Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Maestría en Ciberseguridad y Ciberdefensa

ELEMENTOS DE CIBERSEGURIDAD PARA NEUTRALIZAR LOS ATAQUES CIBERNÉTICOS EN LAS UNIDADES A FLOTE DE LA ARMADA NACIONAL DE COLOMBIA

CAPITÁN DE CORBETA JUAN ERNESTO POSADA ALCALDE

Director de trabajo de grado
MANUEL HUMBERTO SANTANDER PELÁEZ

Bogotá, Colombia; 14 de septiembre de 2021

Dedicatoria

A mis padres quienes con su esfuerzo me brindaron todas las facilidades para salir adelante.

A mi Institución, la Armada de Colombia, que constantemente me brinda los espacios para capacitarme y ser cada día una mejor persona.

A mi Esposa Karen y a mi hijo Juan Pablo por todo el apoyo y acompañamiento durante este proceso.

Agradecimientos

Agradezco de manera especial a las personas que hicieron posible y facilitaron el desarrollo de este trabajo, de manera especial a mi tutor el Señor Manuel Humberto Santander Peláez, quien orientó de manera muy acertada la investigación, así mismo a los Oficiales del Departamento de Armas y Electrónica de la Base Naval ARC “Bolívar” quienes dedicaros su tiempo y esfuerzo para solucionar las dudas que se presentaron y brindar información indispensable para el desarrollo de este trabajo, finalmente a mi esposa y a mi hijo por su comprensión y apoyo en todo momento.

Resumen

Tomando como referente el aumento en cuanto a las cifras de amenazas de carácter cibernético, y siendo la seguridad un aspecto fundamental en las unidades a flote de la Armada Nacional de Colombia, se considero como prioridad la realización de un estudio que determinara las estrategias de ciberseguridad fundamentales para implementar. Es así que para dar respuesta a lo antes planteado, se ejecutaron una serie de pasos determinantes como la identificación de riesgos y con base en ellos precisar las amenazas que subyacen en relación con los hallazgos identificados, a su vez, la descripción de algunas estrategias de ciberseguridad empleadas a nivel Internacional y Nacional, y establecer propuestas que contribuyan a neutralizar los ataques cibernéticos. Para dar cumplimiento a lo anterior se realizo un análisis al protocolo de comunicación NMEA 2000, en el cual se identifico que elementos como GP, ECDIS, las cartas de navegación electrónica ENC y AIS, que al operar en un entorno vulnerable se incorpora al desarrollo de riesgos y amenazas afectando la seguridad. A través de las propuestas establecidas se buscó como primero mitigar los incidentes cibernéticos que se presentan a través de la gestión y análisis de riesgos, como de la conciencia situacional del ciberespacio.

Palabras clave:

Riesgos, amenazas, ataques ciberneticos, ciberseguridad.

Abstrac

Taking as a reference the increase in the number of cyber threats, and security being a fundamental aspect in the afloat units of the National Navy of Colombia, it was considered a priority to conduct a study to determine the fundamental cybersecurity strategies to implement. Thus, in order to respond to the above, a series of decisive steps were taken, such as the identification of risks and, based on them, to specify the underlying threats in relation to the identified findings, as well as the description of some cybersecurity strategies used at international and national level, and to establish proposals that contribute to neutralize cyber attacks. In order to comply with the above, an analysis of the NMEA 2000 communication protocol was carried out, in which elements such as GP, ECDIS, ENC and AIS electronic navigation charts were identified, which, when operating in a vulnerable environment, are incorporated to the development of risks and threats affecting security. Through the established proposals, we sought to mitigate cyber incidents through risk management and analysis, as well as situational awareness of cyberspace.

Key Words:

Risks, threats, cyber attacks, cybersecurity.

Índices de contenido

Abreviaturas

A.R.C: Armada Nacional de Colombia

CA: Ciberamenaza

CAT: Ciberataque

C.E: Ciberespacio

CONPES: Consejo Nacional de Política Económica y Social.

CS: Ciberseguridad

Introducción

Se reconoce que los ataques cibernéticos no solamente son problemáticas de las empresas, sino que estas también involucran la seguridad de un país, es por ello que se requiere determinar las estrategias que se consideran pertinentes implementar, con el fin de minimizar o neutralizar los Ataques Cibernéticos. Como lo afirma Berardi (1996) es necesario que las fuerzas armadas identifiquen y estén preparadas, para responder a la variedad de amenazas y situaciones conflictivas que se presentan en el ámbito marítimo. Con base en lo anterior esta investigación tiene como propósito determinar aquellos controles de ciberseguridad, que permitan neutralizar los diversos ataques cibernéticos; para ello el estudio se lleva a cabo en las unidades a flote de la armada nacional colombiana.

Es así, que para dar cumplimiento a lo planteado en este estudio, surge como pregunta, ¿Cuáles estrategias de ciberseguridad se consideran fundamentales implementar para neutralizar los ataques cibernéticos en las unidades a flote de la Armada Nacional de Colombia?, para dar respuesta a este interrogantes se establece como primer objetivo identificar riesgos y amenazas cibernéticas en las Unidades a flote de la Armada Nacional, como segundo determinar las diferentes estrategias de ciberseguridad a nivel Nacional e Internacional aplicables a las Unidades a flote de la Armada Nacional de Colombia., y por último proponer las estrategias de protección a implementar en relación con los riesgos y amenazas por ataques cibernéticos en las Unidades a flote de la Armada Nacional.

A su vez, el marco conceptual permite realizar un acercamiento a los postulados y definiciones de las variables que se convierten en los factores claves del presente

estudio, siendo estos los ataques cibernéticos, y la ciberseguridad, términos que se convierten en el eje conductor del estudio.

En relación con la metodología, y tomando como base a Hernández, Fernández y Baptista (2014), es fundamental la identificación del enfoque y el diseño del estudio, y los instrumentos a emplear, permitiendo la recolección y análisis de datos; lo cual conlleva a dar respuesta a los objetivos planteadas.

A su vez en los capítulos 3, 4 y 5 se dan respuesta a los objetivos planteados en el estudio el cual y tomando como base la pregunta problema, permite identificar tanto los riesgos, como las amenazas a las cuales se encuentran las unidades a flote de la Armada Nacional, como también permite un acercamiento a los diferentes ciberataques que se pueden presentar.

Con base en la identificación se realiza una selección de estrategias a nivel Internacional, que conlleva a generar propuestas que se puedan implementar en las unidades a flote de las Armada Nacional.

CAPÍTULO I

Planteamiento de Investigación

Estado del Arte

En el siglo XXI, la sociedad de la información da apertura a diversos factores como la globalidad, y la facilidad de acceso a las tecnologías de la información y la comunicación TIC, lo que conlleva a generar mayor posibilidad de los Ataques Cibernéticos (AC). Tomando como referente lo descrito por el Consejo Nacional de Política Económica y Social. En Colombia, se ha incrementado el uso del entorno digital, lo que conlleva a que se dé un alto aumento en relación con (a) las amenazas cibernéticas, (b) la vulnerabilidad y por último (c) los incidentes digitales, estos elementos generan afectaciones en la seguridad tanto de las personas, las organizaciones públicas, privadas, y las infraestructuras, lo que genera ser un foco de interés en los distintos ataques cibernéticos CONPES (2016).

Prototipo de ello son los dados en Estonia en el 2007, en Rusia Georgia en el 2008, (Vásquez et al, 2017), sistemas informáticos del CERN en Ginebra 2008, en Estados Unidos (2009-2012), generados en la administración de Barack Obama, y también en la de George W. Busch en los atentados terroristas del 11 de septiembre (Cruz y Yareli, 2018), las plantas nucleares de Irán en el 2010, ataques en el Líbano, Israel y territorios palestinos en el 2012, entre otros (Villanueva, 2015).

A su vez, el ámbito militar no está excepto de Ataque Cibernéticos, los cuales son considerados como amenazas, teniendo una gran probabilidad que surjan ataques informáticos, los cuales de acuerdo a Días (2020), y Carlini (2016), tienen como finalidad el robar información, dejar sin redes y sistemas tecnológicos, infectar las redes de computadoras con programas manipulados por hackers con el objetivo de emplearlos

a su voluntad, a su vez efectuar ataques concertados. Como también los ataques a cajeros electrónicos, secuestros cibernéticos, entre otros.

Algunos de los casos identificados son como el producido en Inglaterra, cuando afectaron la red del metro, un apagón de 34 minutos en el sur de Londres trastornó la red del metro de la ciudad y el sistema de trenes en el sur de Inglaterra, lo que conllevo a que se afectara un medio millón de personas, como también los servicios en el centro de la capital británica. Otro de los casos es el presentado en una de las redes informáticas del Pentágono, la que sufrió un ataque desde China, por hackers. Los centros Nacionales de Informática, en India, sufrió de ataques para lo cual emplearon las conexiones telefónicas de internet en China, accediendo a los correos electrónicos de ministros, burócratas y funcionarios de defensa.

Tomando como base lo anteriormente enunciado, Richardson (2019), reconoce que las operaciones navales y costeras se han visto involucradas en A.C, por lo cual se considera necesario adoptar prácticas que contribuyan a garantizar tanto la defensa como la seguridad, siendo necesario que se apliquen controles en relación con la seguridad tecnológica que coadyuve a gestionar los riesgos cibernéticos en las diversas operaciones marítimas, es así, que la ciberseguridad y la ciberdefensa permite evidenciar que en el ciberespacio existen amenazas latentes a la seguridad de un estado o una organización. (Vargas, 2014).

Ejemplos de ello está la situación citada por Crawford (2019), con el yate White Rose of Drax, con base a un estudio realizado en la Universidad de Texas en Austin, en el 2013 en el que se reconoció la posibilidad de ciberataque a través de la manipulación de manera remota de los GPS, modelo de ello es el yate “White rose of Drax”, el cual fue atacado a través de señales falsas de GPS, lo que conllevo al control del sistema de

navegación, cuando se encontraba navegando en el Mediterráneo, dicha acción generó un cambio de rumbo, siendo definido por los hackers. Como también el puerto de San Diego en Estados Unidos en el 2018, fue atacado por un ransomware con una pieza de software lo que provocó disrupciones administrativas en la obtención de permisos para el uso del puerto. Y en el 2019, se generaron ataques en los guardacostas de la marina en los EE.UU., en el puerto de NewYork este producido por medio del GPS jamming. Otro de los ataques en ese mismo año, fue el realizado en la naviera MSC provocado por una pieza de software maliciosa lo que causó una disrupción en los sistemas de desintermediación denominados MyMSC (CEPAL, 2020).

Formulación del problema

Con base en lo anterior, se considera que la gestión de la ciberseguridad se ha convertido en un factor esencial lo que conlleva a la prevención de AC, es así que como lo afirma Vasquez, Rojas y Macha (2017), Cruz y Yareli, (2018), y Richardson (2019), quienes afirman que se debe fomentar una cultura de prevención y detención de los Riesgos Cibernéticos (RC), específicamente dando a conocer los peligros que subyacen al desconocer estos o el empleo de estrategias AC existentes, a su vez la manera de desarrollar planes de acción y estrategias que coadyuve a minimizarlos.

Por lo cual, se reconoce que los ataques cibernéticos no solamente son problemáticas de las empresas, sino que estas también involucran la seguridad de un país, es por ello que se requiere determinar las estrategias que se consideran pertinentes implementar, con el fin de minimizar o neutralizar los AC. Tal como lo afirma Berardi (1996) “La variedad de amenazas y situaciones conflictivas en el ámbito marítimo es enorme y las fuerzas especiales de la Armada deben estar preparadas para responder con éxito a todas ellas” (p.2).

Tomando como referente lo anteriormente descrito surge la siguiente pregunta de investigación.

Pregunta de investigación

¿Cuáles estrategias de ciberseguridad se consideran fundamentales implementar para neutralizar los ataques cibernéticos en las unidades a flote de la Armada Nacional de Colombia?

Objetivos de la investigación

Objetivo general

Determinar las estrategias de ciberseguridad que se requieren ante los ataques cibernéticos en las Unidades a flote de la Armada Nacional de Colombia (ARC).

Objetivos específicos

1. Identificar riesgos y amenazas cibernéticas en las Unidades a flote de la Armada Nacional.
2. Determinar las diferentes estrategias de ciberseguridad a nivel Nacional y/o Internacional aplicables a las Unidades a flote de la Armada Nacional de Colombia.
3. Proponer las estrategias de protección a implementar en relación con los riesgos y amenazas por ataques cibernéticos en las Unidades a flote de la Armada Nacional.

Justificación

Los grandes avances en relación con las tecnologías de la información y la comunicación, conlleva a que se genere intranquilidad y preocupación tanto a los gobiernos, como a la sociedad en relación con el manejo de la información, esto debido a los riesgos que se enmarcan por el uso masificado de los datos que circulan en el ciberespacio, datos que en ocasiones son empleados para generar delitos informáticos.

Aunque a nivel de legislación el país viene trabajando para brindar una ciberseguridad, en ocasiones, se han identificado diversos ataques que afectan a la sociedad, razón por la cual es primordial que así cómo evoluciona la tecnología a pasos agigantados, también la Armada Nacional deba aumentar las estrategias de ciberseguridad que permitan el cumplimiento de su misión, “defender la soberanía, la independencia, la integralidad del territorio nacional”, todo ello para contribuir con la seguridad de la población Colombiana.

CAPÍTULO II

Marco de Referencia

Este capítulo permite tener un acercamiento y reconocimiento de la literatura en relación con los riesgos para la seguridad específicamente ataques cibernéticos, y las estrategias de la ciberseguridad, para ello se adentrará en la revisión bibliográfica a nivel Internacional y Nacional.

Marco teórico

La realización de este estudio, requiere de una revisión de la literatura, para ello se tendrá presente los diferentes postulados, y pesquisas que se han trabajado en relación con el tema de estudio, los cuales permiten generar un sustento a la investigación. Estas se establecen a partir de una sinergia existente entre las variables ciberespacio, ciberseguridad, ciberataques, y riesgos cibernéticos. Se dará inicio con la concepción de una palabra en común que es ciber, para luego y con base en su comprensión adentrarse a los demás variables.

Ciber.

La real academia española, define Ciber como un elemento que concuerda con las redes informáticas. Y en relación con el diccionario etimológico se precisa como, kubernetes, “piloto” o “timonel”, es decir quien gobierna o controla, y kybermaein, que significa “manejar el timón, gobernar, pilotear, en referencia al espacio virtual creado por los medios informáticos” (RAE, 2020, p.1). En cuanto a cibernética, Platón citado por (Telles, 2016), se refiere a la ciencia utilizada por el timonel para el pilotaje del navio”, y André Marie Ampére lo define como “las ciencias del control de la sociedad”. (p. 4).

Ciberespacio.

Definiéndolo como el lugar virtual en el cual interactúan diversas personas, con una infinidad de datos virtuales que se generan en el espacio y posibilitan a su vez el uso y almacenamiento de la información, la cual es empleada con disimiles propósitos. Para Lessig (2002), el ciberespacio C.E "es el lugar donde los individuos son, inherentes, libres de control de los soberanos del espacio real" (p.172), a su vez, reconoce como el C.E se convierte en un elemento completo y esencial en las naciones, pero a su vez es compleja su regulación.

Para el C.E se requiere de un entorno con dos elementos como son la electrónica y el espectro magnético, que permite como primero el almacenamiento, para luego modificar e intercambiar información por medio de los sistemas de red y de infraestructuras (Ambos, 2014). Mientras para la OTAN el ciberespacio es entendido como el dominio que pretende seguir misiones de defensa colectiva, esto a causa de un ciberataque en Kosovo cuando sus fuerzas alidas realizaban una operación (Healey & Van Bochoven, 2012, citado por Aguilar, 2020)

Riesgo de Seguridad Digital.

El riesgo es definido por el Consejo Nacional de Política Económica y Social CONPES (2016) como "efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas" y en relación con el riesgo de seguridad digital, categoría de riesgo que se relaciona con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital" (p. 24)

Expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. El cual puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan (CONPES, 2016, p. 24).

Dentro de los riesgos del ciberespacio citados por Sancho (2017), están los espionajes, ataques contra infraestructuras, ataques contra redes y sistemas, ataques a internet, infección con malware, servicio a terceros, amenazas persistentes, robo y publicación de la información sensible, robo de identidad, o fraude, entre otras. Los riesgos a los que Colombia actualmente se puede enfrentar en materia de ciberseguridad, pueden provenir de múltiples fuentes y actividades como el sabotaje, espionaje, fraudes o ciberataques, desde el exterior por otros países, grupos organizados o particulares, entre otros. De igual forma, dichos ataques también se pueden desarrollar desde el interior del país. (Escuela Superior de Guerra, 2020).

Gestión de Riesgos Cibernéticos.

Es un enfoque de políticas adaptable a los diversos cambios del mercado, permitiendo tanto a las organizaciones como a los ciudadanos evaluar y tomar las medidas pertinentes en cuanto a las imprecisiones y riesgos producidos en los entornos digitales. Dicha estrategia permite la toma de decisiones socioeconómicas, y las cuales soportan los objetivos de las actividades socioeconómicas y no las debilitará" (OCDE (2015).

De acuerdo a lo establecido por la Organización Marítima Internacional, en su circular MSC-FAL.1/Circ.3, define por gestión de riesgos cibernéticos "el proceso de

identificación, análisis, evaluación y comunicación de riesgos de índole cibernética y de aceptación, evitación, transferencia o mitigación de esos riesgos hasta un nivel aceptable, teniendo en cuenta los costos y las ventajas para los interesados de las actuaciones emprendidas" (5 julio, 2017). El objetivo de la gestión de riesgo cibernético es "contribuir a la seguridad y a la protección del transporte marítimo, operacionalmente resiliente ante los riesgos cibernéticos." (MSC-FAL.1/Circ.3, del 5 julio 2017).

Amenaza informática.

La amenaza, es definida por el CONPES (2020), como la "posible violación de la seguridad digital que tiene el potencial de ocurrir total o parcialmente en el entorno digital. Se caracteriza por la aparición de una situación donde uno o más actores, adelantan una o varias acciones con la capacidad de alterar una infraestructura física, un sistema de información o la integridad de la información en sí. Estas amenazas pueden darse de manera no premeditada y accidental o, por el contrario, de manera intencional con el fin de causar daño, generar problemas o adelantar una agresión cibernética con el objetivo del propio beneficio o para desestabilizar la población, el territorio y la organización política del Estado. (Ministerio de Defensa de Colombia) (Rec. UIT-T X.800, 3.3.55). (citado por el CONPES; 2020, p.42).

El Ministerio de defensa define la amenaza informática como "La aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado". (Ministerio de Defensa de Colombia). El CONPES 3854 identifica que las amenazas cibernéticas emergentes son cada vez más difíciles de detectar, lo que genera una mayor incertidumbre en la seguridad digital, y que los riesgos asociados a esas incertidumbre no sólo está direccionados a las bases de datos o sistemas de información,

sino que también apunta a la infraestructura crítica nacional, entre la que se encuentran las hidroeléctricas, redes de energía, sistemas portuarios, sistemas de defensa, armamento de guerra, entre otros, que utilizan las redes de comunicaciones para su funcionamiento (CONPES, 2016).

A continuación, se expone la delimitación de las amenazas, desde un ámbito general, en el cual se enmarcan países como Alemania, España, Canadá, y Estados Unidos, todos ellos miembros de la OTAN (Tabla 1).

Tabla 1

Delimitación de las Ciberamenazas.

País	Ciberamenazas (C.A)
Alemania	De acuerdo Germany (2016), citado por (Aguilar, 2020), existen dos tipos de C.A, (a) Civil: fraude en datos, espionaje industrial, daño en sistemas informáticos, cibercriminal. (b). Militar: amenazas hibridas, afectación de sistemas de comunicación, suministro de energía.
España	Con base al Departamento de Seguridad Nacional –DSN-, citado por (Aguilar, 2020), se reconocen las siguientes amenazas. Estados extranjeros, causas técnicas, fenómenos naturales, hacking, conflictos, sabotaje, hacktivista, delincuencia, espionaje, organizaciones terroristas.
Canadá	Ciberamenazas avanzadas, estipulado por CDPS (2010), citado por (Aguilar, 2020), las cuales están conformadas por espionaje, ciberexplotación, robo de la información confidencial, seguridad nacional o propiedad intelectual del Estado, ataque o infraestructura Critica Nacional.
Estados Unidos	Según la EOTPW, 2017, citado por (Aguilar, 2020), hay 4 tipos de amenazas, estas son: (a). amenazas a las redes e información federales. (b). Amenazas a las infraestructuras críticas. (c). Combate al cibercrimen y mejora de notificación de incidentes (d). Amenazas a la economía digital

Fuente: (Aguilar, 2020 p.21)

En cuanto a las principales Ciberamenazas en América Latina, descritas por (Aguilar, 2019) son los malware, entendido como el robo de la información sensible, para ello emplean técnicas como spear-pishing es decir correos electrónicos que tienen

como finalidad infectar computadores personales, watering-hole, que consiste en infiltrarse en los sitios web con el objetivo de enviar códigos maliciosos; troyanos, los cuales conllevan al fraude bancario. Otra de las amenazas es el ciberespionaje, cuyo fin es robar información sensible con propósitos comerciales, políticos o militares, considerándose como la más difícil para detectar, y combatir, esto debido a que son programadas para no interrumpir la ejecución de actividades, ya que son monitoreadas pasando por desapercibidas. (Burton, 2015).

Ciberataques.

Es definida como una acción organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio (Ministerio de defensa). Aranda, Riquelme, y Salinas, (2015), es un acto malicioso, que concierne a la introducción de virus que causan pérdida de información, afectando el funcionamiento de las redes o sitios web. Los Ciberataques son dirigidos a computadores de todo el mundo con el fin, de cometer delitos bancarios o probar la vulnerabilidad de algunos sistemas. Como también el daño de la infraestructura, o la ejecución de bases para ataques futuros. Los ciberataques generan no solo costos económicos, también generan grandes dificultades en la seguridad nacional y a nivel social (Machado, 2014). Los ataques pueden ser procedentes no sólo de hackers informáticos sino de terroristas, organizaciones criminales y extremistas políticos, movimientos fanáticos religiosos, servicios de inteligencia y fuerzas militares adversarias (Instituto Español de Estudios Estratégicos, 2010, p.330).

Características de los ciberataques.

Dentro de las características que emergen en los Ciberataques, son (a) bajo costo, en relación con las herramientas, empleadas las cuales son a muy bajo costo o en

ocasiones gratuitas. (b) ubicuidad y fácil ejecución, es decir no se requiere de estar ubicado en el lugar del ataque, y las herramientas son de un sencillo manejo (c) efectividad e impacto, con base a la organización, planeación y ejecución, pueden conllevar al cumplimiento de los objetivos planteados. (d) reducido riesgo para el atacante, es decir que es muy difícil poder identificar el autor o los autores causantes del daño.

Fases de un Ciberataque.

De acuerdo a Arroyo et al (2020), el ciclo de vida de un ciberataque se denomina cyber kill chain, a su vez se caracteriza por ser cíclico, es decir que después de culminado el ataque puede volver atacar. El ciclo de vida de un ataque esta dado en siete pasos, los cuales son. (a) reconocimiento, búsqueda de la información requerida, empleando las páginas web, correos entre otros. (b) preparación, diseña el método a emplear (c) distribución, transmisión del malware selecciona (d) explotación, se infecta el programa o dispositivo seleccionado (e) instalación, el malware se ubica en un sitio estratégico para atacar (f) comando y control, el virus controla la información y los dispositivos, y por último (g) acciones sobre los objetos, el atacante se apropia de la información requerido o dispositivo para generar el daño.

Tipos de Ciberataques

Para (Crawford, 2019), existe dos tipos de ciberataques, siendo estos los ataques no focalizados y los ataques dirigidos. Los ataques no focalizados, "…los sistemas y datos de un buque son uno de los muchos objetivos potenciales, y los ataques dirigidos, los ". los sistemas y datos son el objetivo deseado" (p.17).

Y en relación con la Oficina Gubernamental (citado por Crawford, 2019), para la ciencia del Reino Unido, reconoce tres categorías, siendo estas (a) activos de empresa,

(b). sistemas de información y por último (c) los GPS. Dentro de las tecnologías que intervienen en relación a los ataques se identifican los ECDIS, la vulneración de los sistemas de cartas electrónicas de navegación, estas remplazan las cartas náuticas físicas. Los AIS que tienen como finalidad la comunicación con naves, e intercambiar posiciones, y datos, esto con el fin de prevenir posibles colisiones; y por último los GPS, definido como el sistema de posicionamiento global, los cuales pueden ser atacados, lo que conlleva a dificultades tanto en el transporte como también en las vidas humanas.

Los ciberataques generan no solo costos económicos, también generan grandes dificultades en la seguridad nacional y a nivel social (Machado, 2014). Los ataques pueden ser procedentes no sólo de hackers informáticos sino de terroristas, organizaciones criminales y extremistas políticos, movimientos fanáticos religiosos, servicios de inteligencia y fuerzas militares adversarias (Instituto Español de Estudios Estratégicos, 2010).

El desarrollo tecnológico ha determinado nuevos conflictos con características propias, con relación a los métodos que afectan intereses de un país, de acuerdo con Izaguirre y León (2017), se identifican dos tipos: la explotación de redes informáticas y los ataques. En relación al primero se encuentran las actividades de espionaje cuyo fin es tomar información específica para lucrarse o para ataques a las redes y con relación a los ciberataques, entendidos como los ataques emanados de las amenazas.

Ciberseguridad.

El concepto de ciberseguridad tiene gran relevancia debido al creciente uso del ciberespacio. En relación a ello el Ministerio de las Tecnología de la Información y la Comunicación, la define como el conjunto de respuestas que tanto el Estado como una

entidad consideran pertinentes emplear en las conductas consideradas como reprochables o causantes de perjuicio social, esto con el objetivo de garantizar la protección de los intereses esenciales de los mismos y de los derechos de los residentes en el territorio bajo su jurisdicción (Min Tic, 2014).

De acuerdo a la Comisión de regulación de comunicaciones, en la Resolución 2258 de 2009, la define como la incorporación de diversas herramientas, y políticas, que tienen como finalidad la protección de las organizaciones y usuarios en el ciberentorno. El CONPES 3995 del (2020) lo define como

> La capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales. La ciberseguridad tiene el fin de proteger a los usuarios y los activos de Estado en el Ciberespacio y comprende el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, practicas idóneas, seguros y tecnologías que pueden utilizarse para dicho fin (p. 43).

A su vez Baralt (2017), la define como el conjunto de políticas, estrategias, métodos de gestión de riesgos, acciones preventivas y seguros tecnológicos que sirven para proteger el ciberespacio de una nación, su patrimonio y los usuarios del ciberentorno, enfocados en la protección de la información digital en los sistemas interconectados. Como elementos de la ciberseguridad están la (a), confiabilidad, la cual tiene como finalidad proteger la información, (b) integralidad, busca que la información almacenada no sea manipulada, ni editada por un tercero, de tal manera que sea

autentica y (c) disponibilidad, como su nombre lo indica es poder tener los datos en el momento que se requiera. (Arroyo, Gayoso y Hernández, 2020).

Hay que tener presenta que la ciberseguridad no solo se alinea con la información trasmitida, esta también contempla activos que pueden presentar riesgos de ataques por las TIC.

Los riesgos a los que Colombia actualmente se puede enfrentar en materia de ciberseguridad, pueden provenir de múltiples fuentes y actividades como el sabotaje, espionaje, fraudes o ciberataques, desde el exterior por otros países, grupos organizados o particulares, entre otros. De igual forma, dichos ataques también se pueden desarrollar desde el interior del país (Escuela Superior de Guerra, 2020).

Definiendo riesgo como la "Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información" (ISO Guía 73:2002). Para la NIST, "los riesgos de ciberseguridad hacen referencia a la protección de la confidencialidad integral o disponibilidad de la información" (Uribe, 2019)

Estrategias de Ciberseguridad

Las estrategias de ciberseguridad son mecanismos fundamentales que advierten las conflagraciones cibernéticas, las cuales pueden tener secuelas desastrosas en comparación con la confrontación militar tradicional (Carlini,2016). El Gobierno Español, establece algunas estrategias las cuales emergen de dos elementos fundamentales, siendo estos los principios rectores y las líneas de acción.

En relación a los principios rectores, se identifican cuatro estrategias, siendo estas. (a) El liderazgo nacional y coordinación de esfuerzos, (b). la responsabilidad compartida, para lo que se requiere el trabajo colaborativo que permita el intercambio

de la información con organizaciones tanto privadas como públicas que contribuyan a la ciberseguridad. (c) la proporcionalidad, racionalidad y eficacia, para ello se requiere como primero gestionar como a través del uso de las TIC se crean riesgos, de tal manera que se identifiquen las posibles amenazas y con base a ello determinar los posibles elementos que contribuyen a la protección, confianza y eficacia.

Y por último la (d) Cooperación Internacional, se convierte en un principio esencial reconociendo que en ocasiones las amenazas son de carácter transfronterizo lo que conlleva a desarrollar una cooperación y coordinación de carácter global entre distintos países (Estrategias de Ciberseguridad Nacional, 2013)

En relación con las líneas de acción, se identifican cuatro, las cuales se describen a continuación (tabla 2)

Tabla 2.

Línea de Acción. Capacidad de prevenir

LÍNEA DE ACCIÓN	ESTRATEGIAS
1. Capacidad de prevenir, detener, responder y recuperarse de la Ciberataques. C.A.	• Ampliación y mejora en relación con detectar y analizar los C.A. • Identificación de la génesis, procedimientos y elaboración de defensas y protección. • Ampliar la capacidad de respuesta a los ciberataques. • Cooperación global. • Capacitación y actualización permanente de prevención y detención de los C.A. • Crear y ejecutar ejercicios de simulación de C.A, que contribuyan a la evaluación y mejora de acciones. • Ampliar, y mejorar la protección de las redes y sistemas de información y telecomunicaciones. • Dinamizar las competencias militares que coadyuve a dar respuestas asertivas en casos de CA.

Fuente: Estrategias de Ciberseguridad Nacional España (2013).

La siguiente línea de acción a explicar es la relacionada con la seguridad en las diversas estructuras críticas en relación con las TIC. Identificando las estructuras críticas de acuerdo a las directivas europeas (2008), en su artículo 2 como el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población, cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones (p.43).

Dicha línea, tiene como finalidad promover las normas de protección de las infraestructuras críticas como también las capacidades requeridas para proteger servicios esenciales, determinando estrategias que coadyuve al cumplimiento del fin planteado (tabla 3).

Tabla 3.

Línea de acción Seguridad de los Sistemas.

LÍNEA DE ACCIÓN	ESTRATEGIAS
Seguridad de los sistemas relacionados con las TIC, como soporte en las estructuras críticas.	• Implementar la participación de los sectores privados en el desarrollo de actividades enmarcadas en simulación de incidentes de C.S. • Llevar a cabo modelos de simulación que tengan como fin el análisis de las infraestructuras críticas y posibles riesgos.

Fuente: Estrategias de Ciberseguridad Nacional España (2013).

La lineación de acción relacionada con la cultura de ciberseguridad, tiene como fin último concienciar a las personas sobre la importancia de la ciberseguridad, como también del uso responsable de las tecnologías y a su vez los servicios de la sociedad de la información, (tabla 4).

Tabla 4

Línea de Cultura en Ciberseguridad

LÍNEA	ESTRATEGIAS
Cultura de ciberseguridad	• Generar actividades de conocimiento y sensibilización en relación a la vulnerabilidad, y Ciberamenazas, que coadyuve a la protección del entorno tecnológico. • Desarrollo de programas de concienciación en ciberseguridad

Fuente: Estrategias de Ciberseguridad Nacional España (2013)

Las investigadoras Dammnet y Núñez (2019), identifican diversas estrategias Nacionales de ciberseguridad en países del Cono Sur, siendo estas.

Argentina, considerado como de los primeros países que comienza a dar respuestas a los diversos incidentes de ciberseguridad. Dentro de sus estrategias establecidas está el diseño de un marco jurídico, en donde se le da la facultad a los diversos órganos gubernamentales la facultad de ampliar respuesta en relación a las amenazas que se presentan. A su vez crean el Ministerio de Modernización, el cual va a fortalecer en relación a la ciberseguridad aspectos ministeriales y gubernamentales; este ministerio trabaja basado en cinco ejes, siendo estos (a) modernización administrativa, (b) gobierno abierto (c) capital humano (d) infraestructuras tecnológicas y (e) ciudadanía inteligente.

Esto permite la creación de un comité de seguridad que busca generar una cultura de ciberseguridad, para ello requiere de un trabajo colaborativo, en donde se hacen presente representantes de los Ministerios de Modernización, Defensa y Seguridad, y Ministerio Publico Fiscal y conforman el Comité de Seguridad con mira a generar una cultura de ciberseguridad.

En el caso de Brasil, en el 2015 fue publicada la estrategia Nacional de seguridad de comunicaciones de Información y seguridad cibernética de la administración pública, la cual tenía como objetivo el fortalecimiento de las políticas y planteamientos de seguridad de la información y la comunicación y de la seguridad cibernética en la administración pública, esto con el fin de la defensa de los intereses tanto del Estado como de la sociedad, en pro de preservar una soberanía Nacional.

Es así que para lograr el objetivo planteado crean un órgano central y un sistema Nacional DSIC, que tiene como fin el seguimiento y evaluación de políticas Nacionales de SIC y SegCiber (seguridad cibernética). Al reconocer la existencia como la evolución de las amenazas cibernéticas, consideran fundamental articular alianzas con sectores tanto públicos como privados en pro de fortalecerse en temas relacionados con la cibernética, a su vez, la estrategia permite garantizar los recursos que se consideran fundamentales para la protección de las estructuras críticas y de Brasil.

Chile. Con el fin de generar políticas que contribuyeran a la protección de la privacidad se crea la política Nacional de Ciberseguridad (PNCS) para ello forman un Comité Interministerial de ciberseguridad, el cual tiene como funciones brindar asesorías al presidente, plantear políticas de ciberseguridad, identificación de amenazas a nivel global. Regional y nacional. Generación de prevención y respuestas rápidas ante posibles incidentes, presentados. A su vez la política enmarca objetivos como la organización de infraestructuras robustas y resiliente, que tenga la capacidad de dar resistir y recuperarse de manera rápida a los ataques, empleando la estrategia de gestión de riesgo, el desarrollo de una cultura de ciberseguridad, establecimiento de relaciones cooperativas en ciberseguridad, promover la creación de industrias de ciberseguridad.

Paraguay. Creación y aprobación del plan Nacional de ciberseguridad, diseñado a través de un trabajo conjunto con la Secretaria Nacional de Tecnología de la Información y la Comunicación, Ministerio de Relaciones Exteriores. Dicho plan tiene como finalidad coordinar políticas públicas de ciberseguridad, y la generación de entornos seguros, confiables y resiliente. El plan se sopesa con principios que lo orientan en relación a cambios culturales con el manejo de la información, creación de ambientes óptimos para el crecimiento, desarrollo y competitividad.

Uruguay. Se diseña la agenda Digital 2020, el cual tuvo como finalidad desarrollar tecnologías, basadas en una transformación con equidad.

Otras pesquisas realizadas en coherencia con las estrategias de ciberseguridad en los países con más poder, están: (Durak, 2020).

Estados Unidos. Diseño de planes que tengan como finalidad descartar las posibles amenazas, adaptar las medidas pertinentes que coadyuven a la protección de las innovaciones tecnológicas de Estados Unidos. Delimitar como infraestructura crítica nacional los ordenadores, software y tecnologías en red con el fin de dar protección ante posibles ataques cibernéticos.

China. Enmarca una serie de estrategias como el (a) desarrollo de medidas que contribuyan a minimizar propósitos en relación a la guerra informática, (b) específicamente las basadas en redes, con el fin de contrarrestar actividades de intervención, (c) diseñar estructuras efectivas contra el espionaje, (d) Apoyo a las capacidades militares, y el desarrollo de estrategias para la protección de las infraestructuras críticas de las fuerzas militares.

Operaciones Cibernéticas

Definidas por (Díaz, 2011), como las acciones realizadas para obtener la superioridad en la información, la cual sea negada a los enemigos. La cual se emplea para interrumpir, perturbar, inutilizar, degradar entre otras. Están distribuidas en tres subgrupos, siendo estos (a) Computer Network Defense (CND), las cuales tienen como finalidad proteger, monitorizar, analizar, detectar y recuperarse ante los ataques, que comprometen la información. (b) Computer Network Exploitation (CNE) esta comprende acciones que conllevan a la recolección y explotación de información de enemigos. (c) Computer Network Attack (CNA), son acciones que tienen como fin último perturbar, denegar y destruir la información que transita en los sistemas enemigos.

Controles críticos de ciberseguridad

Con base a lo establecido por el ministerio de tecnologías de Paraguay, se define como el "conjunto de acciones, priorizadas, ampliamente analizadas y de efectividad probada que pueden ser tomadas por las organizaciones para mejorar su nivel de ciberseguridad" (Ministerio de las Tecnologías, Paraguay s.f)

A su vez, los controles críticos presentan cinco principios que son esenciales, y que a su vez están aportando elementos claves en coherencia con la ciberseguridad. Estos factores son (a). La ofensa informa a la defensa: para lo cual se toma como factor clave los diferentes acontecimiento que se han presentado y con base en ello reconocer los ataques reales, lo que permite la generación de procesos que conlleven a diseñar e implementar respuestas efectivas que coadyuven a minimizar los riesgos, como también a generar defensas asertivas ante los diferentes ataques que se han gestado en el mundo.

(b). La Priorización: Consiste como primero realizar inversiones en controles que contribuyan a reducir riesgos, lo que permite generar protección en relación a los diferentes peligros, que pueden potencializarse en los diferentes entornos tecnológicos. (c). Mediciones y métricas: desarrollar reglas y elementos comunes que contribuyan a que todos los actores pueden comprender el lenguaje en el que se está hablando y con base en ello establezca parámetros comunes que ayuden a evaluar las medidas de seguridad dentro de la organización, de tal forma que los factores evaluados contribuyan a dar respuestas acertivas en relación a las medidas de seguridad. (d) Diagnóstico y mitigación continua. Se deben desarrollar evaluaciones periódicamente de tal manera que permite identificar la efectividad de las diferentes medidas tomadas y de qué forma contribuyen y priorizan las siguientes etapas. (e). Automatización: estructurar las defensas esto con el fin de que las organizaciones alcancen las mediciones requeridas, para a través de las organizaciones se logren las mediciones con un nivel de confiabilidad, y continuidad.

Sistema de Gestión de la seguridad de la información. (SGSI).

Enfoque de riesgo, que tiene como fin crear, implementar, operar, supervisar establecer, operar, revisar, mantener y mejorar la seguridad de la información. Esta organizada en una estructura la cual está compuesta por las políticas, las actividades, las responsabilidades, las prácticas, los procedimientos, los presos y los recursos. (ISO, 27001).

Sistema Integrado de Comunicaciones

El sistema integrado de comunicaciones, corresponde a un conjunto de sistemas y equipos, capaces de operar con subsistemas de voz y datos, permitiendo el tráfico de comunicaciones interno y externo, integrados a través de servidores y

redes de fibra óptica de alta velocidad (600 Mbps), centralizadamente controlados por software desde consolas de operación ubicadas en la Sala de Radio y CIC, de fácil mantenimiento, de reducido número de operadores y mantenedores a bordo (Vásquez, 2003. p.8).

Tácticas y técnicas descritas en la matriz MITRE

Táctica de Inhibición de respuesta

Hace relación a una técnica en la cual se obstaculizan las salvaguardas, conllevando a inhibir función de seguridad, protección. Lo que puede conllevar a pérdida de vidas o destrucción de equipos.

Entre las tácticas se identifican en la tabla (5)

Tabla 5

Táctica de Inhibición de respuesta

Táctica	Técnica	Descripción
Inhibición de respuestas	Activar el modo de actualización de firmware	Evitar que las funciones de respuesta esperadas actúen como reacción a una emergencia o un mal funcionamiento del proceso
	Función de inhibición de respuesta	Los adversarios pueden apuntar a las alarmas de la función de protección para evitar que notifiquen a los operadores sobre condiciones críticas.
	Mensaje de comando de bloqueo	Bloqueo de mensajes de comando para que no llegue a su objetivo para evitando la ejecución del comando
	Bloquear mensaje de informe	Bloquear o evitar que un mensaje de denuncia llegue a su objetivo previsto
	Bloque serial COM	Bloquear el acceso a COM en serie para evitar que las instrucciones o configuraciones lleguen a los dispositivos de destino.

	Destrucción de datos	Destrucción de datos durante el curso de una operación.
	Parada de servicio	Detener o deshabilitar servicios en un sistema para que esos servicios no estén disponibles para usuarios legítimos
	Modificar configuración de alarmas	Como su nombre lo especifica, la modificación de las alarmas por parte de los atacantes conlleva al operador desconocer de su presencia, como también el desconocimiento a peligros inminentes. Los informes generados por mensajes proporcionan información importante del sistemas
	Firmware	En ocasiones los firmwares son actualizados por sus usuarios o a través de redes remotas, lo que puede generar que un atacante acceda a esta y cargue un firmware malicioso, esto puede provocar el acceso al root del sistema.

Fuente. Mitre (2020)

Táctica de Colección.

Consiste en la recopilación de datos sobre los sistemas de control por parte de un adversario. Dentro de las acciones a ejecutar se identifican, capturas de pantalla, la identificación de roles de dispositivos únicos y la recopilación de esquemas de diagramas y sistemas. Al poseer dichos datos el atacante puede hacer emplea de la información lo que puede conllevar a la planificación, ejecución e incluso revisión de un ataque dirigidos (tabla 6)

Tabla 6

Tácticas de colección

Táctica	Técnica	Descripción
Tácticas de colección	Datos de repositorios de información	Los ciberatacantes pueden recopilar información sensible como notas, claves, procesos relacionados al control del sistema de control, entre otros.
	Detectar el modo de funcionamiento	Se presenta cuando el atacante realiza una recopilación de la información que está relacionada con el funcionamiento de los controladores.
	Hombre en el medio	Esta técnica conlleva a que los atacantes tengan acceso a las redes, para modificar el tráfico de datos en tiempo real de la res. Conllevando a bloqueos de mensajes, suplantación, modificación de parámetros o datos.
	Olfateo inalámbrico	Esta técnica consiste en capturar una comunicación que se está ejecutando por radiofrecuencia, empleada para el control remoto y diseño de informes. Los datos pueden ser tomados mediante el empleo de hardware.

Fuente. Matriz de técnicas Mitre

Comando y control

Es una técnica empleada como medio para comunicar y enviar comandos a diversos sistemas, dispositivos, y/o controladores. Dichos dispositivos de comunicación contienen interfaces entre hombre y máquina. En relación a las tácticas de control y comando se encuentran. (Tabla 7)

Tabla 7

Tácticas de Comando y Control

Táctica	Técnica	Descripción
Comando y control	Puerto de uso común	Dicha técnica conlleva a que los atacantes se comuniquen por medio de los puertos que tienen usos comunes con el fin de eludir los cortafuegos, como también sistemas que detectan las redes, integrándose con actividades tradicionales en la red.
	Protocolo de capa de aplicación estándar	Esta técnica se emplea para aprovechar un proxi de conexión el cual tiene como fin enviar tráfico de red a los sistemas, y o ser intermediarios en las comunicaciones. Esto involucra los procesos de red, el monitoreo de los procesos, la captura de paquetes, análisis de protocolos de red.

Fuente. Matriz de técnicas Mitre

Marco Legal

Ley 906 de 2004, en la cual permite identificar el derecho que tiene toda persona a su libertad.

Ley 1952 de 2019, a través de la cual se expide el código disciplinario, se enmarca en el respeto a la dignidad del ser humano.

Ley 1862 de 2017, en la cual se establecen las normas de conducta del personal militar Colombiano, a su vez se expide el código de disciplina militar.

Ley 1712 de 2014, esta ley hace referencia a la transparencia y derecho de acceso a la información pública.

Ley 1341 del 2009, la cual se organizan las Tecnologías de la Información y Comunicación TIC, la creación de la Agencia Nacional del espectro, y la protección de la información y de los datos, como un bien jurídico tutelable.

Ley 1273 de 2009, se establece la tipificación de delitos que tienen como finalidad proteger los datos y los sistemas informáticos de atentados contra la confidencialidad, integralidad y disponibilidad, a su vez los atentados informáticos. Los delitos a los que se incurren son: (a) acceso abusivo a un sistema informático. (b). interceptación de datos informáticos, (c) daño informático, (d) uso de software malicioso (e). Violación de datos personales. (f). Suplantación de sitios web. (g). Hurto por medios informáticos.

Ley Estatutaria 1581 del 2012, en la cual se instaura un marco básico para la protección de datos, divulgación y denuncia de las violaciones de seguridad.

Ley 1266 de 2008 se da a conocer disposiciones generales de habeas data, como a su vez define la regulación en relación al manejo de información.

Ley 1928 del 2018. La cual se aprueba el "convenio sobre ciberdelincuencia" del 23 de noviembre del 2001, realizado en Budapest, en el capítulo II, el cual hace relación a las medidas que deberán adaptarse a nivel Nacional. Título 1. Delitos contra la confidencialidad, integralidad y disponibilidad de datos y sistemas informáticos. En su artículo 2. Acceso Ilícito, en el cual se enmarca la adopción de las medidas legislativas que se consideran pertinentes como delitos en relación con el acceso deliberado a un sistema informático, ya sea parcial o totalmente. Artículo 3. En lo relacionado con la interceptación ilícita. Artículo 4. Interferir en los datos, en relación a los dañar, borrar, deteriorar, alterar o suprimir datos informáticos. Artículo 6: Abuso en los dispositivos. Título II, delitos informáticos, y con los Artículos 7. Falsificación de la información,

introducción, alteración, borrar o suprimir datos, dando lugar a datos no auténticos. Artículo 8. Fraude informático, inferencias en el funcionamiento de un sistema informático. Título 5. Artículo 11. Tentativa y complicidad. (Diario Oficial, 2018).

Ley 599 del 2000, por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa." (CONPES, 2011).

Resolución 2258 de 2009 de la Comisión de Regulación de Comunicaciones, en su artículo 1 de la resolución CRT 1740 de 2007, la cual da a conocer las definiciones de autenticación, autorización, ciberespacio, ciberseguridad, confidencialidad de datos, disponibilidad, entidad, infraestructura critica, integridad de datos, interceptación, interferencia, interrupción, no repudio, pharming, phishing, software malicioso y vulnerabilidad.

Estandares

AG/RES. 2040 (XXXIV-o/2004). Capítulo IV; delitos informáticos. núm. 2, en relación con los delitos cibernéticos, se recomienda la adopción de recomendaciones dadas en la OEA/ser.k/XXXIV.5. núm. 4, en relación con la asignación y la capacitación internacional, numeral 6, participación en reuniones de expertos para la comprensión de desafíos con los delitos informáticos.

Cumbre de Gales de la OTAN en 2014, en la declaración establece los acuerdos en relación a la ciberseguridad en los países que hacen parte de la alianza. (CONPES, 2016).

ISO/IEC 27000, es referenciada parcial o total en el documento y es indispensable para su aplicación.

Norma Técnica Colombiana NTC – ISO/IEC 27005:2011" Gestión del Riesgo de Seguridad de la Información

Norma Técnica Colombiana NTC – ISO/IEC 31001:2011 "Gestión del

Norma Técnica Colombiana NTC – ISO/IEC 27001:2013 "Sistemas de Gestión de Seguridad de la Información - Requisitos

Documento CONPES 3701 de julio del 2011 "política para ciberseguridad y Ciberdefensa".

NIST Cybersecurity Framework. Guía de ciberseguridad que permite una mejor comprensión de los diferentes riesgos de ciberseguridad que pueden presentarse en las diferntes estructuras; lo que conllevaa reducir y administrar de manera indicada los riesgos como también contribuye a la protección de redes y datos. Se enuncian en el NIST, cinco areas siendo estas, identificación, protección, detección, respuesta y recuperación.

NIST SP 800-82 (Guide to Industrial Control Systems (ICS) Security). una guía para la seguridad de los sistemas de control, incluyendo sistemas SCADA (Supervisory Control And Data Acquisition), DCS (Distributed Control System) y otros sistemas que

trabajan en los sistemas de control. A su vez, el documento permite la identificación de las amenazas, y la vulnerabilidad, lo que conlleva a proporcionar algunas recomendaciones y medidas que contribuyan a minimizar los riesgos.

Marco Referencial

El marco referencial permite tener un acercamiento y reconocimiento de la literatura en relación con los riesgos para la seguridad específicamente ataques cibernéticos, y las estrategias de la ciberseguridad, para ello se adentrará en la revisión bibliográfica a nivel Internacional y Nacional.

Investigaciones Internacionales

El estudio realizado por Vasquez, Rojas y Macha (2017), denominado C. Los investigadores justifican su estudio en el fomento de una cultura de prevención y detención de los riesgos cibernéticos en PYMES del Perú, específicamente dando a conocer los peligros que subyace al desconocer los ataques cibernéticos existentes, a su vez la manera de desarrollar planes de acción y estrategias que coadyuve a minimizar los riesgos existente, para lo cual se enmarca como problema medir la relación existente entre la gestión de la ciberseguridad con la prevención de ataques cibernéticos. A su vez, reconocen que los ataques cibernéticos no solamente son problemáticas de las empresas sino que estas también involucran al estado.

En las bases teóricas del estudio, se enuncian ataques cibernéticos estratégicos en Países como Estonia, en el 2007, lo que conlleva a la inhabilitación de instalaciones militares críticas, también en Rusia, Georgia (2008), generando una invasión terrestre. Los resultados del estudio demuestran la importancia de la ciberseguridad, reconociendo a su vez que la empresa carece de procedimientos, y políticas que orienten a una práctica pertinente en el uso de las tecnologías, falta de capacitación a sus empleados

que ayuden a la prevención y posibles amenazas, como tampoco cuenta con personal responsable de seguridad, lo cual hace vulnerable la información de los riesgos cibernéticos.

Dentro de las recomendaciones se reconoce la necesidad de diseñar políticas de ciberseguridad en las empresas con el fin de reconocer su importancia, programar reuniones que coadyuve a identificar las necesidades de herramientas que protejan la información, y el diseño de planes de contingencia que comprometan los sistemas informáticos, para lo cual se requiere protección y resguardo.

La pesquisa realizada por Cruz y Yareli (2018), relacionada con la Ciberseguridad en Estados Unidos: Vulnerabilidad en el hackeo y espionaje sobre información clasificada en materia de política exterior (2009-2012). Tuvo como objetivo, analizar las medidas de ciberseguridad implementadas a partir de la vulnerabilidad en el hackeo y espionaje sobre información clasificada durante la primera administración del presidente Barack Obama 2009-2012.

En el documento se realiza una explicación de los antecedentes que dieron origen a los avances tecnológicos para la seguridad nacional, a su vez abordan la teoría de la globalización, en adición se explicaron las amenazas emergentes como es el uso de virus para penetrar en las vulnerabilidades de la infraestructura cibernética y se analizó la postura de los organismos internacionales para llevar acciones junto con el gobierno para un buen funcionamiento de la ciberseguridad en el ciberespacio mediante el uso de internet y los protocolos de seguridad implementados (Cruz, 2018).

Así mismo, se realiza un recuento de los ataques cibernéticos generados en la administración de Barack Obama, como también las medidas de seguridad cibernética a partir de los atentados terroristas del 11 de septiembre con la administración de George

W. Bush, a la vez, hace un análisis de las estrategias de ciberseguridad a partir de los ataques cibernéticos a la infraestructura crítica estadounidense, analizando las filtraciones en el portal WikiLeaks y las acciones que tomó el gobierno estadounidense para evitar posibles infiltraciones.

Más adelante se analizan las acciones de ciberseguridad y se abordaran los sistemas de ciberespionaje por las agencias de inteligencia y las repercusiones en el ámbito diplomático al filtrarse información en diarios internacionales que obtuvieron la información por medio de un ex agente de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA). Así mismo, se explica el combate contra el ciberterrorismo por parte de Estados Unidos y los principales grupos terroristas que atentan a su Seguridad Nacional y las medidas que se están adoptando para contrarrestar y neutralizar ataques de hackers pertenecientes a las células terroristas que tienen como finalidad provocar desestabilización en los sectores económicos políticos y sociales (Cruz, 2018).

El investigador concluye que las Relaciones Internacionales a partir de la globalización, se ha reconfigurado un orden en la dinámica mundial, mediante el uso del ciberespacio que ha cobrado mayor relevancia al permitir interrelacionarse sin el impedimento del lugar, tiempo y espacio, tomando en cuenta que los riesgos aumentan y cambian constantemente por lo cual la ciberseguridad es primordial para establecer medidas que regulen y protejan la seguridad, sin interferir en la soberanía de los Estados, como lo ha venido haciendo EEUU con los programas de ciberespionaje. De igual forma, concluye que Estados Unidos utiliza las estrategias de ciberseguridad para coordinar al sector público y privado, para hacer frente a las ciberamenazas principalmente por grupos terroristas, por lo que implementa programas de vigilancia

que violan la soberanía de los Estados por la gran cantidad de información que recopilan.

También, se generó un análisis de las medidas de ciberseguridad que se implementaron en los Estados Unidos a partir de la vulnerabilidad en el hackeo y espionaje sobre información clasificada durante la primera administración del presidente Barack Obama y emite opiniones sobre la ciberseguridad nacional de los Estados Unidos.

La investigación denominada Análisis Sistemático de Metodologías y Modelos para la Gestión del Riesgo en las Operaciones Navales y Costeras de República Dominicana, el estudio tiene como finalidad realizar un análisis de las diversas metodologías y modelos actuales, que permitan gestionar las prácticas pertinentes en el tratamiento de los diversos riesgos cibernéticos que impactan negativamente en el desenvolvimiento de las operaciones navales y costeras de República Dominicana. (Richardson, 2019).

El estudio reconoce que las operaciones navales y costeras también se han visto involucradas en ataques cibernéticos, por lo cual considera necesario adoptar prácticas que contribuyan a garantizar tanto la defensa como la seguridad de la República Dominicana, para ello es necesario que se apliquen controles en relación con la seguridad tecnológica que coadyuve a gestionar los riesgos cibernéticos en las diversas operaciones marítimas.

El investigador identifica que en las operaciones navales y costeras se aplican los tres ejes sobre los que están basadas las metas de la ciberseguridad, siendo estas (a) Confidencialidad, que busca que la información que se obtiene no debe ser reveladas por usuarios no autorizados; (b) La Integridad, es decir que no deben ser alterados los

datos o la información que se tiene; y como último (c) Disponibilidad es decir que los sistemas funcionen de la manera indicada siempre (Richardson, 2019).

En relación con las buenas prácticas el investigador considera que se requiere analizar cómo primero las metodologías existentes, las cuales se abordan en relación con la gestión de riesgos marítimos, teniendo como directrices la gestión de riesgo de la Organización marítima internacional (OMI), y las directrices sobre ciberseguridad a bordo de los buques diseñada por Bimco y el sistema de gestión de seguridad de la información- Normas ISO/IEC 27001.

A su vez, en el estudio se analizan las diferentes metodologías y su relación con la gestión de riesgos marítimos, entre estos se encuentran: Directriz sobre la gestión de los riesgos cibernéticos marítimos de la Organización Marítima Internacional (OMI), directrices sobre ciberseguridad a bordo de los buques elaboradas y apoyadas por BIMCO2, CLIA, ICS, INTERCARGO e INTERTANKO (Guía BIMCO), y Sistema de Gestión de Seguridad de la Información – Normas ISO / IEC 27001.

Esta investigación concluye la necesidad de diseñar e implementar, sistemas de gestión de seguridad de la información adaptadas a las operaciones, que den una respuesta efectiva a los riesgos cibernéticos. A su vez, exalta el considerar los SGSI como estándar militar, como también considerar la gestión de riesgos en todas las operaciones navales y costeras (Richardson, 2019).

La investigación realizada por Baralt (2017), denominada Ciberseguridad: Un reto para la Defensa Nacional en entornos intangibles, hace un reconocimiento de la participación de las fuerzas militares que tienen a carga la Defensa Nacional en un nuevo espacio de batalla, empleando la ciberdefensa para ello emplea tanto los recursos disponibles, como las unidades especializadas de las Fuerzas Armadas de la nación, con

el fin de enfrentar la diversas actividades delictivas generadas en los ambientes cibernéticos afectando la infraestructura crítica, las instituciones públicas, los servicios de salud y la banca privada, tomando acciones preventivas, al tiempo que realizan actividades que permiten restaurar los servicios que fueren afectados en el menor tiempo posible (Baralt, 2017).

La investigación tenía como fin determinar cuales son las principales amenazas y riesgos a la seguridad de la información y la creación de diferentes instrumentos tanto para poder detectar, defender, investigar, recuperar los sistemas y dar respuesta de manera acertada a los ataques, actos terroristas, entre otros. Con base en ello enmarca la necesidad de dar respuesta al ¿cómo hacer frente a las amenazas, y prepararse a la contingencia, al desconocer de dónde proviene el ataque?

En el estudio Baralt, se reconoce que en el sistema de ciberseguridad y ciberdefensa, tiene unas defensas de protección, pero se enfrentan a una gran amenaza con los malicious insider, siendo estos unos de los grandes enemigos silencios que están "*dentro de casa*". Como también se visibiliza otro factor que genera entornos vulnerables como la conectividad en internet. A su vez, también reconocen como nuevos riesgos y amenazas cibernéticas para la seguridad y la defensa puntos como el acceso global, el impacto, detención de ataques, la mutación existente entre los virus y troyanos informáticos, el acceso a internet y el bajo costo de los equipos tecnológicos; todo ello conlleva a reconocer la importancia de la ciberseguridad y demás vertientes que subyacen de esta, el cual se debe constituir en una razón prioritaria en los gobiernos, empresas y personas.

Dentro de las conclusiones el estudio reconoce la importancia de: (1) Generar esfuerzos en una legislación que regule el delito cibernético teniendo como referente la

Convención de Budapest, con relación a los delitos cibernéticos; (2) Precisar un modelo basado en la infraestructura crítica, lo que conlleva a judicializar las diversas actividades que generan afectaciones; (3) Diseño de sistemas de confianza regionales; (4) Manifestar diversas estrategias a nivel Nacional de seguridad cibernética; y (5) Establecer equipos de respuesta inmediata ante los incidentes que se puedan presentar. Es fundamental que se genere un sentido moral y ético con relación a la ciberseguridad de una Nación.

La Investigación tiene como objetivo analizar el Sistema de Seguridad Cibernética Nacional frente a los Ciberataques como amenaza a la Seguridad Nacional. A su vez pretende presentar diferentes propuestas en relación con la realidad del Perú respecto de la Gestión de la Ciberseguridad y el desarrollo de Cibercapacidades a través de un análisis de realidades comparadas a nivel mundial, para ello utilizan herramientas como el Informe Bid/OEA 2017 "*Ciberseguridad Estamos Preparados en América Latina*" en el cual se determinan diversos puntos de mejora para países de la región, en ese sentido esta investigación pretende presentar propuestas a la realidad del Perú respecto de la Gestión de la Ciberseguridad y el desarrollo de Cibercapacidades haciendo un análisis de realidades comparadas a nivel del hemisferio en donde se presentan diversos puntos de mejora para países de la región (Taipe, 2020).

En la discusión, el investigador considera fundamental mencionar que los países como Estados Unidos, China, Israel, Rusia e Irán, así como la OTAN plantean la creación de Organizaciones que permitan enfrentar eficientemente estas amenazas, ya que son capaces de afectar todos los ámbitos del poder y potencial nacional, lo cual conlleva a la creación de organismos que están dispuestos a la seguridad de la Información, y a su vez deben hacer frente a las amenazas actuales y futuras siendo

parte fundamental de la evaluación de las prioridades a tener en cuenta en las crecientes medidas de seguridad (Taipe, 2020).

El documento concluye en tres grandes reconocimientos siendo el primero que el estado peruano requiere enfocarse en realizar una estrategia de residencia cibernética. Lo que conlleva a desarrollar capacidades tanto para detectar como para resistir los riesgos emergentes. Como segundo, establecer una línea base de seguridad en las instituciones, y como tercero reconoce la importancia de realizar un trabajo conjunto esto con el fin de proteger el ecosistema digital del estado, como también aumentar la seguridad en las diferentes instituciones educativas (Taipe, 2020).

La pesquisa realizada por Aguirre, J. (2019). Cambios en la seguridad internacional en el marco de la globalización: el caso de la ciberseguridad y sus desafíos para la Seguridad Nacional de México (2012-2018). Universidad Nacional Autónoma de México. Analiza la situación internacional en lo referente a la ciberseguridad para explicar los desafíos que tiene México en materia de seguridad nacional, teniendo en cuenta que los ciberataques, de distintos tipos, seguirán aumentando a medida que exista más innovación tecnológica digital (Aguirre, 2019).

Inicialmente el estudio aborda el aspecto teórico-conceptual que tiene como propósito definir el marco explicativo en lo referente al proceso de Globalización, la Cuarta Revolución Industrial, la seguridad nacional e internacional, y el ciberespacio y sus derivados, seguidamente, se hace un estudio de las principales organizaciones internacionales que desarrollan el tema de la ciberseguridad desde un determinado eje de acción (ONU, UNIÓN EUROPEA, OEA, OTAN, entre otras) (Aguirre, 2019).

A continuación, se realiza un análisis los incidentes en Estonia, las centrifugadoras en Irán, y los problemas ocasionados por “WannaCry”, ejemplos

prácticos que permiten dimensionar los efectos negativos que pueden ocasionar el empleo de ataques cibernéticos, para posteriormente analizar los principales incidentes cibernéticos que ha tenido México, de esta manera, se describen los daños, los principales problemas y las vulnerabilidades que tiene el Estado mexicano en el ámbito de la seguridad cibernética, precisando las instituciones encargadas de atender la problemática en lo referente a ciberseguridad, Ciberdefensa y seguridad nacional. Por último, se analiza la situación de la Seguridad Nacional de México con el fin de plantear los desafíos que tiene México en relación con la ciberseguridad. A su vez, se considera la Ley de Seguridad Nacional del año 2005 para reforzar y hacer hincapié en los problemas y vulnerabilidades que tiene el Estado mexicano ante la coyuntura digital (Aguirre, 2019).

El autor concluye que es indispensable reformar y actualizar la Ley de Seguridad Nacional de México del año 2005, toda vez que requiere ser adaptada de acuerdo a la coyuntura tecnológica-digital, además, a través de su investigación, evidencio que México tiene resultados desfavorables a causa de ataques cibernéticos, así como un rezago en materia jurídica, política, de seguridad y defensa, toda vez que su Ley de Seguridad Nacional se estableció en el año 2005, demostrando que está desactualizada y no cumple con los fundamentos de seguridad requeridos para el contexto de la Cuarta Revolución Industrial, especialmente en materia de innovación tecnológica digital. Por último el autor hace una serie de recomendaciones, encaminadas a mejorarla estrategia de ciberseguridad Mexicana (Aguirre, 2019).

El Instituto Español de Estudios Estratégicos. (2010). Ciberseguridad, Retos Y Amenazas a La Seguridad Nacional En El Ciberespacio. En Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el ciberespacio- cuaderno de estudios estratégicos

en su número 149. Plantea elaborar un cuaderno de estrategia sobre lo que, sin duda, es uno de las principales preocupaciones de seguridad de los países más desarrollados y de las organizaciones internacionales como la OTAN y la UE; En el reciente Concepto Estratégico de la OTAN aprobado en la Cumbre de Lisboa, los ciberataques se consideran uno de los principales riesgos. En el llamado Informe Solana de diciembre de 2008, a los cinco años de la aprobación de la Política Europea de Seguridad y Defensa (PESD) de la Unión Europea, también se consideró necesario incluir esta amenaza entre las principales a tener en cuenta, el tema tratado es un tema poliédrico con múltiples aspectos a considerar. procurado abordar los más importantes desde el ámbito de seguridad y defensa (Instituto Español de Estudios Estratégicos, 2010), así mismo, el documento pretende analizar el panorama actual del ciberespacio y como hacer frente a las amenazas que plantea sobre todo con el creciente uso de Internet, en organizaciones, empresas y ciudadanos en general y en la Seguridad Nacional.(Instituto Español de Estudios Estratégicos, 2010)

En este cuaderno de estrategia inicialmente se realiza un compendio de los principales ataques cibernéticos a nivel internacional, así mismo, se analiza el estado del arte de la Ciberseguridad, así como el concepto de ciberguerra dentro del ciberespacio como quinto dominio de la guerra junto a la tierra, mar, aire y espacio. Se describe el nuevo modelo de computación en nube piedra angular de las nuevas infraestructuras tecnológicas de esta década, así como las tecnologías más disruptivas de la actualidad de impacto en las Ciberamenaza y en consecuencia en las Ciberdefensa. (Instituto Español de Estudios Estratégicos, 2010).

Seguidamente, se realiza un análisis generalista del alcance y ámbito de la Seguridad Nacional en el Ciberespacio. La autora especialista en Tecnologías de la

Información tras examinar las definiciones usuales del ciberespacio y sus implicaciones, se introduce en la descripción y análisis de las consideraciones normativas y gestión de la seguridad en el ámbito español, europeo, norteamericano y OTAN. Como experta en el tema describe los tipos de ataques y de atacantes, cómo han evolucionado los ciberataques y sobre todo las posibles y peligrosas amenazas a las Infraestructuras Críticas de interés nacional. Termina planteando desde la visión general que describe la necesidad de desarrollar unas estrategias de ciberseguridad (Instituto Español de Estudios Estratégicos, 2010, p.43)

Después, en el documento se analiza en primer lugar la expansión del Concepto de Seguridad nacional y la aparición de nuevos escenarios, amenazas y respuesta, en el ámbito de la ciberseguridad y Ciberamenaza, en segundo lugar las respuestas del sistema legal, donde analiza la situación legal a escala mundial, a nivel de la Unión Europea y la perspectiva dentro del Derecho Penal Español y en tercer lugar realiza un balance sobre el debate jurídico creado, analizando las categorías generales del Derecho afectadas por los usos y abusos de las nuevas tecnologías (Instituto Español de Estudios Estratégicos, 2010).

El ciberespacio y el crimen organizado se describen en el capítulo 3 como una nueva realidad que ha dado origen al delito informático y la aparición del hacker, luego describe y analiza la delincuencia organizada y los fraudes que originan tanto en el comercio electrónico como en la banca electrónica, sus dos grandes objetivos. (Instituto Español de Estudios Estratégicos, 2010)

Posteriormente se analiza la Ciberseguridad en el marco internacional y dentro del mismo en la OTAN, presentando la situación actual de la Ciberseguridad en el ámbito internacional y analizando los dos casos más emblemáticos de la ciberguerra que

llevaron a estados de todo el mundo a pensar en la necesaria protección antes amenazas cibernéticas, estos son el de Estonia 2007 y Georgia en 2008.(Instituto Español de Estudios Estratégicos, 2010). Luego, en el documento se analiza la ciberseguridad en el ámbito, haciendo una revisión general de las operaciones cibernéticas en redes y en la OTAN, aquí se plantea ya la organización de la Seguridad de la Información y su normativa en el Ministerio Español de Defensa.

Por último, se realiza el análisis y planteamiento de las estrategias nacionales de ciberseguridad y el ciberterrorismo, realizando la identificación de los agentes de la amenaza (ciberterrorismo y ciberespionaje), el análisis de las infraestructuras críticas y su rol en la Defensa Nacional y a continuación se describen las estrategias nacionales de ciberseguridad en diferentes países y en organizaciones internacionales.

Se concluye con la realización de una serie de recomendaciones prácticas para una futura estrategia nacional de ciberseguridad, pero resaltando que es de gran importancia, por su impacto en la Defensa Nacional, que las estrategias de ciberseguridad deben contemplar una coordinación general no sólo de la Ciberdefensa en las Administraciones Públicas sino también del catálogo de Infraestructuras Críticas, de organizaciones, empresas, industrias, centros científicos y de investigación y también de los ciudadanos, ya que dado que el acceso a Internet, fijo y móvil, entendemos, deberá ser declarado un derecho fundamental, en muy poco tiempo toda la población española deberá tener acceso a la Red como tiene derecho a cualquier otro de los servicios de interés general como la luz, el agua, el teléfono o la electricidad (Instituto Español de Estudios Estratégicos, 2010).

Otro de los estudios que emergen en relación con la ciberseguridad y la defensa es el realizado por el coronel Baral Blanco en República Dominicana, el cual reconoce

como la seguridad ha sido desde la historicidad un aspecto esencial para el hombre, razón por la cual y en pro de sus capacidades cognitivas ha diseñado diferentes artefactos que contribuyen a defenderse de las amenazas.

En relación a lo anterior y la historicidad que enmarca la necesidad de protección, Baralt (2019), reconoce que para poder salvaguardar una Nación de los evidentes ciberataques es necesario la creación de centros que tengan como finalidad atender a las diferentes emergencias que subyacen de los ciberataques, dotando de las herramientas requeridas para cumplir ese fin.

En razón a los diferentes acontecimientos que vienen sucediendo como es el caso del ataque del 11 de Septiembre del 2001en los Estados Unidos, y el del 11 de Marzo del 2004 en España, conllevo a la imperiosa necesidad de un cambio de elementos de seguridad más asociados a lo que el autor describe como naturaleza de guerra, para lo cual y en relación a la función que cumplen las fuerzas armadas de salvaguardar una Nación, es eminentemente necesario un cambio de paradigmas frente al empleo de nuevas tecnologías como las tecnologías disruptivas, el bigdata, integrado con diversos estudios, van a contribuir a estar mejor preparado ante eventos que surjan en relación a la ciberseguridad.

A su vez reconoce la existencia de tres elementos relacionados con la seguridad de información que consiste en preservar la confidencialidad, la integralidad y por último disponer de la información.

Por último el estudio titulado Análisis de ciberseguridad en la industria marina, realizado por Mednikarov, Tsonev y Lazarov, (2020), busca develar y describir los diferentes componentes en relación a las políticas de ciberseguridad en la industria naviera, a su vez determinar los principales tipos, procedimientos, influencias y las

etapas de los ciberataques, como a su vez, realizar una evaluación con base a estrategias tecnológicas que contribuyan en la defensa cibernética.

Los investigadores examinan una gran problemática que se viene incrementando y que conlleva grandes repercusiones y es lo correspondiente a los ataques debido a los dispositivos y artefactos tecnológico empleado como también los diferentes sistemas de comunicación que están utilizando en los transportes marítimos, lo que conlleva a un aumentado de ataques cibernéticos en las diferentes industrias marítimas.

A su vez los investigadores reconocen que para lograr tanto la seguridad como la protección de los buques es necesario el empleo de diversos mecanismos, como también de sistemas marítimos que trabajen de manera continua y simultáneamente. Lo que puede coadyuvar a que industria naviera pueda dar respuestas asertivas y reaccionar de la manera indicada a los diversos ciberataques que se puedan presentar.

Investigaciones Nacionales

Realpe y Cano (s.f). En el estudio sobre las Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia. generan un análisis a nivel macro de la situación Colombiana en el campo de la ciberdefensa, en el que se reconocen las ciberamenazas latentes y que emergen de un instrumento denominado ventana AREM, las cuales afrontan a las tecnologías disruptivas, y cuyo análisis permiten responder a las ciberamenazas por medios de estrategias militares en ciberdefensa.

Fruto de los resultados obtenidos en el estudio los investigadores desarrollan una propuesta militar que tiene como finalidad el desarrollo de las capacidades cibernéticas en las Fuerzas Militares, el cual se fundamenta en un modelo integral que abarca la doctrina, la organización, el material, el personal, la infraestructura, el liderazgo,

entrenamiento y mantenimiento; elementos que permiten dar respuesta a las amenazas cibernéticas que emergen.

En la investigación se reconoce como primero que el ciberespacio al no ser un espacio protegido, ni seguro, es vulnerable tanto a las amenazas como a los ataques cibernéticos, conllevando a grandes pérdidas en los económico, político o social, y a su vez una gran amenaza a la defensa nacional, por lo cual se considera pertinente realizar avances tomando como referente los modelos de defensa actuales, y con base en ello desarrollar propuestas acertadas en pro de la seguridad nacional.

En el estudio la Ciberseguridad y Ciberdefensa: ¿Qué Implicaciones tienen para la Seguridad Nacional? Planteó como objetivo demostrar cómo la ciberseguridad y la ciberdefensa permite evidenciar que en el ciberespacio existen amenazas latentes a la seguridad de un estado o una organización. A su vez, hace un acercamiento de los conceptos de ciberseguridad y ciberdefensa, las distintas amenazas latentes en el ciberespacio, los programas y políticas que los países han diseñado para evitar ataques cibernéticos, como también en la actualidad que está desarrollando Colombia para ser lo menos vulnerable en materia de seguridad en la red.

El documento se divide en tres capítulos, el primero abarca los diferentes términos en relación con la ciberseguridad, ciberdefensa, y ciberguerreros, como a su vez las principales teorías y conceptos de las temáticas a investigar. En el segundo capítulo se determinan los ataques que se han presentado en diferentes países, como también los métodos empleados por esos países para proteger el ciberespacio. En el capítulo final se describe cómo está Colombia en materia de ciberseguridad y ciberdefensa, realizando un acercamiento a las diferentes leyes e iniciativas del gobierno

nacional encaminadas a mejorar la utilización del ciberespacio en Colombia y los estamentos encargados de la ciberseguridad y la ciberdefensa (Vargas, 2014).

Para concluir, el investigador propone que es fundamental estar a la vanguardia de los mecanismos para salvaguardar no solo la información sensible de los pobladores de un país o el ataque a una página oficial que se cataloga como un ataque de baja intensidad, sino también tener sistemas de defensa que permitan proteger las infraestructuras críticas que con el paso del tiempo son más dependientes del ciberespacio y si no se protegen la sociedad estaría presenciando un ataque de alta intensidad; así mismo, expone que en el área política, del derecho y la mayoría de ramas de estudio deben trabajar conjuntamente al igual que las instituciones estatales para en verdad lograr estar a la vanguardia sobre las tecnologías de la información y llegar a innovar en este escenario.

A su vez se hace un énfasis en que es importante la capacidad de ataque, pero muchos más la capacidad de defensa para de este modo minimizar la sensibilidad a la hora de recibir un ataque contra infraestructuras críticas y otro tipo de objetivos que se pueden afectar con un ataque cibernético así como en la necesidad de que los hombres y mujeres que ostentan la responsabilidad de la ciberseguridad y la ciberdefensa deben estar intelectualmente preparados para asumir el compromiso de la defensa de un país en el teatro de operaciones del ciberespacio (Vargas, 2014).

El documento plantea como objetivo, el establecer:

> los lineamientos para desarrollar capacidades ofensivas, defensivas, disuasivas y de inteligencia para la protección del Estado, definiendo estándares y compromisos para asegurar el manejo de la información digital como una forma de gestionar y mitigar el riesgo frente a un ciberataque, manteniendo la

> capacidad de resiliencia para responder, recuperar y restaurar las áreas afectadas" (Escuela Superior de Guerra, 2020, p.6).

Es asi que el documento se desarrolla a través de cinco capítulos en los cuales se expone el contexto global y su relación con Colombia, posteriormente se analizan los riesgos, amenazas y desafíos, y finalmente, se exponen los objetivos y las líneas de acción estratégicas; A su vez se dan a conocer las estrategias centradas en la integración, interacción y cooperación entre el sector público y privado de manera transversal, comprometiendo todos los campos político, económico, sicosocial y militar.

A su vez, integra aspectos legales y estratégicos y la coordinación internacional con énfasis en dos áreas: tecnológico y judicial, en esta se definen los riesgos, amenazas y desafíos; se traza un límite no superior al 2024 para el desarrollo de la industria digital nacional y la gobernanza del internet, teniendo en cuenta los cinco pilares establecidos por la Unión Internacional de Telecomunicaciones: medidas legales; medidas técnicas; medidas organizacionales; capacidades de construcción y desarrollo; y medidas de cooperación. Finalmente, se considera de vital importancia establecer el diseño específico de los diferentes planes de carrera y de capacitación al interior de cada una de las instituciones, lo que finalmente, nos permitirá fortalecer los mecanismos defensivos en Ciberdefensa y Ciberseguridad en nuestro país (Escuela Superior de Guerra, 2020).

El documento concluye la importancia que las diferentes entidades del Estado, así como las privadas, socialicen en todo momento los riesgos que conlleva el uso masificado de la tecnología, tales como las comunicaciones y de la información, en contra de la Ciberdefensa y Ciberseguridad nacional, factores, que inciden en la preservación de nuestros intereses nacionales, de la infraestructura crítica del país, de las entidades gubernamentales y privadas, llegando afectar nuestra Seguridad Nacional.

Así mismo se expone que la Ciberseguridad y Ciberdefensa, son un objetivo prioritario para el Estado Colombiano, de tal manera, que se pueda participar activamente y de forma segura en el ciberespacio, facilitando elementos de entendimiento y confianza mutua, con unas relaciones sólidas en el ámbito de la Seguridad y Ciberdefensa, haciendo énfasis en la necesidad de realizar a nivel nacional, un proceso de identificación, autoevaluación y categorización de nuestros centros de gravedad, que generen conciencia ante las potenciales amenazas en Ciberseguridad y Ciberdefensa, encaminadas a proteger la privacidad de la población, la protección de los datos, organizaciones privadas y gubernamentales, pero lo más importante, hacia la gestión de la protección de los centros de poder de la Nación (Escuela Superior de Guerra, 2020).

El desarrollo tecnológico ha determinado nuevos conflictos con características propias, con relación a los métodos que afectan intereses de un país, de acuerdo con Izaguirre y León (2017), se identifican dos tipos: la explotación de redes informáticas y los ataques. En relación al primero se encuentran las actividades de espionaje cuyo fin es tomar información específica para lucrarse o para ataques a las redes y con relación a los ciberataques, Crawford, (2019), los clasifica en ataques no focalizados y los ataques dirigidos.

Y en relación con la Oficina Gubernamental para la ciencia del Reino Unido, reconoce tres categorías, siendo estas (a) activos de empresa, (b). sistemas de información y por último (c) los GPS. Dentro de las tecnologías que intervienen en relación a los ataques los ECDIS, la vulneración de los sistemas de cartas electrónicas de navegación, estas remplazan las cartas náuticas físicas. Los AIS que tienen como finalidad la comunicación con naves, e intercambiar posiciones, y datos, esto con el fin

de prevenir posibles colisiones; y por último los GPS, definido como el sistema de posicionamiento global, los cuales pueden ser atacados, lo que conlleva a dificultades tanto en el transporte como también en las vidas humanas.

Marco Metodológico

La metodología de la Investigación busca dar respuesta a las siguientes preguntas de investigación, las cuales son las bases de los objetivos específicos planteados. Siendo estas ¿Cuáles son los riesgos y amenazas cibernéticas en las unidades a flote de la Armada Nacional? ¿Cuáles estrategias de ciberseguridad a nivel Nacional e Internacional son aplicables a las Unidades a flote de la Armada Nacional de Colombia? ¿Qué estrategias de protección se pueden implementar en relación con los riesgos y amenazas por ataques cibernéticos en las Unidades a flote de la Armada Nacional?

En cuanto a la metodología se implementará la investigación holística de tipo descriptiva, la cual tiene como objetivo central, lograr la descripción o caracterización de un evento de estudio dentro de un contexto particular. Consiste en identificar las características del evento estudiado (Hurtado de Barrera, 2000), la cual permitirá responder la pregunta de investigación y alcanzar los objetivos planteados mediante la aplicación del ciclo holístico de la investigación, el cual comprende cuatro niveles: perceptual, aprehensivo, comprensivo e integrativo; estos niveles a su vez se manifiestan en 10 estadios, que se corresponden con igual número de fases metodológicas: explorar, describir, comparar, analizar, explicar, predecir, proponer, modificar, confirmar y evaluar (Londoño & Tabares, 2012).

Mediante la aplicación del ciclo holístico, se realizarán las seis primeras fases con el fin de alcanzar el objetivo general y los objetivos específicos del presente trabajo, así:

1. Explorar: Inicialmente se realizará una fase exploratoria documental, en la cual se identificarán los protocolos de comunicación empleados.

2. Describir: En esta fase se realizará un análisis del o de los protocolos de comunicación empleados, con base en ello detallar los riesgos y amenazas que se presentan en el protocolo.

3. Comparar: Se procederá a comparar los riesgos y amenazas cibernéticas existentes, con las estrategias de ciberseguridad nacional en Colombia, obtenidas en la fase exploratoria, de esta manera se podrá identificar las estrategias a implementar en las Unidades a flote de la Armada Nacional.

4. Analizar: En esta fase se analizarán la relación entre las estrategias de ciberseguridad y los riesgos y amenazas cibernéticas identificados.

5. Explicar: Posteriormente, se realizará la explicación de las estrategias de protección a implementar en relación con los riesgos y amenazas por ataques cibernéticos en las Unidades a flote de la Armada Nacional

6. Predecir y Proponer: En esta última fase, se determinarán los retos a los cuales se enfrenta las Unidades a flote de la Armada Nacional, de manera que permita establecer estrategias que potencialicen y optimicen la ciberseguridad y la Ciberdefensa.

CAPÍTULO III

Objetivo 1

Este capítulo permite conocer el procedimiento a tener en cuenta para dar respuesta al primer objetivo, el cual se plantea de la siguiente manera ¿Cuáles son los riesgos y amenazas cibernéticas en las unidades a flote de la Armada Nacional? Es así, que, para dar respuesta a la pregunta descrita anteriormente, se generan dos momentos. En un primer momento se realiza la descripción del protocolo de comunicación NMEA 2000, utilizado en las Unidades a flote de la Armada Nacional.

Como segundo momento y después de haber identificado las características del protocolo se procede a identificar los riesgos que afectan el sistema de comunicación que trabajan bajo el protocolo NMEA 2000, con base en ellos se determinan las amenazas.

Descripción

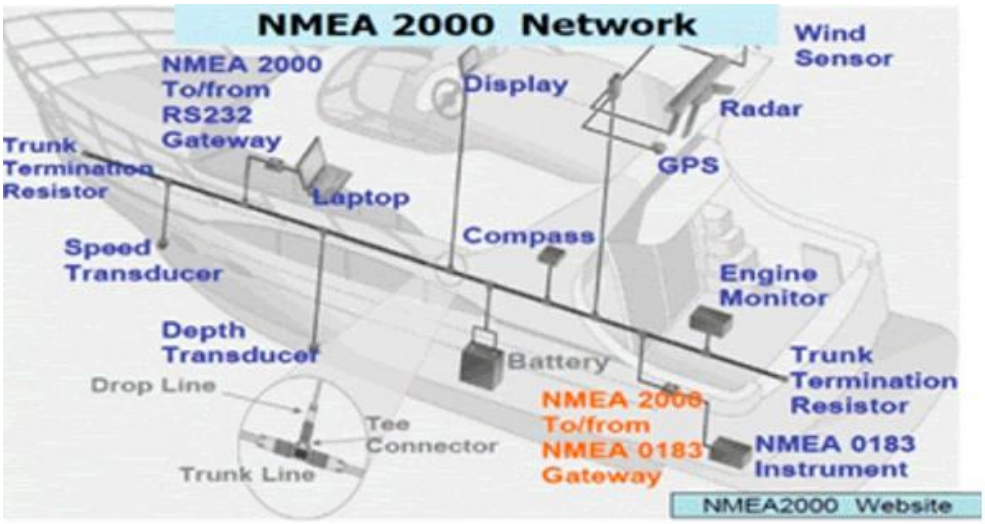
Unidades a Flote

El Centro de Investigación Oceanográfico e Hidrográfico- CIOH. Define las unidades a flote como “todas las naves y artefactos navales de cualquier desplazamiento, diseñadas para el combate o para tareas de apoyo logístico y administrativo, las cuales pueden prestar sus servicios en el mar o en los ríos navegables colombianos”. (CIOH, s.f. p 4). A su vez, enmarca dentro de las unidades a flote los (a) buques de guerra, (b) submarinos oceánicos y tácticos, (c) patrulleros y buques patrulleros, (d) buque escuela (e) buques de apoyo, (f) lanchas de desembarco, (g) los veleros de entrenamiento, (h) botes de instrucción, (i) patrulleras y elementos de combate fluvial, (j) Unidades de apoyo tipo Nodriza Fluvial, (k) aerodeslizadores.

Las Unidades a flote cuentan con dispositivos que controlan las funciones de navegación electrónica, geolocalizacion, identificación de otras embarcaciones, medición de velocidad y profundidad, información de condiciones meteomarinas e información sobre los sistemas de propulsión, los cuales trabajan bajo el protocolo de comunicación NMEA 2000. (Figura 1)

Figura 1

Protocolo de Comunicación NMEA 2000



Fuente. Fonder.org

Protocolo NMEA

El protocolo de comunicación NMEA 2000, definido por la “National Marine Electronics Association”, su finalidad fue sustituir el protocolo NME 0183. Es una norma de comunicación plug-and-play, que se comunica entre diferentes dispositivos electrónicos empleados en embarcaciones y/o barcos que se encargan de fijar protocolos de comunicaciones, como también las especificaciones de los conectores y cableado que se instalan en un circuito.

El NMEA, de acuerdo a Cassidy (1999) se basa en el protocolo de comunicaciones industriales Controller Área Network (CAN), presenta una alta fiabilidad de la señal y está diseñado para el trabajo en red. Este protocolo tributa mayores potencialidades que el NMEA 0183, ya que presenta una velocidad de 250 kilobits por segundo y tiene la posibilidad de conectarse en red con aproximadamente 50 dispositivos electrónicos diferentes

Los mensajes de datos se transmiten como una serie de marcos de datos, cada uno con una sólida verificación de errores y entrega confirmada del marco. Los marcos de datos contienen, además de los bits de control y comprobación de errores, un campo de datos de 8 bytes y un campo de identificación de 29 bits que configura el mensaje. El contenido de datos de una trama de datos es el 50% de los bits transmitidos, este estándar es destinado a admitir mensajes de datos breves que pueden ser periódicos, transmitido según sea necesario, o bajo demanda mediante el uso de comandos de consulta. (Serrano 2019).

A su vez, los datos típicos incluyen parámetros discretos como la posición, latitud y longitud, valores de estado del GPS, dirección comandos a pilotos automáticos, listas de parámetros finitos como puntos de referencia y tamaño moderado bloques de datos como actualizaciones de bases de datos de cartas electrónicas (Cassidy, 1999, p.4)

En cuanto al protocolo de comunicación NMEA 2000, se precisa como potencialidades la facilidad para utilizar y conectar los diversos equipos a la red del buque, mejor velocidad de transmisión de sus datos, a su vez, al tener conectores estandarizados permite instalar productos electrónicos de diversas marcas, como

también admitan que tanto radares como diferentes elementos de navegación acepten datos de otros equipos.

A su vez, permite la interconexión de datos en una serie de equipos electrónicos marinos que están a bordo de embarcaciones. Los cuales, soportan conexiones de manera simultánea de diferentes dispositivos que tanto envían como reciben información.

Dentro de los elementos que cumplen con el estándar NMEA 2000 están los sistemas de GPS, los radares, las cartas de navegación electrónica, los girocompás, los sistemas de identificación automática, las estaciones meteorológicas, la corredera, el ecosonda y los sistemas de monitores y control de la maquinaria principal. Dichos sistemas y dispositivos son conectados a un cable central, llamado columna vertebral, la cual realiza tareas como alimentar a todos los dispositivos conectados, como también permite la transmisión de datos y la conexión de la red.

Para conectarse a esta red se requiere de utilización de puertos USB, puertos RS-232, y los puertos RS-485. Los puertos USB permiten una comunicación bidireccional, de tal manera que genera una integración con los dispositivos allí conectados. En relación a los puertos RS-232, presenta un serial asíncrono, el cual no tiene un orden de envío de datos entre los dispositivos, por lo que se vuelve necesario el cuidar la sincronización del envío para evitar pérdidas de información o fallos en la comunicación.

Otra de sus características principales es ser un protocolo punto a punto, esto es, que solamente permite la comunicación de un dispositivo con respecto a otro empleando una terminal de comunicación determinada. Dentro de las desventajas que se

identifica en este puerto es que no permite la creación de redes (Ramírez, 2013, p.3), este puerto soporta dos dispositivos con distancias aproximadamente de 15 metros.

Entre tanto los puertos RS-485, emplean la topología multipunto, lo cual permite la conexión de varios receptores y transmisores. Soporta la conexión de 256 dispositivos, con distancias aproximadamente de 1200 metros. Trabaja con un modelo half- dúplex, es decir, que solamente puede cumplir una tarea ya sea la de leer o la de escribir.

En relación a la comunicación que se da entre los satélites y receptores, esta es ejecutada mediante el envío de paquetes identificados como el protocolo NMEA 2000, luego de transmitir a la trama del GPS, a través de un software se muestran los diferentes datos. Se identifican tramas o comandos NMEA 2000 soportados por el GPS que son identificados como los "datos fijos del sistema global de posicionamiento" (Rodríguez, I, p.10), a su vez, el GGA tiene como función entregar los datos de localización en 3D. El GSA, "modo de operación de receptor GPS, a los satélites empleados para la navegación de valores y DOP" (Rodríguez, I, p.10), como también proporciona los detalles sobre la corrección, y determina el estado del satélite.

El GSV Identifica el "número de satélites en vista, números de PRN, elevación, azimut, y los valores SNR". (Rodríguez, I, p.10). Permite la muestra y rastrea datos, en cuanto al GLL, se relaciona con la latitud y longitud geográfica (Pascual, 2017). A su vez el RMC, da a conocer los mínimos datos específicos recomendados, y el VTG, que da a conocer la velocidad de la tierra y sobre la tierra. (Rodríguez, s.f. p.10).

Dentro de los tipos de mensajes que proporciona los NMEA 2000 (Cassidy, 1999), se idéntica los grupos de parámetros de administración de red, reconocimiento, básico, acuse de recibo, reclamo de dirección, información de configuración, función de

grupo de comando, información del producto, propietario global, dirigido Función de grupo de lista de PGN recibidos, solicitud básica, solicitar función de grupo, protocolo de transporte, gestión de conexiones, protocolo de transporte, transferencia de datos, función de grupo de lista de PGN transmitidos, grupos de parámetros de aplicación, transporte NMEA 0183, datos de Loran-C TD, datos de rango de Loran-C, datos de la señal Loran-C, datos de la estación de mareas, datos de la estación de salinidad, datos de la estación actual, datos de la estación meteorológica, datos de la estación de boyas amarradas, estado de control GNSS, posición de salida alta GNSS, datos de posición GNSS, configuración de datos de usuario, DOP GNSS, Sats GNSS a la vista, datos de almanaque GPS, residuos de la gama GNSS, estadísticas de ruido de pseudodistancia GNSS, interfaz del receptor de corrección diferencial GNSS, estado de la señal del receptor de corrección diferencial GNSS, hora del sistema, datos de almanaque de GLONASS, COG y SOG de alta velocidad (VTG), ajuste y deriva de alta velocidad (VDR), error de pista cruzada (XTE / HSC), actitud, datos de dirección, datos de navegación (RMB / RMC / BWR / BWC), rumbo y distancia entre dos marcas (BOD, BWW, WNC), registro de distancia (VLW), Hora y fecha (ZDA), tiempo hasta / desde la marca (ZFO / ZTG), estado del buque, estado de la transmisión FNR, interruptores de estado, interruptores de control de carga, parámetros ambientales, parámetros dinámicos del motor, parámetros de viaje, embarcaciones pequeñas, parámetros estáticos del motor, estado de la batería, nivel de combustible y transporte de mensajes del sistema de identificación automática –AIS- (p.17).

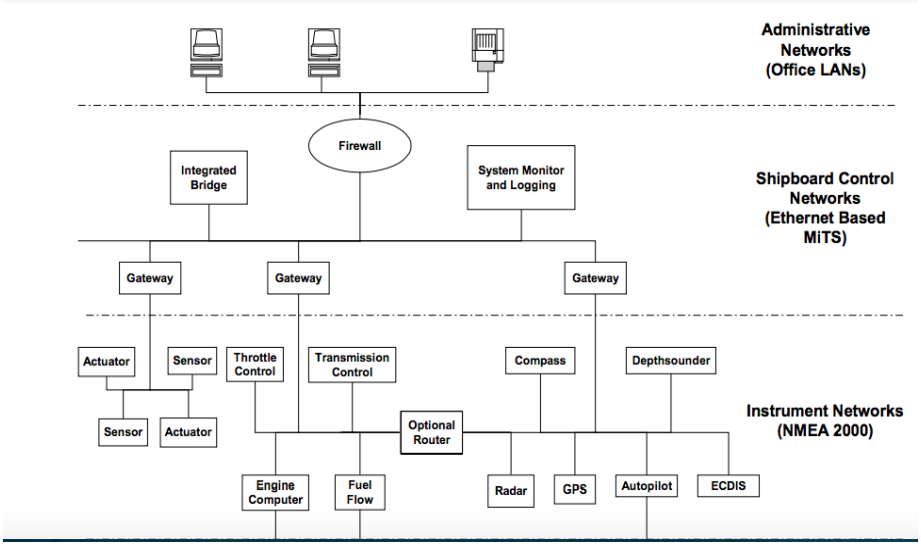
La arquitectura de red está dividida en cuatro subredes, cada una de ellas se identifica por su color. Una red interna color naranja, denominada Business, que va conectada por cables a los computadores de administrativos como a los servidores, la

red de color rosa, establece un vincula con la máquina ECDIS, y con los demás equipos y sensores que tiene la nave, se identifica que con ECDIS intercambia información las redes LAN normal y WAN - NMEA 2000. A su vez, permite acceder a Internet vía satélite directamente a través del puerto de tripulación de Inmarsat.

En cuanto a la conexión de la línea azul, se identifica acceso a la internet a través del satélite (Inmarsat) o a por los puntos de acceso GSM/4G terrestres regulares siempre que el buque esté dentro del alcance. Los enlaces verdes se identifican la red Wi-Fi, la cual se emplea para uso exclusivo de dispositivos privados de la tripulación. (Mendikarov et al, 2020)

Figura 2

Circuito de Interfaz NMEA 2000



Fuente. Cassidy, 1999

Con base en lo anterior se identifica la comunicación entre dispositivos electrónicos y sensores como un anemómetro, girocompás, receptor GPS, sonar, piloto automático a bordo del barco, el uso del protocolo de mensajes serie básico NMEA0183 o NMEA2000. Las comunicaciones con este protocolo no requieren autenticación,

validación ni cifrado, todo va como texto sin formato. La prueba de red indica que, por lo general, las redes WAN/LAN del barco suelen estar unidas en varios puntos.

Basado en la figura 2, la puerta de enlace principal tiene la forma de máquina ECDIS. En este caso, un simple atacante en el medio comprometiendo los mensajes que fluyen a través de la red es suficiente para perturbar el funcionamiento normal de los dispositivos sin notificar a nadie ni estar al tanto de lo que sucede.

Entre los dispositivos que se conectan y son compatibles con el circuito de interfaz NMEA 2000 están los receptores GPS, pilotos automáticos, instrumentos de viento, ecosondas, radares, sensores, routers, instrumentos de navegación, cartas de navegación ECDIS, a su vez los sensores digitales del motor, contadores de las horas, tacómetros, medidor de niveles y tanque del combustible, y agua potable, velocímetro, encuestadores, temperatura del sensor, anemómetro, receptor AIS. Los cuales muestran datos del sensor digital del motor, contador de horas, tacómetro, los niveles y el tanque de combustible y agua potable, en los indicadores numéricos o dispositivos con pantalla colocada en cualquier lugar en el barco.

Para la identificación del estado actual de los satélites, se emplea un sistema global de navegación por satélite identificado como GPGSV y GPGSA. La GPGSA descrito como DOP de GNSS y satélites activos, el cual permite que se suministren números PRN de los satélites utilizados en la solución actual y la dilución de Posición (DOP). Los GPGSV exponen los datos en relación a los satélites, permitiendo determinar la función de su máscara de visualización satelital y su configuración de almanaque.

Dentro del tipo de datos con mayor importancia esta GPGGA, este proporciona datos de corrección de posición actuales, a su vez incluye hora actual, la posición, la

calidad de las fijas y otra información sobre la navegación. Si se da una latitud numérica o longitud, los dos dígitos inmediatamente a la izquierda de la coma decimal son minutos enteros, a la derecha son decimales de minutos y los dígitos los restantes a la izquierda de los minutos completos son grados enteros. Ejemplo, si un receptor hace una frase como '$GPGGA, 123519, 4807·038, N, 01131·000, E, 1, 08, 0, 9, 545·4, M,49·9, M, *47', significa que la latitud y longitud de la posición GPS fijada a las 12:51:19 (UTC) es 48° 07·038' Norte y 11° 31·000' este (Park, Lee, Jeongkeun, Younsil; Yun, Ho; Kee, Changdon, 2013, p.10).

En relación a lo anterior la NMEA 2000 al permitir la comunicación por GPS, da apertura a la integración de los datos de navegación de ECDIS (Electronics Chart display an information systems), como también al AIS sistema de identificación automática, emplea el GPS, VHF, y la señal DSP, que tiene como finalidad la comunicación entre otras embarcaciones.

Dispositivos y sistemas estándar NMEA 2000

Los sistemas globales de navegación por satélite (GNSS)

Los GNSS tienen como finalidad procesar las señales del espacio (SSI), transmitidas por los satélites. Estos proporcionan posiciones, velocidad y longitud. Dentro de su clasificación se identifican receptores para tipografía, receptores de mano, receptores de estación de referencia, receptores o GPS. (Garrido, 2014).

Sistema de posicionamiento global. GPS

Tecnología que para su funcionamiento depende de señales en su navegación satelital. El talón de Aquiles de los GPS, como lo afirma Last, “son las señales extremadamente débiles que llegan a un receptor” (2010, p 5). Dicha señal débil, puede generar fácilmente bloqueos, a su vez, también puede ser afectada la señal con bloqueos

a través de señales con frecuencia similares o con mayor potencia a las emitidas por el GPS.

También se puede presentar la no recepción de las señales fundamentales para poder determinar tanto la hora como la posición de la embarcación. Desde el 2016 se han identificado más de 9883 casos de spoofing en barcos comerciales. Convirtiéndose en un gran riesgo para la seguridad marítima (2019).

En el receptor GPS se pueden presentar cinco fuentes de error los cuales son (a) errores en los satélites, que pueden ser producidos por errores en el reloj, errores de posicionamiento o por errores orbitales generados en el satélite. (b) errores atmosféricos, provocados debido a la propagación de señales de radio a través de la troposfera y la ionosfera, lo que conlleva a que haya un retardo de la señal. (c) Errores de multitrayectoria, esta se produce cuando la señal que llega a la antena GPS solo se refleja, y no llega directa, esto debido a diferentes obstrucciones ya sea por los edificios o elementos naturales, dentro de las sugerencias dadas es que la posición de los GPS debe estar a una suficiente altura para evitar estos sucesos.

A su vez se identifican los d) errores en el receptor, generado por ruidos electrónicos que suelen ser producidos por fuentes internas o externas al receptor o en ocasiones por el reloj (e) por último la disponibilidad selectiva, considerada como una de las principales limitaciones al estar gobernado por los Estados Unidos. La disponibilidad selectiva es un error provocado de manera intencional por el Departamento de Defensa de los Estados Unidos. Esto con el fin de que usuarios que no son autorizados tengan el posicionamiento del dispositivo y puedan emplear esta información para generar un daño. (Marulanda, 2009)

Como también los receptores del sistema de posicionamiento global (GPS) son vulnerables a una serie de ataques diferentes, como el bloqueo, el bloqueo y la falsificación. El objetivo de estos ataques es evitar un bloqueo de posición, o alimentar la información falsa del receptor para que calcule una hora o ubicación errónea. (Mednikarov, et al 2020.). Otra gran problemática que se puede presentar es la generación de falsas señales enviadas al GPS, que hace que crea que está en un lugar y tiempo diferente al real.

La suplantación es un ataque es denominado spoofing –hacerse pasar por otro-, es una técnica que busca suplantar la identidad, a través de un transmisor de radio que es ubicado cerca al objetivo, generando la interferencia de las señales de cualquier GPS, dicha interferencia conlleva a la crear ubicaciones GPS falsas.

Cuando una embarcación es víctima del spoofing, se cree que el barco se encuentra en otro lugar, lo que conlleva a grandes riesgos como colisiones con otras embarcaciones u otro tipo de incidentes. A causa de la vulnerabilidad del sistema GPS, se genera que un dispositivo muestre su ubicación en un lado diferente al que realmente se encuentra.

Humphreys (2016), afirma que la suplantación de identidad del sistema global de navegación por satélite (GNSS-GPS), conlleva a una emisión de señales falsas esto con el fín de que los cápitanes de las diferentes embarcaciones las malinterprete como unas señales auténticas, lo que puede derivar a una corrección de la posición falsa, como también a desface en el reloj falso, dichas correcciones pueden conllevar a generar comportamientos peligrosos en la plataforma del buque, generando una secuencia coordinada de posición o sincronización falsas.

Un ejemplo de ello lo enmarca (Álvarez, 2017) el cual se identifica en la relación desde el posicionamiento global, organizado por la suplantación del sistema GPS, el cual es empleado para mandar drones flotantes en inmersiones no planificadas, lo que genera un desvio de las rutas a las naves. A su vez, las defensas falsas buscan detectar un ataque para advertir al receptor que su corrección de navegación y la compensación del reloj son poco fiable.

Agregando a lo anterior se puede identificar un caso presentado el 22 de julio del 2017, cuando un capitán reporta que el buque que estaba en el puerto ruso de Novorossiysk, su GPS mostraba una ubicación completamente diferente, es decir lo ubica en un lugar equivocado, a más de 32 kilómetros tierra adentro, más específicamente en el aeropuerto de Gelendjik. Al advertir el capitán de lo que estaba sucediendo, se contacta a través del AIS con otros barcos que están a su alrededor, para su sorpresa identifican que aproximadamente veinte de las embarcaciones se encontraban localizadas en el mismo aeropuerto de Gelendjik. De acuerdo a las investigaciones realizadas se determinó que este ha sido el primer ataque de falsificación de las señales GPS, producido GPS spoofing. (Álvarez, 2017).

> El mayor problema al que se enfrentan las fuerzas marítimas respecto al GPS es el *jamming*, el cual crea una interferencia en la señal confundiendo al receptor y bloqueándolo. Sin embargo, el *jamming* hace que el receptor muera, mientras que el *spoofing* hace que el receptor mienta, y para éste último no hay alarmas o formas de saber qué está ocurriendo, de ahí la preocupación acerca de esta nueva arma electrónica. (Álvarez, 2017. Cap. 3).

Esto indica como lo afirma el investigador Todd Humphreys, citado por Álvarez (2017), que aún los buques con los más avanzados sistemas de GPS, se encuentran en

grandes riesgos de ser sacados de su curso, lo que conlleva a que se presenten caos a nivel de seguridad marítima.

Sistema de información y visualización de la carta electrónica **ECDIS**

Tiene como finalidad el recoger todos los elementos relevantes de la cartografía indispensables para la seguridad de la navegación y contiene todos los datos fundamentales para la navegación. Las cartas náuticas electrónicas. ECDIS permite que dos redes como LAN y WAN, generen intercambio de información, lo que hace que sea mucho más vulnerable, generando que la ciberdelincuencia pueda intentar ataques y que accedan a otros dispositivos.

Una gran amenaza es la de acceder, leer, descargar, reemplazar o eliminar cualquier archivo almacenado en la máquina que aloja dicha información, así como modificar o eliminar o reemplazar el contenido de los archivos y gráficos en computadoras a bordo o en tierra. Una vez que se obtiene acceso, los atacantes podrían interactuar con la estación de trabajo o los servidores de las redes marítimas y terrestres. (Mednikarov, et al 2020. p.26). Acción que puede ser realizada a través de la inserción de un dispositivo USB, o por medio de descargas en internet.

Sistema de Identificación Automática (AIS)

Es un transceptor de radio VHF, que se instala en buques, aeronaves, entre otros, tiene como finalidad permitir la comunicación e intercambio automáticamente de información, a través de sus sensores, permitiendo el monitoreo de otros buques como también de estaciones costeras.

A su vez, también facilita la identificación de los mismos. La utilización tanto del radar como el AIS, admite identificar los buques a una gran distancia, empleando para ello los mensajes de voz con frecuencia VHF (Léniz, 2019). Este sistema no solo hace

intercambios de su ubicación básica, sino a la vez una gran cantidad de información como el rumbo que lleva, y la velocidad, información que ayuda a prevenir colisiones en el mar, dicha información de la embarcación se hace visible en el trazador de embarcaciones cercanas.

El AIS es uno de los sistemas de buques más vulnerables. En relación a las investigaciones realizadas en Global Fishing Watch y SkyTruth, citado por Bergman, (2021), han identificado diferentes huellas de barcos que aparecen en ciertos lugares como la Antártida, y también dando vueltas en el desierto de Utah, y en otros lugares que son imposibles de transitar, lo cual ha generado que los analistas se cuestionen si estas posiciones falsas son el resultado de transmisores defectuosos del Sistema de identificación automática (AIS), por el mal uso deliberado de esos transmisores o debido a la interferencia intencional de terceros.

Los ciberdelincuentes a través de un radio con frecuencia VHF puede explotar las debilidades del AIS e interceptar y suplantar datos que se están transmitiendo, como también enviar información falsa lo que puede conllevar a situaciones como modificación de datos, identidad, desvíos de rutas, cambios de velocidad creación de buques «fantasmas» haciendo que los receptores del AIS lo identifiquen como una embarcación genuina, falsas colisiones, entre otros (Mednikarov, et al 2020).

A su vez, pueden hacer envío de información meteorológica falsa, generando que las naves realicen modificaciones ampliando la frecuencia en relación a la trasmisión de datos. Como también la generación de pistas AIS simuladas, lo que representa una gran amenaza significativa para la integridad de los datos, como también recalca la necesidad de estar vigilante para realizar la interpretación de los datos AIS (Bergman, (2021).

Un vivo ejemplo es la identificación de un caso, presentado en la que “Nueve buques de la armada sueca aparecieron como si estuvieran realizando maniobras el 4 y 5 de febrero de 2021, mientras que los oficiales de la marina confirmaron que estas posiciones AIS eran falsas” (Dagens Nyheter, 2021, párr. 1).

Esta noticia publicada por el periódico ruso Dagens Nyheter (2021), titulado Buques navales suecos falsos en posiciones cerca de Rusia, manifiesta como lo afirma Bergman (2021), el análisis de los datos de seguimiento de las transmisiones del sistema de identificación automática revela que se han simulado las ubicaciones para varios barcos, incluidos los militares. Dicha información falsa sobre cómo se mueven los barcos de la Armada sueca en los mares se difunde a través de los servicios de envió en línea, en el cual se informa que “Suecia está actuando de manera ofensiva y más cercana a Rusia, pero en realidad los barcos están en el muelle o en otro lugar, según las fuerzas armadas”. (Dagens Nyheter, 2021).

Esta información como lo afirma Bergman (2021), puede llegar a arriesgar la seguridad de los tripulantes de la embarcación, a su vez reducir la confidencialidad del sistema AIS, como también generar colisiones y desatar conflictos internacionales

Otro de los casos que se identifican son, el del buque Estadounidense USNS, Bruce C.Heezen, que transita hacia el mar Báltico, en relación a los datos del AIS, se identifica que la embarcación recorre desde el 17 al 23 de septiembre el mar del Norte, y el mar Báltico, al realizar el análisis de las posiciones transmitidas en las fechas, se identifica que el patrón AIS es falso, es decir que no se está mostrando la ubicación real del buque. Bergan (2020).

El buque USS Roosevelt, según el patrón de datos falsos dados por el AIS el barco ingresa cuatro millas náuticas dentro del mar territorial ruso, el 26 de noviembre de 2020. Global Fishing watch, (2021). Otros casos de pistas falsas se reconocen:

> Las pistas AIS falsas de seis buques de guerra del Reino Unido, los Países Bajos y Bélgica se superpusieron en una imagen de satélite S2 del mismo día, lo que revela que ninguno de los buques estaba realmente presente en el momento de la adquisición de la imagen S2. (Global Fishing Watch, 2021).

Con base a los casos descritos anteriormente se identifica la amenaza que se puede presentar con el posicionamiento falso, que se identifican en el AIS. “Las pistas AIS falsas como estas podrían usarse para crear una narrativa falsa o incluso una justificación para un ataque a un barco u otra acción militar” (Bergan, 2020, párr,12).

Tomando como referente lo anteriormente descrito, se considera pertinente involucrar el internet de las cosas IoT, término empleado para describir los dispositivos electrónicos que se conectan a una red, para el cumplimiento de tareas específicas. Uribe (2019), las define como “la red de dispositivos capaces de interactuar con otros dispositivos y/o seres vivos a través de sensores y a través de Internet o de una red privada local o global no conectada a internet”. (p. 19).

La integración de una variedad de dispositivos inseguros IoT, y en ocasiones las mismas infraestructuras de la internet conlleva a que se generen ciberataques, en muchas de las ocasiones los atacantes cibernéticos emplean los dispositivos con autenticaciones débiles o software vulnerables. Con base a lo descrito por el FBI (2018)

> Los ciberactores activan y comprometen los dispositivos vulnerables del Internet de las Cosas, para utilizarlos como proxis o intermediarios de las solicitudes de Internet para dirigir el tráfico malicioso, los ciberataques y la explotación de la

> red informática. Los dispositivos, a veces denominados dispositivos "inteligentes", son dispositivos que se comunican con Internet para enviar o recibir datos. Algunos ejemplos de dispositivos son: routers, enlaces de radio inalámbricos, relojes de tiempo, dispositivos de transmisión de audio/vídeo, Raspberry Pis, cámaras IP, DVR, equipos de antena de satélite, abridores de puertas y dispositivos de almacenamiento conectados a la red. (FBI, agosto 2, 2018, p 1)

Dentro de las acciones que identifica el FBI empleados por los ciberatacadores es el uso de dispositivos comprometidos como proxis para él envió de correos electrónicos de spam, mantener el anonimato, ofuscar el tráfico de red, enmascarar la navegación por Internet; generar actividades de fraude por clic, comprar, vender y comerciar con imágenes y bienes ilegales; entre otros (FBI, agosto 2, 2018, p 1).

Análisis

Con base a lo descrito anteriormente y en relación a los diferentes hallazgos encontrados se identifica como factores de vulnerabilidad el GPS, sistema de visualización de cartas electrónicas ECDIS, y el Sistema de Identificación automática AIS.

En cuanto al GPS, los ataques que se identifican son de dos tipos (a) Interferencia, el cual tiene como propósito el bloqueo del servicio de GPS, lo que conlleva a fallas en los sistemas que requieren de información de referencia temporal y posicionamiento GPS. (b) Suplantación de identidad. El cual altera los datos que se recepcionan a través del GPS entre ellos errores tanto en la posición como en el tiempo, generando grandes peligros como colisiones, pérdida de vidas humanas y daño en el ecosistema (Popescu, 2018).

Con base a la matriz MITRE, se identifican, las técnicas y tácticas que se emplean en coherencia con lo descrito anteriormente. Dentro de estas se identifican las siguientes.

Tabla 8

Riesgos y Amenazas GPS

TÉCNICA- TÁCTICA	RIESGO	AMENAZAS
Técnica. Ejecución *Táctica. Interpretación de comando y secuencia de comando.*	Sistemas Informáticos Plataformas: Linux, Red, Windows, macOS	En la cual los atacantes pueden ejecutar comandos arbitrarios, ejecutar comando de forma remota, el malware identificado es el malware Chopstick (palillo).
Técnica. Ejecución *Táctica. Mando y control.*		Canal cifrado: criptografía simétrica. En el cual los atacantes utilizan los algoritmos cifrados, que tienen como fin ocultar las ordenes y controlar el tráfico. Malware utilizado RAT.
Táctica Basadas en la red	Redes	En la que atacantes pueden interceptar o manipular el tráfico de la red. Dentro de las técnicas se identifican. (a) el cambio de protocolo a inseguros; (b) bloqueo o denegación de servicio; (c) escaneo activo, hace referencia a que los atacantes recopilan información, para luego ser empleada en orientación falsa. (Mitre, 2020). (d) señalización de tráfico, se refiere a ocultar puertos abiertos, o cualquier funcionalidad de carácter malicioso, tiene como finalidad el control. (e) evasión de defensa, en la cual el atacante va procurar no ser detectado, dentro de estas se identifica el deshabilitar software de seguridad, encriptar datos. (f) Acceso a sistemas, denegación de control para evitar interactuar con los controles del proceso. (f) Inhibición de respuesta, activación del modo de actualización de firmware evitando reacción a una emergencia o un mal. (g) Acceso a sistemas, denegación de control para evitar interactuar con los controles del proceso. (h)Pérdida de visión. Elimina la imagen de pantalla, y detención del servicio.

Táctica: Descubrimiento	**sistema y la red.**	Es el que el atacante utiliza para tener conocimientos sobre el sistema y la red. Técnicas. (a) Escaneo del servicio de red, en el cual se realizan escaneos al host remoto, para ello utilizan los análisis de puertos y vulnerabilidad de los mismos. (b) Sniffing de red. Consiste en hacer rastrear el tráfico de la red, lo que conlleva a recolectar información y material compartido, así como ubicaciones. (c). Descubrimiento de la ubicación del sistema. El atacante recopila la data con la finalidad de calcular la ubicación geográfica. (d) virtualización- evasión de sandbox. (e) Evasión basado en el tiempo. Se busca tanto detectar como evitar el análisis y la visualización, afectando tiempo de actividad, reloj del sistema y uso de temporizadores.
Táctica Ex filtración automatizada. Duplicación de tráfico.	Redes	Se emplea para realizar análisis a las redes, lo cual conlleva a que se pueda configurarse para duplicar el tráfico. El atacante puede generar modificaciones maliciosas redireccionando el tráfico, como también detección de redes, capturas de entrada, entre otras. (Mitre, 2020).
Técnica: (a) supresión de alarmas *Táctica. Función de Inhibición de respuesta*	Alarmas de señalización, alarma de mensaje del protocolo	Los atacantes actúan sobre la protección de alarmas, en las cuales evitan que se notifique sobre problemáticas críticas que se están presentando. Uno de los métodos empleados es el de supresión, este depende específicamente del tipo de alarma, entre las que se encuentran la alarma de señalización, alarma de mensaje del protocolo. (Mitre, 2020).
Técnica. Hombre en el medio *Táctica Colección*	Tráfico de red GPS Cartas de navegación	El atacante a través del ataque main in the middle (MITM), busca modificar el tráfico de la red en tiempo real. Dentro de las acciones que puede ejecutar en el flujo de la comunicación son (a). bloquear, (b)registrar, y (c) modificar. Los ataques que se pueden realizar a través de los mensajes, son: informe de bloqueo, suplantación de identidad, modificación de patrón y la no autorización.

Técnica. Mensaje de denuncia de falsificación *Táctica de Evasión, control de procesos de deterioro*	Sistemas-mensajería	Se realiza a través de la falsificación de los informes del sistema por medio de los mensajes
Técnica. Modificar el proceso de autenticación. *Táctica. Acceso a credenciales-evasión de defensa persistencia*		Los atacantes generan modificaciones en los mecanismos y en los procesos relacionados con la autenticación para poder acceder a las credenciales de los usuarios, como también permitir el acceso injustificado a las cuentas.

Sistema de Identificación Automática –AIS-

Con base a los diferentes casos que se han presentado a nivel Internacional, los cuales fueron expuestos en la descripción se identifica que dentro de los ataques se reconocieron (a**)** interceptar y suplantar datos que se están transmitiendo, (b) envió información falsa, así como modificación de datos, identidad, desvíos de rutas, cambios de velocidad creación de buques «fantasmas».

En relación con los ataques identificados anteriormente y en correlación con las técnicas y tácticas establecidas en MITRE, se identifican (tabla)

Tabla 9

Riesgos y Amenazas de AIS

Técnica/ Táctica	RIESGOS	AMENAZAS
Técnica **Autenticación del controlador de dominio Autentificación de dispositivos de red.** *Táctica Basadas en la red*	Sistema de Identificación Automática –AIS-	En la que atacantes pueden interceptar o manipular el tráfico de la red. Dentro de las técnicas se identifican. (a) cambiar los de protocolo seguros a inseguros; (b) el bloqueo y/o denegación del servicio; (c) el escaneo activo, que hace referencia a que los atacantes recopilan información, para luego ser empleada con una orientación falsa. (Mitre, 2020). (d) la señalización de

		tráfico, se refiere a ocultar puertos abiertos, o cualquier funcionalidad de carácter malicioso, tiene como finalidad el control. (e) evasión de defensa, en la cual el atacante va procurar no ser detectado, dentro de estas se identifica el deshabilitar software de seguridad, encriptar datos. (f) Acceso a sistemas, denegación de control para evitar interactuar con los controles del proceso. (f) Inhibición de respuesta, activación del modo de actualización de firmware evitando reacción a una emergencia o un mal. (g) Acceso a sistemas, denegación de control para evitar interactuar con los controles del proceso. (h)Pérdida de visión. Elimina la imagen de pantalla, y detención del servicio.
Técnica Servicio Remoto *Táctica. Acceso inicial, movimiento lateral*	Dispositivos de control.	Se ejecuta cuando hay un aprovechamiento de los servicios remotos, los cuales son empleados para mover los archivos y generar segmentaciones en la red. A través de la táctica se pueden ejecutar los ataques a los dispositivos de control.
Técnica Interfaz gráfica del usuario *Táctica Ejecución*		A través de esta los atacantes intentan hacer un ingreso al interfaz gráfico del dispositivo.
Técnica Manipulación de Imagen *Táctica Función de Inhibición de respuesta*	Sistema	La cual puede ser realizada a través de diversos medios que buscan impedir el buen funcionamiento del sistema.
Técnica. Proxy de conexión. *Táctica Comando y control.*	Conexión Proxy	Los atacantes pueden hacer uso de la relación existente que hay entre redes, por medio de esta pueden administrar la comunicación que de esta subyacen.
Técnicas. Señalización de tráfico. *Tácticas de Defensa, Evasión, Persistencia, Mando y Control.*	Dispositivos de red.	Empleada por los atacantes para ocultar la apertura de puertos, u otras funciones maliciosas ejecutadas. La cual se puede maquillar con él envió de paquetes con algunas especificidades como intentos de conexión en puertos que se encuentran cerrados. Los atacantes activan funciones maliciosas en puertos abiertos. En relación a los dispositivos de red.
Técnicas. Abuso de mecanismos de control. *Táctica. Evasión de defensa.*		El atacante busca la forma de no ser detectados, empleando acciones como desinstalación de software de seguridad, encriptación de datos. Ocultar y enmascarar malware. En el cual el atacante emplea diversos métodos para lograr la autorización de los

	usuarios. (a) Omisión del control. Identificación de los privilegios dados por el sistema. (b) Almacenamiento en cache (c) Suplantación de identidad y robo de tokens. El atacante duplica y se hace pasar por el token de otro usuario, esto con el fin de tomar los privilegios. (d) Manipulación de tokens. Se opera bajo el contexto de seguridad del sistema. (e) Hacer y suplantar token, Al realizar una suplantación el atacante aumenta los privilegios, eludiendo controles. (f) Crear imagen en el host. Los atacantes crean imágenes de contenedor en el host, lo que les permite esquivar las defensas.

Fuente. Diseño propio

Sistema de Información Geográfica (ECDIS)

El sistema ECDIS, al generar intercambios de información entre las redes LAN y WAN, lo hace más vulnerable, lo que conlleva a que ciberdelincuencia intente ataques a diferentes dispositivos. Amenazas como acceder a programas o archivos, hacer lectura, descargas, modificar, reemplazar o eliminar archivo almacenado.

Tabla 10

Riesgo y amenazas ECDIS

Técnica/ Táctica	RIESGO	AMENAZA
Técnica. Empleo de datos por medios extraíbles. *Tácticas. Colección*	**Redes** **Dispositivos portátiles**	El objetivo es la recolección de información de interés Búsqueda de información requerida a través de los medios extraíbles. Ejemplo de ello está el empleo de procedimiento aria-body, el que recopila a través de la USB diversos datos. (b) recopilar diversos archivos con datos requeridos (c) capturas de archivos audio, (d) colecciones automatizadas, (e) empleo de datos de los portapapeles, (f) utilización guardada en la nube sin la seguridad requerida, (g) recopilación de datos privados. (Mitre, 2020)

Técnicas. Empleo de los servicios remotos *Táctica. Acceso inicial.*		El atacante emplea diversas técnicas para ingresar a la red. Técnicas. (a) Empleo de los servicios remotos para ingreso a la red, (b) Insertar dispositivos o hardware de red para ingreso. (c) A través de diferentes mensajes se busca acceso al sistema y suplantar la identidad. (d) envió de accesorio sperphishing para ingreso al sistema. (e). Replica de información por medio de dispositivos extraíbles.
Técnica. Cambio de Protocolo a inseguros *Táctica Basadas en la red*	**RED**	En la que atacantes pueden interceptar o manipular el tráfico de la red. Dentro de las técnicas se identifican. (a) El cambio de protocolo a inseguros; (b) bloqueo o denegación de servicio; (c) escaneo activo, hace referencia a que los atacantes recopilan información, para luego ser empleada en orientación falsa. (Mitre, 2020).
Técnica modificación de políticas de seguridad. *Tácticas de Evasión de defensa, escalado de privilegios*	**Redes**	En su técnica, hace referencia a la modificación de políticas de seguridad. Acceso inicial escaneo de bloqueo IP. Identificación del dominio, captura de paquetes, registros, uso de la red, proxy web, detección de instrucciones a través de la red del sistema. Explotar las funciones integradas. (Monitoreo de archivos, perdida de datos. Monitoreo del tráfico de red sospechoso, conficker, es decir realizar una copia de manera automática con dispositivos extraíbles (USB). (MITRE, 2021).
Técnica. Escaneo activo *Táctica. Reconocimiento*	Tráfico de red	Consiste en la ejecución de exploraciones en reconocimiento activo con la finalidad de recopilar información que se puede utilizar durante la orientación. Pueden acceder a servicios remotos externos o públicos.

Técnica. Escaneo de Redes vulnerabilidad. *Táctica. Reconocimiento*	Los escaneos de vulnerabilidades generalmente verifican si la configuración de un host / aplicación de destino (por ejemplo, software y versión) se alinea potencialmente con el objetivo de un exploit específico que el adversario puede intentar usar. (Mitre, 2020)
Técnica. Phishing para obtener información. *Táctica. Reconocimiento.*	Los adversarios pueden enviar mensajes de phishing para obtener información confidencial que se puede utilizar durante la segmentación. El phishing para obtener información es un intento de engañar a los objetivos para que divulguen información, con frecuencia credenciales u otra información procesable.

Fuente. Diseño propio

A su vez, y con base a lo descrito por Álvarez (2017), dentro de las grandes ciberamenazas que se identifican están los ciberataques generados por Jamming, y Spoofing, y Software malicioso Industroyer.

El Jamming

Bloqueo o denegación de servicio. De acuerdo a la National Institute of Standards and Technology, la interferencia de GPS, puede imposibilitar que las aplicaciones que derivan de los diferentes servicios de ubicación, en este caso la aplicación de mapas para la navegación, no funcionen de manera correcta (sf). Los jammer se encargan de transmitir con la misma frecuencia y a su vez con una mayor potencia, lo que conlleva a que se anule la señal del receptor de la nave. Wonn, Youn y Ali (2006) . Es así, y como lo afirma (Camperos y Herrera, 2018), “el receptor no puede escuchar lo que dice el transmisor, porque el jammer está gritando sobre la

conversación. Tanto para el transmisor como para el receptor parece que la conexión se ha perdido". (p.53).

Spoofing

Suplanta la identidad, falsifica o modifica los datos. Permite que un atacante confunda o controle la ubicación en la que el dispositivo calcula su posición. Los hackers usan spoofing para realizar ciberataques. El Spoofer realiza una réplica de los datos y propaga códigos y bits de datos tomados de la seña del GPS, luego hace envió de las señales falsas, falsificando las señales que se están trasmitiendo. Siendo su número de señales falsificada igual al número de señales verdadera, es así que cada señal falsificada presenta el mismo código de expansión. Para que los ataques de suplantación no sean detectados, el Spoofer, debe transmitir características de manera correcta, para realizar esto emplean un meaconing, es decir que se registra la verdadera señal, las cuales son reproducidas a través de un transmisor, lo que genera que se afecte la verdadera señal, el meaconer, tiene gran potencialidad para la falsificación de señales encriptadas como las señales militares.

Software malicioso Industroyer,

Malware, con capacidad de control tanto de los conmutadores como de interruptores. Esta infección maliciosa aprovecha los protocolos de comunicación, que se emplean en las infraestructuras críticas de sectores como sistemas de control de transporte y otros sistemas de infraestructuras críticas. La capacidad de daño que presenta este malware, va desde apagones eléctricos, el cual va a generar daños en el sistema eléctrico, como también daños a las comunicaciones. Es así que la probabilidad

de reajuste de este malware hacia infraestructuras de otras índoles es muy alta. (Mitre, 2020).

A su vez se identifican ataques que son dirigidos a las redes de información, estructuras y protocolos, como la falsificación del protocolo de resolución de direcciones ARP, ataques DOS y DdoS, suplantación de identidad del protocolo de internet, escaneo de puertos. Dentro de otros ataques esos pueden identificar los ataques a la privacidad, entre ellos se destacan dos, el ataque de reconocimiento el cual hace referencia al acceso de redes vulnerables con el fin de generar ataques a una gran escala; y el ataque de escucha, consiste en estar al tanto de las comunicaciones que se establecen, con la finalidad de conocer diferentes datos.

Como también los ataque al control. Dichos ataques están conformadas por once tipos de ataques, siendo estos; ataque MitM, que busca afectar la red a través de los nodos; ataque de la interferencia en radio, la cual se produce a través de los teléfonos inteligentes, como también en la redes que presentan sensores; ataque de inyección, acceder a redes e inyectar datos o software maliciosos en la red; ataque de repetición, intercepción de datos y retransmitirlo; ataque bizantino, se produce cuando al control de los nodos de la red, se realiza de manera interna; ataque de inundación, se produce cuando el atacante inunda el enrutamiento de datos; ataque del agujero del gusano, se identifica cuando dos modos maliciosos divulgan un trayecto diferente y más corto; ataque del gusano de red, ataque sybil, se produce con la suplantación de un nodo malicioso que se disfraza y reclama identidades falsas, se hace presente causando daños en dispositivos de ubicación como el GPS y mapas de navegación; ataque del sumidero, genera enrutamientos falsos (MITRA, 2021).

Ataques a la disponibilidad; en los que se identifican el ataque de interferencia, en la cual los atacantes realicen interferencias en las comunicaciones con la finalidad de deshabilitar la red, lo que conlleva a que los dispositivos no puedan tener acceso. y el ataque de compromiso de nodos, lo que puede generar complicaciones como alto nivel de daño en las redes, el cual captura nodos de comunicación para después emplearlos a su favor, el empleo de paquetes dañados, esto con la finalidad de habilitar autenticaciones de los dispositivos de red, a su vez la apertura de puertos de servicio que se encuentran cerrados, como también generar modificaciones en algunos de los módulos para instaurar malware en los dispositivos.

El reconociendo de los diversos ataques productos de las vulnerabilidades identificadas en el sistema, en los dispositivos y en la red, permite que se tomen los elementos más indicados que conlleva a una buena gestión, es decir dar cumplimiento a la misión que tiene la ciberseguridad que es la de brindar protección a las Unidades a flote de la Armada Nacional y con ellas a toda una sociedad. (Mitre, 2021).

Resultado

El empleo de protocolos de comunicación integrados a los sistema de información geográfica (ECDIS), sistema de identificación automática (AIS), y el sistema de posicionamiento global (GPS), permiten la ejecución de flujos de información entre los diferentes elementos, y la interacción que tienen los equipos entre sí, ejemplo de ello están los sistemas GPS, los cuales envían información a las cartas de navegación electrónicas, al sistema de piloto automático, al sistema de combate, al sistema de control de armas y al sistema de identificación automática.

Así mismo, los sistemas de corredera, ecosonda y estación meteorológica envían la información que recolectan a las cartas de navegación electrónica, a los sistemas de combate y al sistema de identificación automática, como también los radares envían la información a los sistemas de combate, sistemas de control de armas y a las cartas de navegación electrónica.

Por lo cual al identificar un problema de seguridad en el protocolo de comunicación y la posibilidad de materializar un ataque cibernético se podría anular o cambiar la información de la posición del buque, la velocidad o la profundidad, lo que generaría una posible falla en la toma de decisiones por parte de los tripulantes o del sistema de piloto automático, lo que a su vez podría causar colisiones, encallamientos, o lo que es más grave la desorientación de los sistemas de armas.

Con base a lo descrito anteriormente es de reconocer como la navegación de las diferentes unidades de flote, comprometen la realización de diversas operaciones esenciales, acciones que en ocasiones pueden ser afectadas por manos criminales generando riesgos que conlleven a diversos ataques ya sean por ejecución, evasión, descubrimiento, manejos de comandos y controles, impactos, entre otros.

Todo ello a través de la interceptación y suplantación de datos que se están transmitiendo, el envió de información falsa, modificación de los datos ya sean transmitidos o recibidos, realizar lecturas, y descarga de la información generando modificaciones y reemplazando o eliminando los archivo que están almacenados, identidad falsa, el desvíos de las diferentes rutas, los cambios de velocidad, como también la creación de buques «fantasmas» , a su vez y por medio de las redes LAN y WAN, también pueden desarrollarse diversos ciberataques.

Aunque en la información consultada no se identifican datos de sucesos como estos en las unidades a flote de la Armada Nacional de Colombia, se considera pertinente tener un acercamiento y conocimiento de la diversidad de ataques que se vienen dando a nivel mundial, a través de sistemas como el GPS, ECDIS y AIS, con base en ello ejecutar acciones que minimicen los riesgos.

Conclusiones

Este capítulo comienza realizando un acercamiento a diversas realidades que se entretejen en relación a los ataques cibernéticos, todos ellos causados por la vulnerabilidad existente en los sistemas de comunicación. Ciberataques como el presentado el 22 de julio del 2017, el cual se identificó como el primer ataque de falsificación de GPS, producido por el spoofing, en donde se cambia de ubicación a la nave identificándola en el aeropuerto de Gelendjik, cuando su posición real era el puerto ruso de Novorossiysk.

Otro ejemplo en relación a los buques militares es la situación presentada en febrero del 2021 con los buques de la armada Sueca que de acuerdo al análisis de los datos de seguimiento de las transmisiones del sistema de identificación automática revelan que se encontraban cerca de Rusia, estos datos de posicionamiento falso puede generar grandes riesgos tanto para la seguridad de los tripulantes de la embarcación, como también generar colisiones y lo que es aún un agravante mayor el desatar conflictos internacionales.

Como también otros de los casos relacionados son los de septiembre del 2020, y en noviembre del mismo año con los buques estadounidense USNS, Bruce C. Heezen, y el de USS Roosevelt también han presentado dificultades ya que, al realizar el análisis de

las posiciones transmitidas en las fechas, se identifica que el patrón AIS es falso, es decir que no se está mostrando la ubicación real de los buques.

Estos ejemplos bastan para comprender las situaciones que se vienen desarrollando, lo que debe generar unas señales de alerta en la Armada Nacional de Colombia, los diversos ciberataques en los cuales se pueden ver involucraos, dejan entrever la necesidad de reconocer los efectos que conllevan estos ataques, muchos de ellos tienen como finalidad afectar o alterar los sistemas de comunicación. parafraseando a Todd Humphreys, se podría afirmas que aún los buques con los más avanzados sistemas de comunicación, están expuestos a grandes riesgos de ciberataques, generando caos a nivel de seguridad marítima.

CAPÍTULO IV

Objetivo 2

Este capítulo permite tener un acercamiento al segundo objetivo planteado el cual se enmarca en determinar las diferentes estrategias de ciberseguridad a nivel Nacional e Internacional aplicables a las Unidades a flote de la Armada Nacional de Colombia.

Descripción

Después de haber identificado los riesgos, amenazas y ataques que se han generado a nivel Internacional con el empleo del protocolo de comunicación NMEA 2000, y específicamente con los sistemas GPS, el ECDIS, y el AIS, y tomando como precedente que no se identifican registros de casos sucedidos en unidades a flote de la Armada Nacional de Colombia, se identifican como estrategias de ciberseguridad las establecidas por España en la línea de capacidad de prevención, detención y respuesta a los ciberataques, en las que se seleccionan como estrategias (a) detectar y analizar los ciberataques, (b) identificación y procedimientos a seguir en relación a la defensa y la protección, (c) ampliación de las capacidades de respuestas ante los ciberataques, y por último (d) la creación y ejecución de actividades relacionadas con la capacitación y actualización permanente de prevención y detención de los ciberataques con simulacros que contribuyan a la prevención y detención de los diferentes ataques cibernéticos.

A su vez la línea que hace relación a la seguridad de los sistemas relacionados con las TIC, como soporte en las estructuras críticas, se postula como estrategia a integrar, la realización de análisis en las infraestructuras críticas y posibles riesgos, el desarrollo de actividades que conlleven tanto al conocimiento como a la sensibilización en relación a la vulnerabilidad, y ciberamenazas. A estos se integran estrategias

planteada por China y Reino Unido, en coherencia a desarrollar planes contra las infraestructuras críticas de las fuerzas militares, y a su vez, la protección de los datos y sistemas críticos en relación a las ciberamenazas.

Como última estrategia se enmarca la relacionada con la línea de Cultura de Ciberseguridad, en la cual se definen estrategias como (a) diseño de actividades tanto de conocimiento como de sensibilización, (b) y el desarrollo de programas que coadyuven a la generar conciencia de la importancia de la ciberseguridad.

En relación a las estrategias de ciberseguridad establecidas por la República de Francia, se identifican (a) Mantener la independencia a través de potenciar las capacidades de los medios humanos, y científicos (b) generar iniciativas de que contribuyan a un trabajo conjunto a nivel internacional, a través sistemas de seguridad y Ciberdefensa.

En Estados Unidos reconociendo la importancia de la ciberseguridad establecen como estrategias las defensas activas la cuales actúan en relación a “la velocidad de la red, el uso de sensores, software y firmas derivadas de inteligencia para detectar y detener cualquier código malicioso antes de que cause cualquier daño” (Trama, 2017, p. 108). Otra de las estrategias que se implementa es la denominada “Hack the Pentagon”, el cual buscaba retar a hackers estadounidenses a revisar webs fundamentales para el Departamento de Defensa,y reportar los fallos de seguridad que observan, lo cual ayuda a identificar incidentes de seguridad en el ciberespacio militar a su vez identifican recursos humanos con potencialidades en relación a la ciberdefensa, lo que permite reclutar personas que pueden contribuir a la operatividad de las Fuerzas Armadas de los EEUU.

Avanzando con otro país tenemos a China, la cual dentro de sus estrategias enmarcan acciones que contribuyan a la seguridad de sus sistemas, para lo cual se debe hacer revisión de todos los equipamientos críticos, este control debe ser realizado por expertos, como también de forma periódica se deben actualizar tanto el software, como el hardware, esto con el fin minimizar los "agujeros" de seguridad. A su vez, es de carácter obligatorio informar sobre cualquier ataque, y los metadatos de comunicación existentes a su vez, considera fundamental la necesidad de concientización en el manejo de los recursos tecnológicos y la información.

En cuanto a los Países Bajos: establecen seis prioridades como estrategia de ciberseguridad, siendo estas (a) adquisición de enfoques integral. (b) fortalecer las capacidades en la ciberdefensa; (c) Potenciar las competencias de los militares en relación a la cibernética ofensivas; (d) Ampliar las destrezas en relación a la inteligencia en el ciberespacio. (e) contar con un personal humano capacitado. (f) ampliar la cooperación a nivel mundial.

Análisis

En relación a las estrategias establecidas por Europa, España, Estados Unidos, República francesa. China, Reino Unido, y Países Bajos, se visibiliza puntos en común, siendo el primero el factor humano, el cual puede contribuir o afectar tanto los ambientes físicos como lógicos de una organización en relación a la ciberseguridad. Como segundo factor esta la protección de la infraestructura critica. Y como tercer punto en común está el trabajo colaborativo otros países.

Realizando una recopilación de lo anteriormente descrito las estrategias aplicables a las Unidades a flote de la Armada Nacional de Colombia, con base a los ejes comunes propuestos, son.

Estrategias relacionadas con el Factor Humano

Uno de los grandes eslabones que se consideran bastante vulnerable en relación a la ciberseguridad es el factor humano, por lo cual se debe identificar como un elemento clave en relación a la seguridad de una organización. Las estrategias basadas en el factor humano, se convierten en el mayor corta-fuego contra los ciberataques, el reconocer que la gran mayoría de las acciones requieren de la interacción de los seres humanos, permite vislumbrar la necesidad de trabajar con mayor énfasis en acciones como:

Ampliación de las capacidades de respuestas ante los ciberataques, capacitación, y actualización permanente de prevención y detención de los ciberataques, las cuales se convierten en acciones que coadyuvan en la ciberseguridad. Como lo afirman (Caro y Almanza, 2020). la educación en la ciberseguridad es un elemento fundamental y ahora más que nunca cuando se identifican una realidad digital, la cual se muestra cada vez más compleja, incierta y ambigua. Es por eso que una fuerza basada en un trabajo educado va a contribuir en la construcción de ambientes más confiables y seguros. Otro de los puntos clave es en relación a nutrir las alianzas con diferentes actores que tienen como punto de encuentro la ciberseguridad, lo que coadyuva a promover resultados que transformen los escenarios a través de diversas acciones de cooperación.

Creación y ejecución de actividades relacionadas con simulacros contribuyan a la prevención y detención de los diferentes ataques cibernéticos. Tomando como base que así como los atacantes seguirán desarrollando técnicas para realizar ciberataques, es

necesario generar escenarios en donde se desarrollen situaciones en los que el personal encargado se vea enfrentado a diversos ciberataques, esto con el fin de identificar la manera en que responde ante los mismos, con base en ello diseñar actividades tanto de conocimiento como de sensibilización, que contribuyan a dar respuesta de manera anticipada y adapten los elementos necesarios que contribuyan a detectar los riesgos o las amenazas de manera asertiva, a tomar decisiones acordes a las necesidades que se están presentando, para ello es necesario contar con un equipo interdisciplinar que tengan los conocimientos y competencias en el manejo de temas de ciberataques, ciberseguridad, entre otras.

El conocimiento de los diferentes riesgos a los que se enfrentan las organizaciones conlleva a que se desarrollen una diversidad de programas que coadyuven a generar conciencia de la importancia de la ciberseguridad, y que a su vez contribuyan a transformar los diferentes riesgos en oportunidades de mejora, esto con la finalidad de encarar los diversos retos y amenazas que subyacen del ciberespacio.

Identificación de personas con talento en el conocimiento y manejo de aplicaciones para rastrear posibles riesgos cibernéticos. En relación a lo estipulado en los retos de ciberseguridad 2020, establecidos por el Banco Interamericano de desarrollo (BID) y la organización de Estados Americanos (OEA).

> La escasez en la fuerza laboral de profesionales calificados en ciberseguridad es un desafío casi universal, para lo cual sin el financiamiento adecuado para la capacitación y educación profesional, el desajuste entre la oferta y la demanda conlleva el riesgo de retrasar las ganancias de madurez a futuro; también la falta de una base de habilidades de seguridad cibernética de apoyo podría tener efectos negativos en cascada en los esfuerzos de creación de capacidad en otras

> áreas. Estas consideraciones resaltan la necesidad de equilibrar las inversiones en ganancias de madurez a corto plazo para abordar las amenazas de seguridad inmediatas con planes a largo plazo para fomentar habilidades y educación que contribuyan de manera sustancial y auto sostenible a las posturas nacionales de ciberseguridad. (Banco Internacional de Desarrollo, 2020. p. 22)

Reclutar pesonas expertas que contribuyan en operatividad de las Fuerzas Armadas. El contar con personas que presentas altas capacidades tanto a nivel teórico de la funcionaliad de los diferentes sistemas, como a su vez, de los diferentes riesgos que se presentan por el uso de los mismos, va a contribuir a que se reduzcan las amenazas generando de esa manera un manejo indicado ya sea ante los riesgos, como tambien en relación con la seguridad en el ciberespacio.

Mantener la independencia a través de potenciar las capacidades de los medios humanos y científicos. La identificación de las diferentes potencialidades de las tripulaciones de las unidades a flote, va a permitir una mejor organización en relación a las diversas tareas a ejecutar, lo que permite que se realicen de manera más asertiva. A su vez, el generar ambientes que contribuyan al desarrollo de investigaciones en relación a los riesgos que se presentan y la manera de abordarlos va a contribuir a la realización de acciones que contribuyen al bienestar tanto de la organización como de toda una sociedad.

Concientización en el manejo de los recursos tecnológicos y la información. El generar conciencia de los perjuicios que pueden ocasionar el mal manejo de los diversos dispositivos o de la información, contribuye a que se dé un mejor manejo tanto a la data como a los sistemas, lo que conlleva a minimizar los riesgos, y las amenazas.

Potenciar las competencias de los militares en relación a la cibernética ofensivas, va a contribuir al aumento en la capacidad de ciberseguridad, tributando a la creación de y organizacón de campañas de sensibilización en relación a las posibles ofensivas que se pueden generar.

Estrategia de Protección de Infraestructura

Detectar y analizar los ciberataques.

Identificación y procedimientos a seguir en relación a la defensa y la protección, análisis de las infraestructuras críticas y posibles riesgos.

Desarrollar actividades que conlleven tanto al conocimiento como a la sensibilización en relación a la vulnerabilidad, y ciberamenazas.

Desarrollar planes contra las infraestructuras críticas de las Fuerzas Militares.

Revisar todos los equipos, sistemas, redes por manos expertas.

Actualización de los software, y hardware, esto con el fin minimizar los "agujeros" de seguridad.

Informar sobre cualquier ataque, y los metadatos de comunicación existentes, fortalecer las capacidades en la ciberdefensa.

Estrategia basada en el fortaleciendo de Alianzas Internacionales

Generar iniciativas que contribuyan a un trabajo conjunto a nivel internacional, a través de sistemas de seguridad y Ciberdefensa, ampliar la cooperación a nivel mundial. Para ello se puede iniciar con la identificación de los diferentes avances en material de ciberseguridad que vienen desarrollando diversos países, esto permite reconocer la manera en la que se pueden implementar en la organizaciones acciones de mejora que conlleven a tener la suficiente capacidad de hacer frente al contexto actual en materia de ciberseguridad.

Como se afirma en los retos de ciberseguridad 2020, establecidos por el BID y la OEA, se requiere dar continuidad a la cooperación, generando acciones relevantes y a su vez integrar mecanismos que contribuyan al monitoreo, a través de los análisis y evaluaciones que hayan generado un impacto en temas relacionados con la ciberseguridad en otros países; el tener información y datos basados del mundo cibernético va a contribuir a adentrarse a una cultura fundada en la gestión de riesgos cibernéticos. Por lo cual se debe estar preparado a la adaptabilidad de los entornos dinámicos a los cuales se está enfrentando, lo que genera tomar las decisiones basadas en un panorama cambiante en relación a las amenazas.

Para ello se pueden generar estrategias como compartir información en relación a las políticas de ciberseguridad nacional, a través de establecer puntos de contacto, que generen espacios de diálogo en relación a las diversas amenazas cibernéticas, a su vez promover prácticas que contribuyan al fortalecimiento de la seguridad en el ciberespacio.

Resultados

El secretario de la OTAN Jens Stoltenberg compara como los ataques ahora son provenientes a través de la red, y entre la misma red de las computadoras a igual que en un campo de batalla. Dicha afirmación, conlleva a reconocer la realidad que se está viviendo ante peligros eminentes, en relación a las amenazas cibernéticas, de las que se pueden identificar la explotación de redes, interrupción de redes y el sabotaje que tienen como finalidad la destrucción. A su vez, es pertinente reconocer la dependencia que se tiene con el espacio cibernético, ejemplo de ello se identifica con lo expuesto por Trama (2017),

> La dependencia militar del espacio cibernético en Estados Unidos lo constituye la Global Information Grid (GIG), que contiene una amplia gama de medios de comunicación, que incluye satélites, desplegados alrededor del mundo. La red habilita a los Estados Unidos para transmitir información, órdenes a sus tropas, guiar bombas inteligentes a los objetivos utilizando GPS. Si se llega a dañar esta red, los Estados Unidos corrían el riesgo de perder el dominio que actualmente tienen en los campos de batalla de todo el mundo. (Tama, 2017, p.105)

Con base en lo anterior se identifica que la misión por la que se está trabajando deriva en proporcionar ambientes seguros y protegidos en el espacio cibernético, todos los países expuestos en este capítulo identifican que se requiere el empleo de diversas estrategias que contribuyan a proteger y fortalecer, los sistemas de telecomunicación y la redes. Para ello reconocen que la estrategia debe fundamentarse tanto en el factor humano, protección de la infraestructura y la realización de convenios a nivel nacional e internacional que contribuya en mitigar los riesgos y las amenazas.

Para brindar la ciberseguridad requerida es pertinente dar continuidad a programas que tengan como finalidad potenciar las capacidades y las potencialidades de los militares en relación a los temas de ciberseguridad, Ciberdefensa y de ciberinteligencia en correspondencia al espacio cibernético, todo ello con el objetivo de planificar, y ejecutar acciones que coadyuven a anticiparse posibles ciberataques. El desarrollar las competencias necesarias y tener un acercamiento a los riesgos, amenazas, contribuyen a que se puedan anticipar los ciberataques, a su vez poder evaluar las posibles situaciones que se presentan lo que coadyuva a proteger y defender la

infraestructura, y en caso de ser necesario generar la restauración de los sistemas en el menor tiempo posible.

A su vez se debe tener presente que parte esencial en la ciberseguridad es tener una visión holística, es decir visibilizar la totalidad de los factores que emergen tanto en el ciberespacio, en la Ciberdefensa, como también en los avances en relación a las tecnologías de la información y comunicación.

CAPÍTULO V

Objetivo 3

Este capítulo permite dar respuesta al tercer objetivo planteado en el estudio, en el cual es tiene como finalidad proponer estrategias de protección en relación con los riesgos y amenazas por ataques cibernéticos en las Unidades a flote de la Armada Nacional.

Descripción

Con base a los diferentes hallazgos que derivan de los resultados establecidos en los objetivos planteados en la investigación los cuales permiten en coherencia a los resultados obtenidos identificar las estrategias que redunden en la ciberseguridad requerida en las Unidades a flote. En relación a la dinámica aplicada y tomando como referente el marco MITRE, se seleccionaron aquellos elementos que contribuyeran a dar respuestas a los riesgos y amenazas identificados. Es así, que elementos claves a tener en cuenta fueron la identificación del contexto, la protección de los sistemas, y la respuesta que se debe tener en cuenta en relación a los incidentes.

Análisis

Ante los diferentes hallazgos en relación con los riesgos identificados con el empleo de los GPS, el ECDIS, y el AIS. Se propone establecer las siguientes acciones las cuales contribuyen a minimizar los ciberataques.

Dentro de las acciones a ejecutar se requiere integrar acciones de carácter preventivo como.

Contar con sistemas de detección y prevención de intrusiones en la red que utilizan firmas de red, esto con la finalidad de contribuir en la identificación del tráfico de malware adversario específico se pueden utilizar para mitigar la actividad a nivel de red.

Disponer de redes de comunicación con instrumentos electrónicos multitransmisores, receptores bidireccionales, y con capacidad para interconectar diversos dispositivos, con el fin de compartir e intercambiar datos importantes, lo que en ocasiones al no tener la suficiente precaución puede conllevar a ciberincidentes marítimos.

Sensibilizar hacia los controles que se deben tener con los datos y el uso de los diferentes dispositivos.

Precisar programas de acción relacionados con la seguridad cibernética, basada en las diferentes experiencias que han tenidos otros países.

Empleo de técnicas que fortalezcan competencias para detectar y bloquear posibles situaciones que pueden generar ciberataques.

Los sistemas de detección y prevención de intrusiones en la red que utilizan firmas de red para identificar el tráfico de malware adversario específico se pueden utilizar para mitigar la actividad a nivel de red.

Emplear sistemas de prevención de intrusiones de red / host, antivirus y cámaras de detonación para evitar que los documentos obtengan y / o ejecuten cargas útiles maliciosas.

En acciones en relación a tareas ejecutadas por los diferentes usuarios se considera que los diferentes enlaces, como los sistemas de prevención de intrusiones en la red y los sistemas diseñados para escanear y eliminar descargas maliciosas se pueden utilizar para bloquear la actividad. A su vez, se recomiendo la utilización de firmas de red para identificar el tráfico de malware adversario específico lo que contribuye a minimizar la actividad a nivel de red.

En relación al empleo de los software, se recomienda empaquetado del software, lo que contribuye a garantizar definiciones de virus actualizadas y crear firmas personalizadas para el malware observado

Con base a la suplantación de identidad se recomienda el uso de un antivirus que puede poner en cuarentena automáticamente los archivos sospechosos.

En relación a la integridad del arranque se considera pertinente, el uso de proveedores de dispositivos de red integrados los cuales proporcionan firma criptográfica para garantizar la integridad de las imágenes del sistema operativo en el momento del arranque.

Protección de la información confidencial con cifrados más sólidos.

Minimizar la cantidad de información a personal externo.

Actualización de forma periódica del software con regularidad.

Emplear parches para los software y los servidores internos de la organización

Prevenir la recopilación de datos que sean de carácter confidencial en dispositivos de almacenamiento que no tengan la seguridad indicada.

Revisión de los sistemas de prueba de vulnerabilidad para el GPS, el ECDIS y el AIS.

Monitoreo de las redes LAN y WAN

Revisión de los protocolos en relación a la protección de los sistemas de comunicación.

Realización de supervisiones en relación a los flujos de tráfico de la información, los proveedores como todo personal que tenga contacto con la misma.

Realización supervisiones de los diferentes procesos y la argumentación en relación a la línea de comando, esto con el fin de identificar acciones que contribuyan a la recolección de información en relación con la localización de los sistemas, de las diversas herramientas de acceso remoto, y los sistemas operativos que tiene como finalidad la recolección de la información.

Desarrollar programas de capacitación que contribuya a la mejora y fortalecimiento de las competencias relacionadas con la ciberseguridad.

Negar acceso a programas o software que sean vulnerables, esto con la finalidad de minimizar los riesgos por adversarios.

En cuanto a los protocolos de autenticación se recomienda contar con credenciales debidamente protegidas.

Verificar que los datos se encuentre encriptados de manera correcta.

Emplear aplicaciones de seguridad en los diferentes sistemas que contribuyan a minimizar los riesgos con los datos.

Ejecutar acciones de capacitación en relación a identificación de riesgos, esto con la finalidad de reconocer amenazas cibernéticas.

Contar con equipos vitales que contribuyan en la navegación de la información.

Implementar tareas como el control de movimiento de los diferentes software que se emplean, el acceso seguro a la web, teniendo en lo posible una conectividad

mínima en relación a las redes externas involucrando con ellas el uso de los correos personales que puedan generar vulnerabilidad a la redes institucionales.

Generar actividades de conocimiento y sensibilización en relación a la vulnerabilidad, y ciberamenazas, a través del desarrollo de programas de concienciación en ciberseguridad.

Diseñar proyectos que contribuyan en el aumento de la ciberseguridad.

Ampliar la colaboración con instituciones.

Reforzar la seguridad de la infraestructura de red con el fin de evitar posibles ataques, optimizando su referencia para que un ataque pueda ser rápidamente identificado.

Análisis, estudio y la creación de normas para el uso e implementación de esos dispositivos durante el ciclo de vida del producto para garantizar el cumplimiento de los requisitos mínimos de ciberseguridad y privacidad.

Recurrir a estrategias integrales de carácter técnicos, a través de incrementar sistemas que contribuyan a realizar de manera periódicas pruebas de vulnerabilidad.

Integrar herramientas de navegación nano satelital, instalación de simuladores satelitales, diseño de mecanismos que permitan generar alertas tempranas, instalación de cortafuegos digitales y la instauración de equipos de reacción rápida que contribuyan con la defensa cibernética.

En relación a los navegadores WEB, y los correos electrónicos

Emplear protocolos de protección tanto para navegadores, datos, direcciones email, y demás información que requiere ser intercambiada con otros buques;

Intercambio seguro de datos a través de cifrados, evitando de esa manera la ejecución de códigos maliciosos.

Revisión periódica de los diferentes contratos y protocolos de mantenimiento del sistema. En el cual se recomienda que estas revisiones sean como primero de carácter preventivo que permita identificar posibles fallas y defectos inmanentes de carácter correctivo del sistema.

Mantenimientos adaptativos, que permitan la adaptación a los diferentes entornos que requieren de ejecución.

Realizar las actualizaciones de los sistemas operativos, esto con el fin de evitar que sean obsoletos, diseñar flujos de ejecución que permita detectar de manera anticipadas riesgos del sistema.

Diseño de un plan de seguridad, que tenga como objetivo fundamental el enfoque preventivo, y no reactivos.

Identificación de fuentes basadas en informes de los últimos ciberataques que vienen sucediendo en las organizaciones tanto privadas como públicas a nivel nacional e internacional, esto con la finalidad de un acercamiento a las realidades que se vienen entretejiendo en la ciberdelicuencia.

Acercamiento a los diversos informes de inteligencia, sobre los diferentes riesgos y amenazas que se han conocido en la infraestructura crítica, a su vez, tener presenta la legislación y las normas que se establecen a nivel estatal en relación a la ciberseguridad y manejo de las situaciones que se presenten.

Integrar los diferentes acuerdos que se han establecido con otras organizaciones a Nivel Nacional e Internacional, y que contribuyen al conocimiento de los riesgos y posibles ataques que afecten la ciberseguridad de la organización.

Conocimiento de los diferentes protocolos de comunicación, de las redes, sistemas y dispositivos en tiempos reales; con base en ello reconocer tanto la vulnerabilidad, como los potenciales riesgos y amenazas a los que están expuestos.

Diseñar planes de acción que contribuyan a estabilizar los sistemas afectados de la manera más rápida y confiable evitando al máximo afectar a la organización.

Resultados

Es fundamental tener conocimiento de las diferentes situaciones que se estan presentando en relación con las ciberamenazas y los ciberataques a nivel internacional, el tener un acercamiento a estas realidades, permite que se empiecen a tomar acciones de ciberseguridad que contribuyan a la generación de escenarios seguros como también a la toma de decisiones asertivas y con conocimiento de causa sobre la vulnerabilidad existente en los protocolos de comunicación y demás sistemas empleados.

Desarrollar acciones centradas en la prevención de las unidades a flote de la Armada Nacional, como capacitar de manera permanente a todo el personal en cuanto a temas relacionados con riesgos, amenazas, ataque-respuesta, esto con el fin de fortalecer las potencialidades en relación al manejo de las ciberamenazas, lo cual va a contribuir a poder identificar que tipo de riesgos o amenazas cibernéticas se esta presentando.

También reconocer el nivel en el que se encuentra el riesgo y la amenaza, este conocimiento permitirá contribuir en actuaciones que conlleven a la protección de datos que a su vez estarán en la capacidad de detectar software maliciosos, hallar intrusos que esten manipulando los sistemas, o generando modificaciones en las rutas, entre otros.

Como también puedan ejecutar tareas tales como hacer restriciones en relación a la ejecución de códigos que puedan afectar el funcionamiento del sistema, el empleo de métodos seguros para dar inicio a los diferentes sistemas, deshabilitar programas que

generen vulnerabilidad en el sistema, a través del cifrado solido generar protección a la información, evitar la conexión de dispositivos portables que puedan afectar al protocolo o a los sistemas, impedir la instalación de programas que afecten el sistema, realizar segmentaciones de redes con el fin de aislar ya sea los sistemas o las funciones de los protocolos o sistemas.

El generar conciencia en relación a la importancia de la ciberseguridad, va a contribuir en la protección de los unidades a flote de la Armada y por consiguiente a la seguridad del país.

Conclusiones

A través de los grandes avances que se entretejen en relación a las tecnologías, los atacantes cibernéticos vienen adentrándose cada vez más a fondo a los diferentes entornos virtuales, dispositivos y sistemas existente, ingresando con mucha facilidad, y generando apertura a brechas estratégicas, en las que ni el tiempo, ni la distancia, ni los dispositivos tecnológicos son obstáculos en el cumplimiento de sus objetivos, lo que conlleva a causar una diversidad de daños a las organizaciones, y otros actores como el ecosistema.

Situaciones como las presentadas en países de Estados Unidos, España, y Rusia en relación a los ciberataques, permite vislumbrar la necesidad de blindar las unidades a flote de la Armada Nacional de posibles ataques que se puedan presentar, esto a causa de los elementos considerados riesgosos para la organización, de allí parte la necesidad de generar estrategias cada vez más sólidas que contribuyan a desarrollar ambientes ciberseguros, y resilientes.

Esta situación y otras realidades conllevan a que la Armada Nacional busque estrategias que coadyuven a mitigar los riesgos en sus unidades a flote. Con base en las realidades descritas anteriores se hace vital desarrollar estudios en relación a disminuir los posibles ataques, es así que esta investigación plantea la necesidad de potencializar las competencias en relación con identificar, desarrollar y evaluar las diversas estrategias de ciberseguridad que se puedan implementar con el fin de neutralizar ataques cibernéticos en las unidades a flote de la Armada Nacional de Colombia.

Con base en ello se identifica que el protocolo de comunicación NMEA 2000 manifiesta puntos de vulnerabilidad, en los sistemas que son compatibles como el GPS, ECDIS, y AIS, que presentan riesgos lo que conlleva a que sean vulnerables con gran facilidad para violentar el sistema de seguridad, afectando la confiabilidad, disponibilidad e integralidad. A su vez pueden ser empleados como proxis o convertirlos en intermediarios de los ciberatacantes para el robo de datos, tráficos maliciosos, bloqueo de información, cambios de rutas, enmascarar la navegación, buques fantasmas, entre otros.

En relación con los hallazgos identificados, y teniendo en cuenta los riesgos y las amenazas, se identifican tres factores esenciales siendo estos el factor humano, el factor de protección y el trabajo colaborativo a nivel tanto nacional como internacional puede contribuir a que se minimicen los riesgos y por lo tanto las ciberamenazas y los ciberataques, dichos elementos claves que al ser integrados van a contribuir de manera favorable a la organización.

Factores como el acercamiento y conocimiento de los protocolos, la sensibilización ante los riesgos que se pueden presentar, el conocimiento del uso de dispositivos, redes, elementos de seguridad, y el manejo de la información de manera asertiva, van a contribuir a minimizar los ciberataques a los cuales se puede ver implicada la organización.

Dentro de la visión establecida por la Armada Nacional se identifica el “Ser una Armada de proyección e influencia regional, con tecnología y capacidades para la defensa y seguridad nacional”. Es así, que para poder dar cumplimiento a la visión que enmarcan es fundamental que se generen dentro de la organización estrategias acordes a las necesidades en manera de ciberseguridad, evitando en lo posible elementos que

vulneren su seguridad. Por lo tanto, al mitigar las amenazas, se está cumpliendo con la protección de una sociedad.

Tomando como referente los resultados, permite como investigador tener un acercamiento a los grandes riesgos a los que se ven enfrentadas todas las organizaciones en el día a día, con el empleo de las diferentes artefactos tecnológicos, a su vez también permite reconocer que hay elementos claves que al ser integrados en la organización van a contribuir de manera favorable a la organización. Factores como el acercamiento y conocimiento de los protocolos, la sensibilización ante los riesgos que se pueden presentar, el conocimiento del uso de dispositivos, redes, elementos de seguridad, y el manejo de la información de manera asertiva, van a contribuir a minimizar los ciberataques a los cuales se puede ver implicada la organización.

En relación a las limitaciones, se identifica que la mayor limitación que se presenta para la realización de esta investigación se enmarca en poder utilizar información y datos que hay en la organización, pero que por razones de seguridad no es posible incorporar.

A su vez, el identificar los grandes riesgos que presenta la utilización de un protocolo de comunicación, conlleva a que se adentre a nuevas investigaciones en relación a los demás dispositivos, redes, o sistemas que se están empleando en las unidades a flote de la Armada Nacional, esto con el fin de mitigar los ciberataques. A su vez, la investigación abre un espacio a otros estudios en relación a los nuevos ataques que se vienen presentando, como también en el desarrollo de protocolos en correspondencia a los avances tecnológicos.

Referencias

Ambos, K (2014). *Responsabilidad penal internacional en el ciberespacio.* Colombia: Universidad Externado.

AG/RES.2040-XXXIV-O/04 (8 de Junio de 2004). Reunión de Ministros de Justicia o procuradores Generales de las Américas.

Aguilar, J. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *URVIO Revista Latinoamericana de Estudios de Seguridad*, (25), 24-40.

Aguilar, J. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estudios internacionales (Santiago), 53(198), 169-197. https://dx.doi.org/10.5354/0719-3769.2021.57067

Aguirre, J. (2019). Cambios en la seguridad internacional en el marco de la globalización: el caso de la ciberseguridad y sus desafíos para la Seguridad Nacional de México (2012-2018). Universidad Nacional Autónoma de México.

Álvarez, R. (2017). *Se presenta el primer caso de falsificación de GPS: una nueva forma de ataque electrónico.* Xataka. https://www.xataka.com/seguridad/se-presenta-el-primer-caso-de-falsificacion-de-gps-una-nueva-forma-de-ataque-electronico.

Arroyo, D. Gayoso, V. y Hernández, L. (2020). Ciberseguridad. Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro.net/es/ereader/uniminuto/172144?page=16 Baralt, E. (2017). Ciberseguridad: un reto para la defensa nacional en entornos intangibles. Seguridad, Ciencia & Defensa, 3(3), 19

Barald, N. (2019). Infraestructuras críticas y ciberseguridad en las fuerzas armadas Dominicanas. Ministerio de Defensa. Seguridad, Ciencia y defensa. Año V, Nº 5.

Berardi, G. (1996). Operaciones Especiales a flote. *Revista Marina Cl.*

Bergman, B. (2021). El Análisis sistemático de datos revela pistas falsas de buques. https://skytruth.org/2021/07/systematic-data-analysis-reveals-false-vessel-tracks/

Burton, J. (2015). NATO's cyber defence: Strategic challenges and institutional adaptation. *Defence Studies, 15*(4), 297-319. https://doi.org/10.1080/14702436.2015.1108108

Campero, J; Herrera M. (2018). *Análisis de riesgos y elaboración de controles para un prototipo de control y automatización industrial en la empresa intecmo SAS.* [tesis de pregrado, Universidad Piloto de Colombia]. http://polux.unipiloto.edu.co:8080/00004800.pdf

Canduo, J (2009). Seguridad, ciencia y defensa, *Ciberseguridad: hacia una respuesta y disuasión efectiva*. Instituto Superior para la defensa. General Juan Pablo Duarte Diez- INSUDE- Año V-Nº 5.

Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. *bie: Boletín IEEE,* (2), 950-966.

Cassidy, F (1999). NMEA 2000 Explained - The Latest Word, NMEA Standards Committee.

Centro de Investigaciones Oceanográficas e hidrográficas (2021-09-07). https://www.cioh.org.co/index.php/es/371-informacionarcprov.html

Comando Conjunto Cibernético. (2017). Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia. https://www.ccoc.mil.co/recursos_user///PLAN_PUBLICO.pdf

Comisión de Regulación de comunicaciones. Resolución 2258 de 2009, Bogotá, 2009.

Consejo Nacional de Política Económica y Social –CONPES (2011). Documento 3701. Lineamientos de Políticas para ciberseguridad y Ciberdefensa

Consejo Nacional de Política Económica y Social –CONPES (2016). Documento 3854. Política Nacional de Seguridad Digital.

Consejo Nacional de Política Económica y Social –CONPES (2020). Documento 3995. Política Nacional De Confianza Y Seguridad Digital.

Crawford, J. (2019). Ciberataque al transporte marítimo. ¿Una amenaza real o ciencia ficción? Revista de marina, Nº 970 15-23.

Cruz, L. (2017). La política brasileña de ciberseguridad como estrategia de liderazgo regional. Revista Latinoamericana de Estudios de Seguridad, 20, 16–30

Cruz, S y Yareli (2018). Ciberseguridad en estados unidos: vulnerabilidad en el hackeo y espionaje sobre información clasificada en materia de política exterior (2009-2012.) p. 181. https://core.ac.uk/download/files/442/12091513.pdf.

Daricili, B. (2020). ¿Cuáles son los objetivos de las estrategias de ciberseguridad de los países con más poder en el mundo? https://www.aa.com.tr/es/análisis/-cuáles-son-los-objetivos-de-las-estrategias-de-ciberseguridad-de-los-pa%C3%ADses-con-más-poder-del-mundo/2063747.

Dammert, C; Núñez, C. (2019). Enfrentando las ciberamenazas en el Cono Sur. Ministerio de Defensa. Seguridad, Ciencia y defensa. Año V, Nº 5.

Diario Oficial Nº 50664 (24 de Julio de 2018). “Convenio sobre la Ciberdelincuencia “ 23 de Noviembre de 2001. Budapest.

Diccionario Etimológico. http://etimologias.dechile.net/?ciber fecha consulta: (31 de Abril-2021).

Escuela Superior de Guerra. (2020). Estrategia Nacional de Ciberdefensa y Ciberseguridad - ECDIS - 2020-2030.

FBI. (2018-02-08). Public Service Announcement. Federel Bureau of investigation. Ciber Actor use internet of thins devices as proxies for anonymity. https://www.ic3.gov/Media/Y2018/PSA180802.

Garrido, N. (2013). Receptores GNSS-GPS. *Geodesia Espacial*. Nagrvil.webs.upv.es

Hernández, R., Fernández, C., & Baptista, M. (2014). Metodología de la Investigación. En Journal of Materials Processing Technology (Sexta edic, Vol. 1, Número 1).

Hurtado de Barrera, J. (2000). Metodología de Investigación Holística (SYPAL (ed.); Tercera ed).

Instituto Español de Estudios Estratégicos. (2010). Ciberseguridad. Retos Y Amenazas a La Seguridad Nacional En El Ciberespacio. En Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el ciberespacio- cuaderno de estudios estratégicos (Número 149). http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2011/Cuaderno_149.html

Krile, S., Kezic, D., & Dimc, F. (2013). NMEA communication standard for shipboard data Architecture/NMEA komunikacijski standard za arhitekturu podataka na brodu. Nase More, 60(3), 68-81. Retrieved from https://www-proquest-com.ezproxy.uniminuto.edu/scholarly-journals/nmea-communication-standard-shipboard-data/docview/1461400186/se-2?accountid=48797

Lessig, L. (2002). Las leyes del ciberespacio. *THEMIS Revista De Derecho*, (44), 171-179.

Londoño, L., & Tabares, J. M. (2012). Metodología de la investigación holística: Una propuesta integradora desde las sociedades fragmentadas. Uni-pluriversidad, vol. 2 No.3, 2(3), 22–23.

Machado, A. (2014). Ciberseguridad Nacional. Informe N° 002/2014 – CIAEM. Lima: Escuela Superior de Guerra Naval.

Machín, N., & Gazapo, M. (2016). La ciberseguridad como factor crítico en la seguridad de la unión europea. Revista Unisci, (42), 47-68. doi:http://dx.doi.org.ezproxy.uniminuto.edu/10.5209/RUNI.53786.

Marulanda, C. (2009). Integración y configuración gps al sistema de radio para el metro de medellín. Tesis de grado. Universidad Pontificia Bolivariana

Mayorga, A. (2014). *Lineamientos, tendencias y estrategias sobre ciberseguridad y ciberdefensa en Colombia.* (Bachelor's thesis, Universidad Piloto de Colombia).

Mednikarov, B., Tsonev, Y., & Lazarov, A. (2020). Analysis of cybersecurity issues in the maritime industry. Information & Security, 47(1), 27-43. doi:http://dx.doi.org.ezproxy.uniminuto.edu/10.11610/isij.4702

Ministerio de Tecnologías de la Información. Paraguay (sf). Controles críticos de ciberseguridad.

MITRA ATT&CK. (2021). https://attack.mitre.org/techniques/enterprise/

Mittelman, J. H. (1996). Globalization: critical reflections.

Organización Marítima Internacional O.M.I. (5 julio 2017). Circular O.M.I. MSC-FAL.1/Circ.3.. Directrices sobre la gestión de los riesgos cibernéticos marítimos.

Park, B., Lee, J., Kim, Y., Yun, H., & Kee, C. (2013). DGPS enhancement to GPS NMEA output data: DGPS by correction projection to position-domain. Journal of Navigation, 66(2), 249-264. https://doi.org/10.1017/S0373463312000471

Pascual, J. 2017. Adquisición y procesado de información de posicionamiento GPS. Memoría descriptive. Universidad Politécnica de Valencia.

Popescu, S. (2018). *Naval Cybersecurity In The Context Of The Hybrid War*. Bucharest: "Carol I" National Defence University. Retrieved from https://www-proquest-com.ezproxy.uniminuto.edu/conference-papers-proceedings/naval-cybersecurity-context-hybrid-war/docview/2043183297/se-2?accountid=48797

Psiaki, M, y Humphreys. (2016). GNSS Spoofing and detection. *IEEE Xplore. 104* (6), 1258-1270 https://radionavlab.ae.utexas.edu/images/stories/files/papers/gnss_spoofing_detection.pdf.

Realpe, M., & Cano, J. (2020). Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia. Seguridad Informática. X Congreso Iberoamericano, CIBSI 2020, 105–113. https://doi.org/10.12804/si9789587844337.10

Richardson, R. (2019). Análisis sistemático de metodologías y modelos para la gestión del riesgo en las operaciones navales y costeras de República Dominicana. Seguridad, Ciencia & Defensa, 5(5), 40-46.

Rodríguez, I. (s.f). Subsistemas GPS. http://bibing.us.es/proyectos/abreproy/50027/fichero/PFC+Ivan+Rodriguez+Carmona%252FMemoria%252F03-Subsistema+GPS.pdf

Sancho, C. (2017). Ciberseguridad. Presentación del dossier. Revista Latinoamérica de Estudios de Seguridad Número 20, 8.

Serrano, C. (2020). Mejora del sistema de ayuda a la reducción de riesgos de colisión de buques en alta mar.

Taipes, D. (2020). Sistema de seguridad cibernética nacional frente a los ciberataques como amenaza a la Seguridad Nacional. Revista de Ciencia e Investigación en Defensa, 1(2), 43-48.

Tates C y Recalde, H. (2019). La Ciberseguridad en el Ecuador, una propuesta de organización. Revista de Ciencias de Seguridad y defensa. Vol 4, Núm 7, 156-159.

Téllez, R. (2016). Prefijo CIBER: Arqueología de su presencia en la sociedad del conocimiento. *Investigación y desarrollo*, *24*(1), 142-162.

Tovar, M (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. México: revista en estudios de seguridad Nacional. V. 6. Núm 2. DOI: http://dx.doi.org/10.18847/1.12.2.

Trama, G. (2017). Operaciones militares cibernéticas: planeamiento y ejecución en el nivel operacional. 1a ed . Buenos Aires : Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, 1-304 p

Unión Internacional de Telecomunicaciones U.I.T, resolución 181. UIT-Tx 1205. https://www.itu.int/rec/T-REC-X.1205-200804-I/es.

Unión Internacional de Telecomunicaciones (UIT), el Banco Mundial, la Secretaría de la Commonwealth (Comsec), la Organización de Telecomunicaciones de la Commonwealth (CTO), el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN). 2018. *Guía para la elaboración de una estrategia nacional de ciberseguridad* – Participación estratégica en la ciberseguridad. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

Vargas, E. (2014). Ciberseguridad y Ciberdefensa: ¿Qué implicaciones tienen para la seguridad nacional?

Vargas, R. et al. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO, Revista Latinoamericana de Estudios de Seguridad, (20). Recuperado de: https://www.redalyc.org/ jatsRepo/5526/552656641013/html/index.html.

Vázquez, L., Rojas, A., & Macha Moreno, E. L. (2017). Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016.

Vázquez, M. (2003). Una historia de las telecomunicaciones navales. Revista marina https://revistamarina.cl/revistas/2003/4/vasquez.pdf

Villanueva, C. (2015). *La ciberdefensa en Colombia* (Bachelor's thesis, Universidad Piloto de Colombia).

WON, C. YOUN, J. H. ALI, H. Impact of High-Mobility Radio Jamming in Large Scale Wireless Sensor Networks, Lecture Notes in Computer Science, Vol. 4097, 2006, pp. 244-251.

Lista de Tablas