exitosas, mediante proyectos de I+D que busquen satisfacer la necesidad de contar con herramientas especializadas, diseñadas a la medida de situaciones específicas, coadyuvando el cumplimiento de las funciones de las capacidades cibernéticas de la Armada Nacional.

- **División prospectiva cibernética.**

La División de Prospectiva Cibernética es la dependencia encargada de actualizar y analizar los posibles escenarios del estado de conciencia situacional cibernético relacionado con el ciberespacio utilizado por la Armada Nacional y el sector marítimo nacional, así como el que es afectado por las amenazas actuales y potenciales, mediante actividades de análisis de variables que permita tener la visión global de posibles cursos de acción que puedan afectar el desarrollo de las operaciones cibernéticas, anteponiéndose a escenarios cibernéticos futuros que puedan poner en riesgo la infraestructura crítica cibernética naval y marítima, o aquellos que puedan ser explotados en beneficio propio y que coadyuven al cumplimiento de la misión Institucional.

### 4.1.3. Personal.

Para la determinación de personal requerido para el cumplimento de la misión de la ciberdefensa, se toma como evidencia el instrumento de medición y control de las fuerzas militares de Colombia, denominado las tablas de organización y equipo (TOE)4, la dirección cibernética contiene esta planeación de designación del personal hasta su cumplimiento, estando en el momento a un treinta por ciento de su proyección.

Dentro de la rama de personal como factor fundamental, se debe contar con talento humano capacitado, titulación, experiencia y aptitudes o habilidades, que nos permita adquirir la experiencia operacional y optimizar los recursos asignados.

### 4.1.4. Material.

- **Plataforma explotación de información de fuentes abiertas.**

Consola administrativa de gestión de monitoreo para la búsqueda de información de fuentes abiertas para la explotación web de entidades, como la búsquedas de dominios, direcciones de correo electrónico, números telefónicos, servidores DNS.

La plataforma funciona de la siguiente manera:

Mediante él envió de peticiones a los servidores en formato XML utilizando HTTPS, la petición del servidor se da a los servidores TAS que se transmiten a los proveedores de servicios, e identifica comportamiento sospechoso y potenciales compromisos de los sistemas.

---

[4] Documentos de carácter reservado en los que se determina la misión, capacidades, instrucciones especiales, organización y distribución de material, se encuentran normalizadas por el artículo 29 del Decreto 1512 del 2000 del Ministro de Defensa Nacional.

La herramienta permite identificar que tan expuesto se puede estar dentro del ciberespacio

- **Plataforma escaneo de vulnerabilidades.**

Detección de vulnerabilidades de máquinas en red mediante el escaneo de vulnerabilidades por medio de comparación de listas de fallas conocidas.

El propósito es comprobar vulnerabilidades para que puedan ser solucionadas por el administrador del sistema y neutralizar agujeros de seguridad, en un corto periodo de tiempo, con el propósito de iniciar planes de mitigación.

- **Plataforma de test de penetración.**

De modalidad open source de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intruso.

Requiere habilidad y persistencia; empleando metodología

- Los ataques de autenticación
- Ataques de ingeniería social
- Ataques de inyección SQL

Los ataques de explotación de software se pueden utilizar para acceder a los sistemas no autorizados, y obtener privilegios de la cuenta de usuario e instalación de software malicioso (como software espía, virus de, troyanos, adware, etc.) sin el conocimiento de la otra parte.

### 4.1.5. Infraestructura.

En la actualidad la dirección cibernética naval no posee una infraestructura propia, sin embargo, se tiene proyectada una planta de 403 metros cuadrados, que cumpla con las siguientes características:

35 puestos de trabajo; que cada uno se encuentre equipado con 02 tomacorrientes (01 Regulada), 02 Puntos de red (01 de datos, 01 de voz).

Sala de juntas con mobiliario con 06 Tomacorriente (03 Regulada); 06 Puntos de red; 01 Mesa de 08 puestos de trabajo.

Datacenter acuerdo estándar TIA942 (2005)[5], que cumpla con las especificaciones técnicas y de seguridad requeridas.

- El techo estará a una distancia de 2,75 m sobre el piso verdadero y consistirá en una losa maciza de concreto armado con un espesor de 15 cm, conteniendo dos mallas electrosoldadas.
- El falso plafón se colocará 40 cm bajo el techo verdadero con placas de escayola y fibra de vidrio (suspensión con anclajes y tirantes metálicos de acero).
- Las medidas de la puerta de acceso serán de 1,10 x 2,20 m.

[5] ANSI-TIA (American National Standards Institute – Telecomunications Industry Association), clasifica a este tipo de centros en varios grupos, llamados TIER (anexo G), indicando así su nivel de fiabilidad en función del nivel de disponibilidad.

- Los acabados serán perfectamente nivelados, uniformes y aplomados en todas sus caras, esquinas y rincones.
- Se utilizarán resinas epóxicas, pinturas ignífugas lavables e intumescentes.
- El Piso Técnico se instalará 30 cm sobre el piso verdadero y estará constituido por: pedestales y travesaños, y paneles.
- Sistema contra incendios (Extintores, Sensores de humo, Regaderas).
- Sistema eléctrico para equipos que funcionen a 220v.
- Sistema de refrigeración (Aire acondicionado de precisión).

Con 02 Archivadores rodantes de 200 cm de alto x 93 cm de ancho x 45 cm de fondo. Los acabados deben ser resistentes de fácil limpieza, preferiblemente con ventilación natural o mecánica.

Alojamiento que cuente con capacidad para 02 camarotes, baño con ducha, guarda ropa.

Cocina tipo integral con sus respectivos gabinetes, estufa empotrada y espacio para refrigerador y horno microondas.

Baños para hombres y mujeres en cerámica, con ventilación natural o mecánica.

Cuarto de aseo funcional con poceta lava traperos, y almacén.

### 4.1.6. Soporte logístico.

En la actualidad no se cuenta con un plan de soporte integral del ciclo de vida del material y equipo que permita la mejora continua y rentabilidad de la capacidad cibernética.

## 5. Medición de la situación actual de la capacidad cibernética

El enfoque principal fue tomado desde el punto de la valoración de un estado de madurez, tomando como punto de partida el resultado de la investigación desde la apreciación de expertos de la capacidad cibernética de la Armada Nacional y céntranos en un punto de interés del cual pueda ser explotable la materialización de una estrategia.

Como primera parte de la metodología para la valoración del estado de madurez se realiza teniendo en cuenta la valoración del grado de desarrollo de cada habilidad, valorada desdé el **número uno (1) siendo el nivel más bajo hasta el máximo grado que sería el nivel cinco (5) en donde la habilidad estaría a un máximo grado** de sin embargo, teniendo en cuenta el constante avance tecnológico no permite tener una habilidad en un punto de total desarrollo, en la figura cuatro se describen cuáles son las variables tenidas en cuenta apara la valoración de cada uno de las áreas de capacidad del nivel de madurez.

| EVALUACIÓN | DOCTRINA | ORGANIZACIÓN | MATERIAL Y EQUIPO | PERSONAL | INFRAESTRUCTURA | SOPORTE LOGÍSTICO |
|---|---|---|---|---|---|---|
| 1 | No existe ningún tipo de avance en la producción de doctrina | No existe ningún avance en el diseño de la organización | No existe ningún avance en las gestiones requeridas para la adquisición del equipo necesario | No existe ningún avance en relación a la gestión del personal requerido | No existe ningún avance en cuanto a la gestión de la infraestructura necesaria | No existe ningún parámetro establecido en términos de soporte logístico |
| 2 | Existe un plan para el desarrollo de la doctrina requerida. Pero aún no se ha avanzado en su ejecución | Existe el diseño estructural de la organización, pero aún no se ha finalizado su implementación. (Faltan manual de funciones y la estructuración de los procedimientos internos de cada dependencia) | Existe un plan de gestión de material y equipos requeridos, pero aún no se ha avanzado en la ejecución en un porcentaje mínimo | Se tiene definido el personal requerido para el desarrollo de la capacidad, pero aún no se ha gestionado el mínimo porcentaje del mismo | Se tiene definida la infraestructura requerida para el desarrollo de la capacidad, pero aún no se ha avanzado en las gestiones para su adquisición y/o construcción | Se cuenta con la definición de las necesidades generales dentro del ciclo de vida de cada uno de los elementos que hace parte de la capacidad. |
| 3 | Se cuenta con el 30% de la doctrina requerida | La organización está estructurada y tiene el 30% de sus procesos y procedimientos estructurados | Se cuenta con el 30% del material y equipo requerido | Se cuenta con el 30% del personal requerido | Se cuenta con el 30% de la infraestructura requerida | Se tienen establecidas las necesidades logísticas del 30% del ciclo de vida de los elementos que hacen parte de esta capacidad. |
| 4 | Se cuenta con el 60% de la doctrina requerida | La organización está estructurada y tiene el 60% de sus procesos y procedimientos estructurados | Se cuenta con el 60% del material y equipo requerido | Se cuenta con el 60% del personal requerido | Se cuenta con el 60% de la infraestructura requerida | Se tienen establecidas las necesidades logísticas del 60% del ciclo de vida de los elementos que hacen parte de esta capacidad. |
| 5 | Se cuenta con el 80% o más de la doctrina requerida y se cuenta con un plan de actualización y mejora de la misma | La organización está estructurada y tiene el 80% de sus procesos y procedimientos estructurados. Se cuenta con un sistema de gestión de calidad implementado y funcionando | Se cuenta con el 80% del material y equipo requerido y un plan de actualización del mismo | Se cuenta con el 80% del personal requerido y con un plan de carrera implementado. | Se cuenta con el 80% de la infraestructura requerida | Se tienen establecidas las necesidades logísticas del 80% del ciclo de vida de los elementos que hacen parte de esta capacidad. |

**Fig 4. Tabla de valoración del grado de desarrollo de cada habilidad**

Para la segunda parte de la evaluación del estado de madurez se toman los parámetros utilizados por la Organización del Tratado del Atlántico Norte OTAN, de acuerdo con la posibilidad de cumplimiento del ciclo de gestión de incidentes que define las funciones de seguridad cibernética, bajo el concepto de Capacidades y responsabilidades".

Este enfoqué está adaptado específicamente a la seguridad de la información, ya que el ciclo tradicional para la gestión de emergencia tradicional (que comprende cuatro elementos: mitigación, preparación, respuesta y recuperación), mientras el Ciclo de gestión de incidentes se pueden ver los cinco (05) principios: Pro-acción, prevención, preparación, respuesta y recuperación. La respuesta y la recuperación a veces se combinan en un solo elemento: Supresión. Algunas naciones, como los Países Bajos, reconocen otro sexto Elemento: seguimiento / seguimiento. («NationalCyberSecurityFrameworkManual.pdf», s. f.)

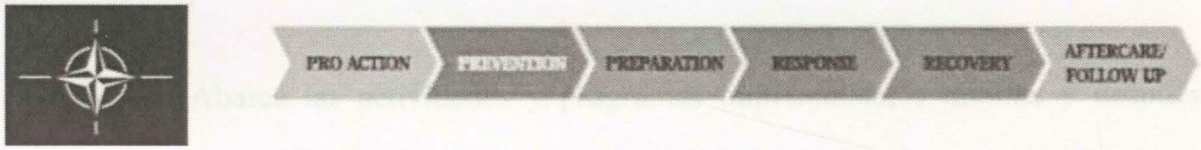


**Fig 5. Modelo de Ciberseguridad OTAN**

**Pro-acción:** Está definida como las actividades que reducen o eliminan las causas estructurales de

inseguridad, consiste en llevar a cabo una evaluación nacional del riesgo (siglas en ingles NRA) para el dominio del ciberespacio, establecer un marco jurídico y un marco organizativo para la seguridad cibernética. Corresponde al nivel de la política decidir cuándo esta brecha identificada se llena (o no).

**Prevención:** En un contexto de gestión de emergencias se ha definido como acciones para evitar un incidente, dentro de este ciclo se usa una definición ligeramente diferente: "acciones para prevenir o reducir los peligros que puedan convertirse en incidentes", estas acciones o medidas preventivas de ciberseguridad buscan reducen la vulnerabilidad del Ciberespacio.

**Preparación:** Definida como "planificación, formación y ejercicio" o "ciclo continuo" compuesto por las actividades o procesos de planificación, organización, capacitación, equipamiento, ejercicio, evaluación y toma de medidas correctivas en un esfuerzo por asegurar una coordinación efectiva durante la respuesta a un incidente.

**Respuesta:** Aborda los efectos inmediatos a corto plazo, busca evitar el daño después que ocurra un incidente.

**Recuperación:** Abarca las actividades y programas implementados durante y después de la respuesta, los cuales están diseñados para devolver la entidad a su estado habitual o a un "Nuevo Normal".

**Control / seguimiento:** Toma en cuenta el impacto psicosociológico de un incidente a (partes de) la población, cubre el manejo de incidentes e incidentes investigación (como la determinación de hechos y la redacción de lecciones identificadas), así el análisis forense, la investigación criminal y el procesamiento de sospechosos.

A continuación, utilizaremos este modelo de seis elementos para junto con sus componentes para la medición de las funciones, capacidades y responsabilidades de tal forma que puedan ser medibles.

| ÁREA DE CAPACIDAD | CAPACIDAD ESPECÍFICA | NIVEL DE MADUREZ | DOCTRINA | ORGANIZACIÓN | MATERIAL Y EQUIPO | PERSONAL | INFRAESTRUCTURA | SOPORTE LOGÍSTICO |
|---|---|---|---|---|---|---|---|---|
| PROACCIÓN | Estrategia | 3 | 3 | 2 | 4 | 2 | 2 | 2 |
| | Política, procesos y procedimientos | 3 | 3 | 3 | 4 | 3 | 3 | 2 |
| | Acuerdos internacionales | 1 | 1 | 2 | 2 | 1 | 1 | 1 |
| | Ejercicios cibernéticos | 2 | 3 | 2 | 1 | 1 | 1 | 1 |
| | Apoyo internacional | 1 | 1 | 2 | 2 | 1 | 1 | 1 |
| | Marco Jurídico | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | Marco Organizacional | 3 | 4 | 4 | 4 | 3 | 2 | 2 |
| PREVENCIÓN | Sensibilización | 3 | 3 | 3 | 3 | 3 | 2 | 2 |
| | Educación / Entrenamiento | 2 | 2 | 3 | 2 | 2 | 2 | 1 |
| | Manejo de Vulnerabilidades | 2 | 2 | 3 | 2 | 2 | 2 | 2 |
| | Monitoreo de Seguridad | 2 | 2 | 3 | 2 | 2 | 2 | 2 |
| | Valoración Dinámica del Riesgo | 2 | 2 | 3 | 2 | 2 | 2 | 2 |
| | Prevención y mitigación de ciberataques | 2 | 2 | 3 | 2 | 2 | 2 | 2 |
| | Obtención de información fuentes abiertas | 3 | 2 | 3 | 3 | 3 | 3 | 3 |
| | Conciencia de la situación | 2 | 2 | 3 | 2 | 2 | 2 | 2 |
| | Controles de seguridad | 3 | 2 | 3 | 3 | 3 | 2 | 2 |
| PREPARACIÓN | Visibilidad y Seguimiento | 1 | 1 | 2 | 1 | 1 | 1 | 1 |
| | Vigilancia Tecnológica | 1 | 1 | 2 | 1 | 1 | 1 | 1 |
| | Detección y Análisis de Ataques Cibernéticos | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| | Escalamiento y comunicación | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| | Análisis de Malware | 3 | 2 | 3 | 3 | 3 | 3 | 2 |
| RESPUESTA | Respuesta a incidentes | 2 | 2 | 2 | 1 | 2 | 2 | 1 |
| | Manejo de incidentes | 2 | 2 | 2 | 1 | 2 | 2 | 1 |
| | Análisis de incidentes | 2 | 2 | 2 | 1 | 2 | 2 | 1 |
| | Mitigación | 2 | 2 | 2 | 1 | 2 | 2 | 1 |
| | Toma de Decisiones en Tiempo Oportuno | 2 | 2 | 2 | 1 | 2 | 2 | 1 |
| | Defensa Activa | 2 | 2 | 2 | 1 | 2 | 2 | 1 |
| | Sistemas de Decepción o Engaño | 2 | 2 | 2 | 1 | 2 | 2 | 1 |
| RECUPERAC | Gestión de Recuperación | 1 | 1 | 2 | 1 | 1 | 1 | 2 |
| | Continuidad | 1 | 1 | 2 | 1 | 1 | 1 | 2 |
| CONTROL Y SEGUIMIENTO | Manejo de Artefactos | 2 | 1 | 2 | 2 | 2 | 2 | 2 |
| | Análisis Forenses | 2 | 1 | 2 | 2 | 2 | 2 | 2 |
| | Investigacion | 2 | 1 | 2 | 2 | 2 | 2 | 2 |
| | Análisis de mejoras | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | Comunicación de la amenaza y riesgo | 2 | 1 | 2 | 2 | 2 | 2 | 2 |
| | Avance Estrategico | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

**Fig 6. Tabla de valoración de nivel de madurez por habilidades**

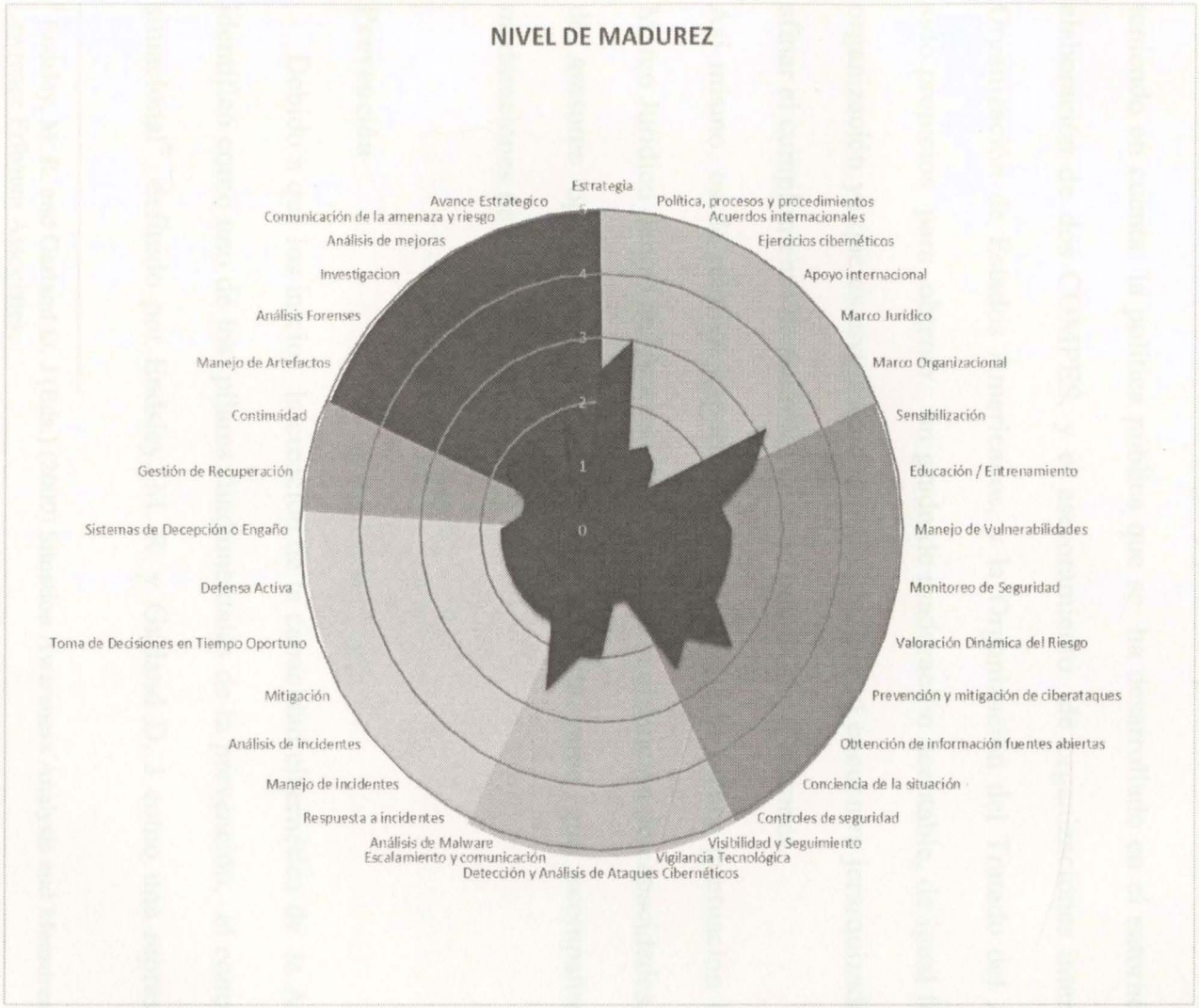


**Fig 7. Tabla de valoración de nivel de madurez por habilidades**

## 5.1. Análisis de los resultados nivel de maduración.

Como resultado del análisis de los valores en la gráfica (Figura.7) , en primera instancia se busca obtener una visión general de la valoración actual de la unidad cibernética, mirarla como el conjunto de capacidades que se resaltan a pesar del poco tiempo de creación y puesta en funcionamiento, dentro del área de PREACCIÓN se observan valores interesantes como los aspectos relacionados con la estrategia y política pública en donde hay avances considerables, teniendo en cuenta la política pública que se ha desarrollado en el entorno, el impulso de la elaboración de dos COMPES, y el asesoramiento de organizaciones internacionales como la Organización de Estados Americanos, y la Organización del Tratado del Atlántico Norte han sido propicios para obtener un grado de maduración aceptable, de igual forma el marco de la organización ya que es una unidad constituida, que se encuentra jerarquizada y en el proceso de afinar el cumplimiento de sus roles en cada una de sus divisiones.

Así mismo, es de relativa importancia destacar que la menor puntuación la recibe el ítem de Marco Jurídico dentro del proceso de la creación u obtención de capacidades, en razón de la falta de asesores operacionales o especialista en esta rama que acompañen los procesos de maduraciones de la capacidad.

**Prevención**

Debido a que los inicios la creación de la capacidad cibernética de la Armada Nacional, se identificó como uno de los pilares fundamentales de la prevención, el concepto de Conciencia situacional[6] definido por Endsley, M. R. y Garland D. J como una representación del estado

[6] Endsley, M. R. and Garland D. J (Eds.) (2000) Situation Awareness Analysis and Measurement. Mahwah, NJ: Lawrence Erlbaum Associates.

mental en la que se comprenden la esencia, actores y factores de una situación específica que para este caso en la interacción del usuario y el ciberespacio que puedan afectar al desarrollo de las tareas humanas en él.(Jajodia, Liu, Swarup, & Wang, 2010)

El contexto de acceso a información de fuentes abiertas junto con el bajo costo de la implementación de esta capacidad ha permitido que las herramientas actuales de análisis de fuentes abiertas cobre relevancia dentro de las capacidades de la dirección, ya que ha permito la adquisición de herramientas para su explotación tecnológica y de soporte.

**Preparación**

Se destaca que se han dado avances en los campos de la preparación compuestos por las áreas de detección, escalamiento y análisis de malware, que al momento está en una fase inicial como capacidad.

También se resalta como puntuación muy baja la "visibilidad y seguimiento", ya que al momento no se cuenta con la capacidad de realizar actividades necesarias para mantener una visibilidad continua y poder realizar seguimiento a las actividades sospechosas sobre las redes de responsabilidad.

La actividad de "Monitorear y observar" sigue en el listado de relevancia con bajo rendimiento, ya que no hay la constancia o un protocolo establecido para la realización de una vigilancia tecnológica que permita identificar las amenazas futuras, nuevos avances técnicos, actividades de intrusos, avances de ciencia y tecnología, así mismo la capacidad preventiva de un monitoreo con acompañamiento judicial o cobertura legislativa en caso de ser necesaria.

**Respuesta**

Se destaca que se han dado avances en los campos de la respuesta donde ya se encuentra la existencia de planes para el desarrollo de esta capacidad en a las áreas respuesta, manejo y análisis de incidentes, mitigación, toma de decisiones en tiempo oportuno, defensa activa, y sistemas de decepción o engaño, al momento no han sido posible materializarse por falta de recursos.

**Recuperación**

Hasta el momento no existe algún avance significativo en el desarrollo de actividades y programas implementación, para actividades de Gestión de Recuperación durante y después de la respuesta, los cuales dejan en grave situación la resiliencia o continuidad de la organización.

**Control y seguimiento**

Se encuentra en desarrollo del plan de cumplimiento para la adquisición de esta capacidad, que busca mediante el empleo de habilidades específicas el análisis forense de los hechos presentados durante el incidente, con el fin de manejar la investigación pueda dar indicios de los posibles culpables y se inicien actos formales disciplinarios o en su defecto judiciales de acuerdo corresponda y culmina con el levantamiento de la lección aprendida

## 6. Matriz DOFA de la capacidad cibernética de la Armada Nacional.

Con el propósito de realizar un diagnóstico y poder generar los pasos que me permitan una planeación estratégica, se realiza la consulta a un comité de expertos con la participación de quince miembros activos cuya función principal está relacionada con la ciberdefensa y la ciberseguridad, se inicia con la fase de diagnóstico de la metodología DOFA en donde se realiza la identificación de los factores, así mismo en este paso se realiza una valoración de los factores teniendo en cuenta el impacto que tiene dentro de la organización, y el evento tomado como el plazo de la materialización de un hecho.

### 6.1. Debilidades

- El no cumplimiento del roll específico de la Dirección de Ciberdefensa, ocasiona que el desempeño de actividades de servicio, conectividad, y monitoreo de tendencias o temas específicos originan la dispersión del esfuerzo en seguridad y defensa del ciberespacio.

  Impacto: Alto

  Evento: Corto

- La Dirección de Ciberdefensa no representa un puesto prioritario dentro de la planeación estratégica de la Armada Nacional, lo que ocasiona falta de recursos.

  Impacto: Alto

  Evento: Mediano

- El lenguaje técnico y los nuevos conceptos empleados en la actualidad en el ámbito de la ciberdefensa no son claros para los tomadores de decisiones dentro de la estructura del alto mando naval, lo cual trae como consecuencia que las propuestas y necesidades no sean claramente entendidas ni apoyadas.

  Impacto: Alto

  Evento: Corto

- La no existencia de un plan de trabajo detallado en tiempo y capacidades que permita el cumplimiento de los objetivos a corto y mediano plazo, o el no cumplimiento del plan existente, que permitan el cumplimiento del objetivo general.

  Impacto: Alto

  Evento: Largo

- No tenemos claridad los protocolos de reacción frente ataques e intenciones maliciosas.

  Impacto: Alto

  Evento: Corto

- No tenemos desarrollada una cultura de I+D.

  Impacto: Medio

  Evento: Largo

## 6.2. Oportunidades

- El aumento de la dependencia tecnológica en todos los procesos (operativos, administrativos) de la Armada Nacional.

  Impacto: Alto

  Evento: Corto

- El reconocimiento de la amenaza cibernética dentro de la Armada Nacional.

  Impacto: Alto

  Evento: Mediano

- Aprovechamiento de los intereses en común con organizaciones y agencias externas a la a la Dirección Cibernética Naval, los cuales pueden representar apoyos en recursos para la obtención de capacidades.

  Impacto: Alto

  Evento: Corto

- Existencia en el mercado de software libre, que puede ser adaptado a necesidades, permita adquirir competencias y bajar los costos.

  Impacto: Alto

  Evento: Corto

- El empleo del quinto dominio como teatro de operaciones, debe apoyar junto a los otros dominios tradicionales en la consecución de objetivos militares.

  Impacto: Alto

  Evento: Mediano

- Fácil acceso a información de los blancos de interés por la explotación de fuentes abiertas.

  Impacto: Alto

  Evento: Mediano

- Situación actual de la crisis con Venezuela y Nicaragua, como cualquier otra que se pueda presentar de la misma magnitud, pueden generar espacios para el desarrollo de las capacidades cibernéticas.

  Impacto: Alto

  Evento: Mediano

- Aprovechamiento del acceso del director de cibernética naval a escenarios de tomas de decisiones de mediano y alto nivel.

  Impacto: Alto

  Evento: Corto

- Necesidad de servicios en ciberseguridad por parte de la empresa (pública y privada).

  Impacto: Alto

Evento: Largo

## 6.3. Fortalezas

- El talento humano que se desempaña dentro del área de la ciberdefensa cumple con el perfil profesional y técnico requerido.

  Impacto: Alto

  Evento: Corto

- El personal que labora en la dependencia cuenta con la experiencia en diferentes áreas de las TIC'S.

  Impacto: Alto

  Evento: Corto

- Actualmente la persona que lidera y direcciona el área de ciberdefensa cuenta con un gran poder de gestión que ha permitido la adquisición de material y equipo.

  Impacto: Alto

  Evento: Mediano

- Existe un grupo de trabajo, aptitudes personales y profesionales que facilita el trabajo en equipo.

  Impacto: Alto

  Evento: Mediano

## 6.4. Amenazas

- Falta de conciencia situacional en todos los niveles de la estructura del personal de la Armada Nacional.

  Impacto: Alto

  Evento: Corto

- Falta de compromiso del Alto Mando de la capacidad cibernética, ocasiona el no comprometimiento con el desarrollo de la capacidad ante una amenaza de naturaleza cibernética creciente.

  Impacto: Alto

  Evento: Mediano

- Dentro del esquema de TIC'S de la Armada Nacional, se le da la prioridad a la conectividad y no a la seguridad de los servicios.

  Impacto: Alto

  Evento: Mediano

- Las amenazas cibernéticas cada de ves son más sofisticadas y evolucionadas, lo cual supera la capacidad de reacción de la unidad cibernética.

  Impacto: Alto

  Evento: Corto

- La facilidad del empleo del ciberespacio para realizar ataques en contra de la institución.

  Impacto: Alto

  Evento: Corto

- Las valoraciones de potenciales en capacidades cibernéticas son desfavorables en relación con las reales y potenciales amenazas.

  Impacto: Alto

  Evento: Largo

- El interés de otras direcciones o unidades de la Armada Nacional de adquirir total o parcialmente los activos de la Dirección Cibernética.

  Impacto: Alto

  Evento: Largo

- Aclaración de los roles de las unidades que están relacionadas con el ámbito tecnología de la información y las comunicaciones.

  Impacto: Alto

  Evento: Largo

# 7. FORMULACIÓN DE LA MATRIZ

Corresponde al cruce de los factores con el propósito de identificar caminos estratégicos, ayuden a tomar otros ángulos de enfoques, que ayuden a desarrollar e implementar políticas nuevas o medidas de preparación (por ejemplo, programa de ejercicios), o puede emplearse útilmente Implementar nuevas iniciativas.

## 7.1. Agrupación de estrategias y acciones

**Debilidades Oportunidades (DO)**: En este grupo de acciones se deben reunir los planes conducentes a cada una de las debilidades que se consideraron como oportunidades de mejoramiento de la unidad o que representan reajustes con impacto positivo.

(Superar las debilidades para aprovechar las oportunidades.)

- Utilizar el acceso del director de cibernética naval a escenarios de tomas de decisiones de mediano y alto nivel que permita orientar y canalizar requerimientos y solicitudes relacionados a actividades de servicio, conectividad, y monitoreo de tendencias o temas específicos, hacia cada una de las dependencias que por su roll se deban encargar, y asumiendo el esfuerzo principal en seguridad y defensa del ciberespacio.

- El aumento de la dependencia tecnológica de la Armada Nacional en todos sus procesos representa la oportunidad en la que la dirección cibernética ejerza jurisdicción sobre los

procesos (operativos, administrativos), como un organismo certificador de seguridad y control de los mismos.

- Elaboración de un plan de trabajo detallado en tiempo y áreas específicas con objetivos claros que comprenda el desarrollo por capacidades (ciberseguridad, ciberdefensa, desarrollo y prospectiva), teniendo en cuenta cada una de las secciones de la Dirección Cibernética Naval, apoyándonos organizaciones y agencias externas con las cuales se posean intereses en común, canalizando los apoyos que puedan ser recibidos focalizándolos en la adquisición de material y capacitaciones alineadas al plan trazado.

- Situaciones de crisis como las presentadas con Venezuela por la violaciones de tratado de límites de 1941 y Nicaragua por litigios de fronteras terrestres o marítimas de acuerdo el fallo de la Corte Internacional de Justicia Caso NICOL de 2012 que afectan los intereses de la nación, así como el desarrollo de cualquier otra que se pueda presentar de la misma magnitud, debe aprovecharse para demostrar capacidades existentes pueden generar espacios para el desarrollo de las capacidades cibernéticas.

- El reconocimiento de la amenaza cibernética dentro de la Armada Nacional nos obliga a la elaboración y puesta en funcionamiento de protocolos de reacción frente ataques e intenciones maliciosas.

- Elaboración de un plan de generación de cultura de investigación y desarrollo, que se apoye en forma principal en la explotación de software libre, permita la adquisición de

competencias profesionales por áreas específicas, reducción de los costos, solución de problemas y sostenibilidad.

**Debilidades y Amenazas DA:** En este grupo de acciones se deben reunir los planes conducentes a cada una de las debilidades que se consideraron como amenazas. Estas acciones deben ser precisas y analizadas, ya que ponen en riesgo directo el éxito.

Como reducir la debilidad y minimizar la amenaza

- Se debe establecer acciones contundentes que permitan evidenciar el estado actual de las capacidades de la dirección cibernética naval, frentes a las capacidades cibernéticas de las amenazas reales o potenciales y como este pueden salir del entorno virtual y tener un impacto físico, razón por la cual es necesario la inversión de recursos.

- Desarrollo de mecanismos que permitan definir y en rutar el roll específico de la Dirección de Ciberdefensa, para minimizar la dispersión del esfuerzo, y focalizar sus medios en seguridad y defensa del ciberespacio, con el fin de acortar la brecha de desventaja ante una amenaza cibernética creciente, lo que puede ocasionar el aumento de la credibilidad en la capacidad tenga como resultado el aumento del compromiso con la unidad.

- Los medios de comunicación formales e informales (oficios, presentaciones, boletines, y otros) que salgan de la Dirección Cibernética a otras instancias deben tener un mensaje y empleo del lenguaje que sea más fácil de entender para el personal que no se desarrolla

en el ambiente cibernético, con el fin que sea más fácil comprender el fenómeno cibernético que le permita entrar en la conciencia situacional de la a estructura del personal de la Armada Nacional.

- Superar la barrera de los rolles entre las unidades relacionadas con las TIC'S dentro de la Armada Nacional, en la medida que esto ocurra, los protocolos que se formulen la diferencia de prevención y reacción ante incidentes informáticos podrán ser claros y efectivos para cada una de las partes, se superará la barrera de la prioridad en la conectividad y no a la seguridad de los servicios, y las unidades se verán como puntos de apoyo y no como competencias.

- Ante la creciente facilidad y sofisticación de los ataques, los planes de adquisición de capacidades, aunque deben tener plazos y objetivos medibles, no pueden ser estáticos debido a que las amenazas evolucionan todos los días, para esto se hace necesaria una fuerte prospectiva y constante vigilancia tecnológica con el propósito de obtener una ventaja frente a la facilidad de los ataques.

- Proyectar el fortalecimiento de un laboratorio de investigación y desarrollo que pueda estar a la vanguardia de la solución de problemas tecnológicos en seguridad y defensa en el ciberespacio, que estas soluciones puedan ser puestas al servicio de la Armada Nacional, desincentivando el interés de otras direcciones o unidades de adquirir total o parcialmente los activos de la Dirección Cibernética.

**Fortalezas Oportunidades FO:** En este grupo de acciones se deben reunir los planes conducentes a cada una de las fortalezas internas o externas que fueron consideradas como oportunidades que se pueden potencializar para asegurar el éxito.

- Establecer un horario semanal o una persona calificada y con experiencia ha dedicación exclusiva a la investigación de mercado de software libre que puede ser adaptado a las necesidades de la Dirección Cibernética, con la de adquirir competencias y bajar los costos.

- Utilizar el acceso y la capacidad de gestión de la persona que lidera y direcciona el área de ciberdefensa, apalancarse sobre las organizaciones y agencias externas a la Dirección Cibernética Naval, para obtener la adquisición de capacidades que con anterioridad se hayan definido como prioritarias.

- Establecer un listado de necesidades de la flota naval, y su departamento de operaciones, aprovechando la experiencia adquirida en otras unidades del personal de la dirección cibernética, con el propósito de establecer líneas de acción para vincular nuestras unidades operativas con las ventajas y amenazas del quinto dominio como teatro de operaciones, mostrándonos como una unidad vinculada totalmente a la misión de la Armada Nacional.

- Realización de simulacros a nivel fuerza de cuales seria las consecuencias físicas que afecten la capa virtual y el dominio cibernético ante la posibilidad del escalamiento de una crisis con Venezuela y Nicaragua, hasta un conflicto regular que permita hacer una valoración de nuestra capacidad de reacción y resiliencia ante este tipo de eventos. como cualquier otra que se pueda presentar de la misma magnitud, pueden generar espacios para el desarrollo de las capacidades cibernéticas.

- Diseñar plan de revista anual que permita la programación y verificación de las unidades en donde se soporten tecnológicamente los principales procesos (operativos, administrativos) de la Armada Nacional, empleando el personal capacitado y con experiencia de la unidad se pueda realizar un diagnóstico y tomar las primeras medidas de control o reacción.

- Empleo de la información obtenida por acceso del director de cibernética naval a escenarios de tomas de decisiones de mediano y alto nivel, con el fin de identificar las necesidades y oportunidades del mando, brindar una respuesta alternativa diferente y complementaria a las que hacen las demás unidades.

- Identificar posibles organizaciones (pública y privada) alineadas a la infraestructura crítica de responsabilidad o relacionadas al poder marítimo de la nación a las que como fuerza pública podamos prestar servicio de ciberseguridad, con el propósito de realizar un convenio donde a cambio de los servicios o asesoramiento prestados podamos recibir recursos que puedan ser optimizados en el auto sostenimiento de la unidad.

**Fortalezas Amenazas FA:** En este grupo de acciones se deben reunir los planes conducentes a cada una de las fortalezas, que de una u otra manera ponen en riesgo permanente el éxito. Estas acciones también son de prioridad muy alta, por lo tanto, deben existir planes detallados que minimicen los efectos negativos que amenazan al proyecto.

- El personal que proviene de unidades externas debe ser empleado como canal de comunicación de sus antiguas unidades, generar vías de comunicación paralelas a oficiales de seguridad de la información que pueda generar conciencia situacional del medio cibernético, al mismo tiempo representar cuáles son los intereses y los servicios en que la Dirección Cibernética estableció su roll diferencia frente a otras dependencias.

- Emplear el talento humano de la dirección cibernética para construir un plan de detección de debilidades apoyado por el comandante de la armada que permita la exposición de vulnerabilidades y fallas de los principales tomadores de decisiones de la organización con sensibilización personalizada evidenciando que, así como ellos como persona son vulnerables, la fuerza también los es, por eso se requiere un mayor compromiso con la capacidad cibernética.

- Utilizar la gestión de la dirección para difundir al nivel de escenarios de gran mayoría de oficiales de insignia y capitanes de navío la situación de desventaja en capacidades cibernéticas frente a las reales y potenciales amenazas, las cuales cada de ves son más

sofisticadas y evolucionadas, buscando el impacto de generar la necesidad de priorizar la adquisición de capacidades que efectúen un balance del potencial.

- Utilizar la experiencia y el talento humano para generar una conciencia situacional desde el punto de vista del usuario, quien a la medida que exige conectividad debe exigir seguridad de los canales de comunicación con el propósito de contrarrestar la facilidad del empleo del ciberespacio para atacar la fuerza.

Con el propósito de establecer un cumplimiento de la estrategia esta se debe establecer un objetivó estratégico, el cual esta definido de la siguiente forma:
Transformación hacia una cibernética Naval de vanguardia con visión al 2025, que asuma roles de la doctrina naval y geoestratégica, con presencia influyente a bordo de todos los componentes de la Amada de la Republica de Colombia, bajo una visión sistémica y con centro de gravedad en su talento humano, propendiendo por un posicionamiento diferencial a partir del fortalecimiento de las capacidades distintivas que brinden la posibilidad de introducción a nuevas tecnologías que permitan complementar y orientar al Poder Naval de la Nación para influir en el desarrollo marítimo y fluvial nacional y Regional.

## Conclusiones

Desde la aparición de la TICS y como estas juegan un papel fundamental en toda organización pública o privada, hasta el momento se ha demostrado que en ellas reposan o se soportan en gran parte de los procesos o servicios, esto sucede en todos los sectores de

importancia, de ahí que el entorno militar no sea diferente, por lo arrojado en una apreciación del estado del arte, existen muchas variables que influyen en el desarrollo de una estrategia, uno principal es el nivel de madurez desde donde se inicia e igual de importante tener una visión clara y realista del estado deseado que se quiere alcanzar.

La estrategia debe ser considerada como un camino para llegar a ese estado deseado u objetivo final, esta debe ser dinámica, cambiante, adaptable, ya que la carrera contra las amenazas cibernéticas que cada día son más sofisticadas y efectivas es casi imposible mantenerse en la delantera, esta investigación ha demostrado que el ciberespacio continúa siendo un dominio fundamental y necesario para el desarrollo de actividades políticas, económicas y militares, que aumenta su importancia como dominio militar ya que contiene la información de las infraestructuras vitales para el sostenimiento y desarrollo de un estado, por lo cual que toda estrategia está influenciada por su entorno y debe ser flexible.

Una vez realizado el estado de madurez utilizando parámetros internacionales como los de la OTAN es evidente la poca madurez de las capacidades, sin embargo, las que se encuentran más desarrolladas ha dependido en forma directa de los recursos destinados en su desarrollo para la obtención de la capacidad, en la medida que los recursos obtenidos sean orientados a la obtención de capacidades especificas estas pueden alcanzar un relativo estado de madurez en poco tiempo.

El diagnósticos de mediante el empleo de la estrategia DOFA posterior a la evaluación del estado de madurez permite realizar una apreciación total de la organización y como el

entorno influye sobre el desarrollo de sus capacidades, que a pesar de tener una bases sólidas en talento humano, procesos y procedimientos, el apoyo de la alta gerencia de la organización encargado de la distribución de los recursos que pueden ser empleados en esta área, junto a la falta de focalización de sus actividades frena el desarrollo de obtención de capacidades de cibernética.

Por lo cual las líneas estratégicas desarrolladas buscan motivar al cambio en la organización, no esperar a que de forma fortuita se puedan superar los principales obstáculos, si no en crear condiciones para que estas por sí solas desaparezcan en la medida que se cumple el objetivos de una capacidad cibernética desarrollada a las medida de las necesidades de la Armada Nacional.

## Recomendaciones

## Referencias Bibliográficas


Abedrapo, J. (s. f.). Latina. Desafíos para la seguridad y. *Revista Ensayos Militares*, *1*(1-2015), 165-177.

Amoroso, E. G. (2012). *Cyber attacks: protecting national infrastructure*. Elsevier.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, *12*(2), 141-165.

Bejarano, M. J. C. (2011). Alcance y ámbito de la seguridad nacional en el ciberespacio. *Cuadernos de estrategia*, (149), 47-82.

Blockmon, R. (2016). *CEH V9: Certified Ethical Hacker Version 9 Practice Tests*. John Wiley & Sons.

CAMERA, J. C. (2014). CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION.

Definición, A. B. C. (2013). Internet. *Definición de Universidad.[Citado 07 junio 2012]. Disponible en: http://www. definicionabc. com/comunicacion/lluvia-de-ideas. php.*

Drucker, P. F., & Drucker, P. (1999). *Los desafíos de la administración en el siglo XXI*. Sudamericana,.

Guía de ciberseguridad para los países en desarrollo. (s. f.). Recuperado a partir de http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf

IBÁÑEZ, E. M. (s. f.). LOS RETOS DE LA CIBERINTELIGENCIA. *3ª ÉPOCA*, 53.

Jajodia, S., Liu, P., Swarup, V., & Wang, C. (2010). *Cyber situational awareness* (Vol. 14). Springer.

Julián David Aponte Díaz. (2015). *Proyecto para la creación del Comando de Ciberseguridad y Ciberdefensa de la Armada Nacional de la República de Colombia*. Univeridad Politecnica de Madrid.

Kesan, J. P., & Hayes, C. M. (2011). Mitigative counterstriking: Self-defense and deterrence in cyberspace. *Harv. JL & Tech.*, *25*, 429.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. *Cyberpower and national security*, 24-42.

León, J. D. (2016). La ciberguerra como realidad posible contemplada desde la prospectiva. *Revista de Pensamiento Estratégico y Seguridad CISDE*, *1*(1), 18-32.

Lichtman, M., Jover, R. P., Labib, M., Rao, R., Marojevic, V., & Reed, J. H. (2016). LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation. *IEEE Communications Magazine*, *54*(4), 54-61.

Marcuello, S. C., & Chaime, A. (2006). . Sociocibernética. Lineamientos de un paradigma. *Institución Fernando el católico.*

Maria Cosntanza bermudez Arciniegas. (2014). Estrategia para la creacion de una unidad cibernetica. Universidad Sergio Arboleda.

Mariña, M. (2002). La Cibernética en el Gobierno de la V Republica. *Trabajo de Ascenso Académico. Caracas: Vicerrectorado Administrativo de la UCV.*

Micheli, J. (2002). Digitofactura: flexibilización, internet y trabajadores del conocimiento. *Comercio Exterior*, *52*(6), 522-536.

MIN TICS. (2016). Conpes 3854- Política Nacional de Seguridad Digital en Colombia -.pdf. Recuperado 7 de mayo de 2016, a partir de file:///C:/Users/PC%201/Documents/MAESTRIA/MAESTRIA%20CIBERDEFENSA/SEMANA%206/Conpes%203854.pdf

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Recalde, L. (s. f.). EL CIBERESPACIO: EL NUEVO TEATRO DE GUERRA GLOBAL. *Revista de Ciencias de Seguridad y Defensa.*

Riascos, J. A. C. (2015). Nada volverá a ser igual: ciberguerra y ciberpoder. *Memorias*, *13*(23).

Trujillo, C. (2014). *The limits of cyberspace deterrence*. DTIC Document.

## Tablas y figuras

## Apéndices (anexos)

### Glosario

1. Responsabilidad: Garantizar que las vulnerabilidades se aborden adecuadamente y hacer cumplir un castigo cuando no lo son.
2. Amenazas Persistentes Avanzadas: Ataques a sistemas informáticos que involucran múltiples técnicas o enfoques. De esta manera si un método es detectado y bloqueado por el software de seguridad, otro medio de ataque causará el daño pretendido.
3. Anónimo: Estar sin ser detectado en Internet para que la gente no sepa que usted está allí y una vez que un ataque ha sido completado no puedan encontrarlo.
4. Antivirus: Software diseñado para identificar virus informáticos y proteger la computadora de su funcionamiento.
5. Atribución: Los ataques cibernéticos pueden realizarse a través de las fronteras, lo que significa que el atacante podría estar en Sudáfrica y usar computadoras en los Estados Unidos para atacar sistemas chinos. Es increíblemente difícil rastrear los ataques a un actor específico, e incluso si pudieras, poner la culpa en ellos es un tiro al revés.
6. Disponibilidad: Garantizar que tanto el hardware como el software están actualizados y funcionan a la máxima capacidad.
7. Puerta trasera: Código que concede al atacante permiso para ingresar una computadora a distancia.
8. Prepararse mejor a los ataques cibernéticos lejanos: Ejecución de simulaciones para probar el software es mejor cuando se involucran personas de diferentes departamentos, organizaciones o países para que pueda fomentar la comunicación y la cooperación, así como aprender de diferentes puntos de vista.

9. Análisis de datos grandes: El análisis de datos grandes se utiliza para encontrar correlaciones en grandes conjuntos de datos que permiten a los analistas categorizar y visualizar las amenazas cibernéticas rápida y eficientemente.
10. Botnet: Red de agentes de software instalados en una computadora (usualmente sin el conocimiento del dueño de la computadora) para explotar los recursos informáticos de una red comparten el desempeño de una tarea, basado en un sistema de software legal instalado en ellos. En el contexto del ciberataque, este término se refiere a la sobrecarga ilegal y encubierta de una computadora desde una distancia, y usarla para realizar tareas que el atacante define.
11. CNA - Computer Network Attack: Ataque a fines de destrucción. La expresión de la destrucción estará en el mundo cinético (ejemplo lejano: borrar la información esencial, apagar la electricidad, detener el flujo de agua, interrumpir los sistemas de armas).
12. CNE - Explotación de Redes Informáticas: Ataque para explotar la información en la computadora / red y la información almacenada en la computadora / red.
13. CNI - Influencia de la Red de Computadores: Ataque para propósitos de influencia psicológica, daño a la moral, conciencia pública de influenza.
14. Nexos y relación civil-militar: La relación de trabajo entre el ejército y el gobierno y cómo pueden o tienen dificultades para coordinar la estrategia de defensa y las políticas públicas.
15. La informática Forense: es una rama de la ciencia forense digital perteneciente a la evidencia encontrada en computadoras y medios de almacenamiento digitales. El objetivo de la informática forense es examinar los medios digitales de una manera forense sólida con el objetivo de identificar, preservar, recuperar, analizar y presentar hechos.

16. Confidencialidad: las medidas adoptadas para garantizar que la información sensible sólo está disponible para aquellos con la debida autorización.
17. Infraestructura crítica: Estructura esencial para el funcionamiento eficaz de un país. A medida que más sistemas de infraestructura están conectados a Internet, aumenta la amenaza de un ataque cibernético.
18. Cyber ataque: La penetración ilegal, en su mayor parte encubierta, de un ordenador, una red informática o cualquier dispositivo conectado a una red controlada por ordenador para diversos fines. Los ataques están divididos por objetivo, tipo, método de ataque y, a veces, por herramientas de ataque.
19. Creación de capacidades cibernéticas: Aumento de las capacidades, programas, tecnología, etc., para combatir las amenazas cibernéticas.
20. Contraterrorismo cibernético: El contraterrorismo cibernético no siempre se trata de encerrar Terroristas fuera de Internet, sino corromper su información. Un ejemplo es el cambio de las direcciones de las bombas para que explote al mismo tiempo.
21. La auditoría forense del delito cibernético: Después de un ciberataque, los analistas forenses tratan de determinar de dónde proviene la amenaza o las repercusiones persistentes del ataque.
22. Cibergobierno: "Un método, sistema de gobierno o gestión del "mundo cibernético".
23. Protección cibernética de la infraestructura crítica: Fortalecimiento de los sistemas que controlan o administran los sistemas de infraestructura contra las amenazas cibernéticas. 100% de protección es imposible, por lo que es necesario establecer prioridades.

24. Defensa cibernéticos: "Acciones tomadas para proteger, monitorear, analizar, detectar y responder a actividades no autorizadas dentro de sistemas de información gubernamental y redes informáticas".
25. Ciberespacio: Área física y no física creada o formada por parte o todos de los siguientes factores: sistemas mecanizados e informatizados, redes informáticas y de comunicaciones, información computarizada de software, contenido transferido de forma informatizada, datos sobre tráfico y control, de los usuarios de estos.
26. Ciberterrorismo: El uso deliberado de redes y sistemas informáticos para causar daño o herir a la gente. Por lo general, los ataques tienen objetivos políticos o ideológicos. Crean turbulencia.
27. Tratado Cibernético: Los tratados internacionales sobre regulaciones sobre el ciberespacio son difíciles de crear y hacer cumplir debido a definiciones vagas e intereses divergentes y conflictivos. Los estados pueden ganar algo de ataques cibernéticos por lo que es difícil acordar las limitaciones.
28. Ciberguerra: Un ataque cibernético que provoca la muerte, lesión o destrucción y se lleva a cabo con métodos y metas políticas.
29. DDoS - Denegación de servicio distribuida: Inunda un sitio de proveedor de servicios con una gran cantidad de falsas consultas, de tal manera que lo bloquea y lo hace colapsar, evitando así el servicio a los usuarios.
30. Desfigurar / cambiar de apariencia: Cambiar la apariencia de un sitio e incrustar mensajes que sirven al atacante.

31. Disuasión: La disuasión en la seguridad cibernética es diferente de la disuasión nuclear tradicional porque se basa en la amenaza de castigo, la negación por la defensa, el **enredo** y los tabúes normativos.
32. Espionaje: El robo de secretos comerciales realizados con la intención de beneficiar a un a un soberano extranjero.
33. Ataques de Hardware / Firmware: Ataques basados en cambios en el hardware (usualmente en la etapa de fabricación) o cambios en el software ubicado en los componentes de hardware con el fin de usar el ordenador de forma preliminar.
34. ¿Cómo podemos organizarnos mejor para la ciberseguridad? Hay demasiada dependencia de cada sector o departamento para asegurar individualmente su infraestructura crítica, pero esto no ocurre porque estas industrias no saben lo suficiente sobre seguridad cibernética. Es necesario que haya más normas gubernamentales de alto nivel sobre la ciberseguridad para asegurar que todo esté adecuadamente protegido.
35. Cómo mejorar la colaboración en la información: La información debe compartirse dentro de una red confiable porque existe el riesgo de que actores malévolos utilicen esa información para desarrollar ataques más complicados.
36. Intercambio de información: Intercambio de datos entre un emisor y un receptor. El intercambio de información es necesario en una burocracia gubernamental eficaz para promover la coordinación y la comunicación.
37. Integridad: Velar por que los datos sigan siendo exactos e inalterados.
38. Internet de las cosas: La creciente red de dispositivos físicos conectados a Internet y entre sí. Un entorno de computación en red global, inmersivo, invisible, ambientado a través de

la continua proliferación de sensores inteligentes, cámaras, software, bases de datos y centros de datos masivos en un tejido de información de alcance mundial.

39. Límites del Estado en el Ciberespacio: El Estado se basa en un territorio físico, pero el ciberespacio existe fuera de las fronteras físicas. La naturaleza descentralizada pero coordinada del ciberespacio no es compatible con la naturaleza del sistema estatal que está altamente centralizado y tiene una coordinación internacional deficiente.
40. Malware, software malicioso: Software / código utilizado por un usuario no autorizado o ilegal de la computadora, para cualquier propósito.
41. Actores no estatales: Piratas informáticos, activistas cibernéticos, ciberdelincuentes, ciberterroristas: Los actores no estatales desempeñan un papel importante en la seguridad cibernética porque la tecnología es más fácil de acceder que los sistemas de armas tradicionales. Tampoco tienen tanto que perder como actores estatales por lo que están más dispuestos a actuar de manera riesgosa.
42. Phishing: Intento ilegal de obtener información de un equipo, como nombre de usuario, contraseña u otros detalles de identificación de personas. Por lo general, el intento se basa en comunicaciones por correo electrónico, mensajería instantánea o redes sociales (por ejemplo, Facebook), y remite al usuario a un sitio que parece confiable y a veces familiares.
43. Privacidad: Tener información personal protegida y no está disponible para cualquiera que la utilice maliciosamente o para la vigilancia.
44. Asociación Público-Privada: "Una iniciativa de cooperación entre los sectores público y privado, basada en la experiencia de cada socio, que mejor responda a las necesidades públicas claramente definidas mediante la asignación adecuada de recursos, riesgos y recompensas".