Acercamiento conceptual de un prototipo del CSIRT : caso armada nacional de Colombia

Carlos Alberto Roa Correa

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

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

2020

Ministerio de Defensa Nacional

Comando General de las Fuerzas Militares

Escuela Superior de Guerra

Maestría en Ciberseguridad y Ciberdefensa

Acercamiento Conceptual de un Prototipo del CSIRT: Caso Armada Nacional de Colombia.

Teniente de Navío Marina de Guerra de Colombia

Carlos Alberto Roa Correa

Maestría En Ciberseguridad Y Ciberdefensa

Trabajo de Grado

Bogotá, D.C - Colombia

2020

Ministerio de Defensa Nacional

Comando General de las Fuerzas Militares

Escuela Superior de Guerra

Maestría en Ciberseguridad y Ciberdefensa

Acercamiento Conceptual de un Prototipo del CSIRT: Caso Armada Nacional de Colombia.

Teniente de Navío Marina de Guerra de Colombia

Carlos Alberto Roa Correa

Director: Magister. Teniente de Navío

Julián David Aponte Díaz

Maestría En Ciberseguridad Y Ciberdefensa

Trabajo de Grado

Bogotá, D.C - Colombia

2020

_____

_____

_____

_____

_____

_____

_____

Jurado

_____

Jurado

_____

Jurado

Nota de aceptación

Bogotá D.C

DEDICATORIA

Este trabajo de grado es dedicado especialmente a Dios como pilar y eje fundamental de todos los seres humanos y el especial al brindarme la sabiduría y capacidad intelectual y mental para el logro de todas mis metas, a mi amada y hermosa familia, a mis padres Alfonso y Lucrecia por todas sus enseñanzas y educación fundamentada en valores y a mi bella y admirable esposa Mary por su invaluable apoyo, entrega, amor y dedicación en los momentos de incansable estudio para lograr culminar las materias vistas dentro de la maestría, a mi adorada Armada Nacional por brindarme el espacio, tiempo y la oportunidad de ampliar y fortalecer mis capacidades profesionales e intelectuales; y en general a todos los docentes, tutores y compañeros de la maestría que de una u otra forma aportaron significativamente en la realización de mis estudios en la Escuela Superior de Guerra dentro del programa de Maestría en Ciberseguridad y Ciberdefensa.

AGRADECIMIENTOS

Agradezco al Gobierno Nacional de Colombia quienes a través del Ministerio de las Tecnologías de la Información y las Comunicaciones TICs concibieron este importante programa para el fortalecimiento y capacitación del talento humano de TICs de las instituciones del estado colombiano. Igualmente, a la Escuela Superior de Guerra y a toda su parte administrativa, investigativa y personal de docentes por generar, diseñar e implementar el programa de Maestría de Ciberseguridad y Ciberdefensa.

Al Magister, Ingeniero y Teniente de Navío Julián David Aponte por su constate trabajo, apoyo y dirección dentro del presente trabajo, los cuales se ven reflejados en la culminación del presente trabajo de grado, igualmente por su orientación y apoyo en los momentos de duda, igualmente al Doctor Carlos Alfonso Castañeda Marroquín quien me apoyo en la orientación inicial de este trabajo y por brindarme su tiempo y dedicación para construir una muy buena parte del mismo y a mi hermosa esposa por su invaluable ayuda, apoyo, tiempo y paciencia dentro de la realización del mismo y a todas las personas que participaron y me ayudaron de manera directa e indirecta para la elaboración y finalización de este proyecto.

RESUMEN EJECUTIVO

La dinámica de las tecnologías de la información sumada a la evolución y el crecimiento exponencial de las TIC[1], instauran una necesidad potencial para la protección al interior de las Fuerzas Militares debido a la manifestación de nuevas amenazas y riesgos para la seguridad y defensa del estado, por lo que se hace necesario diseñar un equipo de respuesta a incidentes de seguridad informática – CSIRT[2] en la Armada Nacional de Colombia.

El cual actuara como punta de lanza en la obtención de información para la prevención y anticipación de ataques informáticos que pretendan afectar las infraestructuras críticas de la Armada Nacional. Por lo cual se hace necesario observar el contexto geopolítico, las capacidades inherentes para el diseño del CSIRT, las diferentes metodologías de diseño y la definición de que es un CSIRT, que tipos existen y que servicios prestan. Logrando formular un acercamiento conceptual de un Prototipo del CSIRT: Caso Armada Nacional de Colombia, integrando las propuestas planteadas por la guía NIST SP 800-61, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), el CERT de la Universidad Carnegie Mellon y la Organización de los Estados Americanos.

Como resultado se planteará el acercamiento conceptual de un Prototipo del CSIRT, determinar los conceptos necesarios para establecer los parámetros iniciales conceptuales, establecer los lineamientos, sugerir la metodología integrada de diseño y un prototipo organizacional que se ajuste a las necesidades propias de la Armada Nacional de Colombia

[1] Sigla de: Tecnologías de la Información y las Comunicaciones
[2] Sigla de: Equipo de Respuesta a Incidentes de Seguridad Informática

y contempla la normativa interna para que posteriormente se logre una implementación exitosa del CSIRT.

Con base en la evidencia, toda organización debe ser responsable de la administración y gestión de sus incidentes, por lo cual, es de suma importancia establecer los mecanismos para la adopción e implementación de un CSIRT, así como los servicios básicos que este pueda asumir en el interior de sus organizaciones.

Palabras Claves: Equipo de respuesta ante incidentes de seguridad informática (CSIRT), Ciberdefensa, Metodología, Prototipo, Capacidades, Servicios.

LISTA DE ABREVIATURAS

APT: Amenaza Persistente Avanzada

ARC: Armada Nacional de Colombia

ARPANET: Advanced Research Projects Agency Network

CARMA: Comando Armada Nacional

CERT o CERT/CC: Computer Emergency Response Team / Coordination Center, equipo de respuesta a emergencias informáticas / Centro de coordinación. Marca registrada en Estados Unidos.

CGFM: Comando General Fuerzas Militares

CIRC: Computer Incident Response Capability, Capacidad de respuesta a incidentes informáticos

CIRT: Computer Incident Response Team, equipo de respuesta a incidentes informáticos

CONPES: Consejo Nacional de Política Económica y Social

CSIRC: Computer Security Incident Response Capablity, capacidad de respuesta a incidentes de seguridad informática

DARPA: Defense Advanced Research Projects Agency

DADIN: Dirección Administrativa de Inteligencia Naval

DICIB: Dirección Cibernética Naval

DNP: Dirección Nacional de Planeación

ENISA: Agencia Europea de Seguridad de las Redes y de la Información

FFMM: Fuerzas Militares de Colombia

FIRST: Forum of Incident Response and Security Teams

FNC: Fuerza Naval del Caribe

FNO: Fuerza Naval del Oriente

FNP: Fuerza Naval del Pacifico

FNS: Fuerza Naval del Sur

GPPi: Instituto Global de Políticas Públicas

IDS: Sistema de Detección de Intrusiones

IHT: Incidence Handling Team, equipo de manejo de incidentes

IoT: Internet de las Cosas.

IRC: Incident Response Center/ Incident Response Capability, capacidad de respuesta a incidentes

IRT: Incident Response Team, equipo de respuesta a incidentes

MDN: Ministerio de Defensa Nacional

NIST: Instituto Nacional de Estándares y Tecnología

OEA: Organización de los Estados Americano

SERT: Security Emergency Response Team, equipo de respuesta a emergencias de seguridad.

SIRT: Security Incident Response Team, equipo de respuesta a incidentes de seguridad.

SOC: Security Operations Center, Centro de Operaciones de Seguridad.

TERENA: Asociación Trans-europea de Redes Nacionales de Investigación y Educación.

TI: tecnologías de la Información.

TICs: Tecnologías de la Información y las Comunicaciones.

UIT: Unión Internacional de Telecomunicaciones.

US-CERT: CERT del Departamento de Seguridad Nacional de Estados Unidos.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

I. INTRODUCCIÓN

Las Fuerzas Militares de Colombia están obligadas a cambiar la forma de ejercer sus funciones constitucionales de seguridad y defensa nacional en todos los dominios de la guerra y en especial en el quinto dominio el ciberespacio, por lo anterior, es de resaltar la importancia que conlleva la generación de un equipo de respuesta a incidentes de ciberseguridad enfocado a la protección de la seguridad nacional que responda de forma efectiva y proactiva a los incidentes de seguridad y ciberataques que puedan desestabilizar de alguna manera al Estado, las FF. MM[3]. y el país.

Actualmente las FF. MM. desarrollan esta actividad y cuentan con algunas capacidades para detectar acciones maliciosas y sospechosas dentro de las redes de datos, pero estas no son suficientes y acorde a las características propias y a las necesidades de la organización y del país, por eso con el desarrollo del acercamiento conceptual de la metodología de diseño y el prototipo organizacional del CSIRT para la Armada Nacional permitiría establecer los servicios esenciales al interior de la ARC[4] y de las otras organizaciones; que permitan que estas sean eficientes para la mitigación y neutralización de incidentes informáticos, afectando de manera positiva la ciberseguridad, permitiendo disminuir la incertidumbre y generando mayor sinergia operacional y ventaja competitiva en pro de obtener mayor seguridad y anticipación ante posibles amenazas que quieran afectar al país.

---

[3] Sigla de: Fuerzas Militares de Colombia
[4] Sigla de: Armada Nacional de Colombia

Partiendo de lo anterior, se buscó identificar el problema de seguridad informática en la ARC, la estructura, la dinámica, las experiencias, actividades, interacciones, percepciones, interpretaciones, similitudes y diferencias de los CSIRT; para luego poder describirlas, interpretarlas y comprenderlas de manera holística, reflexiva y abierta, permitiendo emitir y desarrollar recomendaciones y conclusiones que permitan dilucidar el problema planteado y establecer caminos u hojas de ruta futuras para ampliar el conocimiento y lograr desarrollar el objetivo general de la presente monografía de grado.

Dando lugar al acercamiento conceptual y al prototipo organizacional del CSIRT que permitió definir servicios, y que posteriormente cuente con el personal y las herramientas para desarrollar las funciones de respuesta de incidentes de ciberseguridad, que permitan maximizar las capacidades y generar una dinámica proactiva ante la posible afectación de las infraestructuras críticas de la ARC.

Es decir, se hace necesario establecer las necesidades de la organización para pensar en implementar el CSIRT de la ARC, apoyados en la experiencia, la perspectiva, la asesoría de expertos (Internos y externos) y buenas prácticas internacionales, teniendo claro: "Que se quiere, Como se quiere lograr y cuál es el Fin planteado".

¿Cómo debería ser el prototipo organizacional del CSIRT de la ARC para prestar respuesta a incidentes de seguridad informática?

II. METODOLOGÍA

La presente monografía de grado se desarrolló mediante la aplicación del método de investigación cualitativo (Izcara, 2014) mediante la compilación y análisis de experiencias apoyadas en el uso de metodologías y buenas prácticas de un CSIRT; es decir, se realizó la recopilación de información afín con los CSIRT; igualmente se utilizó el modelo de racionalidad limitada (Rodríguez, 2013), tomando como entrada la información recolectada y analizada, así como la experiencia y experticia del equipo de trabajo conformado por el personal técnico de la Dirección de Tecnologías de la Información y las comunicaciones, la Dirección Cibernética Naval, la Oficina de Planeación ARC y el personal de la División de Informática con el fin de analizar la documentación, y obtener un acercamiento conceptual de un Prototipo del CSIRT: Caso Armada Nacional de Colombia.

Igualmente se busca identificar la naturaleza del problema al interior de la ARC, las experiencias del personal experto orgánico de la institución, documentación existente para luego poder describirlas, interpretarlas y comprenderlas de manera específica, reflexiva y abierta, permitiendo emitir y desarrollar recomendaciones y conclusiones que permitan dilucidar el problema planteado y establecer caminos u hojas de ruta futuras para ampliar el conocimiento y lograr desarrollar el objetivo general de la presente monografía de grado.

De igual forma el proyecto se ha desarrollado teniendo en cuenta las siguientes fases:

Etapa 1: Simplificación de la Información; En esta, se realizó el proceso de selección, recolección, consulta de información y bibliografía relacionada con el tema de estudio objeto de esta monografía, para lo cual se buscó información en internet, bibliotecas

virtuales, Google académico, libros de seguridad de la información, normas técnicas internacionales, indagaciones con expertos en seguridad de la información orgánicos de la ARC.

Dentro de esta etapa se establecen como entradas los requerimientos y necesidades que surgen del problema identificado en la institución y como salida dentro de esta son los documentos que posiblemente servirán de referencia bibliográfica, experiencias adquiridas que se utilizará para fundamentar el caso de estudio en la Armada Nacional, todo lo anterior sin descuidar el objetivo de esta etapa que es hacer más eficiente, manejable e interpretable la cantidad de información encontrada en la etapa de exploración y búsqueda de información.

Etapa 2: Categorización de la Información; En esta, se realizó lectura y análisis de la información y contenidos encontrados de forma minuciosa para determinar los documentos más determinantes y actualizados para el avance y cuerpo del trabajo, permitiendo de esta forma ir seleccionando que material puede ser útil y poderlo emplear como referencia bibliográfica.

Dentro de esta etapa se establecen como entradas los documentos e informaciones encontradas y buscadas de interés, categorizando los documentos que coadyuven a soportar la solución del problema y como salida dentro de este proceso de análisis se plasmó dentro del desarrolló de una matriz de vigilancia tecnológica que agrupa la información más relevante que sirvió como bibliografía dentro de la presente monografía.

Etapa 3: Redacción y Elaboración Final Documento de Monografía; En esta, se plasma el producto final de la observación y análisis de la información trabajada en las etapas

anteriores, se elabora el documento de grado, donde se consigna los diferentes conceptos y marco teórico que apoyen el acercamiento conceptual de un Prototipo del CSIRT: Caso Armada Nacional de Colombia, mediante el resumen general de capacidades del CSIRT, la realización de un análisis cuantitativo de los incidentes al interior de la Armada Nacional durante el año 2018, descripción de los beneficios y servicios básicos, la metodología integrada para el diseño de un CSIRT para la ARC, la gestión de interesados, el prototipo organizacional del CSIRT, así como la descripción de la división CSIRT.

III. OBJETIVO GENERAL

A partir del criterio SMART (Centro de Apoyo al Desempeño Académico, s.f) el cual hace referencia a la definición precisa y clara de los objetivos y metas del proyecto, estos criterios son inmensamente útiles y cruciales al momento de realizar la definición de los objetivos en pro de la planificación y gestión del mismo, teniendo en cuenta lo anterior, se construyó el siguiente SMART para lograr el Acercamiento Conceptual de un Prototipo del CSIRT: Caso Armada Nacional de Colombia y como resultado del mismo se desarrollaron los siguientes objetivos.

3.1 Objetivos

El principal objetivo de la monografía de grado consiste en Establecer los parámetros iniciales conceptuales para el diseño de un Prototipo del CSIRT: Caso Armada Nacional de Colombia.

El objetivo principal se puede descomponer en los siguientes Objetivos Específicos:

1. Determinar los conceptos necesarios para establecer los parámetros iniciales conceptuales para el diseño de un Prototipo del CSIRT: Caso Armada Nacional de Colombia.
2. Establecer los lineamientos (capacidad) y servicios que prestaría el prototipo del CSIRT acorde a las necesidades de la Armada Nacional.

3. Plantear la metodología y el prototipo de organigrama del CSIRT de la ARC que permita mejorar la sinergia operacional cibernética y la seguridad informática en las operaciones.

IV. CAPITULO No. I - DETERMINAR LOS CONCEPTOS NECESARIOS PARA ESTABLECER LOS PARÁMETROS INICIALES CONCEPTUALES PARA EL DISEÑO DE UN PROTOTIPO DEL CSIRT: CASO ARMADA NACIONAL DE COLOMBIA.

Dentro del presente capitulo, el lector encontrará los orígenes, algunos de los CSIRT en Latinoamérica y su función, que es, los diferentes beneficios, los tipos y los servicios de los CSIRT, todo esto con el fin de que el lector entienda y conozca los antecedentes, así como los conceptos necesarios para establecer los parámetros iniciales conceptuales para el diseño de un prototipo del CSIRT: Caso Armada Nacional de Colombia.

4.1 Origen

La red ARPANET (Advanced Research Projects Agency Network), fue una red utilizada como medio de comunicación entre computadores de instituciones académicas y estatales separadas geográficamente y se considera como el predecesor de Internet.

En el año 1988 ARPANET fue atacada por un programa conocido como "gusano de internet", el cual se propagaba y replicaba solo valiéndose de las vulnerabilidades de seguridad del sistema operativo de la mayoría de los ordenadores, afectó casi el 10% de los sistemas conectados a esta red (Ministerio de comunicaciones, 2008; Centro Criptológico Nacional, 2011; Mejía, Muñoz & Uribe, 2015). La reacción a este ataque fue aislada y

descoordinada, lo cual se vio representado en duplicación de esfuerzos y conflictos en la búsqueda de soluciones.

Por lo tanto, se organizó un equipo conformado por expertos de las universidades MIT, Berkley y Purdue, con el fin de determinar y rectificar las vulnerabilidades del sistema operativo y de igual forma plantear y transmitir procedimientos de eliminación. Consecuentemente, una de las primeras acciones de DARPA (Defense Advanced Research Projects Agency), agencia federal del Departamento de Defensa de Estados Unidos, fue el primero en establecer un centro coordinado de equipos de respuesta a emergencias informáticas – CERT/CC, para responder a las amenazas de seguridad informática.

Este centro serviría como punto focal para la identificación y reparación de vulnerabilidades, dentro de sus funciones está el desarrollo de una red de contactos claves, incluidos expertos técnicos, contactos de la industria y agencias investigativas. Fue así como este incidente promovió la necesidad de cooperación y coordinación multinacional para afrontar este tipo de ataques, y la creación del primer CSIRT: CERT/CC, localizado en la Universidad de Carnegie Mellon, en Pittsburgh (Pensilvania, Estados Unidos) (ENISA, 2006; Ministerio de comunicaciones, 2008; Skierka, Morgus, Hohmann & Maurer, 2015).

Posteriormente se crearon varios equipos de expertos en universidades norteamericanas con el fin de analizar la seguridad de las redes y dispositivos, y ofrecer servicios de respuesta a incidentes, informar amenazas y solucionar las vulnerabilidades respecto a la seguridad de estos sistemas. A principios de los años noventa con ayuda del programa técnico de TERENA (Asociación Trans-europea de Redes Nacionales de

Investigación y Educación.), que hoy en día se conoce como GÉANT, se crearon los primeros CERTs en Europa.

El primer CERT se creó en Holanda en el año 1992, conocido como SURFnet-CERT, y un año después se creó el BSI-CERT en Alemania. En 1994 la Universidad Politécnica de Cataluña creó el CERT-UPC y, un año después, en 1995 se formó el Iris-CERT, en América Latina el primer CSIRT nacional se creó en Brasil en 1997. Desde entonces la cantidad de CSIRTs ha incrementado a nivel mundial, según las cifras de FIRTS - Forum of Incident Response and Security Teams (2017), para el año 2016 el total de CSIRT ascendía a 369, cabe resaltar que cada uno cuenta con su objetivo, financiación, difusión y área de influencia. (Centro Criptológico Nacional, 2011; ENISA, 2006; Ministerio de Comunicaciones, 2008; Skierka, et al., 2015). (Ver ilustración No. 1).

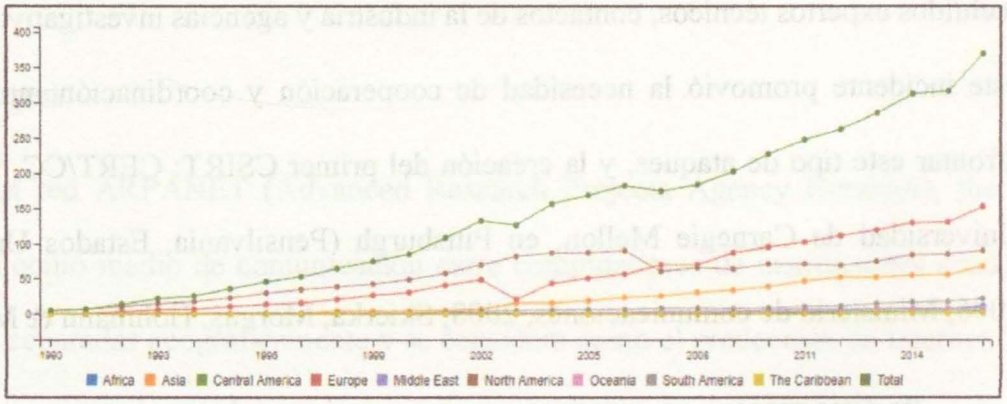

Ilustración 1: Crecimiento del Número de CSIRTs Miembros de FIRTS. Fuente: Tomada de https://www.first.org/about/history

A finales de los años noventa para complementar sus capacidades los CERT empezaron a implementar servicios preventivos y servicios de gestión de la seguridad y se

promovió el uso del término CSIRT, aunque actualmente son considerados sinónimos. (ENISA, 2006).

Desde el año 2000 Internet ha presentado un crecimiento exponencial, según cifras de Internet World Stats, (2017) para el 2017 el crecimiento de usuarios ha sido del 900% lo que representa que más del 50% de la población mundial utiliza internet para actividades económicas y sociales, este crecimiento también conlleva riesgos inherentes de seguridad digital que deben ser gestionados permanentemente debido a las múltiples fuentes de agresión a las que se ven expuestos los usuarios.

Igualmente, la Unión Internacional de Telecomunicaciones (2019), estima que, a fines de 2019, el 53,6% de la población mundial, o 4.100 millones de personas, está utilizando Internet.

En el caso específico de Colombia se está desarrollando una política nacional de seguridad digital enfocada en la gestión de riesgos cuyo objetivo es evitar la materialización de amenazas con sus posteriores efectos económicos y sociales procurando por la integridad de los ciudadanos en el medio digital y contribuir al crecimiento de la economía digital nacional (CONPES, 2016).

4.1.1 CSIRT en Latinoamérica y su Función

Dentro de la presente tabla se muestran algunos de los diferentes CSIRT en Centro y Sur América, los cuales han venido operando de forma articulada en pro de la ciberseguridad de cada una de sus naciones. La siguiente tabla fue construida mediante la recopilación de la información relevante encontrada en cada una de las páginas web oficiales de cada uno de

los países y CERT acá relacionados, así como del informe ciberseguridad 2016 que tiene como título ¿Estamos preparados en américa latina y el caribe? (Observatorio de la Ciberseguridad en América Latina y el Caribe, 2016).

Tabla 1: Cuadro comparativo de los CSIRT en Latinoamérica, población, penetración del internet y su Función.

Ítem	CSIRT Nacional	Nombre CSIRT	Población	Acceso Internet	Penet / Internet	Función / Descripción
1	Argentina	ICIC-CERT	42.980.026	27.937.016	65 %	Centraliza y coordina los esfuerzos para el manejo de los incidentes (Administración Pública Nacional). Cumple funciones de naturaleza eminentemente técnica.
2	Bolivia	CSIRT-BO	10.561.887	4.119.136	39 %	Prevención, detección y gestión de incidentes generados en los sistemas de información de la Administración Pública Nacional y Entes Públicos.
3	Brasil	CERT.Br	206.077.898	119.525.181	58 %	Gestión del Internet brasileño, responsable de recibir, analizar y responder a incidentes. Ayuda a la creación de CSIRTs en el Brasil.
4	Chile	CSIRT-CL	17.762.647	12.789.105	72 %	Fortalecer, promover leyes, buenas prácticas, políticas, reglamentos, protocolos y estándares de ciberseguridad en los órganos del Estado, las Infraestructuras Críticas del país y la República de Chile. Desarrollar un ecosistema digital seguro y resiliente, con la creación de una capacidad de respuesta preventiva, reactiva y proactiva.
5	Colombia	colCERT	47.791.393	25.329.438	53 %	Coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y la defensa nacional.
6	Costa Rica	CSIRT-CR	4.757.606	2.331.227	49 %	Coordinar con los poderes y bancos del Estado, instituciones autónomas, empresas en pro de la seguridad informática y cibernética. Busca prevenir y responder ante incidentes de seguridad cibernética

						e informática que afecten a las instituciones gubernamentales.
7	Ecuador	ecuCERT	15.902.916	6.838.254	43 %	Contribuye a la seguridad de las redes de telecomunicaciones del país y así como al uso del internet. Su alcance se enmarca en la aplicación de la Ley Orgánica de Telecomunicaciones (LOT)
8	El Salvador	SalCERT	6.107.706	1.832.312	30 %	Prevención constante de las vulnerabilidades, coordinando con las instituciones públicas y privadas para el fortalecimiento constante de la ciberseguridad. Mantener una infraestructura de TI.
9	Guatemala	CSIRT-GT	16.015.494	3.683.564	23 %	Coordinar los CSIRT y CERT guatemaltecos, advertir sobre ataques cibernéticos y mitigarlos dentro del marco legal, ayudar a identificar delitos cibernéticos y fortalecer la cooperación y coordinación internacional a través del intercambio de información.
10	Guyana	CSIRT.GY	763.893	282.640	37 %	Brindar asistencia técnica a las agencias públicas para prevenir y responder de manera efectiva a los incidentes de seguridad de la información de importancia nacional.
11	México	CERT-MX	125.385.833	55.169.767	44 %	Prevenir y mitigar las amenazas de seguridad informática que ponen en riesgo la infraestructura tecnológica y la operatividad del país.
12	Panamá	CSIRT-Panamá	3.867.833	1.740.525	45 %	Prevención, identificación, tratamiento y resolución de ataques e incidentes de seguridad sobre los sistemas informáticos de las infraestructuras críticas del país y el acceso a la información de parte de los ciudadanos de Panamá.
13	Paraguay	CERT-PY	6.552.518	2.817.583	43 %	Coordinador central para las notificaciones de incidentes de seguridad en Paraguay, dando el apoyo necesario para dar respuesta.
14	Perú	PeCERT	30.973.148	12.389.259	40 %	Liderar los esfuerzos para resolver, anticipar y enfrentar los desafíos informáticos y coordinar la defensa ante los Ciberataques, con el fin de proveer a la Nación de una postura Segura en el Ámbito de la Seguridad Informática.
15	Trinidad y Tobago	TT-CSIRT	1.354.483	880.414	65 %	Responder a incidentes cibernéticos, a través de técnicas de respuesta efectivas, educación,

						capacitación, concientización, investigación, colaboración y estrategias de gestión eficientes, a fin de restaurar las operaciones de los sistemas de información de nuestros constituyentes. El CSIRT es fue un objetivo estratégico de la Estrategia Nacional de Seguridad Cibernética 2015.
16	Uruguay	CERTuy	3.419.516	2.085.905	61 %	Proteger los activos de información críticos del Estado y promover la conciencia en seguridad de la información de manera que prevenga y responda a incidentes de seguridad.
17	Venezuela	VenCERT	30.693.827	17.495.481	57 %	Prevención, detección y gestión de los incidentes generados en los sistemas de información de toda la Administración Pública Nacional y sectores públicos a cargo de la gestión de infraestructuras críticas de la nación.

Fuente: Observatorio de la Ciberseguridad en América Latina y el Caribe. (2016).

En la tabla anterior, se pueden observar que el país con mayor penetración de internet es chile con un 72 %, y el de menor es Guatemala con un 23 %, dentro de una muestra de 17 países; igualmente realizando un promedio general de los otros 15 países se puede establecer que estos se encuentran entre un 48,6 %.

Por otra parte, basado en el modelo de racionalidad limitada se puede decir que, con el incremento y penetración del internet en cada uno de ellos, es posible que aumente el número de incidentes informáticos que pueden presentarse, viéndose que son directamente proporcionales, por lo cual se hace importante y es de resaltar que estas naciones ya cuentan con CSIRT implementados y en operación para atender todas amenazas potenciales que se les puedan presentar en el ciberespacio.

4.2 ¿Qué es un CSIRT?

El término CSIRT por sus siglas en inglés (Computer Security Incident Response Team), significa equipo de respuesta a incidentes de seguridad informática, también es conocido por otros acrónimos referentes a la gestión de incidentes informáticos (ENISA, 2006; Killmeyer, 2006; Ministerio de Comunicaciones, 2008):

A) CERT o CERT/CC (Computer Emergency Response Team / Coordination Center, equipo de respuesta a emergencias informáticas / Centro de coordinación). Marca registrada en Estados Unidos.

B) CIRC (Computer Incident Response Capability, Capacidad de respuesta a incidentes informáticos)

C) CIRT (Computer Incident Response Team, equipo de respuesta a incidentes informáticos)

D) CSIRC (Computer Security Incident Response Capablity, capacidad de respuesta a incidentes de seguridad informática)

E) IHT (Incidence Handling Team, equipo de manejo de incidentes)

F) IRC (Incident Response Center/ Incident Response Capability, capacidad de respuesta a incidentes)

G) IRT (Incident Response Team, equipo de respuesta a incidentes)

H) SERT (Security Emergency Response Team, equipo de respuesta a emergencias de seguridad)

I) SIRT (Security Incident Response Team, equipo de respuesta a incidentes de seguridad)

Un CSIRT es una organización, equipo, o capacidad de una entidad que tiene como objetivo prevenir, gestionar y responder de forma rápida y efectiva a incidentes o ataques de seguridad informática contra los sistemas de la comunidad a la cual se le presta el servicio (Centro Criptológico Nacional, 2011; Ministerio de Comunicaciones, 2008).

Sin embargo el término CSIRT ha evolucionado de acuerdo a la ampliación de los servicios que prestan, puesto que no solo gestionan los incidentes sino que adicionalmente prestan otros servicios para mitigar riesgos y para la reparación después de que ha sucedido un incidente, según recomendaciones de ENISA, Agencia de Seguridad de las Redes y de la Información de la Unión Europea, es necesario incluir el análisis forense y la gestión de vulnerabilidades en los servicios que presta un CSIRT (Centro Criptológico Nacional, 2011; OEA2016).

La OEA (2016) afirma:

> Los equipos que surgieron principalmente para responder a incidentes han evolucionado y ahora con frecuencia están orientados a ser un modelo integral de gestión de seguridad de la información. En efecto, mientras que el alcance de los CSIRT se limitaba en gran medida a prestar servicios de "respuesta", hoy en día cada vez más adoptan una postura proactiva. Se centran en la prevención y en la detección de incidentes, lo que logran por medio de una mezcla de habilidades y formación de la conciencia, alertas y monitoreo, así como de la difusión de información relacionada con seguridad de la información, el desarrollo de planes de continuidad de negocio, y

el desarrollo de documentos de mejores prácticas y de análisis de vulnerabilidades, entre otros. (p.7).

Un claro ejemplo de la evolución que ha presentado el término CERT o CSIRT es la modificación realizada por el US-CERT (CERT del Departamento de Seguridad Nacional de Estados Unidos), donde el significado de la letra "R" en el acrónimo cambio de significar Response (respuesta) a significar Readiness (preparación), lo que evidencia un cambio en el enfoque proactivo de estos equipos (Centro Criptológico Nacional, 2011).

4.3 Beneficios de un CSIRT

Dentro de la implementación de un CSIRT se conducen múltiples ventajas basado en lo que establece y precisa el (Centro Criptológico Nacional, 2011; ENISA 2006), entre ellas están:

A) Disponer de un equipo centralizado que desarrolle sus actividades bajo políticas y procedimientos establecidos, en pro de identificar y mitigar los riesgos emergentes de forma efectiva.
B) Mejorar los tiempos de respuesta en gestión y tratamiento de incidentes.
C) Aumentar la capacidad de coordinación y comunicación con otros CSIRTs.
D) Ofrecer los conocimientos técnicos necesarios para apoyar y asistir a los usuarios que necesitan recuperarse rápidamente de algún incidente de seguridad.
E) Ahorrar en costos al contar con el conocimiento especializado en un solo punto de contacto, desde el cual se transmitirá a todo el público.
F) Mejorar en la gestión de la calidad de la seguridad de la información.

G) Ampliar los conocimientos de los usuarios mediante el suministro de los aspectos técnicos necesarios para prevenir entornos de riesgo y aumentar el grado de sensibilización de los mismos.

H) Actuar como centro de gestión y coordinación en los aspectos normativos y jurídicos relacionados con los incidentes informáticos y custodio de las evidencias, cuando sea necesario

I) Pertenecer a asociaciones o foros permite conocer los progresos conseguidos a nivel mundial relacionados con la seguridad informática.

J) Implementar indicadores de servicio, calidad, costos y demás temas relacionados con la gestión de los incidentes de seguridad informática.

K) Promover la comunicación y participación en la seguridad de las TICs (Tecnologías de la Información y la Comunicaciones) entre los usuarios a los que presta los servicios.

4.4 Tipos de CSIRT

El propósito y las responsabilidades de un CSIRT varían de acuerdo a los objetivos, la estructura de la organización en la cual se desea implementar y la comunidad objetivo, por lo cual existen diferentes tipos de CSIRT, sin embargo, la clasificación varía de acuerdo al autor como se evidencia en la Ilustración No. 2 (CERT-a, s.f; ENISA, 2006, Killmeyer, 2006; OEA, 2016; Skierka, et al., 2015):

OEA, 2016	Skierka, et al., 2015	ENISA, 2006	CERT-a, s.f
• Académicos • Comerciales • Infraestructuras críticas • Gubernarmentales • Nacionales • Militares • Proveedores • PYMEs	• Nacionales • Sectorial • Organizacional • Proveedores • Comercial	• Académico • Comercial • Infraestructura crítica • Publico • Interno • Militar • Nacional • PYMEs • Soporte	• Interno • Nacional • Centros de coordinacion • Centros de análsis • Proveedores • Comercial

Ilustración 2: Tipos de CSIRTs de Acuerdo a Diferentes Autores. Fuente: Elaboración Propia.

Para fines prácticos en el presente trabajo se tomará la clasificación de CSIRT realizada por la OEA (2016):

4.4.1 CSIRT Académicos

Prestan sus servicios a comunidades académicas, universidades, facultades, escuelas, institutos, centros de investigación y a sus campus virtuales, frecuentemente unifican esfuerzos con otros CSIRT académicos y se pueden especializar en investigaciones. (OEA, 2016).

4.4.2 CSIRT Comerciales

Cuando las organizaciones no cuentan con un CSIRT propio prefieren subcontratar los servicios de gestión de respuesta a incidentes y es ahí donde actúan los CSIRT comerciales, los cuales ofrecen servicios pagos de manejo de incidentes a otras organizaciones. (OEA, 2016).

4.4.3 CSIRT de Infraestructuras Críticas

Son los establecidos para la protección de la información crítica y la infraestructura critica de una nación. (OEA, 2016).

4.4.4 CSIRT Gubernamentales

Son aquellos CSIRT que brindan sus servicios a las instituciones del Estado, con el fin de prevenir incidentes que pongan en riesgo la seguridad de la infraestructura de las tecnologías de la información y de la comunicación del gobierno y que puedan llegar afectar los servicios que prestan a los ciudadanos. (OEA, 2016).

4.4.5 CSIRT Nacionales

Son el punto de contacto principal para asuntos técnicos para las partes interesadas en la respuesta de un incidente que afecte una nación y también son punto de contacto para otros CSIRT nacionales alrededor del mundo. Otra característica es que los CSIRT nacionales deben estar autorizados o formalmente reconocidos por el gobierno al que pertenecen. Los CSIRT nacionales también se consideran como CSIRT de último recurso, puesto que encargan de dar respuesta a los incidentes que no están en el alcance de otro equipo. (OEA, 2016).

4.4.6 CSIRT Militar

Dentro de la presente monografía se plantea que el tipo de CSIRT que más se adapta a las necesidades propias dentro de la Armada Nacional por su rol y función constitucional

será el militar que busca brindar servicios a las instituciones militares las cuales tienen dentro de sus funciones prevenir y contrarrestar toda amenaza de naturaleza cibernética que afecte los valores e intereses de una nación. Adicionalmente, operan las TIC para uso específico militar, incluyendo, por ejemplo, armamento, sistemas de comunicaciones militares, sistemas de armas y radares. (OEA, 2016).

4.4.7 CSIRT de Proveedores

Este tipo de CSIRT tiene como objetivo identificar las vulnerabilidades de un producto específico y mitigar las posibles fallas de seguridad, de igual forma manejan el reporte de las vulnerabilidades en sus productos de software y hardware. (OEA, 2016).

4.4.8 CSIRT PYME

Son los CSIRT que prestan servicios a las empresas de este sector de negocios. (OEA, 2016).

4.5 Servicios de los CSIRT

Una de las principales tareas y que requieren mayor atención durante la creación de un CSIRT es tomar la decisión de cuáles serán los servicios que se ofrecerán a la comunidad objetivo. El conjunto de servicios determinará los recursos, habilidades, y asociaciones que el equipo del CSIRT necesita para funcionar correctamente. La selección de los servicios deberá ser coherente con los objetivos de la comunidad objetivo y de igual forma deberán ser

realistas basados en el tamaño y experiencia del equipo. (CERT-b, s.f; West-Brown, et al., 2003).

La misión de un CSIRT tiene principalmente tres componentes: servicios, políticas y calidad (West-Brown, et al., 2003); Los servicios prestados por un equipo son los métodos usados para llevar a cabo la misión, las políticas son los principios bajo los cuales el equipo trabaja y la calidad es el estándar deseado en el cual todas las actividades deben ser desarrolladas; Igualmente tomando como referencia la estructura del marco de servicios del equipo de respuesta a incidentes de seguridad informática (CSIRT), donde plantea cuatro elementos claves catalogados así: áreas de servicio, servicios, funciones y subfunciones (FIRST, 2019); Las áreas de servicio son aquellas que agrupan servicios relacionados entre sí o que tienen aspectos en común con el fin de tener una mejor organización de los servicios, los servicios son vistos como un conjunto de funciones reconocibles y coherentes orientadas a resultados específicos, las funciones son el conjunto de actividades orientadas a desarrollar un fin específico, las subfunciones son actividades orientadas a cumplir con una función particular.

Cada uno de los servicios que ofrece un CSIRT debe estar lo más detallado posible y debe contener una descripción de los siguientes atributos, ver tabla No. 2 (West-Brown, et al., 2003); Igualmente, dentro del marco de servicios CSIRT (FIRST, 2019); manifiesta que los servicios se deben describir teniendo en cuenta los resultados esperados o requeridos por las partes interesadas de la entidad y propone la siguiente plantilla:

a. Un campo "Descripción" donde se plasma y se describe la naturaleza del servicio.

b. Un campo "Propósito" donde se describe la intención específica del servicio.

c. Un campo "Resultado" donde se describe o describen los resultados esperados y medibles del servicio.

Las descripciones de los servicios son de gran utilidad parar el equipo al momento de definir, implementar y desarrollar el servicio, de igual forma son útiles para aterrizar las expectativas de la comunidad objetivo respecto al servicio ofrecido (West-Brown, et al., 2003).

Tabla 2: Descripción de los Atributos de un Servicio.

Atributo	Descripción
Objetivo	Se busca definir el propósito y naturaleza del servicio
Definición	Se plantea la descripción del alcance del servicio y grado de profundidad en el que el CSIRT lo ofrece
Función	Se establece la descripción de las funciones de cada una de las partes en la prestación del servicio.
Disponibilidad	Las condiciones bajo las cuales el servicio está disponible (para quien, cuando y como).
Aseguramiento de la Calidad	Se definen los parámetros de aseguramiento de la calidad aplicables al servicio.
Interacciones y Divulgación de Información	Se definen las interacciones entre el CSIRT y las partes afectadas por el servicio. Definición de la estrategia con respecto a la divulgación de información.
Interfaces con otros Servicios	Se definen y especifican los puntos de intercambio del flujo de la información entre este servicio y otros servicios del CSIRT con los que interactúa.
Prioridad	Se definen las prioridades relativas de las funciones dentro del servicio, y del servicio frente a otros servicios CSIRT.

Fuente: West-Brown, et al., 2003; Centro Criptológico Nacional, 2011).

Los CSIRT deberán reevaluar periódicamente los servicios que ofrecen con el fin de adaptarse al constante cambio tecnológico, técnico y por consiguiente a las amenazas que

surgen, cabe resaltar que dichos cambios deben ser informados a su comunidad objetivo (West-Brown, et al., 2003).

4.5.1 Categorías de los Servicios

Existen variedad de servicios que un CSIRT puede ofrecer, los servicios que cada CSIRT ofrece están basados en la misión, propósito y comunidad objetivo. Para que un equipo sea considerado un CSIRT debe por lo menos ofrecer el servicio de tratamiento de incidentes. Los servicios de los CSIRT se clasifican en tres categorías (ver ilustración No. 3), servicios reactivos, servicios proactivos y servicios de gestión de calidad de la seguridad.

Ilustración 3: Servicios de un CSIRT. Fuente: (OEA, 2016; West-Brown, et al., 2003)

4.5.1.1 Servicios Reactivos

Son los servicios más importantes que ofrece un CSIRT. En esencia, los servicios reactivos facilitan la respuesta a los incidentes de seguridad cibernética que ocurren en el sector del CSIRT o en su propia infraestructura, estos se pueden derivar de una solicitud de asistencia o de la notificación de terceros o mediante la visualización de registros de un host comprometido, un código malicioso (amenaza o ataque) de amplia difusión y vulnerabilidad de software o algo identificado por un sistema activo de alertas como un sistema de detección de intrusiones (IDS) propio de la entidad u organización; así mismo estos servicios tienen como fin la gestión de incidentes, la respuesta de vulnerabilidades y la respuesta a artefactos (OEA, 2016; West-Brown, et al., 2003).

Este tipo de servicios buscar obtener una atención efectiva de los diferentes eventos e incidentes que afecten la seguridad de las redes e información, todos estos tienen como fin el restablecer la operación, minimizar y mitigar el impacto causado ante la eventualidad de un ataque o afectación a la infraestructura de TIC, dentro de estos servicios se pueden presentar los siguientes: análisis de vulnerabilidades, pruebas de calidad de software, asesoría, atención a usuarios, análisis de incidentes, reportes y recomendaciones.

4.5.1.2 Servicios Proactivos

Son aquellos que buscan anticipar la acción de la amenaza y tiene como objetivo mejorar la seguridad de la comunidad objetivo, mediante la prevención de incidentes o la reducción del impacto cuando se producen. Si los servicios proactivos funcionan de forma

apropiada se reducirá el número de incidentes en el futuro (OEA, 2016; West-Brown, et al., 2003).

Estos servicios se diferencian de los otros porque su fin primordial es prever y anticipar futuros ataques mediante la identificación de patrones o posibles vectores de ataque, estos suministran ayuda con el fin de implementar medidas para proteger y asegurar las infraestructuras tecnológicas dentro de estos servicios se pueden presentar los siguientes: alertas tempranas, vigilancia tecnológica, difusión de boletines, observatorio, monitoreo y análisis de comportamiento de eventos.

4.5.1.3 Servicios de Gestión de Calidad de la Seguridad

También se conocen como servicios de valor agregado, puesto que al prestar estos servicios el CSIRT ayuda a mejorar la seguridad de la comunidad objetivo, identificando los riesgos, amenazas y debilidades del sistema, mediante el análisis de riesgos, la sensibilización y formación de la comunidad objetivo. De igual forma, los servicios de gestión de la calidad se retroalimentan de las experiencias adquiridas durante la prestación de los servicios reactivos y proactivos (OEA, 2016; West-Brown, et al., 2003).

V. CAPITULO No. II - ESTABLECER LOS LINEAMIENTOS Y SERVICIOS QUE PRESTARÍA EL PROTOTIPO DEL CSIRT ACORDE A LAS NECESIDADES INICIALES DE LA ARMADA NACIONAL.

Dentro del presente capítulo el lector encontrara un contexto geopolítico del CSIRT, los lineamientos y capacidades inherentes al prototipo del CSIRT, las necesidades de implementación, los servicios básicos propuestos y las etapas planteadas para lograr una madurez en el tiempo, todo esto con el fin de que el lector entienda y conozca la relevancia institucional que genera contar con este tipo de equipos al interior de la entidad para la gestión de los incidentes en la ARC.

5.1 Contexto Geopolítico del CSIRT en la Región para la Ciberseguridad y la Ciberdefensa de un Estado

Analizar el impacto que se puede generar a nivel regional el desarrollo de un Equipo de Respuesta a Incidentes de Seguridad (CSIRT), implica una revisión exhaustiva de las competencias tecnológicas con las que cuentan los Estados que conforman la región suramericana y las amenazas potenciales a nivel regional, en lo que concierne a las capacidades para ejercer una guerra de la información y una ciberseguridad apropiada de sus intereses (García, 2017).

Las Fuerzas Armadas de todo el mundo en la actualidad dependen de las tecnologías de la información para mantener y desarrollar operaciones militares en las cinco dimensiones

de la geopolítica: dimensión terrestre, dimensión marítima, poder aéreo, poder combinado y los poderes aeroespacial y ciberespacio (Gil, 2017).

Por tal motivo, el ciberespacio cada día toma más terreno y esto se evidencia en la masificación del internet en el mundo, el acceso a herramientas tecnológicas por parte de los individuos, grupos delincuenciales y agentes generadores de violencia, lo que constituye un potencial riesgo para los estados, es por esto que deben estar preparados para afrontar estas nuevas formas de lucha, según (Choucri, 2000) todo esto sumado a la disminución de los costos de las Tecnologías de la Información que han generalizado y descentralizado su acceso y utilización en múltiples fines, generando una desconcentración del poder bélico de las naciones y maximizando el nivel de las amenazas potencialmente presentes en este quinto dominio de la guerra.

Lo anterior permitirá plantearnos el siguiente interrogante ¿Qué tan útil es el CSIRT en el escenario geopolítico regional? lo cual concibe importante establecer y entender que dentro de sus funciones los Estados tienen como función la defensa de la soberanía nacional frente a otro Estado. Así como ejercer el papel fuerte y decidido para proveer de seguridad a sus nacionales incluso en el ciberespacio (Eriksson & Giacomello, 2006).

El CSIRT es importante en el escenario geopolítico regional porqué es una alternativa a la vulnerabilidad de la seguridad regional que se ha generado por la dinámica comercial que supone el aumento de empresas y proveedores de seguridad, que consolidan redes transnacionales e individuos que laboran de manera independiente y que pueden ser desafiantes a la seguridad y a la estabilidad regional, al poder establecer alianzas con

potencias extra regionales que pueden ser generadoras de tensiones entre los Estados que conforman la región (Nye, 2004).

Igualmente, afirma que el poder blando adquiere vital relevancia en la era digital, ya que puedes obtener que otros actores realicen ataques o intrusiones a las redes sin recurrir a presiones o temas de dinero, ya que muchos atacantes realizan estos tipos de actividades por obtener y/o adquirir una reputación, esto ha incrementado debido a la evolución de múltiples canales de comunicación global que trascienden fácilmente la soberanía de las fronteras. Por tal motivo las amenazas que se generan de la falta de una seguridad cibernética y generan preocupaciones e incertidumbres a la sociedad y un riesgo a la seguridad del estado.

Actualmente las redes de computación, sistemas e informática instituyen y establecen un factor primario para el desarrollo social, económico, militar y tecnológico de un país, mencionadas redes hoy en día se han transformado en una buena parte en servicios públicos esenciales y universales, del mismo modo estas son utilizadas para soportar y brindar servicios de gestión y control a redes de infraestructuras públicas como las de agua potable, aeropuertos y la electricidad, entre otros, es tan así, que se han presentado ataques mediante el uso de troyanos, un ejemplo de esto fue el ataque realizado a ucrania el 23 de diciembre con el troyano BlackEnergy, el cual logro dejar sin electricidad a 1,5 millones de habitantes, otro caso similar se presentó en noviembre del 2015 afectando cadenas de televisión y medios (CERTSI, 2016).

Es por esto que la seguridad de las redes de comunicación, el internet de las cosas, informática y sistemas de información, demandan que los países sean conscientes de la importancia para el desarrollo de una nación, los sistemas de información cada vez están más

presentes en los servicios críticos e infraestructuras críticas que prestan servicios vitales para el bienestar de los ciudadanos y que cada vez están más expuestos a virus, troyanos, problemas, errores y ataques informáticos que pretendan desestabilizar la seguridad interna de una nación (García, 2017).

5.2 Lineamientos y Capacidades Inherentes al Prototipo de Diseño de un CSIRT

Dentro de esta sección se plantea como pilar fundamental el uso de la metodología de planeación por capacidades (MDN, 2018), desde el punto de vista, ámbito de planeación administrativa y gestión de proyectos, es el punto de partida de todo proceso visto como la formulación del estado futuro o deseado.

Estos deben ser medidos y controlados para evitar que no lleguen al fin planeado y de encontrar variaciones desarrollar los cursos de acción oportunos para encausarlos en la dirección apropiada para alcanzar los objetivos o metas trazadas, para lograr cumplir con lo anterior, es importante asignar los recursos (humanos, técnicos, tecnológicos, dinero, tiempo, entre otros) convenientes mediante un empleo eficiente en tiempo, costo y alcance (triple restricción de la gerencia de proyectos) en pro de una excelente calidad.

Igualmente, se plantea que son todas aquellas que permiten dar respuesta a los problemas propios del entorno y lugar de actuación y dependen de las necesidades de cada fuerza (ARC) en pro de obtener y alcanzar los retos operacionales derivados de las metas y objetivos trazados, todo esto requiere de una sinergia entre el propósito, la voluntad y dimensión o alcance del mismo.

Observando estas capacidades como el fin planeado, estas deben ser objeto de análisis, medición periódica y constante por parte de la dirección y altos mandos para no perder de vista el rumbo planeado o idealizado.

La ARC dentro de su Plan Estratégico Naval (PEN) establece que

"*Para garantizar la planeación, ejecución y sostenimiento en el tiempo de las operaciones navales, se requiere del empleo de una o más de las capacidades de la Armada Nacional, las cuales fueron identificadas en los años 2016-2017, en desarrollo del programa de Transformación y Futuro 2030 de la Fuerza Pública, liderado desde el 2010 por la Dirección de Proyección de Capacidades del Ministerio de Defensa Nacional, y cuyo fundamento se sustenta en la implementación de un modelo de planeación por capacidades que permita diseñar una estructura de fuerza que se caracterice por su adaptabilidad, flexibilidad y sostenibilidad en el tiempo*". (ARC, 2015).

Tomando como antecedente lo anterior, la ARC estableció en el año 2017 un total de 69 capacidades específicas, las cuales se clasificaron en las siguientes áreas funcionales así:

A) Mando y Control
B) Inteligencia
C) Sostenimiento
D) Fuegos
E) Movimiento y Maniobra
F) Protección y Control

Las cuales deberán ser fortalecidas para contar con una estructura de fuerza[5] adecuada y moderna, que permita el cumplimiento de los objetivos estratégicos de la ARC y la Nación.

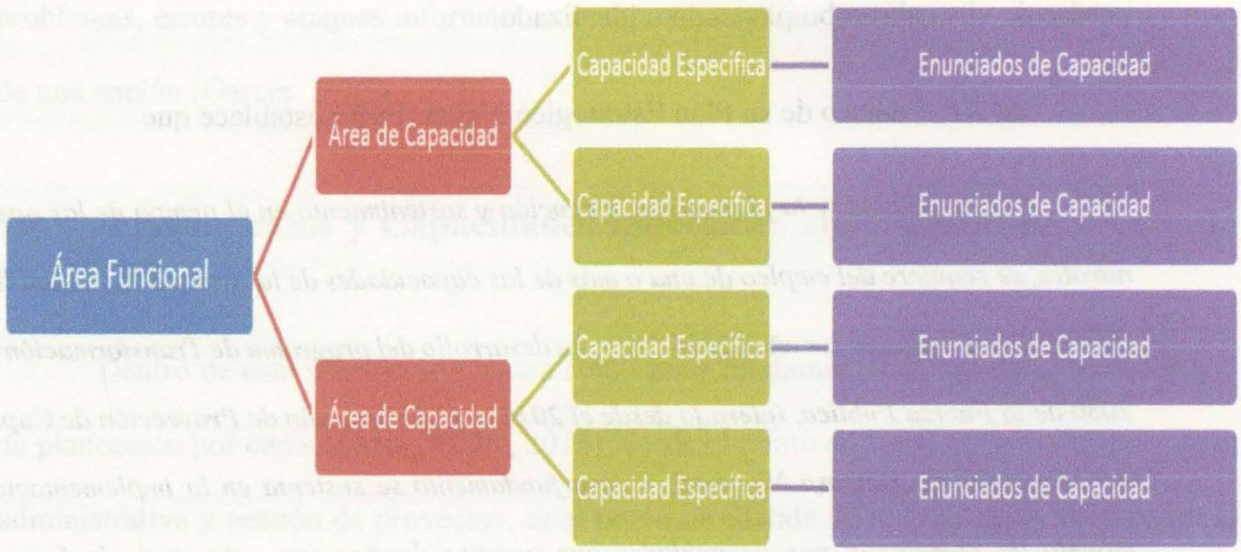

Ilustración 4: Niveles de Desagregación de las Capacidades del Sector Defensa. Fuente: Dirección de Planeación Estratégica. Jefatura de Planeación Naval. 2017.

La anterior ilustración muestra la estructura y forma como se concibieron, identificaron y clasificación las capacidades, para ellos establecieron los siguientes niveles: Área Funcional, Área de Capacidad, Capacidad Específica y Enunciados de Capacidad:

Para las Fuerzas Militares de Colombia (FFMM), la planeación por capacidades es un *"Proceso metodológico que busca identificar las necesidades en materia de seguridad y defensa, a partir de un análisis de las áreas misionales y los sistemas de capacidades requeridos para enfrentar de forma efectiva los retos del futuro. Este proceso define una combinación eficiente de estructuras de fuerza al interior del sistema de seguridad y defensa, de forma que se puedan cumplir*

[5] *Por estructura de fuerza se comprenden los distintos recursos asociados que, al ser empleados en conjunto, permiten el desarrollo de una capacidad militar o policial. En otras palabras, también hacen referencia a los componentes de capacidad DOMPIS. Dirección de Proyección de Capacidades. Ministerio de Defensa Nacional. Guía Metodológica de Planeamiento por Capacidades. Bogotá, febrero de 2017.*

los objetivos estratégicos del sector con las restricciones institucionales y financieras existentes. En este sentido, el fin último es lograr una estructura de fuerza interoperable, adaptable, flexible y sostenible". (CGFM, 2015).

En consecuencia, con lo anterior, la capacidad al interior de las Fuerzas Militares y para la ARC se representa como la habilidad de realizar una acción o tarea, bajo ciertos estándares a través de la sumatoria o integración representada en los siguientes cinco (05) componentes (DOMPI) (CGFM, 2015), igualmente durante el desarrollo de estas capacidades, la oficina de planeacion del CFGM evidencio y ordeno la incorporacion de otro componente para la estructuracion y generacion de las capacidades, la cual esta enfocada en el Soporte Logistico, cuyo unico fin es sortener en el tiempo la capacidad planeada (establece las necesidades logísticas del ciclo de vida de la capacidad); quedando finalmente como DOMPI-S.

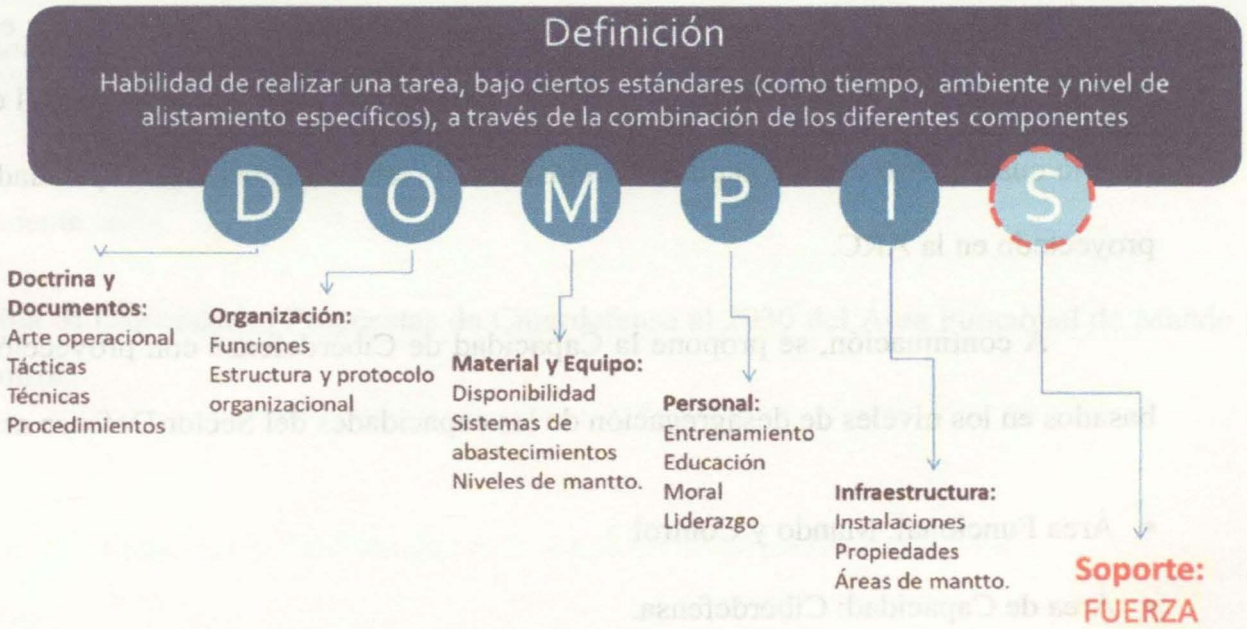

Ilustración 5: Componentes de Capacidad DOMPI-S. Fuente: Elaboración Propia.

A) **Doctrina:** Arte operacional, tácticas, técnicas, procedimientos, tareas (CGFM, 2015).

B) **Organización:** Funciones, estructura, roles y protocolo organizacional (CGFM, 2015).

C) **Material y Equipo:** Disponibilidad, niveles de mantenimiento, sistemas de abastecimiento e instrumentos de trabajo (CGFM, 2015).

D) **Personal:** Entrenamiento, educación, moral y Talento humano habilidades y competencias (CGFM, 2015).

E) **Infraestructura:** Instalaciones, propiedades y áreas de entrenamiento e implementación (CGFM, 2015).

F) ***Soporte Logístico:*** Sostenibilidad en el tiempo de la capacidad (necesidades logísticas del ciclo de vida de la capacidad) (CGFM, 2015).

Para desarrollar esta capacidad dentro de la ARC se contemplarán todos los componentes, partiendo que esta división (CSIRT) no existe en la institución y es necesaria para potencializar las capacidades específicas de la Dirección Cibernética Naval en la ARC; para lo cual, dentro de este capítulo se mostrará el resumen general de capacidades CSIRT, proyectado en la ARC.

A continuación, se propone la Capacidad de Ciberdefensa con proyección al 2030, basados en los niveles de desagregación de las capacidades del Sector Defensa así:

- Área Funcional: Mando y Control.
- Área de Capacidad: Ciberdefensa.
- Área de Capacidad Especifica: Defensa Cibernética.

- Retos al 2030: Se desarrollaron ocho (08) retos.

A continuación, y haciendo uso del modelo de racionalidad limitada y tomando como entrada la información recolectada y analizada, así como la experiencia y experticia del equipo de trabajo conformado por el personal técnico de la Dirección de Tecnología de la Información, la Dirección Cibernética Naval, Oficina de Planeación ARC y el personal de la División de Informática, se realizó el desarrollo de la misma, en donde en primera medida se identifican todas las alternativas de solución posibles para establecerlas dentro de cada uno de los ítems presentes en la tabla los cuales se organizaron así: el área funcional; el área de capacidad, área de capacidad específica y los retos al 2030.

Luego de esto se analizaron los resultados que se obtuvieron de cada uno de los bosquejos planteados, seguidamente se realizó una comparación, verificando la pertinencia, eficacia y eficiencia de cada una de las opciones planteadas para luego y finalmente escoger la solución más adecuada para la Armada Nacional.

Como resultado de la aplicación y desarrollo de la metodología se presenta la siguiente tabla.

Tabla 3: Capacidades Propuestas de Ciberdefensa al 2030 del Área Funcional de Mando y Control.

Área Funcional	Área de Capacidad	Área de Capacidad Específica	Retos al 2030
MANDO Y CONTROL	CIBERDEFENSA	DEFENSA CIBERNÉTICA	1. Mantener e innovar en la forma de alcanzar un estado de Conciencia Situacional a todo nivel sobre las amenazas cibernéticas actuales y potenciales. 2. Mantener e innovar en la forma de monitorear, enfocados a prevenir, detectar y contener ataques cibernéticos en tiempo real (7x24x365) a la infraestructura crítica cibernética naval (CSIRT – Equipo de Gestión y respuesta a Incidentes). 3. Desarrollar capacidades para dinamizar la obtención de información cibernética, mediante el establecimiento de indicadores de compromiso que afecte las infraestructuras críticas de la ARC en pro de la Ciberdefensa. 4. Innovar en el desarrollo e incorporación de capacidades de Ciberdefensa mediante la aplicación de buenas prácticas enfocadas a la protección de las infraestructuras críticas de la ARC. 5. Desarrollar acciones que permitan identificar y anticipar las amenazas en y a través del ciberespacio, así como las acciones contra la infraestructura crítica cibernética naval del país. 6. Mantener las capacidades disuasivas de la Armada en el ciberespacio y coadyuvar en el posicionamiento de Colombia a Nivel Regional en Ciberdefensa. 7. Desarrollar implementar y actualizar las capacidades de Ciberseguridad y Ciberdefensa para la Armada Nacional. 8. Desarrollar, implementar, actualizar y mantener el plan de gestión de respuesta a incidentes cibernéticos del CSIRT de la ARC.

Fuente: Elaboración Propia

Dentro de la propuesta presentada en la tabla anterior, donde se plantean las capacidades de Ciberdefensa al 2030 en la Institución, dentro de la cual se contemplan las funciones específicas y propias de un CSIRT en la ARC, las cuales se enfocarán de manera exclusiva a la protección y gestión de las infraestructuras críticas de la Armada Nacional.

5.3 Análisis de Madurez de las Capacidades de CIBER en la ARC

Dentro del presente apartado se desarrolla un análisis de madurez sobre las capacidades de CIBER, con el fin de establecer un punto de partida entre las necesidades del

CSIRT, las capacidades actuales de la Dirección Cibernética. así como las líneas futuras de apoyo e integración de capacidades para articular esfuerzos y minimizar recursos para fortalecer las capacidades de manera integral en la Armada Nacional, para lo cual se realizaron mesas de trabajo con el apoyo del personal de expertos orgánicos de la Dirección Cibernética Naval, así como de asesores externos con el interés de formalizar y estructurar la capacidad de un CSIRT en la ARC.

Dentro de la estructuración se definió que el máximo valor de evaluación es 5 y el mínimo es 1, las cuales se cruzaron con la estructura DOMPI-S y estas se trasponen dentro de cada uno de los contextos precisos para la orientación de la valoración en cada una de ellos; los cuales se presentan en la siguiente matriz de ponderación y valoración.

Tabla 4: Matriz de Evaluación – DOMPI-S.

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

5	Se cuenta con el 80% o más de la doctrina requerida y se cuenta con un plan de actualización y mejora de la misma.	La organización está estructurada y tiene el 80% de sus procesos y procedimientos estructurados. Se cuenta con un sistema de gestión de calidad implementado y funcionando.	Se cuenta con el 80% del material y equipo requerido y un plan de actualización del mismo.	Se cuenta con el 80% del personal requerido y con un plan de carrera implementado.	Se cuenta con el 80% de la infraestructura requerida	Se tienen establecidas las necesidades logísticas del 80% del ciclo de vida de los elementos que hacen parte de esta capacidad.

Fuente: Elaboración Propia.

Posterior a esto, se estructuro la matriz de madurez tomando como referencia el modelo de ciberseguridad de la OTAN, mediante el desarrollo de una matriz cruzada entre las áreas de capacidad estratégica contra la matriz DOMPI-S, dando como resultado la brecha por cada capacidad especifica.

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

Ilustración 6: Matriz de Capacidad Mediante el Uso del Modelo de Ciberseguridad OTAN – DOMPI-S.

Fuente: Elaboración Propia.

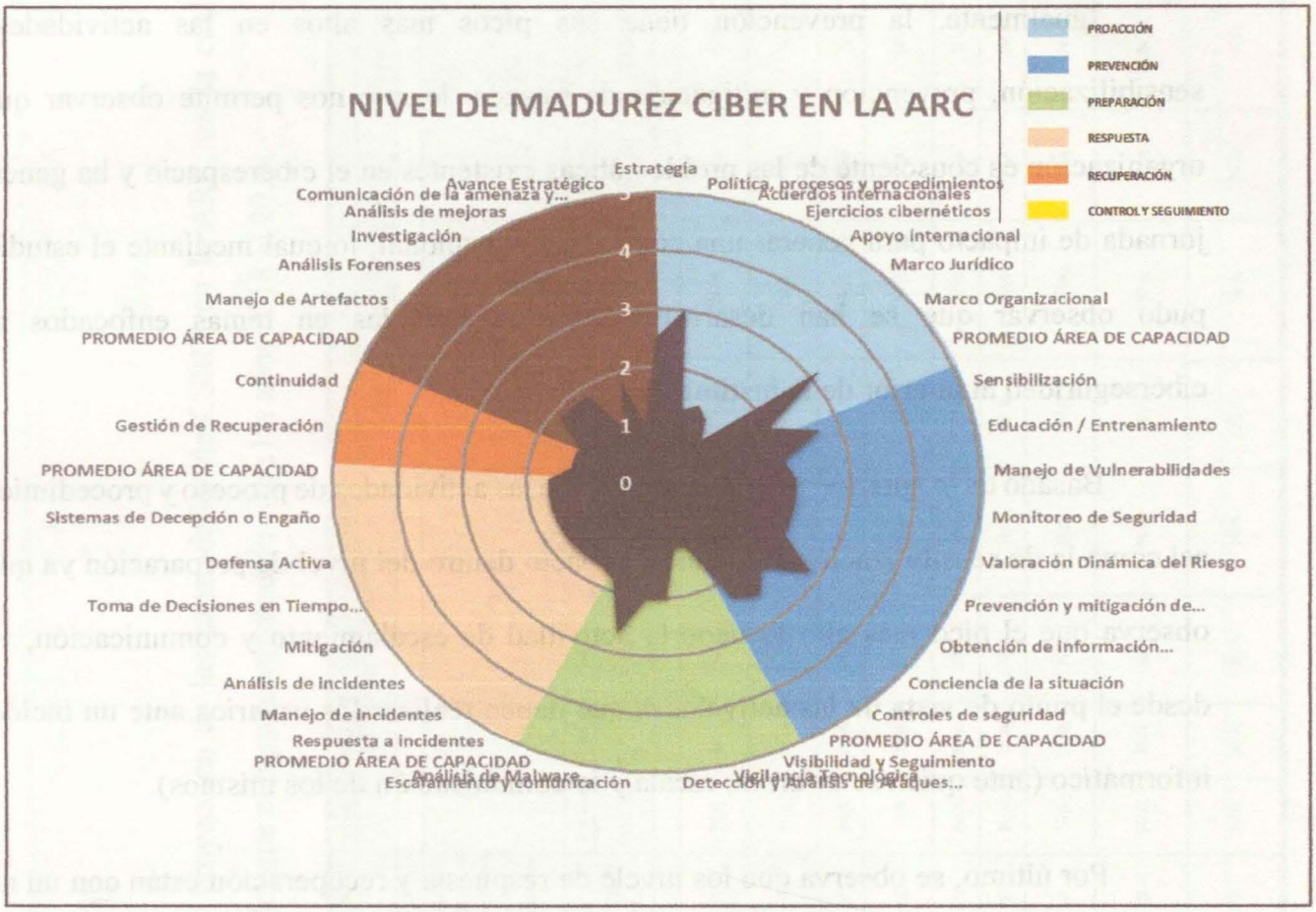

Ilustración 7: Nivel de Madurez – Brecha de CIBER en la ARC. Fuente: Elaboración Propia.

La anterior ilustración, muestra el estado actual y el resultado del análisis de brecha y madurez, la cual fue catalogada entre los valores de 0 a 5; y correlacionada con los seis niveles del modelo de ciberseguridad de la OTAN, para lo cual se observa que el resultado de las diferentes actividades planeadas dentro de este análisis se encuentra en un intervalo de valores del 1 al 3 (punto medio), igualmente en la fase de proacción se destacan dos actividades con valor de 3 la política, procesos y procedimientos y con valor superior a 3 un marco organizacional, lo que demuestra que ya existen documentos formalizadas dentro de la institución.

Igualmente, la prevención tiene sus picos más altos en las actividades de sensibilización, prevención y mitigación de riesgos. lo que nos permite observar que la organización es consciente de las problemáticas existentes en el ciberespacio y ha generado jornada de impacto para generar una conciencia situacional, lo cual mediante el estudio se pudo observar que se han desarrollado cursos virtuales en temas enfocados a la ciberseguridad al interior de la institución.

Basado en lo anterior, se puede inferir que las actividades de proceso y procedimiento, así como la de sensibilización han tenido impacto dentro del nivel de preparación ya que se observa que el pico más alto lo tiene la actividad de escalamiento y comunicación, visto desde el punto de vista de las actividades que deben realizar los usuarios ante un incidente informático (ante quien se informa, escala y la comunicación de los mismos).

Por último, se observa que los nivele de respuesta y recuperación están con un nivel 1 lo cual es muy bajo, así como en el nivel de control y seguimiento no se observaron valores, lo que nos muestra es que se deben fortalecer estos niveles y poner una mayor atención.

5.4 Resumen General de Capacidades CSIRT.

A continuación, se muestra el resumen general y proyección de las capacidades de CSIRT en la ARC, en la cual se desarrollaron los componentes DOMPI-S descritos en el apartado anterior, durante el lapso comprendido entre los años 2018 al 2026.

RESUMEN GENERAL DE CAPACIDADES CSIRT															
VERSIÓN No.: _____					FECHA DE EMISION:								Pág 1 de __		
CAPACIDAD OPERACIONAL:															
ALCANCE DE LA CAPACIDAD OPERACIONAL:		Establecer las Capacidades del CSIRT: Valorar de respuesta 07x24x365; Tipo de riesgo: Tiempo real; Permitiendo: Detectar, Analizar y Recuperarse desde cero (0) ataques cibernéticos y cero (0) actividades maliciosas; Que se presenten contra la Infraestructura Crítica Naval y Marítima en los cuatro (04) teatros operacionales de manera simultanea (Caribe, Oriente, Sur y Pacífico).			2018		2019		2020		2021		2022-2026	
REQUERIMIENTO POR COMPONENTE		DESCRIPCIÓN	FECHA DE INICIO PREVISTA	FECHA DE FINALIZACIÓN PREVISTA	Fuente	Valor $	Fuente	Valor $	Fuente	Valor $	Fuente	Valor $	Fuente	Valor $
					TOTAL	$ -	TOTAL	$ 960.000.000	TOTAL	$ 1.460.000.000	TOTAL	$ 1.560.000.000	TOTAL	$ -
DOCTRINA														
1.	Actualización Guía de Gestión de Riesgos	Actualización y redacción de la guía de gestión de riesgos basada en nuevas amenazas	1-oct-18	20-nov-18	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2.	Actualización Guía de Gestión de Atención y Respuesta a Incidentes	Actualización y redacción guía de gestión de atención y respuesta a incidentes basada en nuevas amenazas	1-oct-18	20-nov-18	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3.	Actualización Guía de Gestión de Activos	Actualización y redacción guía de gestión de activos	1-oct-18	20-nov-18	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4.	Actualización Catálogo de Infraestructuras Críticas ARC	Actualización y levantamiento del catálogo de infraestructuras críticas ARC	1-oct-18	20-nov-18	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5.	Manual de Ciberseguridad	Redacción manual de ciberseguridad	1-oct-18	20-ene-19	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6.	Manual de Operaciones de Ciberseguridad	Redacción manual de operaciones de ciberseguridad	1-oct-18	20-ene-19	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
7.	Actualización Protocolos de Ciberseguridad	Actualización y establecimiento de protocolos de ciberseguridad	1-oct-18	20-nov-18	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8.	Actualización Políticas de Seguridad informática y Protección de Datos	Actualización y estructuración de políticas de seguridad informática y protección de datos	1-oct-18	20-nov-18	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
9.	Actualización Manual CSOC (Centro de Operaciones de Seguridad Cibernética)	Actualización y redacción manual CSOC - CSIRT	1-oct-18	20-ene-19	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

ORGANIZACIÓN																
1.	Dirección Cibernética Naval	Dirección Existente	1-jul-15	11-feb-16	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2.	División CSIRT	Creación de la división	1-oct-18	20-nov-18	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3.	Sección de Gestión de Incidentes Cibernéticos	Creación de la sección	1-oct-18	20-nov-18	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4.	Sección de Gestión y Monitoreo - CSOC	Creación de la sección	1-oct-18	20-nov-18	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5.	Sección de Infraestructuras Críticas	Creación de la sección	1-oct-18	20-nov-18	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6.	Sección de Análisis de Malware	Creación de la sección	1-oct-20	20-nov-21	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
7.	Sección de Informática Forense	Creación de la sección	1-oct-20	20-nov-21	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
MATERIAL Y EQUIPO																
1.	Implementación del CSIRT	Diseño e implementación del CSIRT	1-oct-18	20-nov-26			INVERSIÓN		INVERSIÓN		INVERSIÓN		INVERSIÓN			
2.	Oficinas y Ciberlaboratorios	Diseño e implementación de Oficinas y Ciberlaboratorios.	1-oct-18	20-nov-26			INVERSIÓN				INVERSIÓN		INVERSIÓN			
3.	Protección de Usuarios	Hardware y software necesario para la protección de usuarios	1-oct-20	20-nov-26					INVERSIÓN		INVERSIÓN		INVERSIÓN			
4.	Protección de Activos	Hardware y software necesario para la protección de activos	1-oct-20	20-nov-26					INVERSIÓN		INVERSIÓN		INVERSIÓN			
5.	Monitoreo y Vigilancia - CSOC	Hardware y software necesario para el monitoreo y vigilancia - CSOC	1-oct-18	20-nov-26			INVERSIÓN				INVERSIÓN		INVERSIÓN			
6.	Cloud Vs Redes Carnada	Hardware y software necesario para la instalación y mantenimiento de Cloud vs redes carnada	1-oct-20	20-nov-26					INVERSIÓN		INVERSIÓN		INVERSIÓN			
7.	Análisis de Malware	Hardware y software necesario para el análisis de malware	1-oct-20	20-nov-26					INVERSIÓN		INVERSIÓN		INVERSIÓN			
8.	Capacidad para Desarrollo de APT's	Programación de APT's	1-oct-20	20-nov-26					INVERSIÓN		INVERSIÓN		INVERSIÓN			
9.	Herramientas de Informática Forense	Hardware y software necesario para la recuperación de información en dispositivos informáticos y gestión de evidencias.	1-oct-20	20-nov-26					INVERSIÓN		INVERSIÓN		INVERSIÓN			
10.	Adquisición de Equipos de Trabajo, Comunicación y Transporte	Hardware y software necesario para el trabajo de oficina, comunicaciones y transporte.	1-oct-18	20-nov-26			INVERSIÓN				INVERSIÓN		INVERSIÓN			
11.	Capacitación y Entrenamiento	Capacitación y entrenamiento en capacidades de CSIRT.	Continuo	Continuo			INVERSIÓN		INVERSIÓN		INVERSIÓN		INVERSIÓN			

PERSONAL														
1.	06 Oficiales	Se Necesitan 06 Oficiales se requiere gestionar 03 Oficiales para completar la División de CSIRT	1-ene-16	31-dic-19	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2.	30 Suboficiales	Se Necesitan 30 Suboficiales se requiere gestionar 15 Suboficiales para completar las 05 secciones del CSIRT.	1-ene-16	31-dic-19	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
INFRAESTRUCTURA														
1.	Oficina con 36 Puestos de Trabajo - Archivo Evidencias Físicas y Digitales.	Adecuar el espacio para contar con 36 puestos de trabajo para el personal de la división CSIRT.	1-oct-18	20-nov-19	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2.	Área de Gestión y Monitoreo - CSOC	Remodelar y Adecuar el espacio para la gestión y monitoreo (CSOC)	1-oct-18	20-nov-19	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3.	Ciberlaboratorios 02	Adecuar el espacio para Construir y contar con 02 Ciberlaboratorios (Análisis de Malware - Informática Forense)	1-oct-18	20-nov-19	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
SOPORTE LOGÍSTICO														
1.	Presupuesto para Mantenimiento y Actualización de Hardware y Software	Asignar los recursos para mantener actualizado hardware y software	Continuo	Continuo	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2.	Presupuesto para Capacitación Continua del Personal	Asignar los recursos necesarios para la capacitación continua del personal	Continuo	Continuo	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3.	Presupuesto para el Mantenimiento de Instalaciones	Asignar el presupuesto necesario para mantener las instalaciones	Continuo	Continuo	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4.	Presupuesto para el Sostenimiento de los Servicios de Comunicación (Celular, Internet, Telefonía)	Asignar el presupuesto necesario para mantener los servicios de comunicación	Continuo	Continuo	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5.	Presupuesto para el Sostenimiento de los Vehículos	Asignar el presupuesto necesario para mantener los vehículos	Continuo	Continuo	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Ilustración 8: Resumen General de las Capacidades del CSIRT – DOMPI-S. Fuente: Elaboración Propia.

En la ilustración anterior, se muestra el resumen general y la proyección de las capacidades del CSIRT en la ARC, las cuales fueron estructuradas mediante la metodología por capacidades dentro de cada uno de los componentes DOMPI-S y apoyados en el modelo de racionalidad limitada, tomando como entrada principal la experiencia y experticia de la Dirección Cibernética Naval (DICIB) y el personal de la División de Informática, dentro de este apartado se analizó la temática de forma holística, integrando las capacidades actuales de la DICIB con las visualizadas dentro del CSIRT y las futuras proyectadas al 2026, en donde en primera medida se identifican todas las alternativas en cuanto al funcionamiento y optimización de medios, para evitar duplicidad de funciones, desgaste operacional y poder llegar a la solución esperada.

Igualmente dentro de este apartado se planearon las diferentes referencias institucionales para la generación de doctrina, la cual será actualizada a medida que se aprenda y mejoren las capacidades propias del mismo, seguidamente se plantea la organización, el material y equipos previendo sus actualizaciones a medida que la tecnología avanza y mejoran las herramientas y las formas de afrontar estas amenazas, con las cuales se planea mitigar los riesgos presentes y futuros en una constante línea de aprendizaje para el personal, pensando también en la forma de conformar un relevo generacional y continuo del personal y acompañado del soporte y mantenimiento propio, preciso e incesante de las capacidades instaladas.

5.5 Necesidades de Implementación en la ARC y Servicios del CSIRT

Las Fuerzas Militares y la ARC están innovando y evolucionando en la forma de ejecutar su misión constitucional y legal en pro de la seguridad y defensa nacional en los dominios de la guerra, pero en particular dentro del presente trabajo de monografía realizaremos énfasis en el quinto dominio el "Ciberespacio" (DNP, 2011).

Dentro de las problemáticas de la Armada Nacional, es el tipo de red de datos y de comunicaciones que posee, toda vez que maneja una topología distribuida, igualmente tiene una diversidad de marcas y cantidad de equipos (comerciales - militares) en ocasiones desactualizados y fuera de soporte a lo largo del territorio nacional, lo cual genera vulnerabilidades y riesgos potenciales que pueden ser capitalizados por los grupos al margen de la ley, enemigos internos y externos del país que busquen desestabilizar la integridad, disponibilidad y confidencialidad de los sistemas de la ARC.

Igualmente, es importante precisar la cantidad y criticidad de la información táctica, operacional y estratégica que circunda y es consumida a diario y de forma simultánea a través de estas infraestructuras críticas de seguridad nacional, basadas en tecnologías de la información y la operación; tales como: intranet, repositorios de archivos, bases de datos operacionales, sistemas de información operacionales, sistemas de controles de armas navales, sistemas de navegación marítimos, fluviales, terrestres y aéreos, sistemas de comunicación operacional (digital – análogo), entre otros; los cuales son vitales para salvaguardar la vida de los tripulantes y maximizar el éxito de las operaciones militares.

Para ayudar en esta protección en el mercado de las TIC existe una gran variedad de herramientas tecnológicas que permiten realizar una gestión de incidentes de seguridad, pero esto no es suficiente se requiere de un CSIRT conformado por un equipo interdisciplinario y de expertos en seguridad informática capaz de responder de forma efectiva y proactiva a los incidentes de seguridad y ciberataques que puedan desestabilizar de alguna manera al estado, las FF.MM y el País.

Actualmente las FF. MM. y la ARC desarrollan esta actividad y cuentan con algunas capacidades y elementos que permiten de algún modo identificar ataques o acciones maliciosas y sospechosas dentro de las redes de datos, sin embargo, no se cuenta con estructuras tipo CSIRT, con personal preparado y entrenado para reaccionar de forma activa y efectiva.

Por otra parte, el prototipo de CSIRT debe tener capacidades para responder ante las amenazas de forma accionable mediante el desarrollo de diseños modulares, flexibles, dinámicos para la respuesta a incidentes acorde a cada tipo de servicio (reactivos, proactivos y de gestión de la calidad de la seguridad) y a las necesidades de la organización y del País.

Con el prototipo organizacional del CSIRT de la Armada Nacional se podrían establecer los servicios esenciales del mismo acorde a las capacidades actuales y realizar una gestión de incidentes al interior de la ARC y de las otras organizaciones e instituciones que requieran del servicio; igualmente se disminuirá el tiempo de respuesta y se tomarán las acciones que permitan que estas sean más eficientes para la mitigación y neutralización de incidentes informáticos, afectando de manera positiva la ciberseguridad, permitiendo disminuir la incertidumbre y aumentando sus estándares de seguridad mediante el uso

efectivo de las TIC y en materia de defensa nacional para el óptimo y oportuno asesoramiento estratégico en el Proceso Militar para la Toma de Decisiones6 (Tamara, 2014).

Igualmente permitirá optimizar y aprovechar las capacidades del talento humano y los recursos técnicos y tecnológicos existentes y pertenecientes a la ARC en temas como Ciberseguridad, Ciberdefensa y Ciberinteligencia, generando mayor sinergia operacional y ventaja competitiva en pro de obtener mayor seguridad y anticipación ante posibles ataques e incidentes informáticos que quieran afectar al país.

Así mismo es importante resaltar la importancia que el documento CONPES 3854 que trata sobre la "Política Nacional de Seguridad Digital", el cual representa para las FF. MM. y a la ARC una oportunidad para la creación del CSIRT, toda vez que este CONPES sugiere la importancia y lo necesario de promover la creación de nuevos equipos de respuesta a incidentes informáticos sectoriales, que permitan la adecuada gestión de incidentes digitales, con capacidad de reacción ante incidentes especializados por sector y con capacidad real de interacción con los diferentes fabricantes, agencias de ley y otras agencias del gobierno (DNP, 2016).

Seguido de lo presentado en el párrafo anterior, es importante decir que el Gobierno Nacional en su afán de minimizar los riesgos potenciales en el ciberespacio lanzó una estrategia de Ciberseguridad y Ciberdefensa en el año 2011 representada en el CONPES 3701 y teniendo en cuenta que la evolución de la amenaza, instaura una estructura nacional para hacerle frente, es así como en el año 2015 se empieza a actualizar la estrategia presente en el

---

[6] Sigla de PMTD

CONPES 3701 y mudamos a una estrategia de seguridad digital atendiendo la tendencia mundial.

Esa política se produce en el año 2016 con el CONPES 3854, pero al mismo tiempo, el Comando General de las FFMM preocupado de las amenazas nacientes y teniendo en cuenta la situación política que atraviesa el país replantea su Estrategia Militar y desarrolla y estructura un Plan Militar que por primer vez en más de 50 años, ya no es un Plan de Guerra sino un Plan de Estabilización y Consolidación Nacional, el cual se enfoca en atender más a las amenazas emergentes entre las cuales se destaca la amenaza cibernética.

Por lo anterior, se estructuró el Plan Victoria donde se ordenó a las fuerzas crear los CSIRT, mencionado plan, fue estudiado y es de este, que se estructura el plan del Comando de la Armada Nacional, al cual designo como el Plan de Campaña SIRIUS, para dar cumplimiento al Plan Victoria del CGFM, dentro de este plan la ARC establece unas líneas de acción, actividades para neutralizar y minimizar los riesgos potenciales que se pueden materializar al contar una red descentralizada a nivel nacional, lo cual dificulta de la implementación de medidas proactivas y preventivas que contribuyan a minimizar las amenazas cibernéticas.

Sumado a lo anterior, existe una gran cantidad de fuentes de amenaza que pueden estar motivadas e interesadas en la búsqueda de los medios y métodos técnicos, tecnológicos y físicos para afectar las infraestructuras críticas de la ARC, es por esto que se hace necesario contar con la capacidad de reacción eficiente frente a incidentes o acciones maliciosas.

Igualmente, dentro del presente trabajo de monografía se realizó un análisis cuantitativo de los incidentes detectados y/o informados al interior de la Armada Nacional dentro del periodo comprendido desde el 01 de enero del 2018 hasta el 31 de diciembre del 2018, los cuales fueron catalogados y agrupados por fuerza naval (concentrando sus unidades subalternas), las cuales fueron objeto de recolección, análisis, tratamiento y tabulación al interior de la misma, es de resaltar que dentro de este análisis se cuantificaron las amenazas detectadas por el Centro de Operaciones de Seguridad (SOC) así como las reportadas por los diferentes oficiales de seguridad informática, vigías de seguridad o encargados de sistemas y TIC de cada unidad, basado en lo anterior, se presentaran las siguientes estadísticas en unidades de porcentaje, lo cual demuestra de manera general y especifica la cantidad de eventos e incidentes informáticos detectados durante el año, así como los tipos de amenazas que pretendieron vulnerar la seguridad al interior de la ARC.

Tabla 5: Eventos por Fuerza Naval en la ARC.

EVENTOS POR FUERZA NAVAL	AÑO 2018
CARMA	103
FNC	49
FNS	9
FNP	13
FNO	7
TOTAL	**170**

Fuente: Elaboración Propia.

Ilustración 9: Eventos por Fuerza Naval en Porcentajes. Fuente: Elaboración Propia.

Teniendo en cuenta el análisis realizado, se evidencia y se puede deducir que la unidad que presentó la mayor cantidad de amenazas fue el Comando de la Armada con un 57% del total de los ataques, seguido de la FNC con un 27% y las de menor porcentaje fueron la FNS con un 5% y la FNO con un 4% del total de la totalidad de los ataques, donde el 100%. equivalente a 170 ataques.

Tabla 6: Amenazas por Fuerza Naval en la ARC.

TIPOS DE AMENAZAS DETECTADAS	AÑO 2018
Exploit	30
APT	1
Rescate de Software (Ransomware)	2
SQL Inyección	4
Acceso no Autorizado a Sistemas y Redes	6
Actividad Remota	7
Troyanos	25
BACKDOOR. Double Pulsar	13
Malware	24
Código Malicioso	4
Suplantación (Phishing)	12
RISKWARE/Coinhive	14

Ataque de Fuerza Bruta (Brute Force)	1
Ataques Contra Aplicaciones Web	1
Botnets (Red de Bots - Software robot)	7
Uso de software no Autorizado	3
Spyware (Software Espía)	1
Virus	8
Vulnerabilidades SSL/TLS	4
Ultrasurf (Navegación de forma anónima)	1
Saturación de Canal	2
TOTAL	**170**

Fuente: Elaboración Propia

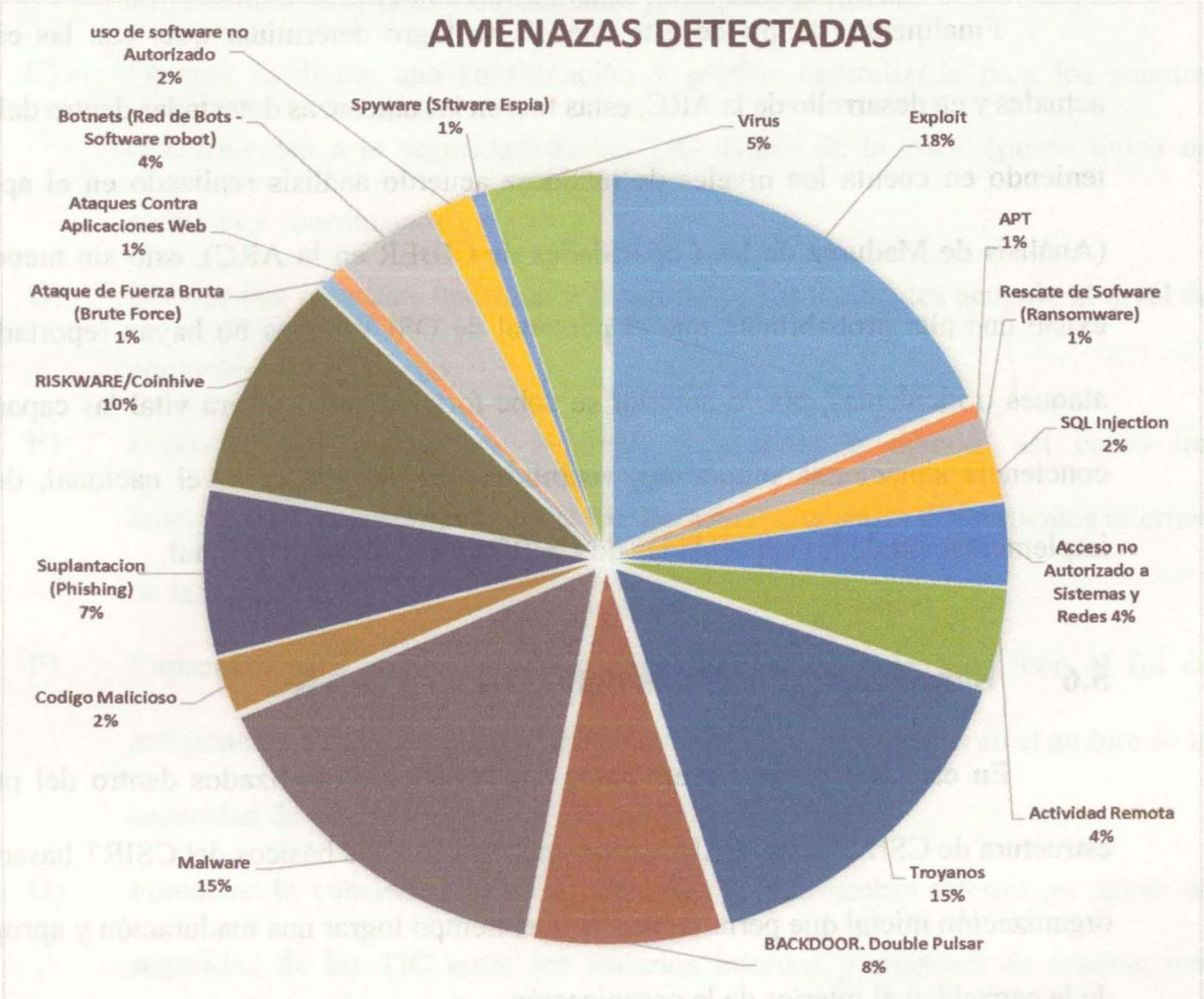

Ilustración 10: Amenazas Detectadas en Porcentajes. Fuente: Elaboración Propia.

Teniendo en cuenta el análisis realizado y los resultados obtenidos dentro del presente trabajo, los cuales se evidencian dentro de las estadísticas realizadas y presentadas en los apartados anteriores se puede deducir que los exploit tienen el mayor porcentaje con un 18% de la totalidad de acciones, seguido de los troyanos y malware con el 15%, igualmente que los de menor recurrencia fueron las Amenaza Persistente Avanzada (APT), ataque de Fuerza Bruta, ataques contra aplicaciones web y spyware (software espía) con un 1% de la totalidad de los ataques, donde el 100%. Equivalente a 170 ataques.

Finalmente, dentro de este análisis se logró determinar que, con las capacidades actuales y en desarrollo de la ARC, estas fueron las amenazas detectadas dentro del año 2018, teniendo en cuenta los niveles de madurez acuerdo análisis realizado en el apartado 5.4 (Análisis de Madurez de las Capacidades de CIBER en la ARC), esto sin mencionar que existe una alta probabilidad que el personal de OSI y vigías no hayan reportado algunos ataques o incidentes, por lo anterior se debe fortalecer de manera vital las capacidades de conciencia situacional, monitoreo, visibilidad de las redes a nivel nacional, detección e implementación de las capacidades de CSIRT en la Armada Nacional.

5.6 Beneficios y Servicios del CSIRT en la ARC

En este apartado se presentarán los beneficios idealizados dentro del prototipo y estructura de CSIRT para la ARC, así como los servicios básicos del CSIRT basados en una organización inicial que permita mediante el tiempo lograr una maduración y apropiamiento de la capacidad al interior de la organización.

5.6.1 Beneficios

Dentro de los principales beneficios del CSIRT al interior de la ARC, están los siguientes:

A) Disminuir el nivel de riesgo Cibernético dentro de la infraestructura crítica cibernética naval al contar con un equipo dedicado en el ámbito militar.

B) Realizar una gestión y mitigación de incidentes críticos, así como a proteger las infraestructuras críticas y capacidades propias de la fuerza.

C) Obtener mediante una coordinación y gestión centralizada para los asuntos concernientes a la seguridad de las TIC dentro de la ARC (punto único de contacto y coordinación).

D) Brindar una respuesta oportuna y focalizada a los incidentes acuerdo el nivel de competencia del mismo.

E) Disponer de los recursos humanos y técnicos a tiempo, así como los conocimientos específicos necesarios para apoyar y asistir a los clientes internos de la ARC.

F) Capacidad para realizar una vigilancia tecnológica adecuada, con el fin de anteponerse a nuevos riesgos (futuros) y amenazas emergentes en el ámbito de la seguridad de las TIC.

G) Fomentar la concientización, cooperación e intercambio interno en temas de seguridad de las TIC entre los usuarios internos y externos de interés; que permitan una sinergia organizacional que apoye y fortalezca las capacidades propias de la ARC.

H) Contar con un medio de intercambio seguro de lecciones aprendidas y buenas prácticas al interior de la organización (sensibilización).

5.6.2 Primeros Servicios del CSIRT

Dentro de los servicios ofrecidos por un CSIRT y en especial el planteado para la ARC dentro de la presente monografía, el cual dependerá de unos requisitos indispensables como los recursos (humanos, técnicos y tecnológicos), el tamaño, la infraestructura orgánico funcional y las capacidades propias y adquiridas de los miembros del equipo.

Basado en lo anterior y según la OEA. (2016), dentro de su guía de buenas prácticas plantea que los servicios se pueden dividir en tres (básicos, intermedios y avanzados), y según (West-Brown, et al., 2003) señala los servicios en tres categorías (servicios reactivos, servicios proactivos y servicios de gestión de calidad de la seguridad). Por lo anterior, y según los esquemas de servicios se puede deducir que es es altamente probable que estos puedan crecer y aumentar dentro de cualquiera estructura de CSIRT a medida que el equipo adquiera mayores capacidades, experiencia y madures con el tiempo.

Ilustración 11: Evolución de los Servicios de un CSIRT. Fuente: OEA. (2016)

Para el prototipo de CSIRT de la ARC en su fase de iniciación se planea que solo prestara servicios a sus usuarios internos (Oficiales de Seguridad Informática, Departamento de TIC y Usuarios Internos). Así como la gestión y coordinación entre los diferentes actores y responsables de las infraestructuras de TIC en las unidades desplegadas y ubicadas alrededor del territorio colombiano en los asuntos relacionados con la ciberseguridad de las TIC.

Lo anterior, apoyado en las necesidades observadas mediante las diferentes mesas de trabajo y conversaciones realizadas con el personal de la División de Informática de la ARC para la estructuración de los servicios básicos de este tipo de capacidad en su fase inicial de implementación en la organización, así mismo en las mesas de trabajo de expertos con el personal orgánico de la Dirección Cibernética Naval para sacar el resumen general de

capacidades CSIRT, capacidades de Ciberdefensa, la brecha de madurez de capacidad en la ARC y las estadísticas de los ataques o incidentes presentados en la ARC durante el años 2018.

Igualmente se realizó una observación de lo que plantea (OEA. 2016 y West-Brown, et al., 2003) acerca de los servicios y teniendo en cuenta lo expresado anteriormente, se proyecta y se recomienda que los servicios iniciales dentro del prototipo de CSIRT en la ARC sean los que se presentan en la siguiente ilustración:

Ilustración 12: Servicios de Iniciación CSIRT ARC. Fuente: Elaboración Propia.

Apoyados en los resultados y análisis obtenidos en los apartados 5.2, 5.3, 5.4 y 5.5 del presente trabajo de monografía y apoyados la aplicación del modelo de racionalidad limitada y tomando como insumo la experiencia y experticia del equipo interdisciplinario de trabajo conformado por el personal técnico de la Dirección Cibernética Naval y el personal de la División de Informática, se plantearon los servicios de iniciación del CSIRT, y verificando la capacidad de atención, pertinencia, eficacia y eficiencia de cada servicio, en consenso se establecieron los servicios que se presentan en la ilustración anterior.

1. Alertas y advertencias en la ARC y CSIRT FF.MM: Dentro de este servicio se realizará difusión de las alertas detectadas a través de los diferentes equipos y métodos implementados dentro de la ARC, así como de las diferentes publicaciones que surtan del ejercicio del CSIRT con el fin de tener y generar una buena cultura de auto protección al interior de la institución.
2. Tratamiento, análisis y respuesta a incidentes (Centralizado ARC): Dentro de este servicio se realizará toda la gestión de incidentes que se puedan presentar dentro de las infraestructuras críticas y red de la ARC, Igualmente se brindará asistencia técnica y especializada a los OSI de la ARC como primeros respondientes del incidente de no lograr mitigar y resolver el incidente se prestará la asistencia en sitio sin importar en cuál de las cuatro fuerzas navales se haya presentado el incidente. Las cuales están distribuidas a nivel nacional.
3. Tratamiento de Vulnerabilidades ARC (Básico): Dentro de este servicio se realizará toda la atención y recomendaciones para atender y resolver las vulnerabilidades que se detecten en la red y los equipos, mediante asistencia técnica y apoyo para el parcheo de sistemas operativos de PC, servidores, aseguramiento de las redes y en general apoyo en la aplicación de buenas prácticas dentro de los sistemas de TIC distribuidos a nivel nacional.
4. Tratamiento de Artefactos en ARC Básico (Virus): Dentro de este servicio se realizará toda la gestión de los virus detectados por parte de las consolas de antivirus de las unidades, así como todos aquellos que se detenten mediante otros equipos activos para el análisis, monitoreo y comportamiento de la red.

5. Observatorio tecnológico y difusión de información de seguridad: Dentro de este servicio se realizará toda la vigilancia tecnológica y observación de las diferentes publicaciones a nivel nacional, regional y mundial sobre nuevas amenazas y formas de afrontarlas, igualmente dentro de esta se realizará difusión de boletines enfocados a minimizar riesgos en la red.
6. Campañas de sensibilización y consultoría básica sobre el manual de seguridad ARC: Dentro de este servicio se realizará toda la gestión de la capacitación y entrenamiento del personal desde los niveles de usuario básico hasta nivel OSI dentro de la ARC, también será la responsable de gestionar los recursos para incentivar y mejorar la conciencia situacional dentro de la ARC.
7. Otros servicios: Dentro de estos coexisten otros servicios propios de los CSIRT, con una amplia gama y posibilidad de incorporación y expansión, pero en este momento no se podrán brindar o contemplar por falta de capacidades técnicas, tecnológicas y humanas. Los nuevos servicios serán incorporados a medida que se fortalezca la división en pro del mejoramiento continuo del CSIRT, los resultados y aprendizaje adquirido con el proceso de gestión piloto que se presenta más adelante.

Posterior a la estructuración de los servicios del CSIRT es importante resaltar que una adecuada forma de implementación es mediante la generación de un equipo o grupo pequeño de usuarios "PILOTO" para prestarle los servicios básicos durante un periodo de tiempo "CORTO" con el fin de organizar y reorientar los imprevistos o impases que se puedan presentar y poder obtener una retroalimentación y opinión que permita tener una mejora continua dentro del CSIRT, lo cual es una buena práctica de iniciación y difusión de los servicios del CSIRT.

Basado en lo anterior, se propone utilizar el siguiente esquema metodológico de seguimiento, el cual presentare en la siguiente ilustración, este nos ayudara a organizar y establecer tiempos, capacidades, actividades y expectativas de los clientes con el fin de afinar los posibles servicios del CSIRT.

Ilustración 13: Proceso de Gestión Piloto. Fuente: Elaboración Propia.

Posterior a esta fase de iniciación mediante la ayuda y recomendaciones del equipo piloto y el análisis de los resultados se podrán poner en consideración la incorporación o salida de servicios y enfocar los esfuerzos de esta capacidad en los puntos o temáticas de mayor interés o relevancia para nuestros clientes, así como la probabilidad de ampliar y mejorar el portafolio de servicios del CSIRT.

Apoyados en el modelo de racionalidad limitada y tomando como insumo la experiencia y experticia del equipo interdisciplinario que participo en la presente monografía, se planteó un proceso de gestión piloto, dentro del cual se encuentran las siguientes etapas las cuales explicaremos a continuación así:

1. **Etapa de Inicio**

Dentro de esta etapa se reciben los requerimientos y necesidades de los diferentes usuarios, las cuales se catalogarán acuerdo ubicación geográfica, tipo, descripción, sistema afectado entre otros; se le asigna un número de incidente y un responsable dentro del CSIRT y se procede a realizar toda la documentación propia para poder garantizar un seguimiento y fin del mismo; es importante dentro de esta fase contar con toda la información del usuario para ir retroalimentándolo del trabajo que se realice para la atención del incidente, igualmente dentro de esta etapa se formaliza el inicio de la etapa de tratamiento del incidente y servicio.

2. **Etapa de Tratamiento**

Dentro de esta etapa se entra a recolectar la evidencia si es el caso, a revisar, estudiar, analizar, evidenciar comportamientos, vector de ataque y documentar todo lo referente al mismo, establecer posibles soluciones, equipos, medios y métodos acuerdo el tipo de caso e incidente y a generar un informe con toda la información pertinente del mismo, posteriormente se realizan las actividades de sanitización y se deja en monitoreo para evidenciar que si fue solucionado del todo el incidente o evento.

3. **Etapa de Mejora**

Dentro de esta etapa se entra a verificar que acciones se pueden realizar para mejorar los tiempos de respuesta, los procedimientos de atención, los protocolos de levantamiento de pruebas y evidencias digitales, optimizar equipos, medios y técnicas de solución, igualmente dentro de esta etapa se evalúan las competencias, fortalezas y debilidades del responsable de solucionar el evento, esto con el propósito de reentrenar, fortalecer y solucionar las fallas que

puedan evidenciarse apuntando a obtener una eficacia, eficiencia y efectividad dentro del proceso.

4. Etapa de Cierre

Dentro de esta etapa se verifican los resultados de las demás etapas, se evidencia que estén acorde al procedimiento y se informa al usuario sobre el cierre del incidente, pero esta etapa es la que define y permite dar por terminado el seguimiento y alcance de mejora dentro del proceso, notificando las observaciones y cosas por mejorar a los responsables de cada etapa y así garantizar una retroalimentación y poder tomar medidas correctivas o de mejora en pro de la optimización del mismo.

5.7 Intercambio de Información Clientes Internos con el CSIRT ARC.

Dentro de la Armada Nacional esta implementada una mesa de ayuda para la gestión de incidentes y requerimientos de soporte técnico, por lo cual dentro del CSIRT se necesario implementar una herramienta con capacidades parecidas pero más enfocadas a la gestión propia de los incidentes con capacidad para la generación de lecciones aprendidas con el fin de retroalimentar a los diferentes OSI de la Armada distribuidos en el país; por lo anterior, al momento de la implementación se utilizara una aplicación de software libre con el fin de economizar gastos y poder ajustarla a las necesidades que se puedan generar dentro de la dinámica propia de la organización.

VI. CAPITULO No. III - SUGERIR LA METODOLOGÍA Y EL PROTOTIPO DE ORGANIGRAMA DEL CSIRT DE LA ARC QUE PERMITA MEJORAR LA SINERGIA OPERACIONAL CIBERNÉTICA Y LA SEGURIDAD INFORMÁTICA EN LAS OPERACIONES.

Dentro del presente capitulo el lector encontrará la revisión documental de cuatro metodologías para el diseño de un CSIRT, donde se enumeran los pasos que cada una establece dentro de su modelo y a partir de estas, se construye la metodología que más se acomoda a las condiciones propias de la organización, bajo el principio de que la Armada Nacional es una organización piramidal y castrense, así mismo podrá encontrar el prototipo organizacional propuesto, la descripción de la División de CSIRT propuesta para la ARC.

6.1 Metodologías de Diseño de un CSIRT

Mediante la aplicación del modelo de racionalidad limitada y tomando como insumos la información, la experiencia y experticia del equipo interdisciplinario de trabajo conformado por el personal técnico de la Dirección Cibernética Naval y el personal de la División de Informática, se procedió al desarrollo de la misma, en donde en primera medida se identifican todas las alternativas posibles para establecer el diseño; luego de esto se analizaron los resultados obtenidos de cada uno de ellos y se realiza una comparación verificando la pertinencia, eficacia y eficiencia de cada una de las opciones planteadas para

finalmente escoger la solución más adecuada, dando como resultado la Metodología Integrada para el Diseño del CSIRT de la ARC.

Basado en lo anterior, también se realizó una comparación y análisis de cada una de las cuatro metodologías acá presentes para el diseño de un CSIRT, realizando un estudio de cada metodología, identificando sus pasos y secuencia, dando como resultado la siguiente tabla.

Tabla 7: Diferentes Metodologías para el Diseño de un CSIRT.

NIST, 2012	CERT, s.f
1. Creación de una política y plan de respuesta a incidentes 2. Desarrollar procedimientos para el manejo y el reporte de incidentes 3. Establecer los lineamientos para la comunicación con las partes externas o terceros en relación a los incidentes 4. Seleccionar la estructura del equipo y el modelo del equipo de trabajo 5. Establecer las relaciones y las líneas de comunicación entre el equipo de respuesta de incidentes y otros grupos, bien sean internos o externos 6. Determinar los servicios que proveerá el equipo de respuesta a incidentes 7. Capacitar al personal del equipo de respuesta a incidentes	1. Obtener el apoyo y la "decisión de compra" por parte de la gerencia 2. Determinar el plan estratégico del CSIRT 3. Recopilar información relevante 4. Diseñar la visión del CSIRT 5. Comunicar la visión y el plan operativo del CSIRT 6. Comenzar la implementación del CSIRT 7. Comunicar la operatividad del CSIRT 8. Evaluar la efectividad del CSIRT.
ENISA, 2006	**OEA, 2016**
1. Determinar el público objetivo 2. Elección de los servicios adecuados	1. Identificar a las partes interesadas. 2. Crear el documento de constitución del CSIRT

3. Análisis de los clientes atendidos y de los canales de comunicación adecuados 4. Declaración de los servicios. 5. Desarrollar el plan comercial. - Definir el modelo financiero. - Definir la estructura organizativa. - Contratar personal. - Utilizar la oficina y equiparla. - Desarrollar una política de seguridad de la información. - Buscar socios con los que cooperar. 6. Promover el plan comercial. - Conseguir que se apruebe el modelo de negocio. - Encajarlo todo en un plan de proyecto. 7. Establecimiento de flujos de procesos y procedimientos educativos y técnicos 8. Capacitar al personal.	- Misión - Visión - Marco institucional - Marco legal 3. Definir alcance - Público objetivo - Definición de servicios 4. Establecer la estructura organizativa y las responsabilidades del personal 5. Seleccionar y contratar el personal 6. Definir las instalaciones y la infraestructura del CSIRT 7. Definir las políticas y los procedimientos operacionales

Fuente: Elaboración Propia

Existen diferentes metodologías para el diseño de un CSIRT y cada una tiene un enfoque diferente, la metodología propuesta por el NIST (National Institute of Standards and Technology) está enfocada en el manejo de incidentes; la metodología propuesta por el CERT de la Universidad de Carnegie Mellon tiene un enfoque gerencial; la metodología propuesta por ENISA tiene un enfoque comercial y la metodología propuesta por la OEA está enfocada a diseñar un CSIRT nacional. Por lo tanto, se hace necesario integrar y ajustar los aspectos particulares de las metodologías existentes a un procedimiento que pueda ser utilizado para diseñar el CSIRT que se ajuste a las necesidades de la Armada Nacional de Colombia y que

permitan cumplir con toda la normatividad interna de la institución para poder llevar a cabo un diseño adecuado y una posterior implementación exitosa.

6.1.1 Metodología Integrada para el Diseño del CSIRT de la ARC.

El resultado del análisis, comparación e integración de los pasos de las cuatro metodologías presentadas anteriormente, fue construido y desarrollado con el modelo de racionalidad limitada dentro del cual se llegó a un consenso resultado de las mesas de trabajo con el personal de expertos técnicos de la Dirección Cibernética Naval y la División de Informática, dando como salida que estas son las fases y pasos que debe tener la metodología de diseño del CSIRT en la ARC, basados en las necesidades y misión de la institución.

Tabla 8: Metodología Integrada para el Diseño de un CSIRT para la ARC.

METODOLOGÍA INTEGRADA PARA EL DISEÑO DEL CSIRT DE LA ARC
1. Fase de inicio del CSIRT - Identificar las partes interesadas - Recopilar información relevante - Obtener el apoyo por parte de los directivos 2. Crear el documento de constitución del CSIRT - Misión - Visión - Marco institucional - Marco legal - Definir alcance y Público objetivo - Establecer la estructura organizativa y las responsabilidades del personal - Determinar los servicios que proveerá el equipo de respuesta a incidentes - Definir las políticas y los procedimientos operacionales

- Establecer los lineamientos para la comunicación con las partes internas o externas en relación a los incidentes
- Definir las instalaciones y la infraestructura del CSIRT
- Seleccionar y contratar el personal (Si es el caso)

3. Desarrollar el Plan de Proyecto
   - Determinar el plan estratégico del CSIRT
   - Conseguir que se apruebe el modelo del proyecto del CSIRT.
4. Capacitar al personal del equipo de respuesta a incidentes
   - Establecimiento de flujos de procesos y procedimientos educativos y técnicos
   - Capacitar al personal.
5. Comunicar la operatividad del CSIRT
6. Monitorear y evaluar la efectividad del CSIRT
7. Retroalimentación y mejora continua.

Fuente: Elaboración Propia

Basados en la metodología presentada en la tabla anterior, se plantea el siguiente prototipo organizacional de CSIRT para el caso de estudio Armada Nacional. Igualmente, para los trabajos futuros se recomendará tomar como guía la metodología anterior, pero para efectos del presente trabajo de monografía se desarrollarán algunos puntos enunciados dentro de la misma, toda vez que el alcance del presente trabajo no contempla la realización y estructuración total de un CSRIT para la ARC, sino un prototipo de iniciación de la capacidad en la organización.

A continuación, se explicará cada una de las fases planteadas dentro del modelo establecido para la ARC.

6.1.1.1 Fase de Inicio del CSIRT

Esta es una de las fases más importantes y transcendentales del modelo, ya que desde acá parte el éxito del mismo, toda vez que dentro de ella se contemplan las actividades como: Identificar las partes interesadas, recopilar información relevante y obtener el apoyo por parte de los directivos y para el caso de la ARC de los altos mandos navales.

El objetivo de esta fase es cautivar la atención y apoyo de los directivos, lograr el financiamiento y sostenibilidad del CSIRT, lograr que sea visto como una capacidad operativa de transcendencia organizacional por el carácter de criticidad, seguridad y protección que requiere la información e infraestructura TIC de la ARC.

La manera de evaluar esta fase es con la carta o documento de autorización por parte de los directivos donde manifiesten de forma clara y precisa que están de acuerdo con el proyecto y que se puede continuar con la construcción del acta de constitución.

6.1.1.2 Crear el Documento de Constitución del CSIRT

Esta fase inicia con la salida de la fase anterior (documento donde manifiestan el apoyo por parte de los directivos), dentro de esta es importante establecer todas las variables, marcos legales, institucionales para poder definir y estructurar de forma adecuada la capacidad proyectada, es por esto que esta fase se ocupa de toda la formalización documental del CSIRT entre los cuales mencionare unos ejemplos como la visión, marco institucional, legal, establecer la estructura organizativa y las responsabilidades del personal, determinar los servicios que proveerá el equipo de respuesta a incidentes, definir las políticas y los

procedimientos operacionales, establecer los lineamientos para la comunicación con las partes internas o externas en relación a los incidentes entre otras.

6.1.1.3 Desarrollar el Plan de Proyecto

Esta fase inicia con el perfeccionamiento de la fase anterior, en esta parte del modelo se pone a prueba todo lo desarrollado en la constitución del mismo, es decir en esta pasamos de toda la parte documental a la operación y puesta en funcionamiento del CSIRT, en esta se comienza a poner a prueba la parte operativa con el fin de evidenciar gestión y respuesta, dentro de esta fase se encuentran el plan estratégico del CSIRT y conseguir que se apruebe el modelo del proyecto del CSIRT, ya en su parte misional y funcional.

6.1.1.4 Capacitar al Personal del Equipo de Respuesta a Incidentes

Dentro de esta fase se inicia una actividad clave para todo tipo de estructura funcional y operativa que es el entrenamiento y reentrenamiento del personal, es de vital importancia contar con flujos de procesos y procedimientos educativos y técnicos, así como contar con estrategias claras para capacitar al personal en búsqueda de un mejoramiento de capacidades y ampliación de servicios, dentro de este tipo de proyectos de tecnología donde la innovación y el desarrollo son constantes y variables en el tiempo de forma tan rápida que si no entrenas a tu personal quedaras rezagado y obsoleto en un muy corto tiempo y no podrás afrontar los retos y nuevas amenazas de forma rápida y efectiva.

6.1.1.5 Comunicar la Operatividad del CSIRT

En esta fase lo que se busca es tener estrategias claras de comunicación interna y externa para logra ser visibles dentro de la institución, es decir poder demostrar los avances

y resultados del CSIRT, obtener y mantener una comunicación fluida en todos los niveles de la ARC, para demostrar el éxito, impacto e importancia del mismo.

Teniendo claro el tamaño de la ARC y con el fin de llegar a la mayor cantidad de usuarios internos es de vital importancia para esta fase hacer uso efectivo de los canales de comunicación existentes como la intranet, correos internos, boletines, revista interna, charlas en las escuelas de formación, entre otras.

6.1.1.6 Monitorear y Evaluar la Efectividad del CSIRT

En esta fase se busca desarrollar metodologías de seguimiento y control mediante la realización e incorporación de planes de acción e indicadores de gestión enfocados a la parte misional y administrativa del CSIRT, dentro de esta fase es de vital importancia logra medir el impacto que se está obteniendo a medida que es más visible la capacidad al interior de la ARC.

Uno de los productos dentro de esta fase son los planes de mejoramiento y acciones realizadas para mejorar los resultados y/o optimizar los recursos y medios.

6.1.1.7 Retroalimentación y Mejora Continua.

En esta fase la principal entrada es la fase anterior, por lo cual la retroalimentación se debe desarrollar de forma casi que natural en pro de establecer las mejoras en cada una de las actividades y procedimientos propios del CSIRT, dentro de esta fase se hace necesario contar con estrategias de financiamiento para poder tomar acción de forma inmediata a las fallas detectadas y optimizar los procesos y resultados del CSIRT.

Dentro de cada uno de los indicadores o metas diseñadas para evaluar tanto la eficiencia, eficacia y efectividad del CSIRT es de vital importancia realizar una retroalimentación efectiva tanto de los temas negativos o por mejorar como de los positivos con el fin de incentivar al personal y reconocer el trabajo realizado por cada uno de los componentes que soportan la capacidad estratégica del CSIRT en la ARC.

6.2 Prototipo de un CSIRT: Caso Armada Nacional.

Dentro de la estructuración del presente prototipo se construyó la matriz de interesados del CSIRT acuerdo los lineamientos internos de la gestión de proyectos de la ARC, igualmente se tuvieron en cuenta las capacidades actuales de la Dirección de Cibernética Naval de la ARC, pero dentro del apartado 5.4 Análisis de Madurez de las Capacidades de CIBER en la ARC, el cual fue parte del análisis realizado y es necesario para poder establecer los siguientes apartes dentro de la presente monografía; partiendo de lo anterior, se delimita la presente monografía al prototipo de organigrama de la dependencia, la descripción y función de cada una de las áreas que lo conforman.

6.2.1 Gestión de Interesados

Dentro de este apartado se desarrolla la administración y gestión de interesados "Stakeholder Management". Esta gestión resulta primordial dentro del CSIRT y en especial para el caso de estudio en la ARC, igualmente esta, tiene una organización (piramidal), este plan será desarrollado mediante el formato estandarizado por la institución y es utilizado para captar la participación activa y eficaz de los potenciales participantes o interesados a lo largo

de las fases del ciclo de vida del CSIRT, es trascendental realizar un análisis preciso de las expectativas, actitudes (positiva, neutral o negativa), interés y poder que estos ejercer para el desarrollo y éxito del mismo.

A continuación, se desarrolla el formato de registro de interesados del proyecto, el cual es requerido y ordenado por la Jefatura de Planeación Naval a través de la Dirección de Proyectos Especiales de la ARC, los cuales son las dependencias rectoras para la estructuración de cualquier tipo de proyecto dentro de la institución; y para lo cual, utilizare información real referente al proyecto, pero los nombres de los encargados no fueron relacionados en el formato primero por temas de seguridad del personal, así como por la alta rotación y variación de los mismos al interior de la ARC.

Tabla 9: Registro de Interesados del CSIRT.

ARMADA NACIONAL REPUBLICA DE COLOMBIA			**FORMATO REGISTRO DE INTERESADOS DEL PROYECTO**				
			Proceso: Gestión de Proyectos Institucionales			**Autoridad:** JEPLAN	
Código: GEPROI-FT-3238-JEPLAN-V02			**Rige a partir de:** 25/06/2016			Página **x** de **y**	
CONTROL DE VERSIONES DEL REGISTRO							
VERSIÓN	**FECHA**	**RESPONSABLE**		**MOTIVO**			
2	2019-01-01	Gerente de Proyecto		Presentación de Proyecto			
INTERESADOS DEL PROYECTO				**EVALUACIÓN**	**CLASIFICACIÓN**		
NOMBRE	**ORGANIZACIÓN**	**ROL**	**INFORMACIÓN DE CONTACTO**	**EXPECTATIVAS PRINCIPALES**	**ACTITUD (Positiva, Neutral o Negativa)**	**INTERÉS (1=Min, 5=Máx)**	**PODER (1=Mín, 5=Max)**
COARC	ARC	Project Manager, Patrocinador Proyecto	Oficina COARC	Garantizar la Sostenibilidad y Ejecución del Proyecto	Positiva	4	5
CARMA-JONA	ARC	Cliente	Oficina JONA	Obtener Información para Apoyo a Operaciones	Positiva	4	4
Fuerzas Navales	ARC	Clientes	Comandantes y/o JEM	Mantener el Grado de Seguridad de la Información (Disponibilidad,	Positiva	4	3

				Integridad y Confidencialidad)			
JINA	ARC	Gerente del Portafolio Proyecto	Oficina JINA	Obtención Total de los Objetivos del Proyecto	Positiva	5	5
JEPLAN	ARC	Proveedor de Recursos Funcionales	Oficina JEPLAN	Ejecución de los Recursos Presupuestales	Positiva	5	5
OPLAIN	ARC	Equipo de Gestión y Apoyo del Proyecto	Oficina OPLAIN	Planeación Efectiva, y Aprobación	Positiva	5	3
JOLA	ARC	Clientes, Proveedor de Recursos Funcionales	Oficina JOLA	Mantener la Seguridad de la Información	Neutral	3	3
DITEL - DINFO	ARC	Principal Cliente, Infraestructura Critica, Proveedor	Oficina DITEL - DINFO	Mantener la Seguridad de la Información	Positiva	4	3
DICIB	ARC	Dueño de la Capacidad	Oficina DICIB	Compartir Experiencias, Protección de la Fuerza	Positiva	5	5
Oficinas Telemáticas ARC (Oficiales de Seguridad Informática)	ARC	Clientes, Coordinadores Unidades	Oficinas Telemáticas	Compartir Experiencias, Protección de la Fuerza, Primer Actor ante un Incidente	Positiva	4	3
Oficinas Telemáticas Otras Fuerzas (Ejército, Fuerza Aérea)	FF.MM	Clientes, Proveedores, Cooperación Conjunta.	Oficinas Telemáticas	Compartir Experiencias, Protección de la Fuerza	Neutral	3	3
J8	CGFM	Clientes, Proveedores	Oficina J8	Mantener la Seguridad de la Información	Positiva	4	2
CCOC	CGFM	Cliente, Coordinador CSIRT FF.MM	Oficina CCOC	Compartir Experiencias, Protección de la Fuerza	Positiva	4	3
CSIRT Gobierno	Externo Público	Cooperación	Coordinador CSIRT	Compartir Experiencias, Protección y Seguridad	Positiva	4	2
CSIRT PONAL	PONAL	Clientes, Proveedores, Cooperación Conjunta.	Coordinador CSIRT PONAL	Compartir Experiencias, Protección y Seguridad	Positiva	4	2
COLCERT	Externo Público	Cooperación	Coordinador COLCERT	Compartir Experiencias, Protección y Seguridad	Positiva	4	2
CSIRT Sectoriales	Externo Público – Privado	Cooperación	Coordinadores CSIRT	Compartir Conocimiento y Experiencia	Positiva	3	2
Empresas (Infraestructuras	Externo Público – Privado	Clientes, Proveedores,	Coordinadores de TIC	Compartir Experiencias,	Neutral	3	3

Criticas Asignadas)		Cooperación Conjunta.		Protección y Seguridad			
Proveedores de Soluciones	Externo Privado	Cooperación	Ing. de Ventas o Consultor	Compartir Conocimiento y Experiencia	Positiva	4	2

Fuente: Elaboración Propia.

Dentro del resultado obtenido de la gestión, identificación y análisis de interesados a través de la cuantificación y valoración desplegada en la tabla anterior, lo cual, evidencia que el proyecto se encuentra entre la escala de 4 a 5 puntos en el eje de poder y en casi la misma proporción con relación al interés, lo que nos permite obtener una posición inicial del proyecto favorable; Lo cual ocasiona y concibe desafíos importantes dentro de esta gestión, para lograr conservar y mantener unos niveles altos de interés con relación al CSIRT, generando la creación de medidas para cautivar a los otros interesados que están en un estado neutral y bajo. Como se puede ver en la siguiente ilustración.

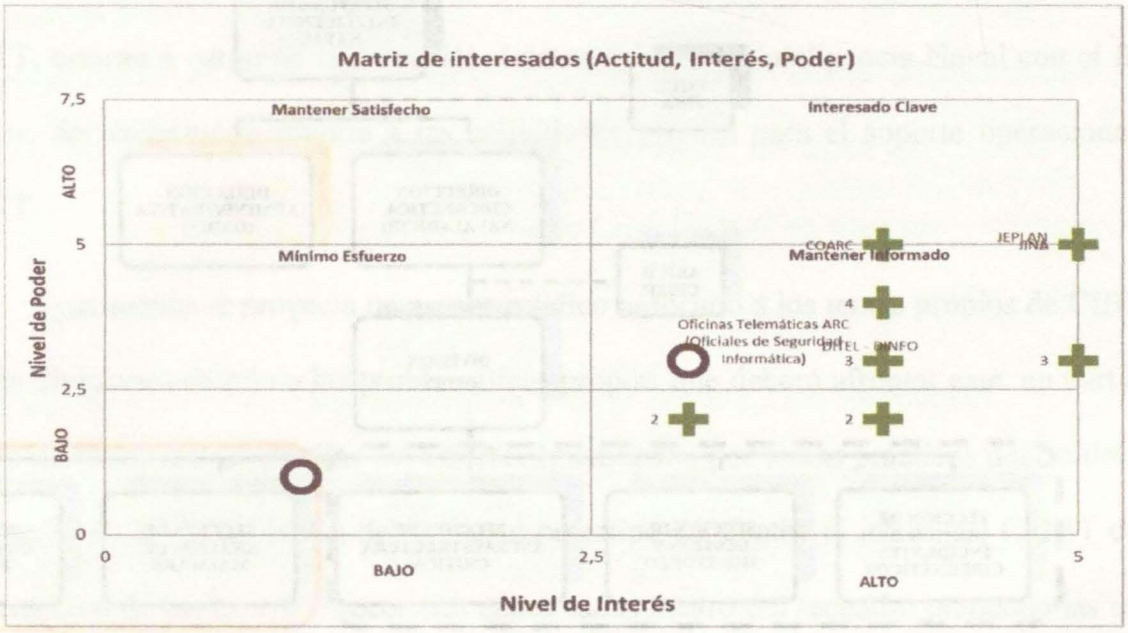

Ilustración 14: Matriz de Interesados del Proyecto. Fuente: Elaboración Propia.

6.2.2 Prototipo de Organigrama del CSIRT.

Dentro de este, se presenta el organigrama propuesto para la Armada Nacional, basado en las capacidades con las que debería contar este tipo de división, se explicarán las capacidades, toda vez que los servicios fueron presentados en el apartado 5.6.2 Primeros Servicios del CSIRT, acuerdo la ilustración No. 12: Servicios de Iniciación CSIRT ARC, igualmente se plantearán las funciones específicas de cada una de las secciones que están demarcadas con el recuadro negro con líneas punteadas y las secciones que están en color naranja, igualmente se aclara que estas últimas se proyectan desarrollar a mediano y largo plazo toda vez que no se cuentan en este momento con ninguna capacidad especifica en la ARC para afrontar estos temas.

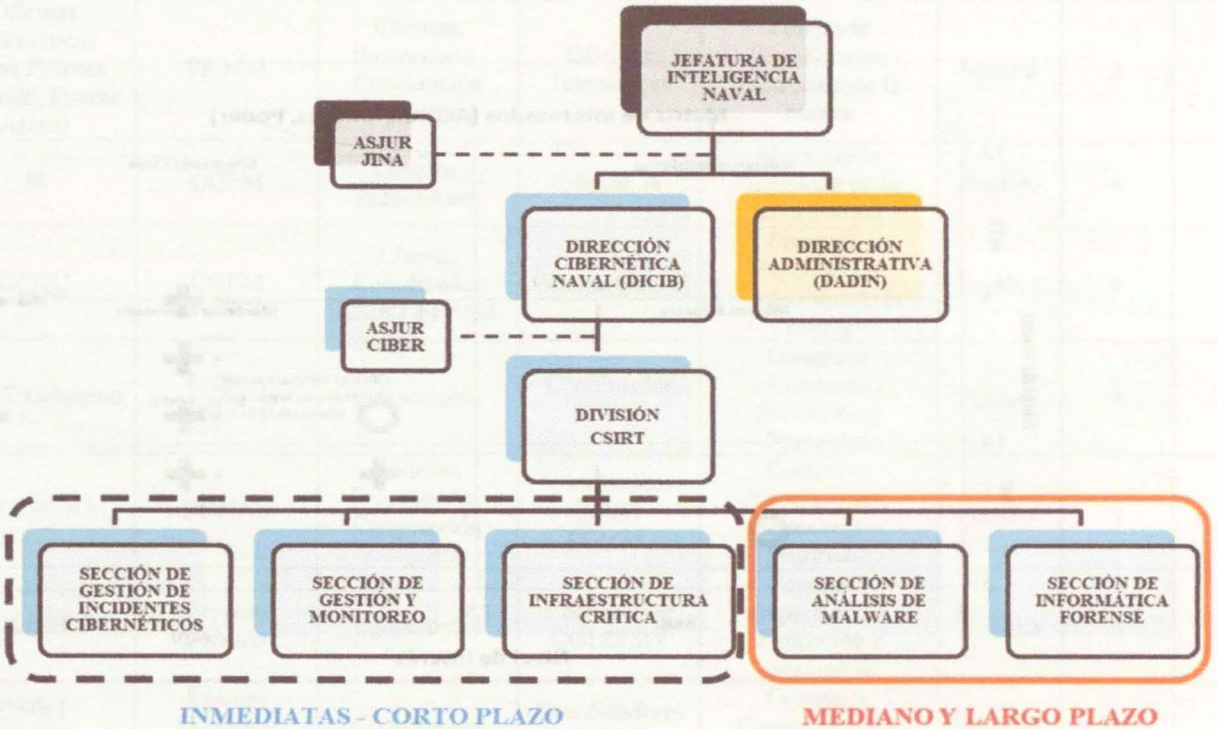

Ilustración 15: Organigrama Proyectado para el CSIRT. Fuente: Elaboración Propia.

Con el anterior organigrama (Ver ilustración anterior), y los contenidos desarrollados dentro del apartado 6.2.2 Prototipo de Organigrama del CSIRT, se da respuesta a la pregunta de investigación: ***"¿Cómo debería ser el prototipo organizacional del CSIRT de la ARC para prestar respuesta a incidentes de seguridad informática?"***, incesante, dentro del prototipo se plantea una estructura organizacional jerárquica piramidal con visión global del problema, adecuada a las necesidades potenciales y futuras de la ARC.

Esta unidad está inmersa dentro de la Jefatura de Inteligencia Naval, bajo el liderazgo de la Dirección de Cibernética Naval, la cual tendrá dentro de su estructura el control operacional la División de CSIRT y esta a su vez estará conformada por cinco (05) secciones, todas estas con su rol o función particular y específica dentro del funcionamiento orgánico funcional de un CSIRT, así mismo, dentro de este prototipo, se plantea que la unidad encargada de asumir o gestionar todos los temas logísticos y administrativos dentro del CSIRT, estarán a cargo de la Dirección Administrativa de Inteligencia Naval con el fin de asumir, dar solución y soporte a las actividades propias para el soporte operacional del CSIRT.

Igualmente se proyecta un asesor jurídico enfocado a los temas propios de CIBER y demás divisiones debido a las problemáticas propias que deberá afrontar este, en particular dentro de las temáticas propias del CSIRT. Igualmente, por temas prácticos dentro del caso de estudio en la ARC, dentro del presenté prototipo se plantea el inicio del CSIRT con la construcción de las tres (03) secciones enmarcadas dentro del recuadro punteado las cuales se plantean sean desarrolladas de forma inmediata o a corto plazo las cuales se describirán

más adelante, mientras que las dos (02) secciones enmarcadas en color naranja serán implementadas en mediano y largo plazo.

Igualmente, dentro del presente prototipo se plantea que el CSIRT para la ARC sea centralizado, ubicado en la ciudad de Bogotá ya que permite un mayor despliegue administrativo y logístico para atender de forma rápida y oportuna los incidentes que se puedan presentar en cualquier parte del país. Teniendo en cuenta la cantidad de incidentes presentados durante el año 2018, los cuales fueron consolidados y tamizados de manera explícita en la Tabla No. 5: Eventos por Fuerza Naval en la ARC y en la Ilustración No. 9: Eventos por Fuerza Naval en Porcentajes dentro del apartado 5.5 de la presente monografía, esto apoya de manera cuantitativa el tipo de CSIRT para la ARC.

El Comando de la ARC es la zona geográfica en donde se encuentran implementados la mayor parte de controles, equipos de monitoreo, seguridad perimetral y redes de comunicación, actualmente es donde existe la mayor concentración de infraestructura critica de la ARC y es desde allí donde se gobierna y gestiona más del 70% de las comunicaciones digitales y análogas de la ARC y el otro 30% está distribuido en las otras zonas (FNC, FNP, FNO y FNS).

El prototipo del CSIRT en la ARC estará conformado por un equipo interdisciplinario (tripulantes de tiempo completo) especializado en temas de tecnología, redes, seguridad, matemáticos, desarrolladores entre otros, los cuales estarán acantonados y tienen como función única y primordial la acción proactiva, preventiva y reactiva frente a eventos y/o acciones maliciosas en toda la institución, con el fin de aprovechar y optimizar los recursos

humanos, técnicos, tecnológicos, físicos y funcionales de esta capacidad en proyección y construcción al interior de la ARC.

6.2.2.1 Dirección Administrativa (DADIN)

Esta dirección es la encargada de dirigir y apoyar toda la gestión logística dentro de la Jefatura de Inteligencia Naval, la cual dentro de su función y misión principal es brindar todo el apoyo administrativo, logístico requerido y necesario para el cumplimiento de la misión principal de las otras direcciones operativas propias de la jefatura (ARC, 2012).

Dentro de sus divisiones se encuentran todas las relacionadas a la parte de gestión del talento humano, gestión de servicios generales (mantenimiento), gestión de adquisiciones de bienes y servicios, gestión de gastos reservados operacionales y planeación, así como el resto de productos propios para el normal y oportuno funcionamiento de las direcciones y unidades desplegadas a nivel nacional.

Es por esta razón, que esta dirección es presentada dentro de la ilustración No. 15, debido a su importancia para el desarrollo e implementación de la capacidad de CSIRT dentro de la Armada Nacional.

6.2.2.2 Dirección Cibernética Naval (DICIB)

Esta dirección es la encargada de comandar, organizar, dirigir y proyectar las capacidades cibernéticas dentro de la Armada Nacional, la cual organizacionalmente hace parte de la Jefatura de Inteligencia Naval, dentro de su función y misión principal es la de prevenir, detectar, neutralizar y contrarrestar la ocurrencia de todo riesgo, amenaza o ataque

de naturaleza cibernética que afecte los intereses marítimos, fluviales e infraestructura crítica asignada a la Armada Nacional (ARC, 2017).

Igualmente, tiene como responsabilidad direccionar y proyectar las políticas, estrategias y capacidades de ciberdefensa y ciberseguridad al interior de la Armada Nacional.

Es por esta razón, que dentro del presente trabajo de monografía se propone que el CSIRT dependa organizacional y operativamente de esta dirección, teniendo en cuenta la naturaleza con la cual fue creada y la capacidad que se proyecta al corto y mediano plazo.

6.2.2.2.1 Asesor Jurídico CIBER

Esta oficina Jurídica será la encargada de dirigir, proteger las actuaciones enmarcadas dentro de la legalidad y la ley de todas las actividades y capacidades cibernéticas al interior de la Armada Nacional, la cual organizacionalmente hace parte de la Dirección Cibernética Naval, dentro de su función y misión principal es la de asesorar al Director de Cibernética Naval, sobre las implicaciones jurídicas y cambios legales que surtan del ejercicio del quinto dominio de la guerra, así como velar por la apropiada aplicabilidad de las capacidades cibernéticas dentro del marco de la legalidad y la constitución política colombiana.

Apoyar y gestionar la construcción y elaboración de políticas relativas al buen uso de las capacidades del CSIRT, así como el apoyo en la adecuada cadena de custodia de todo el material objeto de prueba que pueda servir dentro de una investigación ante la ocurrencia de un incidente informático al interior de la ARC.

6.2.2.2.2 División CSIRT

Esta División será la encargada de gestionar, dirigir, atender los eventos que afecten la ciberseguridad al interior de la Armada Nacional, la cual organizacionalmente hace parte de la Dirección Cibernética Naval, dentro de su función y misión principal es la de responder, apoyar y dirigir todas las actividades realizadas en el centro de operaciones de seguridad cibernética de la ARC, con el fin de prevenir, detectar, predecir y neutralizar posibles ataques informáticos.

Implementar planes de conciencia situacional, capacitación y sensibilización al interior de la ARC, basado en lo evidenciado y analizado por medio del proceso de vigilancia tecnológica, inteligencia de amenazas, vulnerabilidades y riesgos al interior de la ARC.

Mantener coordinación continua con el Centro de Respuesta a Incidentes de Colombia (colCERT) y los Centros de Respuesta a Incidentes CSIRT de países aliados, el Comando Conjunto Cibernético (CCOC) y de las Fuerzas.

Efectuar una adecuada gestión de datos y conocimientos al interior de la ARC, mediante la implementación de servicios para ayudar a adquirir, procesar, difundir de forma oportuna y eficaz conocimientos, bases de datos de indicadores de compromiso y catálogos o huellas de software maligno que puedan o hayan afectado la infraestructura tecnología de la ARC.

Desarrollar, actualizar y documentar los procedimientos específicos y la Doctrina Naval Cibernética que permitan a los administradores de TICs ARC, a mantener actualizado

con los parches de seguridad y las medidas de seguridad necesarias a las plataformas tecnológicas que soportan los procesos críticos de la Institución.

a. Sección de Gestión de Incidentes Cibernéticos

Esta Sección será la encargada de todos los servicios relacionados para la gestión de incidentes de ciberseguridad al interior de la Armada Nacional, la cual organizacionalmente hace parte de la División CSIRT, dentro de su función y misión principal es la de gestión de eventos de ciberseguridad, la gestión de alertas, coordinación de recolección, respuesta, contención, mitigación y recuperación de un incidente cibernético al interior de la infraestructura de TIC de la ARC.

Analiza y procesa la información recolectada por los especialistas de las otras secciones, generando un análisis del o los incidentes presentados y emitiendo las ordenes, recomendaciones y acciones a implementar por parte del encargado de cada infraestructura TIC a nivel nacional (Oficiales de Seguridad Informática y encargados de las oficinas de TICs de cada unidad).

Coordinar, atender y responder oportunamente a las alertas e inteligencia compartida sobre potenciales amenazas que se detecten, afecten o se compartan con otros CSIRT.

Coordinar y apoyar la gestión del Oficial de seguridad Informática de la Dirección de tecnologías de la información y las comunicaciones de la ARC, la evaluación y cumplimiento de las acciones y restricciones de seguridad informática a los servicios críticos de la ARC, así como la evaluación y mitigación de riesgos. Apoyados en el manual de Seguridad de la información y las políticas y directrices vigentes en la Armada Nacional.

b. Sección de Gestión y Monitoreo

Esta Sección será la encargada de monitorear las capacidades cibernéticas dentro de la Armada Nacional, la cual organizacionalmente hace parte de la División CSIRT, dentro de su función y misión principal es la de realizar la correcta gestión y monitoreo de seguridad para reforzar los esquemas perimetrales que permitan tener una visión global en cuanto a la amenaza cibernética actual y potencial.

Monitorear de forma activa toda la actividad digital que circula a través de la infraestructura Crítica Cibernética Naval, a través de la operación de sistemas de seguridad, gestión de vulnerabilidades y gestión de incidentes de seguridad, permitiendo mitigar las amenazas e incidentes potenciales de forma preventiva, detectándolos, conteniéndolos y neutralizándolos de forma proactiva y oportuna reduciendo el impacto en la institución.

Monitorear las Infraestructuras Críticas y minimizar los riesgos informáticos asociados con la información estratégica de la Armada Nacional, así como reforzar la protección de los sistemas informáticos.

Monitorear y garantizar la operatividad y seguridad de las plataformas tecnológicas y servicios en la Armada Nacional.

Efectuar el correspondiente monitoreo de los eventos que se reflejan con mayor relevancia, así como los diferentes incidentes de seguridad reportados como detectados, investigando y analizando las causas y recomendando las mejores prácticas, con el fin de evitar nuevos sucesos.

Elaborar protocolos y procedimientos para atención, respuesta y cierre de incidentes, así como velar por el correcto funcionamiento de los canales de comunicación y difusión de información del SOC.

c. Sección de Infraestructura Critica

Esta Sección será la encargada de promover y coordinar las capacidades cibernéticas dentro de la Armada Nacional, la cual organizacionalmente hace parte de la División CSIRT, dentro de su función y misión principal es gestionar y coordinar con la Dirección de Informática de la Armada Nacional, los mecanismos necesarios para la seguridad de las Infraestructuras Críticas Cibernéticas Navales, a través de la participación de todos los involucrados en la seguridad informática, generando confianza e integrando esfuerzos para minimizar los riesgos ante Amenazas Cibernéticas actuales y potenciales.

Atender y responder oportunamente ante cualquier incidente Cibernético que genere de una u otra forma afectación e impacto a las Infraestructuras Criticas digitales de la fuerza, logrando oportunamente y en tiempo real su detección y ágil neutralización.

Elaborar y mantener actualizada con la coordinación de Infraestructuras Críticas Civiles y Fuerza Pública la guía de gestión y catalogación de Infraestructuras Críticas cibernéticas Navales, Marítimas y fluviales del país.

Definir, catalogar y mantener actualizadas las Infraestructuras Críticas Digitales en la Armada Nacional y en el ámbito marítimo a fin de ser protegidas.

Elaborar alertas que permitan desarrollar acciones preventivas y correctivas que puedan anticipar o mitigar los incidentes cibernéticos.

d. Sección de Análisis de Malware

Esta Sección será la encargada de analizar el software maligno que pretenda comprometer y afectar las capacidades cibernéticas dentro de la Armada Nacional, la cual organizacionalmente hace parte de la División CSIRT, dentro de su función y misión principal es la de efectuar analizar y comprender la naturaleza de artefacto digital malicioso, entender su comportamiento y vector de ataque y lograr realizar ingeniería inversa para determinar las características propias del mismo.

Estudiar y comprender la táctica, técnica y procedimientos propios del Malware, su patrón de ataque y dentro del sistema informático y redes para llevar a cabo las actividades maliciosas dentro de la infraestructura de la ARC.

Identificar su estructura básica como metadatos, huella o firma del archivo, sitios de instalación y camuflaje, malignidad, tipos de archivos que utiliza entre otros, todo esto con el fin de generar acciones para mitigar sus daños y obtener una pronta recuperación.

Lograr descubrir puntos de familiaridad con otros artefactos maliciosos, determinar tendencias o similitudes y lograr identificarlos para contrarrestar sus consecuencias y obtener un catálogo unificado de estos.

e. Sección de Informática Forense

Esta Sección será la encargada de recolectar las evidencias digitales mediante el uso de equipos técnicos forenses especializados al interior de la Armada Nacional, la cual organizacionalmente hace parte de la División CSIRT, dentro de su función y misión principal es la de análisis de medios, con el fin de analizar datos, comportamientos del

sistema, software, redes informáticas, almacenamiento digital y medios extraíbles (USB, DD, entre otros).

Colectar, almacenar y analizar las pruebas digitales de medios como equipos de red, PC, discos duros, dispositivos móviles celulares, Tablet, almacenamiento extraíble USB, almacenamiento en la nube, así como otros activos de información contenido en documentos y multimedia.

Realizar análisis forense digital mediante la aplicación de técnicas científicas y especializadas a la infraestructura tecnológica de la ARC afectada, que permita reconstruir el activo informático, examinar datos residuales, mediante la colección, identificación, preservación, utilización de estos para generar un análisis pericial y forense de evidencia, datos e información; que sirvan como soporte y prueba dentro de una investigación.

Recolectar toda la evidencia informática disponible en el activo informático afectado, observando la cadena de custodia de la prueba y el debido proceso, garantizando la integridad, confidencialidad y disponibilidad de la misma.

VII. CONCLUSIONES.

Basados en la determinación de conceptos propios para la creación de un CSIRT, para la Armada Nacional de Colombia el tipo que más se adapta a sus necesidades es el militar, basados en la función y misión particular.

Basados en el nivel de madurez de las capacidades de CIBER y los tipos de servicios de los CSIRT, la Armada Nacional de Colombia solo puede prestar servicios básicos (estableciendo tiempos, capacidades, actividades y expectativas), toda vez que tiene problemas graves de personal (falta de personal), el talento humano existente no cuenta con las capacidades intelectuales (capacitación y experiencia), técnicas (equipos) y tecnológicas (herramientas especializadas) para prestar servicios de mayor complejidad como análisis de malware y análisis forenses, entre otros.

La Armada Nacional de Colombia es consciente de sus limitaciones, deficiencias y riesgos, los cuales son generados al contar con una red distribuida conformada por una diversidad de equipos comerciales, militares soportados bajo tecnologías de comunicación critica conectada y disponible en todas sus unidades a nivel nacional, por la cual viaja información sensible de tipo táctico, operacional y estratégico; Por lo anterior, es primordial y necesario que se adelanten las gestiones presupuestales para implementar el CSIRT al interior de la organización, con el fin de minimizar los riesgos, neutralizar amenazas, detectar vulnerabilidades, realizar una gestión adecuada de sus tecnologías e infraestructuras críticas nacionales y maximizar la eficiencia de prevención, detección y resiliencia ante incidentes de seguridad.

De acuerdo a los datos analizados, la Armada Nacional de Colombia sufrió la mayor cantidad de incidentes y ataques informáticos en las instalaciones del Comando de la Armada Nacional, toda vez que allí se encuentra alojada y contenida la gran mayoría de su infraestructura crítica y servicios TIC, adicionalmente desde allí se realiza la gestión y atención de los diferentes tipos de requerimientos es por esto que son más recurrentes los incidentes en comparación con otras zonas del país, teniendo en cuenta los antecedentes anteriores se propone que el prototipo de CSIRT para la ARC funcione de manera centralizada en la ciudad de Bogotá, sumado a las ventajas geográficas que esta ciudad ofrece por su facilidad logística (Transporte, Tecnología y Equipos) y así minimizar gastos, optimizar esfuerzos, explotar y aprovechar capacidades.

Tomando como referencia las iniciativas, convenios y legislación para hacerle frente a las amenazas en el ciberespacio; la Armada Nacional debe fortalecer e implementar capacidades para trabajar bajo esta línea de cooperación interinstitucional e internacional para la mitigación de los ciberataques que buscan debilitar la seguridad y sinergia de las operaciones; por lo anterior es vital la creación e implementación de CSIRT para dinamizar y facilitan el intercambio de alertas, información, capacitación y buenas prácticas.

Basados en el análisis y estudio realizado, la ARC debe contemplar la posibilidad de desarrollar e implementar la metodología y el prototipo organizacional de CSIRT presentado en el trabajo de grado, toda vez que esta se ajusta a las necesidades propias y forma de operar de la ARC, adicionalmente se conformó extrayendo de las cuatro metodologías más usadas las características relevantes que servían para la institución y fue concebida y alineada bajo

las directrices institucionales de la planeación por capacidades que exige el Comando General de las FFMM y la Armada Nacional.

La Armada Nacional actualmente dentro de su infraestructura vital digital contempla diferentes sistemas asociados a TI y la operación; tales como: bases de datos operacionales, sistemas de información geográficos operacionales, sistemas de controles de armas navales, sistemas de navegación incorporados en buques, submarinos y aviones, sistemas de comunicación operacional tanto digitales como análogos, entre otros; los cuales son indispensables para el desarrollo de las operaciones. Por lo anterior, la institución debe enfocar sus esfuerzos para implementar las capacidades planteadas en el trabajo de grado dentro del cuatrienio 2019 – 2022 para fortalecer sus capacidades de Ciberdefensa que permitan enfrentar de forma proactiva y efectiva los intentos de afectación de su infraestructura critica naval para minimizar los riesgos potenciales dentro de la Armada Nacional de Colombia.

Apoyados en los análisis realizados, la Armada Nacional debe trabajar y pensar en realizar una estructuración organizacional a la Dirección Cibernética Naval, ya que actualmente no tiene incorporado dentro de su organización la División de CSIRT con todas las secciones y capacidades planteadas dentro del trabajo, ni tampoco al asesor jurídico CIBER, lo cual genera grandes vacíos procedimentales y jurídicos para ejercer una adecuada gestión de incidentes ante este tipo de amenazas en el ciberespacio.

La Armada Nacional debe implementar el CSIRT y los servicios de forma incremental, esto basado en el proceso de gestión piloto planteado dentro del trabajo, el cual debe funcionar en intervalos cortos de tiempo, que permita organizar y reorientar

imprevistos, buscando una retroalimentación activa entre las partes en pro de la mejora continua dentro del CSIRT, lo cual es una forma adecuada de iniciación y difusión de los servicios del CSIRT al interior de la institución.

El prototipo organizacional propuesto del CSIRT, el cual se desarrolló teniendo en cuenta las capacidades actuales de la dirección cibernética y agrupando capacidades e incorporando personal capacitado, este trabajo representa un importante punto de partida y marco de referencia para que la ARC pueda continuar con las demás fases para la implementación de esta capacidad en el corto y mediano plazo.

VIII. REFERENCIAS BIBLIOGRÁFICAS

Armada Nacional de Colombia (2012). Manual de Funciones Dirección Administrativa de Inteligencia Naval.

Armada Nacional de Colombia (2017). Manual de Funciones Dirección Cibernética Naval.

Armada Nacional de Colombia (2018). Manual de Seguridad de la Información Armada Nacional.

Armada Nacional de Colombia (2015). Plan Estratégico Naval 2015 – 2018. https://www.armada.mil.co/sites/default/files/plan_estrategico_naval_2016_v2.pdf [Último acceso: 24 Noviembre 2017].

Banco Interamericano de Desarrollo – BID. Organización de los Estados Americanos – OEA. (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?. https://publications.iadb.org/bitstream/handle/11319/7449/Ciberseguridad-Estamos-preparados-en-America-Latina-y-el-Caribe.pdf [Último acceso: 24 Noviembre 2017].

Centro Criptológico Nacional. (2011). Guía de seguridad (CCN-STIC-810). Guía de creación de un CERT / CSIRT. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf [Último acceso: 24 Noviembre 2017].

Centro de Apoyo al Desempeño Académico. (s.f). Guía para definir objetivos basada en el método SMART. Universidad del Desarrollo. https://cada.udd.cl/files/2018/11/2.-B-.pdf

CERT-a. (s.f). CSIRT Frequently Asked Questions (FAQ). http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm

CERT-b. (s.f). CSIRT Services. http://www.cert.org/incident-management/services.cfm

CERT-c. (s.f). Create a CSIRT. Software Engineering Institute. Carnegie Mellon University. https://www.cert.org/incident-management/products-services/creating-a-csirt.cfm [Último acceso: 24 Noviembre 2017].

Choucri, N. (2000). Introduction: cyberpolitics in international relations.

Cichonski, P., Millar, T., Grance, T., Scarfone, K. (2012). Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. Special Publication 800-61 Revision 2. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [Último acceso: 24 Octubre 2017].

Comando General Fuerzas Militares. (2015). Las Fuerzas Militares y de Policía se preparan para nuevos escenarios de 2030. http://www.cgfm.mil.co/wp-content/uploads/2017/05/36-LAS-FUERZAS-2015.pdf [Último acceso: 24 Noviembre 2017].

Comisión Europea (2013). Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro. http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es

Consejo nacional de política económica y social – CONPES – 3854. (2016). Política nacional de seguridad digital República de Colombia. Departamento nacional de planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación. (2011). Lineamientos de política para Ciberseguridad y Ciberdefensa. Documento CONPES 3701, Bogotá D.C., Colombia: DNP. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Departamento Nacional de Planeación. (2016). Política Nacional de Seguridad Digital. Documento CONPES 3854, Bogotá D.C., Colombia: DNP. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

ENISA. (2006). Cómo crear un CSIRT paso a paso. Recuperado de FIRST - Forum of Incident Response and Security Teams. FIRST History. https://www.first.org/about/history

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR) relevant theory. International political science review, 27(3), 221-244.

FIRST - Forum of Incident Response and Security Teams. FIRST. (2019). Computer Security Incident Response Team (CSIRT). Services Framework Version 2.1.0. https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf

FIRST - Forum of Incident Response and Security Teams. FIRST History. https://www.first.org/about/history [Último acceso: 24 Octubre 2017].

García, J (2017), El ciberejército de Putin, Magazine Digital, 26 de marzo. http://www.magazinedigital.com/historias/reportajes/ciberejercito-putin

Gil, J. (2017). La Integración del Ciberespacio en el Ámbito Militar. Revista de Estudios en Seguridad Internacional. http://www.seguridadinternacional.es/?q=es/content/la-integraci%C3%B3n-del-ciberespacio-en-el-%C3%A1mbito-militar [Último acceso: 11 Noviembre 2019].

INCIBE-CERT (2016), BlackEnergy y los sistemas críticos. https://www.incibe-cert.es/blog/blackenergy-sistemas-criticos

Internet World Stats. World internet usage and population statistics. June 30, 2017 Update. http://www.internetworldstats.com/stats.htm

Izcara Palacios, S. P. (2014). Manual de investigación cualitativa. Fontamara. http://dide.minedu.gob.pe/handle/123456789/4613

Killmeyer, J. (2006). Information Security Architecture: An Integrated Approach to Security in the Organization, Second Edition. CRC Press. https://books.google.com.co/books?id=Mf3NBQAAQBAJ&pg=PA201&lpg=PA201&dq=csirt+ARMY&source=bl&ots=HAoDUb8cjN&sig=R9Amxd4lygfJiYfrXEAlKAFZG0M&hl=es&sa=X&ved=0ahUKEwjTk_X85cvVAhWGYiYKHS9mBSEQ6AEIOjAC#v=onepage&q=csirt%20ARMY&f=false

Martín, E. (2016). Los retos de la Ciberinteligencia. Cuadernos de la Guardia Civil, (53), 53 – 67. http://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/local_repository/documents/18605.pdf

Mejía, J., Muñoz, M., & Uribe, E. (2015). Services Establishment in the Computer Security Incident Response Teams: A Review of State of Art. 2015 10th Iberian

Conference on Information Systems and Technologies (CISTI 2015), 858-863. doi: 10.17013/risti.e3.1-15. http://www.scielo.mec.pt/pdf/rist/nspe3/nspe3a02.pdf [Último acceso: 4 Octubre 2017].

Ministerio de Comunicaciones. (2008). Diseño de un CSIRT De Colombia para la estrategia Gobierno en Línea. República de Colombia. http://www.vive.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/3._Diseno_de_un_CSIRT_Colombiano.pdf

Ministerio de Defensa Nacional. (2018). Guía Metodológica de Planeamiento por Capacidades. http://capacitas.mindefensa.gov.co/storage/biblioteca/Guia_Metodologica_de_Planeacion_por_Capacidades.pdf

Ministerio de Defensa Nacional. (2016). Resolución Ministerial No. 0940 de 2016 por la cual se aprueba la Disposición No. 001 del 12 de enero de 2016, expedida por el Comandante General de las Fuerzas Militares. Bogotá, D.C.: Ministerio de Defensa Nacional.

Mosso, J. (2015). Ciberseguridad Inteligente. Bacchuss, División Ciberdefensa. https://arxiv.org/pdf/1506.03830.pdf

Muñoz, M., & Rivas, L. (2015) Estado actual de equipos de respuesta a incidentes de seguridad informática. Revista Ibérica de Sistemas y Tecnologías de la Información – RISTI (spe3), 1 – 15. Doi: 10.17013/risti.e3.1-15. http://www.scielo.mec.pt/pdf/rist/nspe3/nspe3a02.pdf

Nye Jr, JS (2004). Poder en la era de la información global: del realismo a la globalización. Routledge.

Observatorio de la Ciberseguridad en América Latina y el Caribe. (2016). Informe ciberseguridad. ¿Estamos preparados en américa latina y el caribe?. https://www.academia.edu/38576559/Ciberseguridad_Estamos_preparados_en_Am%C3%A9rica_Latina_y_el_Caribe_Mejorando_vidas_Organization_of_American_States

Organización de los Estados Americanos – OEA. (2016). Buenas prácticas para establecer un CSIRT nacional. https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Ramírez, H. & Mejía, J (2015). Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT). Revista Electrónica de Computación, Informática, Biomédica y Electrónica. (Vol. 4 No. 1).

Robert Morgus, R., Skierka, I., Hohmann, M., Maurer, T. (2015). National CSIRTs and their role in computer security incident response. http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response_November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf

Rodríguez, Y. (2013). El impacto de la racionalidad limitada en el proceso informacional de toma de decisiones organizacionales. http://www.acimed.sld.cu/index.php/acimed/article/view/401/282

Skierka, I., Morgus, R., Hohmann, M., & Maurer, T. (2015). CSIRT Basics for Policy-Makers. The History, Types & Culture of Computer Security Incident Response Teams. Global Public Policy Institute – GPPi. http://www.digitaldebates.org/fileadmin/media/cyber/CSIRT_Basics_for_Policy-Makers_May_2015_WEB_09-15.pdf

Tamara, N. (2014). Enfoque Gerencial de las Fuerzas Militares de Colombia: Caso Ejército Nacional De Colombia. (Ensayo de Administración de Empresas). Universidad Militar Nueva Granada. Bogotá, DC. http://repository.unimilitar.edu.co/bitstream/10654/12882/1/1.%20ENFOQUE%20GERENCIAL%20DE%20LAS%20FUERZAS%20MILITARES%20DE%20COLOMBIA.pdf

Unión Internacional de Telecomunicaciones (2019), Estadísticas. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx [Último acceso: 06 Abril 2020].

West-Brown, M., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

Whitman, M., Herbert, J., Mattord, H., & Green, A. (2013). Principles of Incident Response and Disaster Recovery. Cengage Learning. https://books.google.com.co/books?id=d9MbBQAAQBAJ&pg=PA241&lpg=PA241&dq=OBJECTIVES+CSIRT&source=bl&ots=hZqS8mknro&sig=dU21FqBAjUIq6q16SaA6yJIrBvM&hl=es&sa=X&ved=0ahUKEwiVvJqNtNjVAhWB6SYKHa22A_U4ChDoAQgjMAA#v=onepage&q=OBJECTIVES%20CSIRT&f=false