



Aplicabilidad de una arquitectura de seguridad
adaptativa para el despliegue de un Security
Operations Center Inteligente ISOC en la Armada
Nacional

John Deivy Díaz Narváez

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

TMCIBER 2018

004

Ej. 2

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA



"General Rafael Reyes Prieto"
Unión, Proyección, Liderazgo

APLICABILIDAD DE UNA ARQUITECTURA DE SEGURIDAD ADAPTATIVA
PARA EL DESPLIEGUE DE UN SECURITY OPERATIONS CENTER
INTELIGENTE (ISOC) EN LA ARMADA NACIONAL

ALUMNO JOHN DEIVY DÍAZ NARVÁEZ

DIRECTOR MANUEL HUMBERTO SANTANDER PELÁEZ

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE MAGISTER EN
CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTÁ D.C. – COLOMBIA

2018

586505

Dedicatoria

Nota de aceptación

Este trabajo es dedicado principalmente a Dios como creyente fundamental para el logro de todos mis objetivos, a mi señora esposa por su constante apoyo y dedicación en los momentos de estudio, a la Armada Nacional por brindarme la oportunidad de realizar y crecer en mi formación profesional y en general a todos los tutores y compañeros quienes contribuyeron significativamente en mis estudios de maestría en Ciberseguridad y Ciberdefensa.

Jurado

Jurado

Jurado

Dedicatoria

Este trabajo es dedicado principalmente a Dios como eje fundamental para el logro de todos mis objetivos, a mi señora esposa por su constante apoyo y dedicación en los momentos de estudio, a la Armada Nacional por brindarme la oportunidad de realizar y crecer en mi formación profesional y en general a todos los tutores y compañeros quienes contribuyeron significativamente en mis estudios de maestría en Ciberseguridad y Ciberdefensa.

Agradecimientos

Agradezco al Gobierno Nacional-Ministerio de las Tecnologías de la Información y las Comunicaciones TIC's por generar espacios que contribuyen al fortalecimiento del talento humano de las entidades del estado colombiano. A la Escuela Superior de Guerra por diseñar, crear y poner en marcha la Maestría de Ciberseguridad y Ciberdefensa.

Al Ingeniero Manuel Santander por su constante apoyo y direccionamiento en cada una de las etapas que comprendieron este trabajo de grado y a todas las personas que directa e indirectamente también ayudaron a la realización de este proyecto.

Resumen

La evolución de las tecnologías de la información y las comunicaciones (TIC's) han permitido avances a la sociedad en diferentes sectores, así mismos la ciberdelincuencia y los delitos en el ciberespacio durante los últimos años han tenido una evolución en el mundo, llegando a generar desafíos para los países y organizaciones; es así como en la actualidad se están presentando un gran número de eventos de seguridad en las FFMM-ARC y donde surge la necesidad de implementar un centro de operaciones de seguridad (SOC) que permita mitigar los riesgos de Ciberseguridad originados por los eventos presentados.

Se pretende dar a conocer definiciones, arquitectura y funcionamiento de un SOC, así como su evolución a centros de operaciones de seguridad impulsados por inteligencia (ISOC) los cuales se basan en efectuar análisis avanzados de datos bajo una arquitectura de seguridad adaptativa que permitan funcionar bajo el ciclo de prevenir, detectar, responder y predecir ataques. Igualmente se buscan determinar las necesidades para el SOC de la Armada Nacional a partir del análisis de las capacidades en Ciberseguridad y Ciberdefensa requeridas para la institución, estableciendo los componentes requeridos en las variables de personas, procesos y tecnología para el correcto funcionamiento del ISOC y finalmente establecer un modelo propuesto de capacidades de Ciberseguridad de la ARC para la gestión, operación y funcionamiento de un ISOC.

Palabras Claves: Centro de Operaciones de Seguridad (SOC), Centro de Operaciones de Seguridad inteligentes (ISOC), seguridad adaptativa, Ciberseguridad.

Keywords: Security Operation Center (SOC), Intelligence Security Operation Center (ISOC), Adaptive security, Cybersecurity

Abstract

The evolution of information and communication technologies (ICTs) have allowed advances in different sectors of society, as well, in recent years the digital environment, cybercrime and crimes have had an evolution in the world; overcoming new challenges for countries and organizations. Currently, we are observing that there are a large number of security events in the National Armed Forces and here is where there is a necessity to implement a security operations center (SOC) to mitigate the cyber security risks to which the institution's information assets are exposed.

For this reason, this project intends to make the reader aware of the existing definitions, architecture and operation of a SOC security operations center, as well as, the evolutionary processes that have been taking place throughout history until reaching the last generation of SOC, which are known as intelligence-driven security operations centers (ISOCs). These (ISOCs) provide advanced data analysis based on an adaptive security architecture that allows them to operate under the cycle of preventing, detecting, responding and predicting attacks.

Likewise, it seeks to determine the needs for the SOC of the National Navy from the analysis of the capabilities in Cybersecurity and Cyberdefense required for the institution; setting up the required components in the variables of people, processes and technology for the proper functioning of the ISOC. Finally to establish a proposed model of Cybersecurity capabilities of the ARC for the management, operation and operation of an ISOC.

Keywords: Security Operation Center (SOC), Intelligence Security Operation Center (ISOC), Adaptive security, Cybersecurity.

Tabla de contenido

Introducción	11
Problema de Investigación	12
Pregunta de Investigación	13
Justificación	14
Objetivos	16
Objetivo General	16
Objetivos Específicos.....	16
Metodología	17
Estado del arte.....	18
1. Definición de Security Operation Center.....	18
1.1. Funcionamiento de un SOC	19
1.2. Arquitectura global de un SOC	21
1.3. Capacidades de un SOC	23
2. Evolución de los SOC.....	24
2.1. SOC de primera generación 1975-1995	24
2.2. SOC de segunda generación 1996-2001	26
2.3. SOC de Tercera generación 2002-2006	28
2.4. SOC de cuarta generación 2007-2012.....	29
2.5. SOC de quinta generación 2013 -.....?	31
3. Requerimientos del ISOC de la Armada Nacional	34
3.1. Capacidades en Ciberseguridad necesarias en una institución que se dedique a la Ciberdefensa.	34
3.2. Comparación de componentes de Personal, Doctrina, Material y Equipo en la Armada Nacional.	37
3.3. Análisis de capacidades de un ISOC en los componentes de Doctrina, Personal, Material Y Equipo.....	39
4. Componentes de arquitectura ISOC para la Armada Nacional	43
4.1. Componentes de capacidades que intervienen en los procesos de operación y gestión de un Intelligence Security Operations Center	43
4.1.1. Componente de Material y Equipo	46
4.1.2. Componente de Doctrina (Procesos)	47
4.1.3. Componente de Personal.....	48
4.2. Parámetros para el funcionamiento del Centro de Operaciones de Seguridad de la Armada Nacional	49

4.3.	Caracterización de plataformas SOC existente en la Armada Nacional	53
5.	Arquitectura de referencia para ISOC.....	58
5.1.	Definición de Intelligence-drive Security Operation Center.....	58
5.2.	Opciones de tecnología de los ISOC.....	60
5.2.1.	Plataformas de administración de vulnerabilidades y amenazas.	60
5.2.2.	Análisis de comportamiento de usuarios y de la entidad.	61
5.2.3.	Plataformas de respuesta a incidentes.....	61
5.2.4.	Plataformas de automatización de operaciones de seguridad.....	62
5.2.5.	Plataformas de engaño.	62
5.3.	Capacidades de un ISOC.....	64
5.4.	Plataformas ISOC a nivel mundial.....	69
6.	Aporte del ISOC al modelo de capacidades de ciberseguridad de la Armada Nacional	72
6.1.	Capacidades del ISOC en la Armada Nacional.....	72
6.2.	Gestionar el Programa de ciberseguridad.....	73
6.3.	Administración de personal.....	74
6.4.	Conciencia situacional.....	75
6.5.	Intercambio de Información y Comunicaciones	76
6.6.	Gestión de amenazas y vulnerabilidades.....	76
6.7.	Respuesta a eventos e incidentes, continuidad de operaciones y restauración de servicios	77
6.8.	Gestión de Riesgos	78
Conclusiones		80
Recomendaciones		82
Referencias Bibliográficas		83
Listado de Figuras.....		87
Listado de Tablas		88

Tabla de Abreviaturas

• Análisis de comportamiento de usuarios y de entidad.	UEBA
• Análisis impacto del negocio.	BIA
• Armada Nacional Republica de Colombia.	ARC
• Centros de operaciones de seguridad impulsados por inteligencia.	ISOC
• Comando General Fuerzas Militares.	CGFM
• Fuerzas Militares de Colombia.	FFMM
• Organización del Tratado del Atlántico Norte.	OTAN
• Plataformas de administración de vulnerabilidades y amenazas.	TVM
• Plataformas de respuesta a incidentes.	SIRP
• Plataformas de automatización de operaciones de seguridad.	SOAP
• Planes de continuidad de negocio.	BCP
• Security Operation Center.	SOC
• Tecnologías de la información y las comunicaciones.	TIC's
• Tecnologías información.	TI

Introducción

Los avances significativos de los sistemas de computadores brindados en el mundo de hoy y la gran cantidad de información que se genera y envía por la red de redes han motivado a las empresas a implementar equipos de seguridad que permitan vigilar los canales de comunicación, no solo para tener certeza sobre la información que sale de las entidades, sino también para estar alertas ante cualquier tipo de ataques e incidentes cibernético de los que puedan verse afectados por lo que se hace imprescindible realizar procesos de conciencia situacional que permitan mitigar los riesgos cibernéticos en las redes de las entidades. Igualmente con la evolución del internet surgieron ataques más sofisticados y elaborados que no se valdrían solamente de los virus, gusanos y troyanos para afectar a las organizaciones, por lo cual las empresas se vieron en la necesidad de implementar centros de operaciones de seguridad cibernética (SOC) que han evolucionado en el transcurso del tiempo y con las capacidades tecnológicas y computacionales para solventar los ataques informáticos que se vienen presentando a través de técnicas avanzadas, pero estos SOC (1ra-4ta generación) tampoco han podido solucionar la problemática de los ataques cibernéticos de última generación basados en malware, Apt's, ataques dirigidos, Ransomware, debido a que los atacantes también han evolucionado y modificado sus técnicas, por lo cual surge una nueva concepción de centros de seguridad impulsados por inteligencia (ISOC) los cuales ahora tienen los mecanismos y capacidades para prevenir, detectar, responder y predecir futuros ataques informáticos basados en comportamientos y el diseño de indicadores de compromiso, además que tienen la fortaleza de interactuar y compartir información con centros de inteligencia de amenazas de diferentes organizaciones para efectuar un proceso más eficaz en las etapas de predicción de posibles amenazas, todo esto basado en una arquitectura de seguridad adaptativa que usa herramientas y procesos de analítica de datos.

Problema de Investigación

La rápida evolución de las guerras y la sociedad han planteado el desafío de modernización tecnológica e innovación en las Fuerzas Militares para hacer frente a la amenaza de un enemigo que se renueva y adapta constantemente a un mundo globalizado que exige estar actualizado en el quinto dominio de la guerra “el Ciberespacio”. Igualmente la evolución tecnológica a nivel mundial y los continuos incidentes de seguridad que se presentan en las organizaciones dados a conocer durante los años 2014 y 2015 en los reportes emitidos por las empresas de seguridad Kaspersky, McAfee, cisco, Symantec y diferentes CSIRT del mundo (David Emm, Andrey Nikishin, Alexander Gostev, 2015) (cisco Lab. Talos Security Intelligence and Research, 2015) , se observa la necesidad de que las entidades establezcan medidas de seguridad cibernética que permitan efectuar un control efectivo y eficiente para prevenir, detectar, responder y predecir ataques cibernéticos a los que están expuestos sus activos de información; y es así como se logra evidenciar la necesidad de que no solo basta con los SOC (Security Operations Center) existentes en el Comando Conjunto Cibernético (en adelante: CCOC), el grupo de respuesta e emergencias cibernéticas de Colombia (en adelante: Colcert) y el Centro cibernético policial (en adelante: CCP), los cuales tienen la capacidad de efectuar monitoreo a sus activos y redes informáticas, y que cuentan con una gran cantidad de equipos de seguridad (Antivirus, firewall, IPS/IDS, DLP, Correlacionadores de eventos, etc.) para el monitoreo, supervisión y gestión de la seguridad en sus entidades, sino que es de mayor relevancia e interés establecer una arquitectura de seguridad adaptativa para la ARC por intermedio de un ISOC (Intelligent Security Operations Center) que permita gestionar correctamente los riesgos y a su vez genere productos de las actividades en el ciberespacio que intentan explotar vulnerabilidades de los sistemas de información de la

organización y que podrían llegar a causar daños a los sistemas y por tal motivo generar desventajas estratégicas a la fuerza y a la nación. Además, el concepto de seguridad de la información ha venido evolucionando con el tiempo, así fue como la Seguridad de la Información fue pasando de lo técnico a la gestión y de aquí a la institucionalización bajo normas universales como son los estándares de seguridad del NIST, la ISO/IEC 27000, para actualmente fortalecer la toma de conciencia que la seguridad es parte de los negocios, puesto que la información es un activo corporativo crítico para mantener sustentables las operaciones. Igualmente al no tener implementadas políticas claras de inteligencia operacional para enfrentar ataques informáticos avanzados se presentan problemáticas de no efectuar una correcta gestión de incidentes, malos planes de recuperación de desastres (BCP) y lo que es peor no se puede llegar a tener una visión clara y efectiva que permita mejorar la toma de decisiones por parte del alto mando.

Pregunta de Investigación

¿Qué capacidades en ciberseguridad y ciberdefensa genera una arquitectura de seguridad adaptativa de un ISOC en la Armada Nacional?

Justificación

La pertinencia del futuro proyecto es de alta relevancia y prioridad para la Armada Nacional, dado por el inminente desarrollo y evolución que están teniendo actualmente las TIC's y en especial el dominio del ciberespacio que día a día se convierte en el escenario de mayor interés para las diferentes acciones delictivas (Ciberataques, ciberespionaje, crimen organizado, ciberterrorismo, entre otros) que pueden llegar a afectar el funcionamiento y la sostenibilidad de las plataformas informáticas y los activos críticos de la institución. Además se alinea completamente con la estrategia y objetivos misionales de la ARC-FFMM, dado en el documento Plan Estratégico Naval 2015 – 2018, y como lo describe el objetivo específico No. 3 “Desarrollar y fortalecer las capacidades de defensa, explotación, respuesta y resiliencia frente a las amenazas cibernéticas” (Armada Nacional de Colombia, 2015), igualmente en lo generado en el proceso de planeación, responsabilidades y requerimientos establecidos a las instituciones del estado en el documento CONPES 3854 del 11 de abril del 2016 (CONPES 3854, 2016) para la protección de las infraestructuras críticas del país, la seguridad digital y de esta manera lograr alcanzar unas entidades del estado con capacidades fuertes en talento humano, equipos, procesos e infraestructura, que permitirán tener un desempeño profesional eficiente, efectivo y eficaz por parte de su personal para contrarrestar los posibles eventos que se produzcan en el ciberespacio y que puedan generar desventajas estratégicas a la fuerza y a la nación,

Igualmente el proyecto está orientado al gobierno corporativo en las organizaciones (FFMM-ARC) que desean mejorar las características de gestión de riesgos de seguridad digital utilizando una arquitectura de referencia que permite efectuar una mejor estrategia para la prevención, detección, respuesta y predicción de ataques cibernéticos, para un mejor control de los

activos de información, realizando una rápida respuesta ante una posible materialización de un riesgo y así lograr efectuar una respuesta ágil, oportuna y eficiente ante un evento de seguridad que pueda llegar afectar a la institución.

La apuesta a la aplicabilidad de la arquitectura de referencia de seguridad adaptativa ISOC está orientada por los diversos beneficios que brinda la analítica de datos y lo que está puede brindar a las instituciones, como son el incremento en la eficiencia en la gestión de riesgos y predicción de posibles incidentes de seguridad que se puedan presentar, además conocer el nivel de aceptación ante cada riesgo de carácter cibernético que se pueda llegar a materializar y poder realizar una respuesta eficiente ante un evento de seguridad.

También es de señalar que aunque en la actualidad existen normatividad de gestión de la seguridad de la información como la de la familia ISO 27000, la ISO 31000, ISM3 (Information Security Management Maturity Model) y normativas de cumplimiento como COBIT, PCI, el estándar NIST 800-53, entre otros, se cree que la propuesta contribuirá a fortalecer la ciberseguridad y ciberdefensa en la institución, debido a que permitirá efectuar una gestión más eficiente y eficaz generando respuestas optimas y efectivas a los encargados de administrar la seguridad cibernética de la institución y que permitirán mejorar la toma de decisiones por parte del alto mando naval y la Dirección Cibernética Naval.

Objetivos

Objetivo General

Definir la arquitectura de referencia para el servicio ISOC en la Armada Nacional para la prevención, detección, respuesta y predicción de ataques informáticos.

Objetivos Específicos

1. Identificar las necesidades para el ISOC de la Armada Nacional a partir de las capacidades en Ciberseguridad y Ciberdefensa requeridas para la institución.
2. Determinar los componentes requeridos en las variables de personas, procesos y tecnología para el ISOC.
3. Determinar el apoyo del modelo propuesto del ISOC al modelo de capacidades de Ciberseguridad de la Armada Nacional.

Metodología

Este trabajo inicia de una investigación cualitativa-comparativa, mediante una serie de entrevistas semiestructuradas al personal que labora en las áreas de TIC y seguridad Cibernética en la institución y que permitan efectuar la comparación de los componentes de Personal, Procesos y Tecnología, que podrían ser parte esencial para el funcionamiento de un ISOC (SOC Inteligentes). Igualmente está basada en fundamentación de los conceptos y descripciones a través de la revisión de fuentes bibliográficas existentes, con la finalidad de identificar y promover una arquitectura de referencia innovadora orientada a la seguridad adaptativa para el fortalecimiento de la Ciberseguridad y Ciberdefensa en las FFMM-ARC. Buscando conocer los beneficios y capacidades que podría ofrecer efectuar una gestión efectiva y eficiente de las amenazas cibernéticas que intentan vulnerar los sistemas tecnológicos de las instituciones, bajo un nivel de investigación aplicativo el cual logra proveer tecnologías o esquemas de acción para la aplicación de diferentes conocimientos teóricos.

El documento se encuentra dividido en capítulos a través de los cuales se van desarrollando los objetivos planteados, para finalmente generar unas conclusiones que confieren aplicabilidad al mismo.

1. Definición de Security Operation Center

Según (Renaud, 2005) Security Operation Center (en adelante: SOC) es un componente de las operaciones en el ciberespacio que se basa en plataformas informáticas que ayudan a las empresas a efectuar control y detección de eventos cibernéticos para prevenir incidentes con la información.

(León, 2009) Indica que un SOC se compone de personas, procesos, infraestructura y tecnología dedicados a gestionar, tanto de forma reactiva como proactiva, amenazas, vulnerabilidades y en general incidentes de seguridad de la información, con el objetivo de minimizar y controlar el impacto en la organización.

También un SOC es un equipo formado principalmente por analistas de seguridad organizado para detectar, analizar, responder, informar y evitar incidentes de ciberseguridad. (Committee on National Security Systems, 2010)

Por lo tanto para delimitar el concepto de SOC que se desea manejar durante este proyecto, se puede llegar a determinar que es una combinación de las definiciones dadas por (León, 2009) y el (Committee on National Security Systems, 2010), quedando de la siguiente manera: Un SOC es una estructura conformada por personas con capacidades en ciberseguridad y ciberdefensa, entrenados para prevenir, detectar, responder y predecir futuros ataques informáticos, a través de procesos, infraestructura y tecnología dedicados a gestionar la seguridad de la información de una institución.

1.1. Funcionamiento de un SOC

Un SOC prepara la información y la seguridad con los eventos en una red, por tal motivo logra generar una visibilidad de los eventos que pueden estar produciendo problemas y del impacto que estos pueden ocasionar, con esto los encargados de gestionar la seguridad pueden tomar decisiones fundamentadas sobre cómo reaccionar de manera efectiva de acuerdo a las políticas de seguridad que manejan. (Joanne, 2005)

Sin embargo los SOC basan su funcionamiento en las distintas etapas de su arquitectura para lo cual maneja procesos (Ver Figura.1). Así mismo, la operación es un trabajo continuo las veinticuatro horas del día, durante los siete días de la semana y los 365 días del año. Y en el cual según (Renaud, 2005) se encuentra compuesto por cinco (05) módulos diferentes que son:

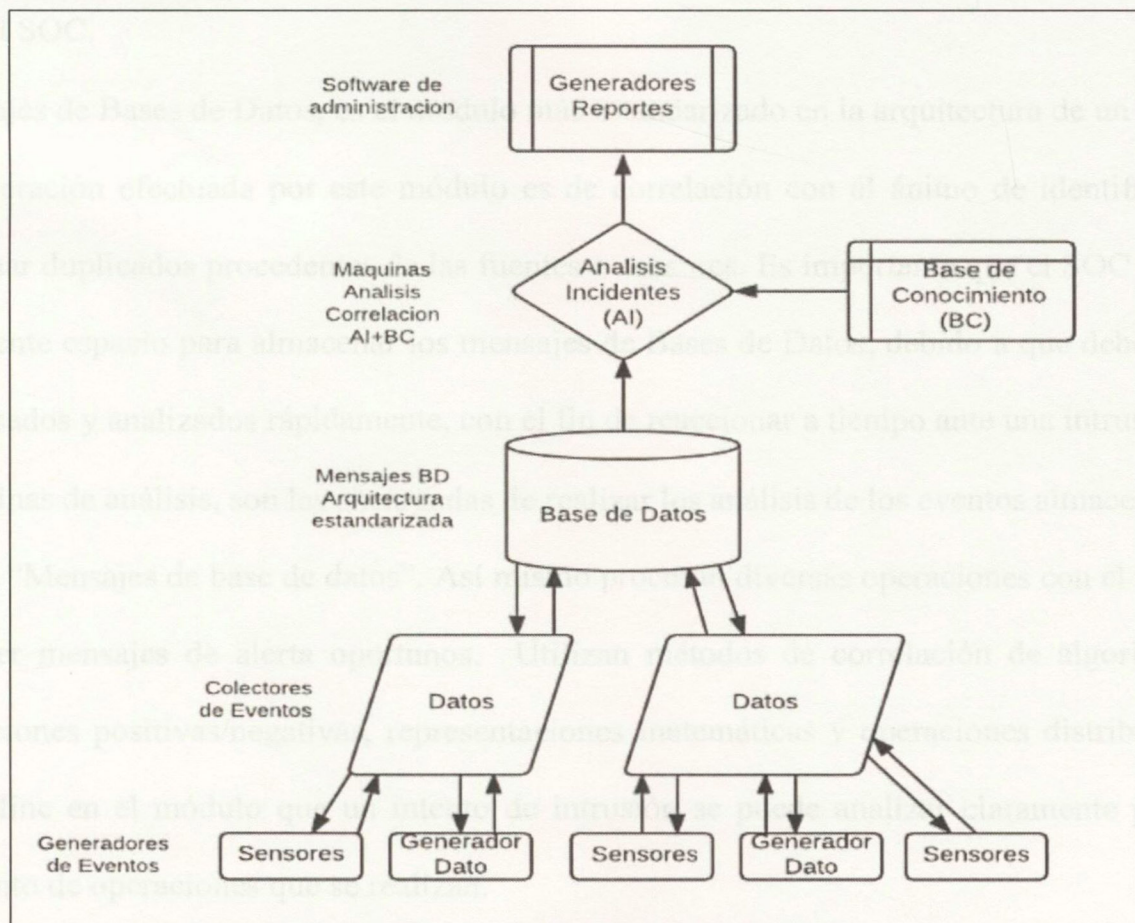


Figura 1 Módulos Funcionamiento SOC (Renaud, 2005)

- Sistemas generadores de eventos, plataformas que se encargan de generar los eventos que se presentan en un SOC, existen dos fuentes los que se basan en los eventos que producen los diferentes sensores (Firewall, IDS/IPS, equipos de red) y los generadores de datos apoyados en los estados como son las alertas del sistema operativo, alertas del hardware y alertas de la bases de datos llamados Pollers , los cuales de manera conjunta crean eventos según la reacción a una situación que se presente con un equipo, por ejemplo un evento de respuesta a una prueba de Ping en el protocolo ICMP, control sobre la integridad de datos y/o un intento de acceso no autorizado a un servicio.
- Colector de Eventos, la función principal es el de almacenar la información proveniente de los sistemas generadores de eventos y convertirla a un formato estándar para tener una base de datos con mensajes claros. La disponibilidad y robustez de este módulo es muy relevante para el SOC.
- Mensajes de Bases de Datos, es el modulo más estandarizado en la arquitectura de un SOC. La operación efectuada por este módulo es de correlación con el ánimo de identificar y eliminar duplicados procedentes de las fuentes o sensores. Es importante que el SOC tenga suficiente espacio para almacenar los mensajes de Bases de Datos, debido a que deben ser procesados y analizados rápidamente, con el fin de reaccionar a tiempo ante una intrusión.
- Máquinas de análisis, son las encargadas de realizar los análisis de los eventos almacenados en los “Mensajes de base de datos”. Así mismo procesan diversas operaciones con el fin de proveer mensajes de alerta oportunos. Utilizan métodos de correlación de algoritmos, detecciones positivas/negativas, representaciones matemáticas y operaciones distribuidas. Se define en el módulo que un intento de intrusión se puede analizar claramente por el conjunto de operaciones que se realizan.

- generación de reportes utilizadas para reaccionar a los eventos que se generan en el sistema examinado.

Arquitectura global de un SOC

La construcción general de un SOC según (Renaud, 2005), realiza los cinco (05) módulos

itos. Sin embargo asociado al aspecto técnico involucrado como implementación, es

ario considerar la supervisión de la Infraestructura de TI. En la Figura 2 se pueden observar

ferentes etapas de funcionamiento de un SOC y como cada módulo en el sistema opera para

tizar la funcionalidad requerida.

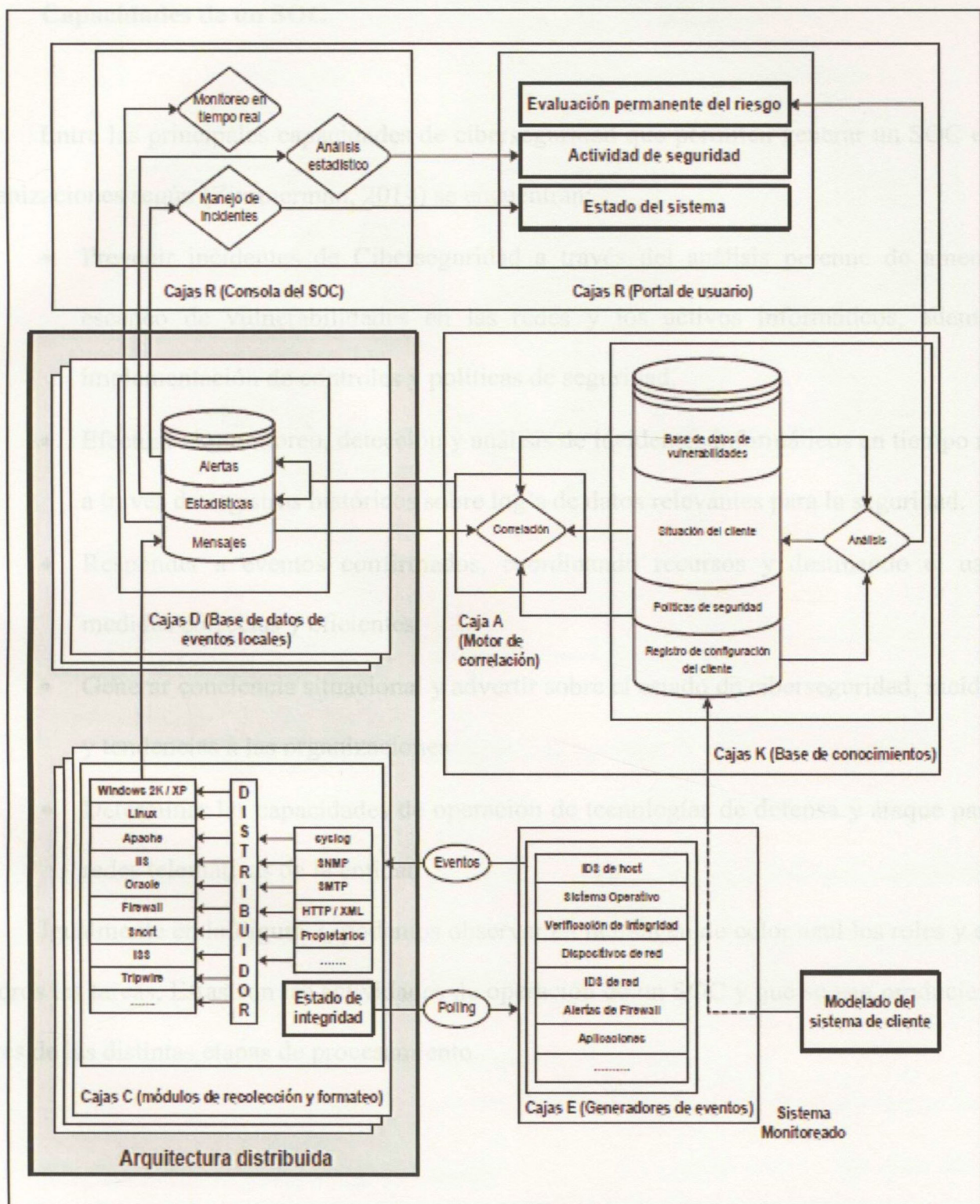


Figura 2 Arquitectura SOC (Renaud, 2005)

1.3. Capacidades de un SOC

Entre las principales capacidades de ciberseguridad que permiten generar un SOC en las organizaciones según (Zimmerman, 2014) se encuentran:

- Prevenir incidentes de Ciberseguridad a través del análisis perenne de amenazas, escaneo de vulnerabilidades en las redes y los activos informáticos, además la implementación de controles y políticas de seguridad.
- Efectuar el monitoreo, detección y análisis de incidentes informáticos en tiempo real y a través de registros históricos sobre log's de datos relevantes para la seguridad.
- Responder a eventos confirmados, coordinando recursos y destinando el uso de medidas correctas y eficientes.
- Generar conciencia situacional y advertir sobre el estado de ciberseguridad, incidentes y tendencias a las organizaciones.
- Determinar las capacidades de operación de tecnologías de defensa y ataque para las redes telemáticas de la entidad

Igualmente en la Figura 3, podemos observar en la imagen de color azul los roles y en los cuadros las tareas, Estas son las actividades de operación de un SOC y que se van produciendo a través de las distintas etapas de procesamiento.

2.1 SOC de primera generación 1975-1995

Conocida como la generación de los programas molestos y el mínimo impacto en la era del código malicioso según (Hewlett-Packard, 2015). Los SOC de primera generación estuvieron

ligados a los inicios de la red de Internet. Las compañías en este tiempo no tenían medidas de seguridad. La adopción del Internet por parte de las empresas, generó la explotación y el abuso de las redes informáticas. En esta era las detecciones de abuso fueron los resultados del pensamiento creativo e imaginativo con respecto al normal funcionamiento de los dispositivos que formaban parte de los computadores y la resolución de problemas con respecto a la configuración del hardware de los equipos, pero estos no fueron organizados ni repetibles. Se dice que las herramientas de seguridad que surgieron inicialmente fueron antivirus y software de firewall, seguidos por proxies y sistemas de IDS. Igualmente en esta generación las "Operaciones de Seguridad" fueron determinadas para monitorear y administrar estos productos y responder a amenazas. Además las operaciones de seguridad eran de una sola persona y generalmente con un conocimiento amplio en las redes informáticas, que era aprovechado para administrar y gestionar los dispositivos de seguridad de una organización. Por lo tanto los centros funcionales de operaciones de seguridad comienzan a aparecer en organizaciones gubernamentales y militares durante la segunda mitad de esta generación. También el análisis que se realizaba en los SOC de esta generación era de tipo no estructurado. Por lo tanto, se puede llegar a decir que en la actualidad este no se define como un SOC, sino como las herramientas básicas, mínimas y necesarias que debe tener una organización para minimizar los riesgos en la seguridad perimetral de su red informática.

En la Figura 4 se evidencian una serie de eventos de interés que ocurrieron en esta generación de SOC, y que permitió a las organizaciones iniciar procesos para la implementación de centros de operaciones de seguridad.

1970's	Phreaking takes advantage of telecommunications systems
1972	First full duplex modem introduced with 1,200 bps
1974	Ethernet developed
1979	Kevin Mitnick uses social engineering to gain access to DEC systems by getting a dial-in password reset
1980	Ethernet commercially introduced
1981	Hayes SmartModem (14.4 kbs) BBS's emerge (and remote connectivity connects living rooms and dorms around the world)
1983	"War Games" movie released
1984	"2600: Hacker Quarterly" magazine begins publication
1986	"The Cuckoo's Egg" is published—bringing IT security espionage to print
1986	Computer Fraud and Abuse Act and the Electronic Communications Privacy Act makes it a crime to break into computer systems
1987	Christmas Tree Exec, first widely disruptive self-replicating program
1987	tcpdump created
1987	McAfee Associates creates antivirus software
1988	November—Morris Worm, first worm to spread in the wild (BSD Unix variants)
1988	IRC protocol created by Jarkko Oikarinen
1989	SANS Institute formed
1991	Symantec creates Norton Antivirus software
1992	DEC SEAL, the first commercial firewall is shipped
1993	Windows 3.11 released with peer to peer network capability
1993	USAF creates 67th Air Intelligence Wing (AFCERT) based out of Lackland AFB (San Antonio, TX) to focus on Cyber Intelligence
1993	Bugtraq security mailing list created
1995	Wheelgroup launches first intrusion detection system: NetRanger
1995	"Concept" first macro virus

Figura 4 Eventos de interés 1G-SOC (Hewlett-Packard, 2015)

2.2. SOC de segunda generación 1996-2001

Conocida como la era de la Epidemia de malware y detección de intrusos, según (Hewlett-Packard , 2015) Las operaciones de seguridad en la segunda generación pueden catalogarse como la era de los brotes del malware, incluyendo virus y gusanos que generaron pérdidas en las redes corporativas y gubernamentales. La segunda generación de SOC forjó el seguimiento de las vulnerabilidades y el sistema de parches formalizados por parte de las empresas.

Los SOC se encontraban en organizaciones gubernamentales y militares y comenzaron a surgir en las organizaciones comerciales más grandes. Las compañías comenzaron a comercializar

los servicios de monitoreo y administración de seguridad y ofrecían estos servicios el cual fue conocido como el modelo de “Managed Security Service Provider”. Igualmente en esta era hay una explosión de productos de nueva tecnología con variedades de firewalls, antivirus, proxies, escaneo de vulnerabilidades y sistemas de detección de intrusiones. El foco principal durante este período fue la detección de intrusiones. Algunas organizaciones gubernamentales y militares tenían implementaciones robustas de reglas de SNORT¹ y TCPDUMP²; Así mismo, las empresas privadas comenzaron a comprar versiones comercializadas de sistemas IDS. Igualmente los estados nación comenzaron la explotación de la red cibernética, la defensa y los programas de ataque en los últimos años de esta era, sin embargo, ninguno de estos programas era aún conocido por el público. El análisis de eventos de seguridad se realizó en gran medida mediante el uso de scripts, consolas IDS y otras herramientas locales. La definición de monitoreo de eventos de información de seguridad (SIEM) fue introducido al final de esta generación como una tecnología utilizada para correlacionar eventos de seguridad. Sin embargo, los analistas no confiaban en este único panel en las operaciones diarias hasta la próxima generación.

De esta era se puede observar que el tipo de herramientas definidas en esta generación forman parte integral de un sistema de gestión de seguridad de la información en las compañías que desean implementar centros de operaciones de seguridad SOC y además que estos equipos son implementados en empresas de mediano y gran tamaño, entre las compañías que tienen estos equipos se encontraban entidades públicas de los países, sector bancario, empresas de seguros, industria automotriz, sector salud, empresas petroleras, entre otras; así mismo estos servicios eran ofrecidos por compañías de seguridad que prestan servicio de seguridad administrada a terceras partes como un sistema de outsourcing de servicios.

¹ <https://www.snort.org/> Sistema de Prevención y detección de Instrucciones en red

² <http://www.tcpdump.org/> Analizador de paquete de trafico de red

2.3. SOC de Tercera generación 2002-2006

La tercera generación de SOC es conocida por la propagación de Botnets³, crimen cibernético, la prevención de intrusiones y el cumplimiento de normativas en algunos sectores. Según (Hewlett-Packard , 2015). Igualmente fue más conocida por la expansión y organización de los sindicatos de cibercrimen que usaron las Botnets para robar información de identidad y financiera. Esta generación se inició en el año 2003 con malware de gran impacto, como el SQL Slammer⁴ y Blaster⁵, el cual causó la interrupción masiva de Internet. Además ese mismo año, se formó el US-CERT⁶. A medida que esta generación continuaba, el malware pasaba de los gusanos perjudiciales a ataques dirigidos. En esta era se crean la Ley Sarbanes Oxley que dicta controles de seguridad de TI y responsabilidad individual para ejecutivos, también se crea el framework de metasploit (Año 2003), las empresas de seguridad (Kaspersky, McAfee) empiezan a crear productos de antimalware en su portafolios de servicios y las organizaciones gubernamentales, militares y de proveedores de servicios gestionados (MSSP) ya habían desarrollado centros de operaciones de seguridad. También en esta era la industria de tarjetas de pago formó el consejo PCI y exigió a los proveedores que se adhirieran a los estándares de seguridad y protección de datos. Finalmente las capacidades de explotación cibernética de los estados nación como China se notó por primera vez durante este período, el ejército estadounidense y varios contratistas de defensa fueron blancos de China como parte de la Operación “Titán Rain”. Y los equipos de respuesta a incidentes informáticos formalizaron los procedimientos de gestión de crisis y se hace

³ <https://blog.kaspersky.es/que-es-un-botnet/755/> redes de computadores infectados con una variedad de malware

⁴ <http://www.pandasecurity.com/spain/homeusers/security-info/38199/information/Slammer>

⁵ <http://www.pandasecurity.com/spain/homeusers/security-info/40369/information/Blaster>

⁶ <https://www.us-cert.gov/> US-CERT Security Operations Center (SOC) RFC 2350

principal fuerza en las capacidades de detección temprana. Igualmente la aceptación de programas de seguridad en el sector privado aumenta y se comienzan a detectar y divulgar grandes filtraciones de datos al público como resultado de las nuevas leyes de notificación de infracciones.

En conclusión en esta era se logra determinar que los centros de operaciones de seguridad SOC, los tenían implementados los países potencias mundiales como son: EEUU, Rusia, China, Japón, Inglaterra, Alemania, Italia, España, y que son utilizados como mecanismo de defensa en el ciberespacio (Hewlett-Packard , 2015). Igualmente se observa la implementación de SOC por parte de grandes compañías de seguridad como son SYMANTEC, MCAFEE, KASPERSKY así como el sector bancario por su prioridad al cumplimiento de normativas como PCI, y algunas empresas que gestionan información sensible como petroleras, gasíferas, sector industrial, sector telecomunicaciones (Movistar, Orange, AT&T), la Agencia de Seguridad de la Información Europea (ENISA), todos buscando mitigar los riesgos que se estaban presentando para garantizar la protección de la información.

2.4. SOC de cuarta generación 2007-2012

Era de la ciberguerra, el hacktivismo, las amenazas avanzadas persistentes (en adelante: APT), y la detección de fuga de información según (Hewlett-Packard , 2015). Las operaciones de seguridad de cuarta generación se caracterizaron por la publicidad de las amenazas cibernéticas con motivación política. Además los titulares de las noticias situaron de manifiesto que los estados se atacaban entre sí con el propósito de robar la propiedad intelectual o el sabotaje. El primer uso público de ataques cibernéticos en el contexto de un conflicto armado cambió la manera en que se vio la guerra cuando Rusia atacó a Estonia en 2007. Igualmente las organizaciones "hacktivistas"

ganaron notoriedad por sus exitosos ataques contra organizaciones e individuos por medios de coordinación y difusión de la información en redes sociales.

También las empresas conciben que las intrusiones ocurrirán sin importar las tecnologías preventivas de seguridad, y el centro de atención cambia de la detección y de la prevención de intrusiones a la detección y a la contención de la exfiltración de datos, afectación a sistemas de información crítico, daño en el hardware y cifrado de la información. Además las entidades se dan cuenta de la importancia que tiene gestionar, mitigar los riesgos de seguridad cibernética y los impactos que estos producen para las organizaciones, así como tener planes de recuperación que contribuyan a generar unos tiempos de resiliencia eficientes para la continuidad de sus operaciones. En esta era surgen herramientas para el monitoreo y gestión de la información como son los DLP (Data loss prevention), los sistemas de sandboxing, sistemas para gestión de riesgos y vulnerabilidades, las cuales operan basadas en esquemas de comportamiento del código malicioso o su forma de interactuar con los sistemas. Debido al incremento en los diferentes tipos de ataques cibernéticos y la fuga de información que se estaban cometiendo en el mundo la mayoría de países empiezan con procesos de implementación de centros de operaciones de seguridad cibernéticas para monitorear sus redes informáticas gubernamentales, entre los que se encuentran ya no solo los países citados en la 3ra generación de SOC, sino también países como Brasil, Colombia, Argentina, Venezuela, México, países europeos como Estonia, Bélgica, Portugal, Austria, Bosnia y Herzegovina, Bulgaria, Chipre, Ciudad del Vaticano, Croacia, Dinamarca, Eslovaquia, Eslovenia, Finlandia, Francia, Gran Bretaña, Grecia, Hungría, Irlanda, Islandia, Letonia, Liechtenstein, Lituania, países asiáticos como Irán, Irak, Corea del Norte, Corea del Sur, Emiratos Árabes Unidos, Israel, India, igualmente las compañías de mediano tamaño o pequeñas compañías que manejan información sensible de clientes empezaron a implementar o contratar

servicios de seguridad gestionada que les permitiera conocer cómo se está moviendo su información en las redes informáticas de su institución y los riesgos a los que están expuestos, además los gobiernos empiezan a crear planes para acercar los temas de ciberseguridad a la población civil y a las compañías brindando asesorías y servicios para que las empresas empiecen a tomar conciencia y ver la importancia de crear mecanismo para proteger su información como un activo estratégico de sus negocios, finalmente grandes compañías de diversos sectores como Telecomunicaciones, tecnología, salud, retail, bancario han fortalecido su talento humano generando capacitaciones para su personal de TI en el área de ciberseguridad y ciberdefensa.

2.5. SOC de quinta generación 2013 -.....?

Conocido como los SOC que se gestionan con analítica de datos y big-data⁷, basados en metodología de inteligencia artificial, permuta de información, perspectiva del enemigo en los actos de los seres humanos. Además los 5G/SOC inspeccionan el cambio en el panorama de las amenazas y están abordando el desafío de forma holística. Si bien los estándares y los esfuerzos de cumplimiento han mejorado la adopción de productos y prácticas de seguridad, los 5G/SOCs se dan cuenta de que los programas de seguridad deben ser activos, comprometidos e inteligentes.

Por lo tanto los 5G/SOCs son eficientes, automatizan las actividades que la mayoría de los analistas de SOC de cuarta generación realizan manualmente, incluyendo la contención de incidentes y a los ciclos de respuesta humana se aplican análisis avanzados para la detección rápida de eventos. Los SOC de esta generación utilizan herramientas de big data como son los ecosistemas de Hadoop, Apache spark, Apache Tika, Apache Hive (infraestructura dataware house que facilita

⁷ <https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/>

la consulta y gestión de grandes conjuntos de datos que residen en almacenamientos distribuidos), los cuales ofrecen un framework que utiliza modelos de programación simples para el procesamiento distribuido de un gran conjunto de datos a través de varias máquinas conectadas y con rapidez de procesamiento, también para el manejo de grandes volúmenes de datos (Bases de datos) se usan bases de datos como MongoDB, CouchDB, Cassandra, HBase, Neo4j, Riak, Hypertable, que brindan la posibilidad de gestionar datos estructurados, semiestructurados o datos no estructurados. Los cuales al estar operando de manera conjunta permiten efectuar análisis más rápidos que generan respuestas más eficientes y por lo tanto permiten realizar actividades de predicción. Igualmente están recopilando ingentes conjuntos de datos estructurados y no estructurados dentro y fuera de su organización, y finalmente utilizan avanzadas herramientas analíticas para obtener inteligencia y hacer predicciones basadas en patrones recién descubiertos. De igual forma combinan herramientas de inteligencia de negocios (BI) e inteligencia de seguridad para crear una comprensión contextual de la empresa y sus riesgos. Entre las que se encuentran Open source (Pentaho Community Edition, Spago BI, Jaspersoft, Talend), Propietarias (Tableau, Excel 2013, Qlikview, SQL Server Reporting Services) o Soluciones en la nube (Microstrategy Cloud, Google Big Query, Google Fusion Tables, Microsoft Azure) El personal de analistas de los 5G/SOC incluyen matemáticos, estadísticos, teóricos y grandes científicos de datos para lograr sus objetivos. Y principalmente es reducir el riesgo para una organización mediante la detección de amenazas antes de que causen daño y que no se puedan remediar. Para cumplir con este objetivo, el 5G/SOCs debe colaborar con otros que también están siendo atacados (Inteligencia de amenazas). Ninguna organización tiene toda la información necesaria para detectar todas las amenazas, (David Chismon, Martyn Ruks, 2016) los servicios de "Inteligencia de Amenazas" no son lo suficientemente eficientes solos. Los líderes de los SOC's de 5G están formando grupos

activos de intercambio de información y relaciones directas dentro de su industria y aprovechan la experiencia de otros para igualar el ingenio con el de los adversarios. Por lo tanto los SOC's de 5G son adaptables.

Por lo tanto es claro que los 5G/SOCs empujan el desarrollo. La estructura organizacional y las tácticas operativas utilizadas cambiarán la naturaleza de los eventos en el ciberespacio. Los gobiernos y las grandes organizaciones ya mantienen equipos de ataque y defensa (Equipos Rojo y Azul) para probar continuamente sus capacidades. En un 5G/SOC, los constantes ejercicios de ataque y defensa están haciendo que las empresas sean más seguras contra las amenazas del mundo real. Además, los equipos de inteligencia están colaborando con otras organizaciones para compartir detalles sobre métodos, técnicas y herramientas del adversario. Igualmente los equipos de investigación dan un paso atrás en el Triage de alertas y utilizan los grandes almacenes de datos para buscar ataques previamente desconocidos e invisibles.

Como conclusión de la evolución de los SOC's, se tiene que los SOC de 5G deben basarse en la historia y las capacidades de todas las generaciones anteriores de SOC's. Es decir deben cubrir seguridad perimetral, seguimiento de vulnerabilidades, detección de malware y respuesta a incidentes, deben tener la capacidad de detectar amenazas internas y externas, así como lograr detectar Apt's. Deben poder monitorear a los usuarios y su actividad referente a la exfiltración de datos y deben utilizar efectivamente inteligencia de amenazas y grandes herramientas de datos para encontrar ataques previamente desconocidos. Se deben utilizar tácticas y técnicas e implementar nuevas tecnologías y automatizar los procesos existentes. Además es necesario contar con personal altamente capacitado y motivado que debe colaborar para reducir el riesgo para las empresas.

3. Requerimientos del ISOC de la Armada Nacional

En este capítulo se trabajaran en identificar las necesidades para el ISOC de la Armada Nacional a partir de las capacidades en ciberseguridad y ciberdefensa requeridas para la institución, basado en estudios, requerimientos de organismos internacionales y la comparación de los componentes de Personal, Doctrina, Material y Equipo, necesarios para el fortalecimiento de las capacidades cibernéticas.

3.1. Capacidades en Ciberseguridad necesarias en una institución que se dedique a la Ciberdefensa.

Basado en modelos de ciberseguridad y ciberdefensa según (Dutta, A. McCrohan, K., 2002) En la Figura 5, se observa que la ciberseguridad en las organizaciones requiere un enfoque integral bajo la premisa de una seguridad proactiva, que identifica y gestiona los riesgos que amenazan a los ciudadanos, las empresas y el estado. Conceptos que son complementados por el documento del NIST SP800-53 (NIST Special Publication 800-53. Security and Privacy Controls for Federal Information Systems) el cual define la defensa en profundidad como una estrategia de la seguridad de la información que contempla las actividades operativas cotidianas, las tecnologías y las personas, para establecer un conjunto de barreras y controles implementados en múltiples capas de la organización (H. Jara; F. G. Pacheco, 2012).

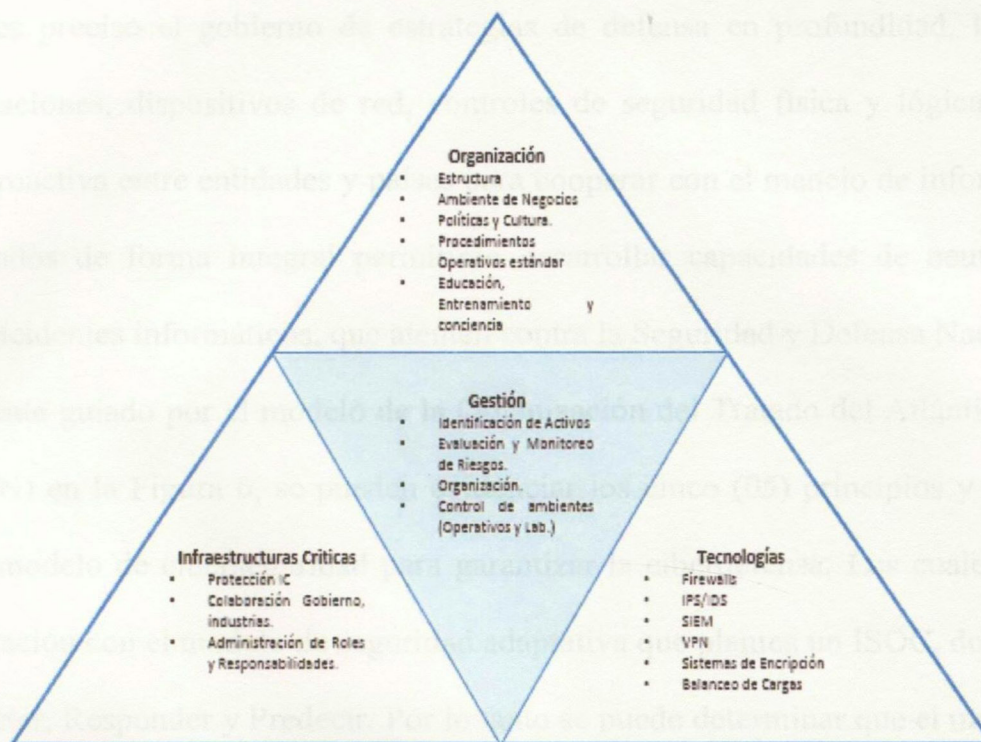


Figura 5 Modelo de Ciberseguridad (Dutta, A. McCrohan, K., 2002)

Por tal motivo la seguridad se ha orientado exclusivamente desde una perspectiva de “Ciberseguridad”, orientada en la defensa y protección de las redes frente a incidentes e intrusiones en las mismas y ha surgido una disciplina, la “Ciberdefensa” que tiene lugar en la fase operativa y se desarrolla mediante la defensa a los ciberataques. Por lo cual es necesario generar planes estratégicos que permitan una adecuada gestión de la seguridad de la información (SGSI), análisis y gestión de riesgos en el ciberespacio, planes de recuperación de desastres y continuidad de negocio sumado a procesos de implantación y mejora continua que permitan la vigilancia, monitorización de incidentes de seguridad (SOC) bajo esquemas de monitorias internas (Auditorias), monitorias externas (Cibervigilancia, Ciberinteligencia) y los planes de continuidad de negocio (BCP) y el área jurídica; igualmente para la defensa de las personas crear estrategias, planes de concientización, sensibilización, cultura y capacitación en los diferentes niveles organizacionales de los usuarios que interactúan con servicios TIC’s; en los procesos de gestión

de incidentes es preciso el gobierno de estrategias de defensa en profundidad, hardening de sistemas, aplicaciones, dispositivos de red, controles de seguridad física y lógica, además de colaboración proactiva entre entidades y países para cooperar con el manejo de información. Los cuales gestionados de forma integral permitirán desarrollar capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la Seguridad y Defensa Nacional.

Igualmente guiado por el modelo de la Organización del Tratado del Atlántico Norte (en adelante: OTAN) en la Figura 6, se pueden evidenciar los cinco (05) principios y los seis (06) elementos del modelo de ciberseguridad para garantizar la ciberdefensa. Los cuales finalmente brindan una relación con el modelo de seguridad adaptativa que plantea un ISOC, donde se busca Prevenir, Detectar, Responder y Predecir. Por lo tanto se puede determinar que el modelo OTAN puede ser usado como insumo en el proceso de creación del SOC de la ARC, pues el fundamento a seguir en la arquitectura de referencia será el modelo de Gartner, pero se incorporaran elementos del modelo de la OTAN, porque es un modelo validado por una organización internacional de la que Colombia hace parte (Mayo 2018) y que le permite el acceso de las Fuerzas Armadas de Colombia a un portafolio de capacitaciones y entrenamientos.



Figura 6 Modelo de Ciberseguridad OTAN

3.2. Comparación de componentes de Personal, Doctrina, Material y Equipo en la Armada Nacional.

Para verificar la aplicabilidad de un ISOC en la ARC y medir si éste sería viable para apoyar los objetivos misionales de la institución en la protección y gestión de sus infraestructuras críticas, así como la de sus activos de información y el correcto manejo de incidentes se planteó efectuar una comparación a través de una serie de preguntas (ver Tabla 1 pág. 38) al personal de tecnologías de la información y la Dirección Cibernética Naval, enfocadas al cubrimiento en cada uno de los componentes que podrían ser parte esencial para el funcionamiento de un ISOC, (Ver Figura 7-10) y poder determinar si con ese estudio comparado es viable aplicar la tecnología ISOC en los procesos doctrinales de la institución en especial para la gestión de riesgos, gestión de vulnerabilidades, gestión de incidentes y el correcto control que se le debe dar al dominio del ciberespacio desde la Dirección Cibernética Naval como organismo rector en la institución.



Figura 7 Resultado estadístico Respuesta preguntas en el componente Personas

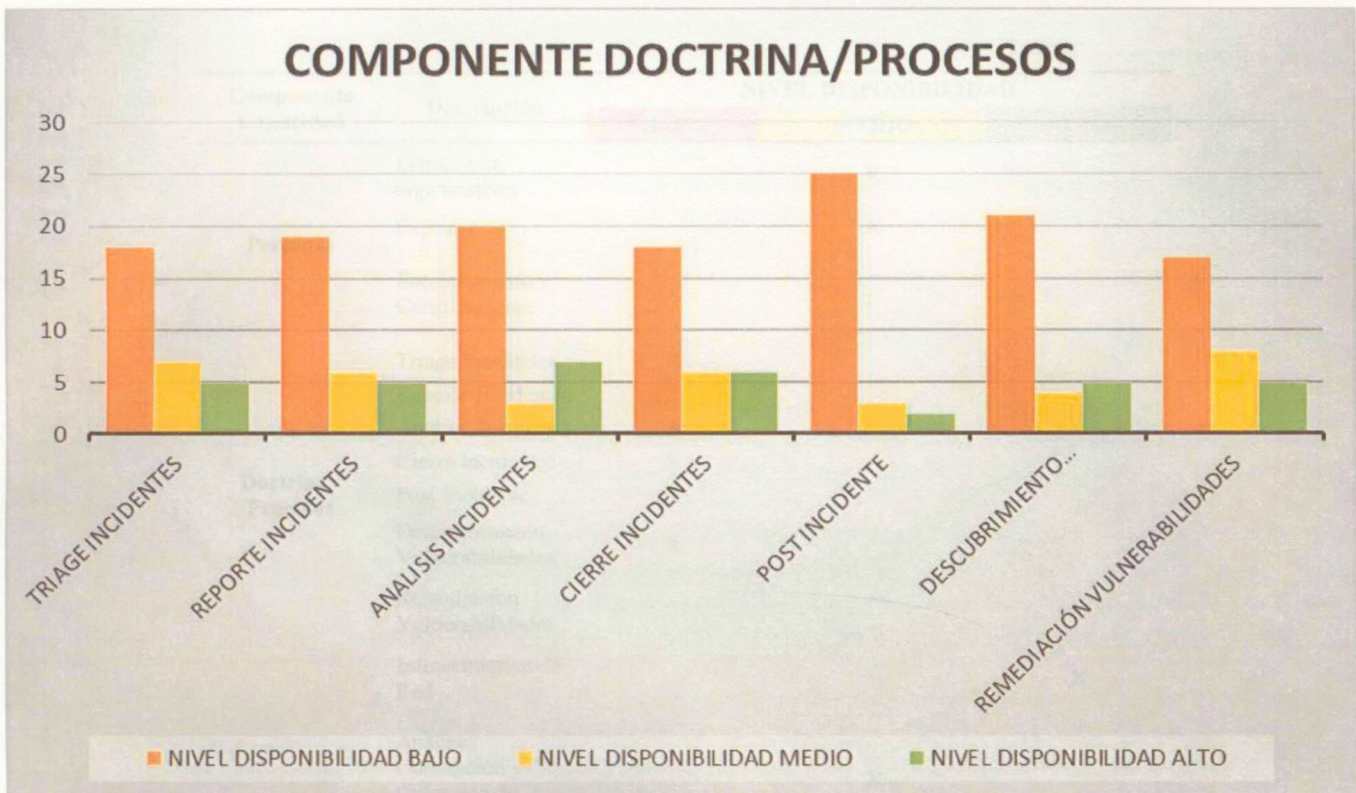


Figura 8 Resultado estadístico Respuesta preguntas en el componente Doctrina/Procesos

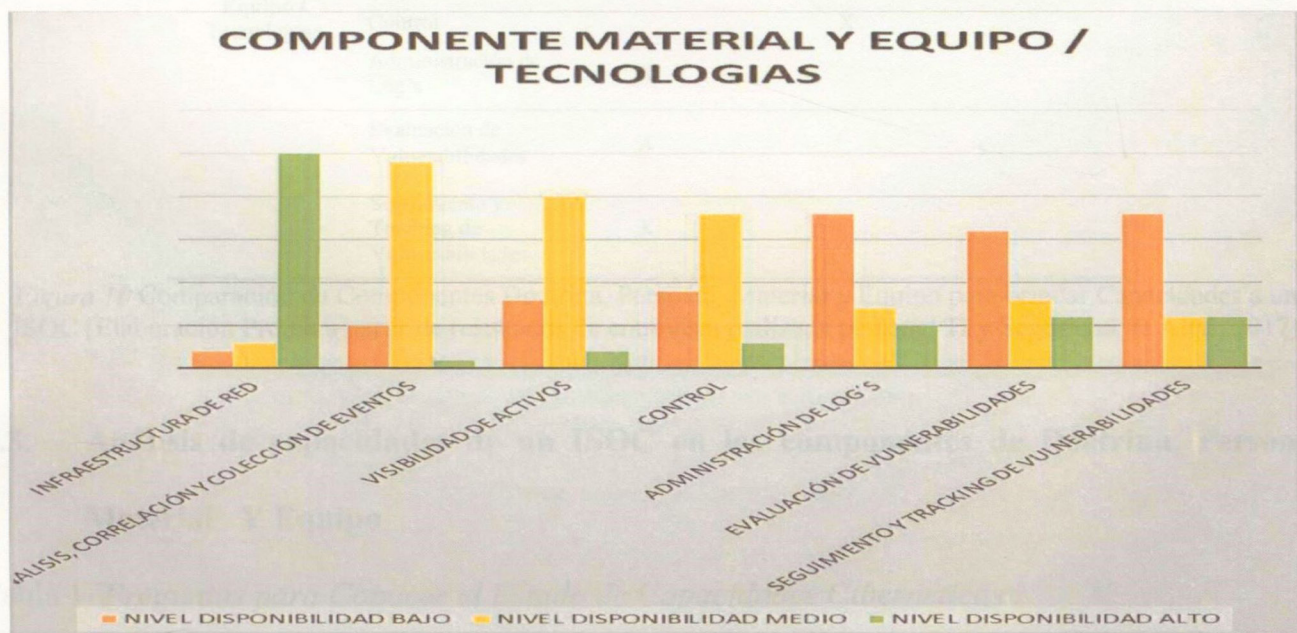


Figura 9 Resultado estadístico Respuesta preguntas en el componente Material y Equipo / Tecnologías

Componente Capacidad	Descripción	NIVEL DISPONIBILIDAD		
		BAJO	MEDIO	ALTO
Personas	Estructuras organizativas		X	
	Experiencia		X	
	Entrenamiento y Certificaciones	X		
Doctrina / Procesos	Triage Incidentes	X		
	Reporte Incidentes	X		
	Análisis Incidentes	X		
	Cierre Incidentes	X		
	Post Incidente	X		
	Descubrimiento Vulnerabilidades	X		
	Remediación Vulnerabilidades			
Material y Equipo / Tecnologías	Infraestructura de Red			X
	Análisis, Correlación y Colección de eventos		X	
	Visibilidad de Activos		X	
	Control		X	
	Administración de Log's	X		
	Evaluación de Vulnerabilidades	X		
	Seguimiento y Tracking de Vulnerabilidades	X		

Figura 10 Comparación de Componentes Doctrina, Personal, Material y Equipo para brindar Capacidades a un ISOC (Elaboración Propia a partir de resultados de entrevista realizada personal TI y Seguridad de ARC, 2017)

3.3. Análisis de capacidades de un ISOC en los componentes de Doctrina, Personal, Material Y Equipo

Tabla 1 Preguntas para Conocer el Estado de Capacidades Cibernéticas

Preguntas que buscan conocer el estado de la capacidad cibernética de la Armada Nacional en los factores del DOMPI. D = Doctrina, O = Organización M = Material y Equipo P = Personal I = Infraestructura	
INFORMACIÓN ORGANIZACIONAL	1. Nombre de la organización
	2. Superior jerárquico
	3. Área misional dentro de la Fuerza
	4. ¿El área actual es proporcional a la cantidad de personas y equipos de su dependencia?
	5. ¿Número de Personas que laboran en el área de Seguridad de la Información?

	6. ¿Equipos? ¿Cuenta con equipos asignados? Si o No 7. ¿Área? ¿Tiene área específica y propia para las actividades de seguridad de la información? Si o No 8. ¿Funciones y roles que cumple y realiza su organización y su área? TI o Seguridad de la Información.
DOCTRINA	1. ¿Qué tipo de Doctrina ha realizado Ud. Y sus unidades subalternas en los últimos dos años, referentes a sus funciones organizacionales y rol misional? (Cibernética, OSI) 2. ¿Han emitido directivas, circulares o generado alguna política sobre el tema que compete a su rol misional? 3. ¿Conoce si existen procedimientos de seguridad de la información, gestión de incidentes, planes de gestión de riesgos en la institución? 4. ¿Sabe cómo identificar incidentes de seguridad de la información? 5. ¿Conoce procedimientos para reportar, identificar un incidente? 6. ¿Conoce si existen procedimientos para análisis, descubrimiento y remediación de vulnerabilidades? 1. ¿Cuántas personas apoyan la labor que realiza en seguridad de la información? 2. ¿Con qué perfiles profesionales cuenta? 3. ¿Cuántos personas laboran en el área de la seguridad de la información y que profesiones tienen? * ¿Personal de Oficiales? * ¿Personal de Suboficiales? * ¿Personal Civil? 4. ¿Indique los años de experiencia con que cuenta desempeñándose en el área de seguridad de la información? 5. ¿Cuántos profesionales cuentan con cursos, diplomados o certificaciones de seguridad de la información? 6. ¿Indique los tipos de Certificaciones? Certificación con EC-COUNCIL en ECH, ENSA y ECSA, CHFI, ISACA, entre otras, web. Exploit, hardening, ISC^2.
TALENTO HUMANO	6. ¿Qué formación referente a la labor que realizan han recibido o tiene el personal? ¿Indique cuándo fue la última capacitación en temas de seguridad de la información? 7. ¿Indique si el personal cuenta con especializaciones, maestrías, diplomados o cursos que hayan recibido por parte de la institución? 1. ¿Cuenta con infraestructura física permanente para las actividades de seguridad de la información y es proporcional a la cantidad de personas y equipos de la dependencia? 2. ¿Cuentan con área forense para el desarrollo de su labor? 3. ¿Cuentan con área para monitoreo de herramientas para el desarrollo de su labor? Ejemplo UN SOC, un Laboratorio.
INFRAESTRUCTURA FÍSICA MATERIAL Y EQUIPO	4. ¿Cuentan con software o hardware especializado que apoye el desarrollo de sus labores de seguridad de la información?, SI o NO. 5. ¿Qué tipo de software/hardware poseen? (IPS/IDS, Firewall, Antivirus, SIEM, herramientas de malware, análisis de tráfico, etc.) 6. ¿Tienen herramientas de evaluación y seguimiento de vulnerabilidades? 7. ¿Han desarrollado software?, si es afirmativo, ¿para qué áreas lo utilizan? 8. ¿Cuenta con un deposito forense que facilite el aseguramiento de equipos y material para una investigación interna?

Nota: Elaboración Propia.

Como resultados al análisis de las preguntas desarrolladas al personal de TI y la Dirección cibernética Naval (ver tabla 1) para el componente que conforma el talento humano (Personas) se evidenció que en el área que atiende estructuras organizativas y experiencia se puede llegar a

determinar que la institución se encuentra en un nivel medio (ver Figura 7 y 10), dado por las respuestas brindadas a las preguntas acerca de cómo está conformada cada una de las áreas que tienen que responder en los temas del ciberespacio, ciberdefensa, ciberseguridad, gestión de TICs.

Así mismo a la deficiencia de personal para cubrir cada una de estas áreas de conocimiento, al efectuar preguntas (ver tabla 1) en cuanto al nivel de capacitación, entrenamiento y certificaciones en temas de Seguridad informática, hacking ético, análisis forense, gestión de vulnerabilidades, continuidad de negocio, gestión de riesgos, las respuestas no fueron las mejores, demostrando que el personal que conforma las áreas de ciberseguridad, ciberdefensa no tiene las formaciones académicas y certificaciones mínimas necesarias para poder efectuar estas actividades con un alto grado de eficiencia (ver Figura.7 y 10), y su labor la efectúan más por la experiencia que han ido adquiriendo por el transcurrir de los años, por lo que para el estudio en mención es un componente crítico con un alto grado de deficiencias.

Para el componente de procesos (Doctrina) (ver tabla 1), se evidenció que en el área que conforma la identificación, tratamiento, gestión, cierre, remediación de incidentes y vulnerabilidades la institución se encuentra en un estado bajo de madurez (ver Figura.8 y 10), dado que para cada una de las preguntas efectuadas en las áreas mencionadas aunque se tienen procedimientos, manuales y guías procedimentales que demuestren el cómo se deben efectuar y gestionar cada una de estas actividades ante un evento o incidente que pueda llegar a afectar las plataformas (Infraestructuras críticas cibernéticas navales) y procesos críticos de la institución, los mismos no son gestionados, ni actualizados de la manera correcta para lograr efectuar una respuesta eficiente y resiliente de la mejor manera.

Finalmente en el análisis de las preguntas (ver tabla 1), efectuadas al componente de Material y equipo (Tecnologías), el estado es similar a lo encontrado en los dos componentes

anteriores, porque aunque en las respuestas dadas por los administradores de las herramientas y el personal directivo de TIC's (ver Figura 9-10), demuestran que la entidad ha efectuado un esfuerzo grande para conseguir recursos económicos que permitan adquirir tecnologías de seguridad (Soluciones UTM, Firewall, NGIPS, Antivirus, Sistemas DLP, herramientas anti DDos, herramientas de control de acceso, herramientas de análisis de tráfico, SIEM, sistemas de big data e inteligencia de negocios) estas se han implementado en varios casos de manera no muy efectiva, otras solo para ciertas áreas de la organización y en algunas situaciones no se han tenido los recursos necesarios para continuar con los procesos de actualización y despliegue de los proyectos, al igual que no se tienen documentado ningún procedimiento que permita establecer un plan de operación de cada una de estas soluciones.

La planeación por Capacidades en el proceso administrativo que realizan las Fuerzas Armadas de Colombia tiene como etapa inicial la plantación, que "consiste en la formulación del estado futuro deseado para una organización y con base en ello, plantear cursos alternativos de acción, evaluarlos y así definir los mecanismos adecuados a seguir para alcanzar los objetivos propuestos, además de la determinación de la asignación de los recursos humanos y físicos necesarios para un empleo eficiente" (Cuellar, 2013).

Por otra parte (Chiavenato, 1986) describe la planeación como "la función administrativa que determina anticipadamente cuáles son los objetivos que deben alcanzarse y qué debe hacerse para alcanzarlos, se trata de un modelo teórico para la acción futura". Basado en las anteriores definiciones queda determinada que la planeación brindada, como un proceso cíclico en el que se definen objetivos, políticas y planes detallados para lograrlos, y la organización, establece la planeación para poner en práctica las decisiones, e incluye una revisión del desempeño y retroalimentación.

4. Componentes de arquitectura ISOC para la Armada Nacional

En este capítulo se busca determinar los componentes requeridos en las variables de personas, procesos y tecnología para el ISOC buscando prevenir, detectar, responder y predecir ataques cibernéticos, a través del análisis de procesos de operación y gestión, así como la caracterización de plataformas SOC existentes que contribuyen al fortalecimiento de capacidades en ciberseguridad en la institución.

4.1. Componentes de capacidades que intervienen en los procesos de operación y gestión de un Intelligence Security Operations Center

La planeación por Capacidades en el proceso administrativo que realizan las Fuerzas Militares de Colombia tiene como etapa inicial la planeación, que “consiste en la formulación del estado futuro deseado para una organización y con base en éste, plantear cursos alternativos de acción, evaluarlos y así definir los mecanismos adecuados a seguir para alcanzar los objetivos propuestos, además de la determinación de la asignación de los recursos humanos y físicos necesarios para un empleo eficiente” (Cuellar, 2013).

Por otra parte (Chiavenato, 1986) describe la planeación como “la función administrativa que determina anticipadamente cuáles son los objetivos que deben alcanzarse y qué debe hacerse para alcanzarlos, se trata de un modelo teórico para la acción futura”. Basado en las anteriores definiciones queda determinada que la planeación brindada, como un proceso cíclico en el que se definen objetivos, políticas y planes detallados para lograrlos, y la organización, establece la planeación para poner en práctica las decisiones, e incluye una revisión del desempeño y retroalimentación.

Igualmente debido a las nuevas amenazas para la seguridad y defensa del estado, caracterizadas por ser múltiples, difusas y cambiantes, y donde el adversario puede no estar completamente identificado, la planeación militar empezó a ser relevada hacia los noventa por un nuevo modelo denominado “Planeación por capacidades”, el cual fue desarrollado a partir de un trabajo de investigadores del Naval War College, publicado en el año 1990, en el que se plantea ajustadamente la necesidad de formalizar una metodología que le asegure a EE.UU, contar con los recursos militares necesarios para enfrentar las nuevas amenazas a la Seguridad y a la Defensa, esto en un escenario de riesgos múltiples, en permanente y creciente evolución (Puig M., M., 2015) para lo cual a partir de esta publicación, se han desarrollado y aplicado en múltiples Fuerzas Armadas del mundo, diversos modelos formales para efectuar el proceso de planeación por capacidades.

También para las Fuerzas Militares de Colombia, 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 los objetivos estratégicos del sector Defensa con las restricciones institucionales y financieras existentes. En este sentido, el objetivo es lograr una estructura de fuerza interoperable, adaptable, flexible y sostenible de acuerdo a lo planteado por los análisis desarrollados por el CGFM. (Comando General Fuerzas Militares Colombia, 2015). Además una capacidad se refiere a la habilidad de realizar una actividad, bajo ciertos estándares a través de una combinación de diferentes medios y modos. Esta habilidad se logra a partir de la conjunción de cinco componentes (DOMPI) (Comando General Fuerzas Militares Colombia, 2015).

- a. Doctrina: Documentos emitidos como marco de referencia para el accionar.
- b. Organización: Funciones, estructura y roles de la institución.
- c. Material y Equipo: Herramientas de trabajo disponibles y/o necesarias.
- d. Personal: Talento humano con competencias.
- e. Infraestructura: Instalaciones y áreas de ejecución.

Para efectos de este documento, se tomarán como ejes los componentes de doctrina, personal, material y equipo los cuales se pueden llegar a determinar cómo los pilares fundamentales para el correcto funcionamiento y operación de un ISOC, los cuales requieren ser caracterizados y evaluados en la Armada Nacional, para de esta forma brindar capacidades de Ciberseguridad, Inteligencia y Respuesta. Ver Figura. 11 (TN. Julián D. Aponte D., 2014)

CAPACIDAD	OBJETIVO
Defensa	Prevenir, detectar, reaccionar y recuperarse frente a ataques, intrusiones, interrupciones o cualquier tipo de acción hostil que pueda comprometer la información que transita dentro de la red cibernética naval, las redes utilizadas por las infraestructuras críticas y las redes que se encuentren dentro del área de responsabilidad de la Armada Nacional de la República de Colombia.
Inteligencia	Recopilar, analizar y procesar toda información relacionada con las tecnologías y sistemas utilizados por los adversarios.
Respuesta	Desplegar medidas y acciones que se deban tomar frente a amenazas y ataques que se presenten dentro de las redes de interés institucional o cualquier sector del ciberespacio donde se requiera la acción de la Armada Nacional.

Figura 11 Capacidades generales de ciberdefensa (TN. Julián D. Aponte D., 2014)

4.1.1. Componente de Material y Equipo

Este componente comprende las herramientas, las tecnologías empleadas en ciberseguridad y ciberdefensa. Para la defensa en particular, se pueden encontrar, la habilidad de los administradores para acceder, buscar y procesar información relevante sobre amenazas; así mismo, los “log’s de equipos de seguridad perimetral, sistemas de detección de intrusos y otras tecnologías de seguridad, son importantes en el análisis de ataques, y otros log’s como los de correo electrónico, DNS y son necesarios para identificar ataques de phishing y accesos a sitios maliciosos” (Dr. Boiney, L., Connolly, J., Dr. Skorupka, C., Krueger, S., & Dr. Summers, A., 2015).

Igualmente un desafío considerado por (Manuel Pérez Cortés, 2013) es la necesidad de monitorización y auditoría continua de los sistemas, traducida en implementación de buenas prácticas y herramientas para el control del funcionamiento de los activos de información organizacionales. “La mayoría de técnicas de ataque y amenazas en el ciberespacio se basan en la detección o existencia de errores en la configuración de la seguridad de los sistemas, obsolescencia o falta de actualización de las infraestructuras tecnológicas y fallos de programación o diseño en las arquitecturas de seguridad y comunicaciones” (Israel Martínez Lacabe, Josep Castells Rafel, José Antonio Castrillo, 2016) es allí, donde se hace necesaria la implementación del componente de doctrina.

4.1.2. Componente de Doctrina (Procesos)

Es importante dar a conocer que en el año 2013 el comando conjunto cibernético (En adelante: CCOC) generó la Directiva Operacional N°. 140 de activación de centro de operaciones de seguridad, en la cual impartía lineamientos de cómo establecer la misión, funciones, responsabilidades y alcance del Centro de Operaciones de Seguridad (SOC), así como definir las capacidades y servicios que prestará el centro de Operaciones de seguridad (SOC) y el establecimiento de los roles, responsabilidades, funciones, procesos y procedimientos del SOC, además de servir como modelo de referencia para la creación de CSIRT "Equipo de respuesta a emergencias informáticas" o SOC "Centro de operaciones de seguridad" en cada una de las fuerzas militares y de policía del país (Ejército, Armada, FAC y PONAL). Basado en lo anterior y siguiendo los lineamientos impartidos por el ente rector en temas de ciberseguridad y ciberdefensa en la FFMM, la ARC definió la doctrina como el componente que se encarga de generar, estructurar y definir los procesos y procedimientos de acción, gestión y operación del ISOC, entre sus responsabilidades, roles y funciones se encuentran la creación de protocolos, medidas de seguridad, métodos, procedimientos, productos, concienciación, cultura de seguridad y personal especializado en su aplicación y manejo. De igual manera para una correcta gestión de la seguridad y gestión de respuesta a incidentes, es fundamental disponer de plataformas especializadas que se centran en la misión de los sistemas de información y de las redes bajo la responsabilidad de la organización. Y para el proceso de implementación del ISOC en la ARC, se pretende usar como guía los parámetros impartidos en la guía de Gestión de Incidentes del SOC-CCOC y para la identificación de partes interesadas la norma NIST

800-53. Finalmente debe definir las políticas, servicios, formas de notificación de incidentes, el método de triage, identificación y sistema de asignación, así como la coordinación de la respuesta a incidentes, gestión oportuna de las comunicaciones y apoyo entre las partes relevantes para la recuperación y aprendizaje del incidente.

4.1.3. Componente de Personal

Para el componente de Personal el estudio de capacidades define que es necesario contar con talento humano, que tenga los conocimientos bien definidos en el área de interés a desempeñar (ciberseguridad y ciberdefensa, TI) (CONPES 3854, 2016), así mismo crear un plan de capacitaciones que permita al personal alcanzar las competencias mínimas y necesarias para lograr una adecuada gestión de sus roles y funciones. Y posteriormente que se puedan cumplir cada uno de los procesos, procedimientos y servicios diseñados por el área de doctrina. Igualmente basado en los parámetros impartidos en la Directiva Operacional 140 del 2013 del CCOC, para el componente de Personal que conforma el SOC del CCOC, se tomó de guía de referencia para definir los roles y responsabilidades que tendrán cada uno de los tripulantes que conformaran el ISOC de la ARC para lograr responder a los requerimientos de gestión de incidentes, análisis de vulnerabilidades, grupo de conciencia situacional y sensibilizaciones (Ver tabla 2). Finalmente se requiere contar con una dotación mínima de personal de quince (15) funcionarios entre los que se encuentran dos (02) oficiales, trece (13) suboficiales (Ver tabla 3) con especialidad ingenieros de sistemas, telecomunicaciones y/o electrónica; y con un plan de carrera que incluya capacitación continua y actualizaciones en Redes telemáticas, sistemas operativos,

lenguajes de programación, gestión de bases de datos, hacking ético, informática forense, procesos jurídicos de afectación en el ciberespacio, gestión de incidentes y riesgos, planes de continuidad de negocio, analítica de datos.

Tabla 2 *Perfil del Personal*

PERFIL DEL PERSONAL	
OFICIALES	<ul style="list-style-type: none"> • Ingeniero de sistemas, telecomunicaciones o electrónica • Especialización en seguridad informática o de la información. • Curso en Redes y Sistemas Operativos • Especialización profesional en seguridad y defensa nacional o Seguridad de la información. • Certificaciones de seguridad (Hacking ético, forense, ISO 27000, ISC) • Tecnólogo o Técnico en sistemas, electrónica o telecomunicaciones.
SUBOFICIALES	<ul style="list-style-type: none"> • conocimientos en informática. • Especialidad en informática o inteligencia naval. • Cursos de programación, gestión de bases de datos
PLAN DE CARRERA	<ul style="list-style-type: none"> • Fundamentos de Linux básico y avanzado • Fundamentos de sistemas operativos, • Cursos de “Administración en seguridad de redes, Metasploit, cisco, bases de datos, ethical hacking, penetration tester, manejador de incidente.” • Curso de investigador forense, análisis de malware. • Especialista en Criptografía y sistemas criptoanálisis • Maestría ciberseguridad y ciberdefensa • programación python, assembler, web, programación de aplicaciones móviles, programación en lenguaje C, programación java, programación delphi, programación ruby.

Nota: Elaboración propia

4.2. Parámetros para el funcionamiento del Centro de Operaciones de Seguridad de la Armada Nacional

El ISOC busca efectuar labores de monitoreo en tiempo real de la red de la Armada Nacional y la infraestructura crítica asignada, llevando a cabo la detección de intrusos y Seguridad preventiva, a través de actividades de gestión de incidentes, gestión del riesgo, conciencia situacional, gestión de activos y vulnerabilidades, manteniendo informado al Comandante de la institución de las situaciones de carácter operacional cibernéticos, asegurando el enlace y la coordinación con las unidades subordinadas y efectuando el control y seguimiento sobre los

medios asignados. En la tabla 3 se puede observar el modelo organizacional propuesto para el ISOC y en la Figura 12 el organigrama planteado para el ISOC. De igual manera en la Figura 13 se evidencia el proceso de gestión y operación de incidentes en el ISOC para la ARC.

Tabla 3 *Modelo organizacional ISOC en ARC*

Nombre	Centro de Operaciones de Seguridad Armada Nacional SOC-ARC
Responsable	Jefe de Inteligencia Naval (JINA) – Director Cibernética Naval (DICIB) – Director Centro de Operaciones de Seguridad (SOC)
Objetivo	Garantizar un sistema adecuado de Comando y Control que optimice la toma de decisiones estratégicas, consolidando, procesando y analizando la información en tiempo real de las diferentes fuentes de información, con el fin de asesorar y apoyar la toma de decisiones al Comandante Armada Nacional (COARC) y a su Estado Mayor en el desarrollo de las operaciones.
Normatividad	<ol style="list-style-type: none"> 1. Constitución política de Colombia 2. Directiva Permanente 101 CGFM-JEMC-CCOC 29.52 Agosto 2014 1. Política Integral de Seguridad y Defensa para la prosperidad. 2. Documento CONPES 3854 del 11 de abril de 2016 Política Nacional de seguridad Digital 3. Documento CONPES 3701 del 14 de julio de 2011. 4. Directiva Permanente DIR2014-18 Políticas de Seguridad de la Información para el sector Defensa 5. Ley 527 de 1999 “Comercio Electrónico” 6. Ley 599 de 2000 “Código Penal” 7. Ley 1273 de 2009 “Delitos Informáticos” 8. Ley 1581 de 2012 “Protección de Datos Personales” 9. Ley 1621 de 2013 “Inteligencia y Contrainteligencia” 10. Ley 1266 de 2008 “Habeas Data” 11. Directiva Operacional 140 del 2013 del CCOC
	Descripción
a. Capacidades	El Centro de Operaciones de Seguridad de la Armada Nacional, tendrá un proceso cíclico de la gestión en la seguridad cibernética, contando con componentes que permitan un modelo de monitorización del SOC, implementación y mejora constante de la infraestructura tecnológica de seguridad constituyendo el núcleo funcional y estructural de este proceso.
b. Funcionamiento operacional	<p>Supervisa las actividades y los resultados de los especialistas en monitoreo, técnicas y operaciones, para el desarrollo de las actividades, se deberá tener en cuenta el enfoque del ciclo PHVA, (<i>Planear, Hacer, Verificar y Actuar</i>), como proceso de mejora continua.</p> <p>Planear define todo el trabajo previo que tiene que ocurrir para permitir una respuesta rápida ante cualquier riesgo, amenaza o ataque. Esto significa tener en el espacio específico al personal idóneo, las políticas, los procedimientos, los equipos y la infraestructura necesaria para realizar las tareas asignadas.</p> <p>Hacer se enfoca a los cambios en la infraestructura informática para responder o contrarrestar ataques o actividades maliciosas. Estos cambios pueden deberse a la información obtenida durante el análisis y el manejo de un incidente, artefacto, o</p>

vulnerabilidad. Este proceso consiste en la mejora de la infraestructura basado en amenazas conocidas, se recomienda las mejores prácticas y estrategias de mitigación.

Verificar se define como el proceso de mejora constante el cual garantiza la continuidad del negocio, asimismo se encarga de analizar los eventos que requieren nuevas medidas o tratamiento.

Actuar es donde se clasifican los eventos de acuerdo a las categorías y prioridades para maximizar la eficacia de la respuesta predefinida.

Horario de operación los siete días de la semana, las veinticuatro horas del día (7*24) en turnos de guardia.

c. Parte de Personal

Se requiere como mínimo la participación de 15 funcionarios para su eficaz, eficiente y efectivo desarrollo, distribuidos de la siguiente manera:

- 02 oficial
- 13 suboficiales

d. Funciones por cargos

Director Centro de Operaciones de Seguridad Cibernética ARC (DSOC)

- Dirige 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.

Coordinador Gestión y administración del SOC

- Supervisa las actividades y resultados de los especialistas en monitoreo, técnicas, operaciones e Incidentes

Analista Amenazas Cibernéticas

- Efectúa el monitoreo permanente de las redes y sistemas de información institucionales de la ARC e infraestructura critica asignada, con el objetivo de evidenciar e informar de manera oportuna incidentes informáticos, violaciones a la seguridad y/o actividades sospechosas presentadas.

Técnico Gestión y Monitoreo

- Desarrolla operaciones de Ciberseguridad y entrega la información de interés al nivel superior, con el propósito de combatir o minimizar el impacto de las amenazas que afecten los activos informáticos institucionales.

Especialista Gestión de Respuesta Incidentes

- Procesa la información recolectada por los especialistas en monitoreo, operaciones e infraestructura critica, efectuando el análisis correspondiente y emitiendo las recomendaciones de acciones a tomar por parte del nivel superior.

Coordinador Gestión de incidentes y riesgos

- 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.

Técnico Gestión en Infraestructura Crítica

- Evalúa e implementa las técnicas y herramientas que usarían los especialistas en operaciones.

Analista de conciencia situacional y sensibilización

- Implementar planes de conciencia situacional y sensibilización al interior de la institución basado en lo evidenciado por inteligencia de amenazas y riesgos.

Coordinador y Operador de inteligencia de amenazas

- Atender y responder oportunamente a la inteligencia de amenazas que se evidencien, se compartan, se generen con otros SOC y CSIRT.

Nota: Elaboración propia

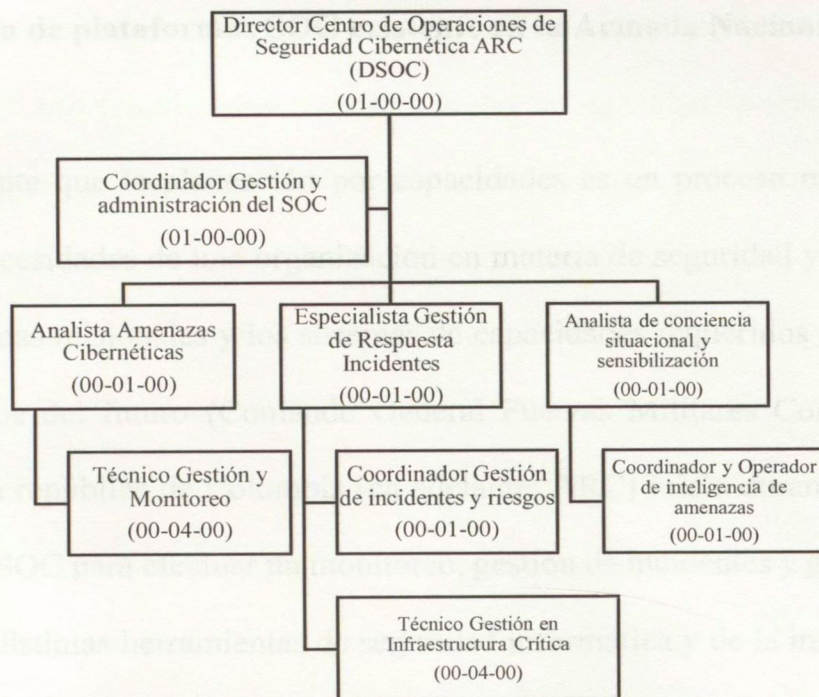


Figura 12 Organigrama ISOC ARC

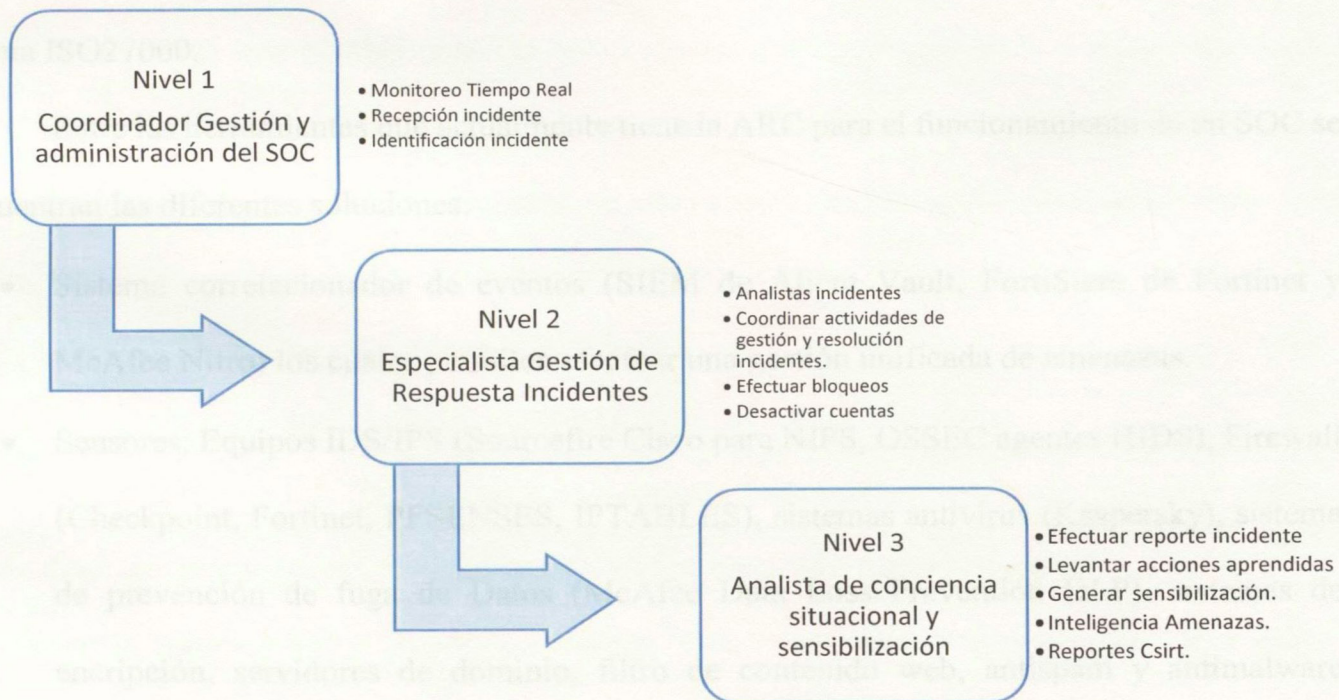


Figura 13 Proceso Operación y Gestión Incidentes en ISOC ARC

4.3. Caracterización de plataformas SOC existente en la Armada Nacional

Teniendo presente que la planeación por capacidades es un proceso metodológico que busca identificar las necesidades de una organización 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 (Comando General Fuerzas Militares Colombia, 2015) la Armada Nacional de la república de Colombia (en adelante: ARC) inicio durante el año 2008 la implementación de un SOC para efectuar un monitoreo, gestión de incidentes y gestión del riesgo, basado en agrupar las distintas herramientas de seguridad informática y de la información que se habían adquirido en años anteriores, todo bajo el ciclo de seguridad de la información, control operacional, políticas de seguridad, gestión de riesgo y cumplimiento, siguiendo como estándar la norma ISO27000.

Entre las herramientas que actualmente tiene la ARC para el funcionamiento de un SOC se encuentran las diferentes soluciones:

- Sistema correlacionador de eventos (SIEM de Alient Vault, FortiSiem de Fortinet y McAfee Nitro) los cuales permiten efectuar una gestión unificada de amenazas.
- Sensores: Equipos IDS/IPS (Sourcefire Cisco para NIPS, OSSEC agentes HIDS), Firewall (Checkpoint, Fortinet, PFSENSES, IPTABLES), sistemas antivirus (Kaspersky), sistema de prevención de fuga de Datos (McAfee Data Loss Prevention DLP), sistemas de encriptación, servidores de dominio, filtro de contenido web, antispam y antimalware perimetral, analizadores de vulnerabilidades y sistemas de análisis Forense.

Teniendo en cuenta la infraestructura que se tiene actualmente en la ARC, se puede observar que hacen falta componentes que permitan lograr la capacidad de tener un SOC de 5G (ISOC), entre los que se encuentran la necesidad de adquirir Equipos, herramientas de análisis de comportamiento de usuarios y de entidad (UEBA), plataformas de respuesta a incidentes (SIRP), así como, algunas soluciones de tecnologías de engaño. También la necesidad de efectuar un Diseño de Procesos y Procedimientos del ISOC de Acuerdo con políticas FIRST y/o ENISA - (European Union Agency For Network and Information Security), los cuales deben servir a los Procesos misionales de la ARC (estratégicos, tácticos, operativos y administrativos), Procesos Tecnológicos (Administración de Sistemas, Manejo de Configuraciones, Diseño) y Procesos Analíticos (Actividades orientadas a detectar comportamientos o eventos adversos, gestión de Incidentes).

En la Tabla 4 se pueden observar la soluciones que conformarían la implementación del ISOC en la ARC bajo la adquisición de herramientas de fabricantes líderes en el mercado y con la reutilización de las que se han comprado en años anteriores, las cuales permiten cumplir cada una de las etapas que requiere un SOC de 5G.

Tabla 4 *Soluciones Implementación ISOC en ARC*

SISTEMAS DE SOPORTE OPERACIONAL DEL ISOC	
SIEM	LogRhythm Enterprise ⁸ & TLM, IBM Security QRadar SIEM, Alient Vault, FortiSiem, RSA NetWitness Suite security.
Manejo y Almacenamiento de Logs (Tamaño recomendado: +20 TB)	IBM Security QRadar Log Manager, FortiAnalyzer y RSA NetWitness Logs & Packets, LogRhythm Enterprise, RSA NetWitness packets .
Monitoreo de Tráfico de Red y detección de Anomalías Proactiva	LogRhythm NetMon, IBM Security QRadar Risk Manager, Cisco source Firepower-AMP
Manejo de Vulnerabilidades	LogRhythm TLM, IBM Security QRadar Vulnerability Manager,
Manejo Forense de Incidentes en Red	LogRhythm NetMon, IBM Security QRadar Incident Forensics, RSA NetWitness event.

⁸ <https://logrhythm.com/pdfs/datasheets/lr-security-intelligence-platform-datasheet.pdf>

Inteligencia de amenazas	AlienVault Threat Intelligence, Cisco Talos Security Intelligence, LogRhythm's AI Engine Labs
Sistema de Prevención de Intrusiones de Nueva generación. (NGIPS)	Cisco source Firepower
Sistema de Prevención de Pérdida de Datos (DLP)	Intel Security-McAfee Data Loss Prevention (DLP)
Manejo y Control de Políticas (Cumplimiento)	Tripwire Configuration Compliance Manager (CCM), LogRhythm TLM
Monitoreo de Integridad y Cambio de Archivos	Tripwire File Integrity Monitoring (FIM), Alient Vault USM
Análisis de Vulnerabilidades	Qualys Guard, CORE IMPACT Professional y Tenable Nessus
Análisis Avanzado de Malware en la red	Cisco Advanced Malware Protection (AMP)
Equipos de seguridad Perimetral Firewall	Checkpoint, Fortinet
Sistema manejo de Tickets - Mesa de Ayuda	Support Center Plus – Enterprise, LogRhythm Enterprise, Alient Vault USM
Sistemas de Encriptación	Symantec encryption desktop corporate, Symantec encryption management server, Symantec Endpoint Encryption
Servidor Blade Center	Chasis Blade System c7000 Platinum (Blade Center soportará los Blades que albergarán la Virtualización. Cuatro (04) Blades con 2 Procesadores cada uno y 2 Discos Duros a cada servidor de 600 Gb y 7200 rpm. Para soportar la Virtualización.
Sistema de Almacenamiento tipo SAN	SAN - RAID 5 - Capacidad de almacenamiento efectivo de 20 TB, discos SAS
Equipo Switch de Core	Cisco Nexus 5548 UP Chassis 32 10GbE Ports 2 PS 2 Fans, configurado en HA
Herramienta de Virtualización	Vmware Essential Plus, Vmware Data Protection
Licenciamiento de herramientas Windows	Licenciamiento Windows 2012 Server
Estaciones de Trabajo y Teléfonos IP	Equipos MacBook PRO Core i7 16Gb RAM 1 Tb Disco Duro y Equipos Workstation con doble monitor Core i7 16 Gb RAM 1Tb disco Duro.
Canales de Acceso a Internet	Servicio Internet – Min. 100 MB Banda Ancha.
Seguridad Física e infraestructura	Sistema CCTV, Sistema de Control de Acceso (Biométrico, iris, palma de la mano), Puertas y cerraduras de seguridad, Sistema de Alarmas, UPS, Sistema de Detección y Extinción de Incendios

Nota: Elaboración a partir de datos tomados de Gartner SIEM 2016

Por lo tanto se puede determinar que las capacidades que requiere la ARC para tener un ISOC completamente funcional no solo van enmarcadas en tener herramientas tecnológicas que permitan efectuar el monitoreo y gestión de incidentes, sino que también se deben enfocar en optimizar y definir claramente los roles y responsabilidades de cada una de las áreas que prestan,

operan, administran y manejan servicios de TI y de seguridad de la información en la institución, para garantizar de esta manera que se diseñen procesos y procedimientos acordes a las tareas asignadas, igualmente en el área de talento humano es prioritario que desde el alto mando naval se tenga conciencia situacional de la importancia de la ciberseguridad y ciberdefensa para la institución y que se asignen el personal con capacidades y conocimientos en las áreas de TI, seguridad de la información, telecomunicaciones, sistemas y afines a la naciente Dirección Cibernética Naval, con el fin de fortalecer las capacidades y productos que la nueva dirección pueda llegar a brindar a la institución.

Igualmente se puede llegar a determinar que la ARC necesita un SOC de 5G (ISOC), inicialmente por la importancia de los procesos misionales que maneja y por las responsabilidades asignadas como Fuerzas Militares de Colombia (en adelante: FFMM), además con las responsabilidades asignadas bajo el desarrollo del documento CONPES 3854 del 11 Abril de 2016 como política Nacional de seguridad Digital (CONPES 3854, 2016) y para la protección de las infraestructuras críticas asignadas como responsabilidad de la institución para garantizar las medidas de ciberseguridad y ciberdefensa de las entidades públicas y privadas del país, así mismo porque la implementación de una solución de esta categoría permitiría no solo posicionar a la FFMM, ARC, como una organización que se encuentra a la vanguardia tecnológica de nivel mundial, sino porque daría al país un nivel mayor de seguridad en los procesos de ciberseguridad y ciberdefensa que se están manejando en el mundo por parte de los diferentes centros de amenazas cibernéticas y porque genera servicios y productos de: Monitorización continua de la seguridad en las distintas redes de la institución, detección y gestión de vulnerabilidades a través de auditorías automatizadas y manuales, centralización, tratamiento y custodia de log's que permiten correlacionar eventos de seguridad de múltiples fuentes con la intención de detectar situaciones

anómalas para posteriormente realizar análisis y búsquedas complejas sobre los eventos, a través de analítica de datos, responder y predecir elaborando respuestas y activando planes de resolución que permitan neutralizar las amenazas considerando aspectos tan importantes como la peligrosidad del ataque, criticidad de los activos implicados, e impacto sobre los mismos. Igualmente brindar asesoría de seguridad no solo a la institución sino también a las entidades que lo requieran en el país y generar activamente programas de prevención a través de vigilancia permanente de nuevas amenazas e implantar los controles preventivos que mitiguen el riesgo de aparición de incidentes de seguridad, todo esto basado en una conciencia situacional constante sobre todos los procesos que se desarrollen en el ISOC.

Un Security Operation Center inteligente (en adelante ISOC) Genera a las organizaciones ventajas para lograr detección y poder responder ante ataques poco conocidos, a través de la inteligencia de amenazas (HP Enterprise, 2016)

Así mismo, los SOC deben ser planificados para promover inteligencia operacional, transformar los datos de servidores, aplicaciones, equipos de red, dispositivos de seguridad, bases de datos en información única y precisa independientemente de cuál sea su tipo de organización.

La inteligencia operacional permite comprender en tiempo real lo que está sucediendo en los sistemas de TI y en la infraestructura tecnológica para poder tomar decisiones bien fundamentadas abarcando una arquitectura de seguridad adaptativa (capaz de detectar eventos de seguridad en la red, generación de alertas y control en la aplicación de medidas para proteger los activos) para convertirse en una inteligencia impulsada en el control de la situación. (Oliver Richmond, Neil MacDonald, 2013)

5. Arquitectura de referencia para ISOC

En este capítulo se explicará la arquitectura de referencia para los SOC de última generación, el cual se basa en arquitecturas de seguridad adaptativa, los cuales buscan mitigar los riesgos de ciberseguridad en las organizaciones, a través de las actividades de prevención, predicción, detección y respuesta, utilizando tecnologías de analítica de datos, bigdata y compartiendo inteligencia de amenazas entre organizaciones.

5.1. Definición de Intelligence-drive Security Operation Center

Un Security Operation Center inteligente (en adelante: ISOC) Genera a las organizaciones ventajas para lograr detección y poder responder ante ataques pocos conocidos, a través de la inteligencia de amenazas (HP Enterprise, 2016)

Así mismo, los SOC deben ser planteados para promover inteligencia operacional, transformar los datos de servidores, aplicaciones, equipos de red, dispositivos de seguridad, bases de datos en información única y precisa independientemente de cuál sea su tipo de organización.

La inteligencia operacional permite comprender en tiempo real lo que está sucediendo en los sistemas de TI y en la infraestructura tecnológica para poder tomar decisiones bien fundamentadas abarcando una arquitectura de seguridad adaptativa (capaz de predecir eventos de seguridad en la red, generación de alertas y control en la aplicación de medidas para proteger los activos) para convertirse en una inteligencia impulsada en el contexto de la situación. (Oliver Rochford, Neil MacDonald, 2015)

Igualmente los equipos de seguridad de las organizaciones deben entender cómo los SOC's inteligentes utilizan herramientas, procesos y estrategias para protegerse contra las amenazas modernas. Por lo tanto un SOC impulsado por inteligencia se enfoca en utilizar estratégicamente y tácticamente la inteligencia de amenazas de múltiples fuentes, es decir el trabajo en conjunto que se desarrolla con otros ISOC (Nacionales o Extranjeros), así como con empresas de seguridad y equipos de respuesta a incidentes (Cert), igualmente debe utilizar herramientas que permitan realizar procesamiento y análisis de grandes volúmenes de información para lograr operacionalizar la seguridad, y lograr automatizar los procesos siempre que sea factible,. En la Figura 14 se puede observar las tecnologías usadas en una arquitectura de seguridad adaptativa.

(Neil MacDonald, Peter Firstbrook, 2016) Definen una arquitectura de seguridad adaptativa en cuatro (04) dominios críticos que son Prevenir, Detectar, Responder y Predecir, para lo que los ISOC incorporan la implementación operacional de esa arquitectura basado en la inteligencia de la seguridad que se deriva de la amenazas externas y la inteligencia operacional basada en la información que se recopila de dispositivos internos de seguridad y la información compartida a través de la inteligencia de amenazas que son la guía efectiva para la detección y respuesta de los SOC's impulsados por inteligencia.

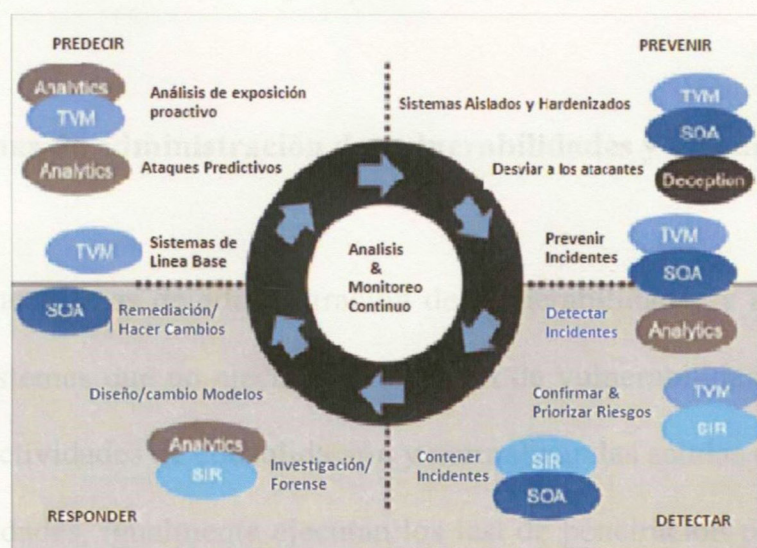


Figura 14 Arquitectura de seguridad adaptativa (Neil MacDonald, Peter Firstbrook, 2016)

Finalmente entre las características principales de un ISOC se encuentran el uso de técnicas de análisis avanzado (Analítica de datos) que permiten verificar de una forma más eficiente (mayor gestión en el volumen de información, altas velocidades de procesamiento) los procesos de la seguridad en el cual Gartner los define como analítica avanzada y en la que se usan métodos cuantitativos sofisticados entre los que se encuentran análisis de estadísticas, machine learning (Aprendizaje basado en patrones), data mining predictivo y descriptivo (recopilación y simulación de información basado en datos estructurados, no estructurados y semiestructurados), simulación y optimización (Generación de escenarios posibles para contribuir a una mejor toma de decisiones). Un ISOC debe proporcionar la velocidad que se necesita para detectar y responder a las amenazas avanzadas y para proporcionar un ciclo de retroalimentación para adaptarse y evolucionar.

5.2. Opciones de tecnología de los ISOC

Entre las opciones de tecnología que se utilizan para la implementación de los ISOC según (Oliver Rochford, Neil MacDonald, 2015) se pueden encontrar:

5.2.1. Plataformas de administración de vulnerabilidades y amenazas.

Las Plataformas de administración de vulnerabilidades y amenazas (en adelante: TVM) Son sistemas que no ejecutan evaluación de vulnerabilidades por sí mismas, sino que realizan actividades de consolidación y normalizan las salidas de múltiples soluciones de vulnerabilidades, igualmente ejecutan los test de penetración para analizar y priorizar

las vulnerabilidades que serán aplicadas a la inteligencia de amenazas y a los modelamientos de riesgos. Algunas de las plataformas comerciales de TVM que se pueden encontrar en el mercado son las de los fabricantes RedSeal, RiskSense, Kenna and NopSec.

RSA Network

5.2.2. Análisis de comportamiento de usuarios y de la entidad.

5.2.4. Plataformas de automatización de operaciones de seguridad.

Las soluciones de análisis de comportamiento de usuarios y de entidad (en adelante: UEBA) son sistemas que permiten detectar actividades maliciosas e ilegales, así mismo estas pueden consolidar y priorizar eventos y alertas de seguridad. Entre las plataformas comerciales de UEBA en el mercado son NIARA Analyzer (NIARA, Larry Lunetta, 2016), (Splunk® UBA) Splunk User Behavior Analytics (splunk.com, 2017), Análisis de Comportamiento de Usuario “DataAlert” de la firma Varonis (DATALEERT Varonis, 2017), Advanced Threat Analytics (ATA) de Microsoft, SQRRL ENTERPRISE (Sqrrl Enterprise, 2017), Risk Fabric de la firma Baydynamics y LogRhythm.

5.2.3. Plataformas de respuesta a incidentes.

Las soluciones de plataformas de respuesta a incidentes (en adelante: SIRP) se utilizan para formalizar, aplicar y automatizar respuestas, políticas y procesos de respuesta a incidentes, así como para proporcionar plantillas para gestionar escenarios típicos de incidentes de seguridad, estas soluciones son frecuentemente apoyadas por analítica, visualización, correlación de inteligencia de amenaza y capacidades de recolección de evidencia forense, Entre los fabricantes de tecnologías de seguridad que ofrecen SIRPS se

encuentran IBM con la solución IBM Resilient Incident Response Platform Standard IRP. (IBM Resilient Incident Response Platform Standard, 2017), Blue Coat - Effective Incident Response de SYMANTEC, Hexadite Automated Incident Response Solution (AIRS™) y RSA Netwitness.

5.2.4. Plataformas de automatización de operaciones de seguridad.

Las soluciones de plataformas de automatización de operaciones de seguridad (en adelante: SOAP) proporcionan una selección de conectores, scripts y plantillas para reparar dispositivos y aplicaciones de terceros que se pueden utilizar para automatizar o semiautomatizar las actividades de operaciones de seguridad. Algunos proveedores de estas soluciones son FireEye con la Solucion “FireEye Helix”, Ayehu, Swimlane, Hexadite, CyberSponse (Cybersponse, 2016), Demisto, IBM, Phantom, LogRhythm, Siemplify con la solucion ThreatNexus (Siemplify, 2017) .

5.2.5. Plataformas de engaño.

Los sistemas utilizados para efectuar procesos de engaño detectan e interrumpen un ataque mediante el uso de técnicas de engaño y trampas, ejemplo simulando un sistema o servicio vulnerable para provocar que un adversario acceda a él. Algunos proveedores de estas soluciones disponibles que proporcionan capacidades de engaño son TrapX Security, CyberTrap o GuardiCore. (Guardicore, 2016), NG Honeypot TOPSPIN, Elasticsearch Honeypot, Glastopf y HonnyPotter.

En la Figura 15 se puede observar el funcionamiento e interoperabilidad de un ISOC con los diferentes módulos y herramientas que interactúan en una arquitectura de seguridad adaptativa, donde se puede observar que el Core del modelo de operación del ISOC es el proceso de análisis y monitoreo continuo. (Neil MacDonald, Peter Firstbrook, 2016)

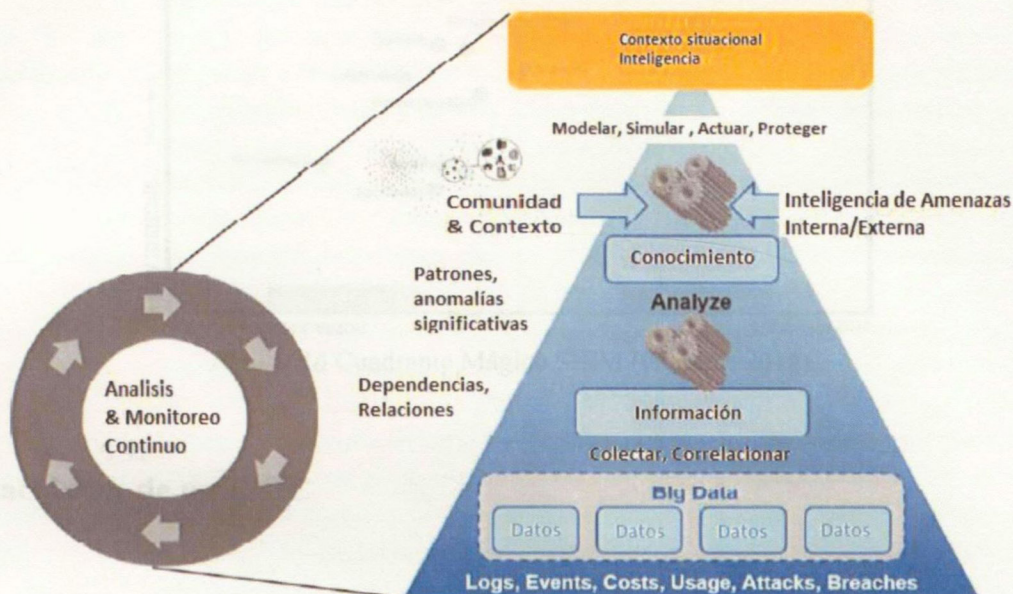


Figura 15 Modelo de operación ISOC (Neil MacDonald, Peter Firstbrook, 2016)

Igualmente en la Figura 16 según el reporte de Gartner (Kelly M. Kavanagh, Oliver Rochford, Toby Bussa, 2016) para sistemas de gestión de eventos y seguridad de la información (SIEM) se certifica que los principales proveedores de soluciones SIEM incorporarán funciones avanzadas de analítica y UEBA en sus productos.

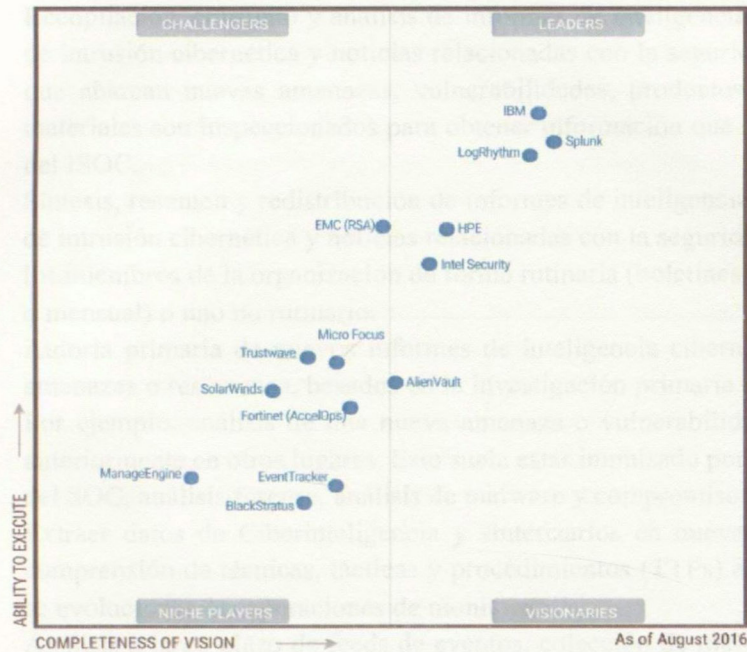


Figura 16 Cuadrante Mágico SIEM (Gartner, 2016)

5.3. Capacidades de un ISOC

Según (Zimmerman, 2014), un ISOC satisface las necesidades de monitoreo y defensa de la red de responsabilidad ofreciendo un conjunto de servicios. En la tabla 5 se muestra una descripción de las principales capacidades que debe cumplir un ISOC para responder ante un incidente cibernético.

Tabla 5 Capacidades de los ISOC

Nombre		Descripción
Análisis en tiempo real		
Atención al Público	al para	Generar reportes de incidentes y solicitudes de servicios del centro de seguridad, son recibidos vía telefónica, correo electrónico, portal web del ISOC o por otros métodos.
Ciberseguridad		Este servicio es similar a una mesa de ayuda de TI tradicional, excepto que es específico para el centro de seguridad.
Monitoreo en tiempo real y Triage	en y	Triage y análisis rápido de los feeds de datos en tiempo real (como registros del sistema y alertas) por posibles intrusiones. Después de un límite de tiempo especificado, los incidentes sospechosos son escalados al equipo de análisis y respuesta de incidentes para un estudio posterior. Generalmente también con los analistas de nivel 1 del ISOC, centrándose en los feeds de eventos en tiempo real y otras visualizaciones de datos.
Inteligencia y Tendencias		

Ciberinteligencia Recolección y Análisis		Recopilación, consumo y análisis de informes de inteligencia cibernética, informes de intrusión cibernética y noticias relacionadas con la seguridad de la información, que abarcan nuevas amenazas, vulnerabilidades, productos e investigación. Los materiales son inspeccionados para obtener información que requiera una respuesta del ISOC.
Distribución de la Ciberinteligencia		Síntesis, resumen y redistribución de informes de inteligencia cibernética, informes de intrusión cibernética y noticias relacionadas con la seguridad de la información a los miembros de la organización de forma rutinaria (boletines electrónico semanales o mensual) o uno no rutinario.
Creación de Ciberinteligencia		Autoría primaria de nuevos informes de inteligencia cibernética, como avisos de amenazas o resúmenes, basados en la investigación primaria realizada por el ISOC. Por ejemplo, análisis de una nueva amenaza o vulnerabilidad que no se ha visto anteriormente en otros lugares. Esto suele estar impulsado por los propios incidentes del SOC, análisis forense, análisis de malware y compromisos adversarios.
Fusión de Ciberinteligencia		Extraer datos de Ciberinteligencia y sintetizarlos en nuevas firmas, contenido y comprensión de técnicas, tácticas y procedimientos (TTPs) adversarios, con lo que se evolucionan las operaciones de monitoreo.
Tendencias		Análisis a largo plazo de feeds de eventos, colección de malware e información de incidentes para evidencia de actividad maliciosa o anómala o para entender mejor los TTPs del adversario. Esto puede incluir análisis de datos no estructurados, abiertos y de profundidad en varios feeds, tendencias y correlación durante semanas o meses de datos de registro, análisis de datos y métodos de detección de anomalías.
Evaluación de amenazas		Estimación holística de las amenazas planteadas por diversos actores contra los usuarios, sus enclaves o líneas de negocio, o equipos cibernéticos. Esto incluirá el aprovechamiento de los recursos existentes, tales como los feeds y las tendencias de información cibernética, junto con la arquitectura de la empresa y el estado de la vulnerabilidad. A menudo se realiza en coordinación con otras partes interesadas en la seguridad cibernética.
Análisis y Respuesta de incidentes		
Análisis de Incidentes		Análisis prolongado y en profundidad de posibles intrusiones enviados por otros miembros del ISOC. Esta capacidad suele ser realizada por analistas del nivel 2 y superiores dentro del proceso de escalada de incidentes del ISOC. Debe completarse en un lapso de tiempo específico para apoyar una respuesta relevante y efectiva. Esta capacidad suele implicar un análisis que aproveche diversos datos para determinar quién, qué, cuándo, dónde y por qué de una intrusión, su extensión, cómo limitar el daño y cómo recuperarse. Un analista documentará los detalles de este análisis, usualmente con una recomendación para acciones adicionales.
Análisis Manual		Los compromisos de los adversarios cuidadosamente coordinados, en los que los miembros del ISOC realizan un estudio y análisis sostenidos de los TTP de los adversarios, en un esfuerzo por comprenderlos mejor e informar el monitoreo continuo. Esta capacidad está estrechamente apoyada por tendencias y análisis de malware e implantes y a su vez, puede apoyar la creación de inteligencia cibernética.
Coordinación de respuesta a incidentes		Trabajar con los componentes afectados para reunir más información sobre un incidente, entender su importancia y evaluar el impacto de la misión, esta función incluye coordinar las acciones de respuesta y los informes de incidentes. Este servicio no involucra al ISOC implementando directamente contramedidas.
Implementación de contramedidas		Implementación real de las acciones de respuesta a un incidente para disuadir, bloquear o cortar la presencia o daño del adversario. Posibles contramedidas incluyen

Respuesta a incidentes en sitio	a	el aislamiento lógico o físico de los sistemas involucrados, bloques de firewalls, DNS, bloquear IP, desplegar parches y desactivación de cuentas.
Respuesta a incidentes remota	a	Trabajar con los componentes para responder y recuperarse de un incidente en sitio. Esto normalmente requerirá que los miembros del ISOC que ya están localizados en un lugar que los constituya o que viajen a ellos, apliquen experiencia práctica para analizar los daños, erradicar los cambios dejados por un adversario y recuperar los sistemas a un buen estado conocido. Este trabajo se realiza en asociación con propietarios de sistemas y administradores.
		Trabajar con los afectados para recuperarse de un incidente de forma remota. Esto implica el mismo trabajo que la respuesta en sitio del incidente. Sin embargo, los miembros del ISOC tienen comparativamente menos participación práctica en la recolección de datos o sistemas de recuperación. Por lo general, el soporte remoto se realizará a través del teléfono y el correo electrónico o en terminales remotas o interfaces administrativas como Microsoft Terminal Services o Secure Shell (SSH).

Análisis de los hechos

Manejo forense de Artefactos		Recopilación y almacenamiento de artefactos forenses (unidades de disco duro o medios extraíbles) relacionados con un incidente de manera que apoye su uso en procedimientos legales. Dependiendo de la jurisdicción, esto puede involucrar la manipulación de los medios de comunicación al tiempo que documenta la cadena de custodia, garantizando un almacenamiento seguro.
Análisis de Malware e Implantes	de	También se conoce como ingeniería inversa de malware o simplemente "reversing". Extraer malware (virus, troyanos, implantes, droppers, etc.) del tráfico de red o imágenes de los medios y analizarlos para determinar su naturaleza. Los miembros del ISOC normalmente buscarán el vector de infección inicial, el comportamiento y potencialmente, la atribución informal para determinar el alcance de una intrusión y para apoyar una respuesta oportuna. Esto puede incluir análisis de código estático a través de descompilación o análisis de tiempo de ejecución. Esta capacidad está destinada principalmente a respaldar un seguimiento y una respuesta eficaz. Aunque aprovecha algunas de las mismas técnicas que la "medicina forense" tradicional, no se ejecuta necesariamente para apoyar el procesamiento legal.
Análisis forense de Artefactos		Análisis de artefactos digitales (medios, tráfico de red, dispositivos móviles) para determinar el alcance total y la verdad de un incidente, generalmente estableciendo un cronograma detallado de eventos. Esto aprovecha las técnicas similares a algunos aspectos del malware y el análisis de implantes, pero sigue un proceso más exhaustivo y documentado. Esto se realiza a menudo utilizando procesos y procedimientos de tal manera que sus conclusiones pueden apoyar acciones legales contra aquellos que pueden estar implicados en un incidente.

Herramientas que soportan el ciclo de vida del ISOC

Dispositivo de Protección Borde O&M	de	Operación y mantenimiento (O&M) de los dispositivos de protección de fronteras (firewalls, proxies web, proxies de correo electrónico y filtros de contenido). Incluye actualizaciones y políticas del ciclo de vida de dispositivo, a veces en respuesta a una amenaza o incidente.
Infraestructura SOC O&M		O&M de las tecnologías ISOC fuera del alcance de la sintonización de sensores. Esto incluye el cuidado y la alimentación del equipo SOC: servidores, estaciones de trabajo, impresoras, bases de datos relacionales, sistemas de tickets, redes de área de almacenamiento (SANs) y copias de seguridad. Si el ISOC tiene su propio enclave, esto probablemente incluirá el mantenimiento de sus routers, switches, firewalls y controladores de dominio, si los hubiere. Esto también puede incluir O&M de sistemas de monitoreo, sistemas operativos (OS) y hardware.

Afinamiento de Sensores y Mantenimiento	Cuidado y alimentación de plataformas de sensores propiedad y operadas por el ISOC: IDS, IPS, SIEM, etc. Esto incluye la actualización de los sistemas IDS/IPS y SIEM con nuevas firmas, afinando sus conjuntos de firmas para mantener el volumen de eventos a niveles aceptables, minimizando los falsos positivos y manteniendo el estado de operación de los sensores y de los datos. Los miembros del ISOC que participan en este servicio deben tener una conciencia aguda de las necesidades de monitoreo del ISOC para que el ISOC pueda mantener el ritmo de un entorno de consistencia y amenaza en constante evolución. Los cambios en cualquier dispositivo de prevención en línea (HIPS/NIPS) generalmente se coordinan con el NOC u otras áreas de operaciones de TI.
Creación personalizada de firmas	Creación e implementación de contenido de detección original para sistemas de monitoreo (firmas de IDS, casos de uso de SIEM, etc.) sobre la base de amenazas, vulnerabilidades, protocolos, misiones u otros detalles específicos para el entorno de responsabilidad. Esta capacidad aprovecha las herramientas a disposición del ISOC para llenar las lagunas dejadas por las firmas comercializadas o proporcionadas por la comunidad. El ISOC puede compartir sus firmas personalizadas con otros SOC.
Ingeniería e implementación de herramientas	Investigación de mercado, evaluación de productos, creación de prototipos, ingeniería, integración, despliegue y actualizaciones de equipos SOC, principalmente basados en software libre o de código abierto (FOSS) o tecnologías comerciales de venta directa (COTS). Este servicio incluye el presupuesto, la adquisición y la recapitalización regular de los sistemas SOC. El personal que apoya este servicio debe mantener un buen ojo en un entorno cambiante de amenazas, lo que aportará nuevas capacidades en cuestión de semanas o meses, de acuerdo con las demandas de la misión.
Investigación y Desarrollo de Herramientas	Investigación y desarrollo (I+D) de herramientas personalizadas en las que ninguna capacidad comercial o de código abierto adecuado satisface una necesidad operativa. El alcance de esta actividad abarca desde el desarrollo de código para un problema conocido y estructurado hasta la investigación académica plurianual aplicada a un desafío más complejo.

Auditoría y amenaza interna

Recolección de datos de auditoría y Distribución	Recopilación de una serie de fuentes de datos relevantes para la seguridad para fines de correlación y análisis de incidentes. Esta arquitectura de la recolección también puede ser apalancada para apoyar la distribución y la recuperación posterior de los datos de auditoría para fines de investigación o análisis bajo demanda fuera del ámbito de la misión SOC. Esta capacidad incluye la retención a largo plazo de datos relevantes para la seguridad para uso de los componentes fuera del SOC.
Auditoría de creación de contenido y administración	Creación y adaptación de SIEM o contenido de mantenimiento de registros (LM) (correlación, cuadros de mando, informes, etc.) con el fin de servir a la revisión de auditoría de los componentes y la detección de uso indebido. Este servicio construye la capacidad de distribución de datos de auditoría, proporcionando no sólo un feed de datos sin procesar, sino también contenido construido para los componentes fuera del SOC.
Soporte de casos de amenazas internas	Apoyo al análisis e investigación de amenazas internas en dos áreas relacionadas pero distintas: 1. Encontrar indicaciones para posibles casos de amenazas internas (por ejemplo, uso indebido de recursos de TI, fraude con tarjeta de tiempo, fraude financiero, espionaje industrial o robo). El SOC dará a conocer los órganos de investigación apropiados (policía, Inspector General, etc.) con un caso de interés.

2. En representación de estos organismos de investigación, el SOC proporcionará más monitoreo, recopilación de información y análisis en apoyo de un caso de amenaza interna.

Investigación de caso de amenaza interna El ISOC aprovecha su propia autoridad reguladora o legal independiente para investigar la amenaza interna, para incluir el monitoreo enfocado o prolongado de individuos específicos, sin necesidad de apoyo o autoridades de una entidad externa. En la práctica, pocos SOC's fuera de la comunidad policial tienen tales autoridades, por lo que usualmente actúan bajo la dirección de otra organización.

Escaneo y Evaluación

Mapeo de Redes Mapeo sostenido y regular de las redes para comprender el tamaño, la forma, las interfaces perimetrales, a través de técnicas automatizadas o manuales.

Escaneo de vulnerabilidades Interrogación de los hosts para conocer el estado de vulnerabilidad, usualmente centrándose en el nivel de revisión de cada sistema y cumplimiento de seguridad, normalmente a través de herramientas distribuidas y automatizadas. Al igual que con el mapeo de red, esto permite que el ISOC entienda mejor lo que debe defender. El ISOC puede proporcionar estos datos a los miembros del equipo de seguridad, en forma de informe o resumen. Esta función se realiza con regularidad y no forma parte de una evaluación o ejercicio específico.

Evaluación de Vulnerabilidades Los miembros del ISOC trabajan con propietarios de sistemas y administradores de sistemas para examinar de manera holística la arquitectura de seguridad y las vulnerabilidades de sus sistemas a través de exploraciones, examen de la configuración del sistema, revisión de la documentación del diseño del sistema y entrevistas. Esta actividad puede aprovechar las herramientas de exploración de redes y vulnerabilidades, además de tecnologías más invasivas utilizadas para interrogar sistemas de configuración y estado. A partir de este examen, los miembros del equipo producen un informe de sus hallazgos, junto con la remediación recomendada. Los SOC aprovechan las evaluaciones de vulnerabilidad como una oportunidad para ampliar la cobertura de monitoreo y el conocimiento de sus analistas.

Test de Penetración Sobre conocimiento limitado de un área específica. Los miembros del SOC realizan un ataque simulado contra un segmento para evaluar la resiliencia del objetivo a un ataque real. Estas operaciones generalmente se llevan a cabo sólo con el conocimiento y la autorización de los ejecutivos de más alto nivel dentro de la entidad y sin previo aviso de los propietarios del sistema. Finalizada la operación, el equipo elaborará un informe con sus conclusiones, de la misma manera que una evaluación de la vulnerabilidad. Sin embargo, debido a que las actividades de pruebas de penetración tienen un conjunto estrecho de metas, no cubren tantos aspectos de la configuración del sistema y las mejores prácticas como lo haría una evaluación de vulnerabilidad

OTRAS CAPACIDADES

Evaluación de Productos Prueba de las características de seguridad de los productos puntuales que están siendo adquiridos. Análogamente a las evaluaciones de vulnerabilidad, estas pruebas permiten un análisis en profundidad de las fortalezas y debilidades de un producto en particular desde una perspectiva de seguridad. Esto puede implicar pruebas "internas" de productos en lugar de una evaluación remota de sistemas de producción o preproducción.

Consultoría de seguridad Proporcionar asesoramiento en materia de seguridad cibernética a los miembros fuera del ámbito del equipo de seguridad; Apoyo al diseño de nuevos sistemas,

		continuidad de negocios y planificación de recuperación ante desastres; Política de seguridad cibernética; Guías de configuración seguras y otros esfuerzos.
Formación y sensibilización	y	Acercamiento proactivo a los usuarios que apoyan la capacitación general, boletines y otros materiales educativos que les ayudan a entender varios temas de seguridad cibernética. Los objetivos principales son ayudar a los constituyentes a protegerse de amenazas comunes tales como esquemas de phishing/pharming, mejores sistemas finales seguros, aumentar la conciencia de los servicios del ISOC y ayudar a los usuarios a reportar correctamente los incidentes.
Conciencia situacional		Reempaquetado y redistribución periódica y repetible del conocimiento de los activos del SOC, redes, amenazas, incidentes y vulnerabilidades de los equipos. Esta capacidad va más allá de la distribución de información cibernética, mejorando la comprensión de los equipos, de la postura de seguridad cibernética de la entidad y áreas de la misma, impulsando una toma de decisiones efectiva en todos los niveles. Esta información se puede entregar automáticamente a través de un sitio web del SOC, portal Web o lista de distribución de correo electrónico.
Redistribución de TTPs		Compartir sostenidamente los productos internos del SOC con otros consumidores, como SOC's asociados o subordinados, en un formato más formal o estructurado. Esto puede incluir casi cualquier cosa que el SOC desarrolle por sí solo (por ejemplo, herramientas, información cibernética, firmas, Informes de incidentes y otros observables en bruto). El flujo de información entre SOC's es bidireccional.
Relaciones con los medios		Comunicación directa con los medios de comunicación. El SOC es responsable de divulgar información sin afectar la reputación.

Nota: Elaboración Propia tomado de datos de (Zimmerman, 2014),

5.4. Plataformas ISOC a nivel mundial

A continuación se enlistas algunos de los ISOC existentes a nivel mundial, (Samir_Kapur, 2014) Symantec abre un SOC de última generación en Sidney Australia. Este ISOC tiene como finalidad el compromiso de la compañía de proporcionar capacidades de seguridad expandidas a los clientes en la región de Asia-Pacífico y Japón.

(IBM, 2015) Centro de Operaciones Inteligentes de IBM para las Ciudades Inteligentes, este ISOC es una solución que ofrece un entorno de colaboración centralizado y en tiempo real, para planear, organizar, monitorear y compartir información entre departamentos y agencias municipales.

Mnemo, consultora española especializada en tecnologías de la información y en ciberseguridad, ha presentado al mercado IntellSOC, su Centro de Operaciones de Seguridad Inteligente. (Mnemo, Roberto Peña, 2016), busca prestar servicios de seguridad gestionada para el monitoreo de redes empresariales.

Igualmente España tiene un Centro Inteligente de Operaciones para gestión de las ciudades inteligentes, basado en tecnologías de Big data, servicios cloud y nuevos modelos de relación entre los agentes de la ciudad que sustentan las soluciones de gestión inteligente de las ciudades. (esmartcity.es, 2014) EL ISOC o como lo llamaron “Centro Inteligente de Operaciones de IBM” permite monitorizar y gestionar los servicios y sistemas de la ciudad ofreciendo una visión única y centralizada de las operaciones.

También el S2Grupo inaugura ISOC, Centro de Operaciones de Ciberseguridad Industrial, ubicado en Valencia y es el primero especializado en monitorización de infraestructuras críticas en España. (Gallego, 2013)

En Río de Janeiro (Brasil), se implementó un Centro Inteligente de Operaciones (IOC) para la gestión de emergencias, que integra todas las etapas de la gestión de emergencias y ofrece una visión integrada de las infraestructuras más importantes de la ciudad las 24 horas del día, basado en herramientas de analítica de datos. Entre los fabricantes de la solución se encuentran IBM y socios como Cisco, Cyrela, Facilities, Malwee, Oi y Samsung. (Pequerul, 2013)

Implementación de SOC para la Seguridad Pública en Memphis (EE.UU.) la tecnología de análisis predictivo de los ISOC, en el departamento de policía de Memphis ha logrado mejorar significativamente el problema de criminalidad de la ciudad, reduciendo en más de un 30% la tasa de criminalidad y en un 15% los crímenes violentos desde 2006.

Microsoft implementa ISOC en New York, La nueva instalación inteligente de guerra cibernética está considerada como el corazón de la nueva campaña de Microsoft “cuyo objetivo es el de reconstruir su reputación en el espinoso tema de la seguridad”. (Castro, 2015)

El Centro Global de Operaciones de Seguridad de Prosegur (Colombia) responde ante los retos de seguridad digital, el cual asume el desafío de contribuir a mitigar los riesgos asociados a las actividades digitales para proteger la información de empresas y personas en el país. Este SOC tiene cuatro ejes de acción que son, Seguridad Lógica que consiste en el monitoreo continuo e identificación de brechas de seguridad en la infraestructura tecnológica, Vigilancia Digital permite generar reportes periódicos o alertas en tiempo real sobre contenidos en la web que puedan afectar las organizaciones, Ciber-inteligencia que se centra en la detección de amenazas en fuentes abiertas y ocultas de internet, para identificar, contener y evitar fraudes y fugas de información y servicios de consultoría en aspectos inherentes a la seguridad de la Información. (Álvaro Hernández Gerente PROSEGUR Colombia, 2016)

(Ariel Pontón CEO Telefonica Colombia, 2016) El Centro de Operaciones de Seguridad de telefónica en Colombia como propuesta de ciberseguridad está destinado a la protección integral de los datos de las empresas y pymes del país, igualmente tiene como finalidad detectar, monitorear y alertar sobre incidentes de seguridad cibernética y funciona con un sistema de inteligencia artificial para correlacionar datos y advertir a los clientes de manera oportuna que es víctima de un ciberataque.

- Gestión de amenazas y vulnerabilidades
- Respuesta a eventos e incidentes, continuidad de operaciones y restauración de servicios
- Gestión de Riesgos

6. Aporte del ISOC al modelo de capacidades de ciberseguridad de la Armada

Nacional

En este capítulo se trabajaran las capacidades ofrecidas para el ISOC propuesto en la institución, después de haber realizado una comparación y análisis de los componentes de Personal, Doctrina, Material y Equipo que se tiene en la ARC, orientadas a las que aportarían mayores beneficios al modelo de capacidades de ciberseguridad de la institución.

6.1. Capacidades del ISOC en la Armada Nacional

Las capacidades definidas para el ISOC en la ARC estarán enmarcadas utilizando una arquitectura de modelos por dominios del departamento de energía de los estados Unidos (The Department of Energy (DOE), 2014) que servirán como estructura para generar valor en ciberseguridad a la institución. Los dominios definidos para el ISOC de la ARC son:

- Gestionar el Programa de ciberseguridad.
- Administración de personal.
- Conciencia situacional.
- Intercambio de Información y Comunicaciones.
- Gestión de amenazas y vulnerabilidades
- Respuesta a eventos e incidentes, continuidad de operaciones y restauración de servicios
- Gestión de Riesgos

6.2. Gestionar el Programa de ciberseguridad

A través de esta actividad se busca establecer y mantener un programa de ciberseguridad institucional que proporcione gobernabilidad, planificación estratégica y patrocinio para las actividades de seguridad cibernética de la Dirección Cibernética Naval (DICIB) de manera que se alineen los objetivos de seguridad cibernética con los objetivos estratégicos de la entidad (ARC) y el riesgo a la infraestructura crítica cibernética.

Además con la implementación de este dominio se busca que a través de la Dirección Cibernética Naval y el ISOC, se rijan los principios que enmarcan el programa de ciberseguridad y ciberdefensa en la ARC, dado por los alcances y capacidades que permite generar un SOC de 5G, el cual garantizara que se cumpla la estrategia planteada desde el alto mando Naval, garantizando que las políticas puedan llegar a todo el personal de usuarios.

Así mismo para consolidar la capacidad se hace necesario establecer cuatro (04) objetivos que deben ser desarrollados por la institución.

1. Establecer la estrategia del programa de ciberseguridad.
2. Patrocinar el Programa de Seguridad Cibernética con asignación de recursos económicos, talento humano, herramientas y el alto mando naval.
3. Establecer y mantener la arquitectura de ciberseguridad.
4. Desarrollar actividades de control y gestión del cumplimiento e implementación de la estrategia de ciberseguridad.

6.3. Administración de personal

Con los productos que se generan desde el ISOC, se buscan establecer y mantener planes, procedimientos, tecnologías y controles para crear una cultura de seguridad cibernética, asegurar la idoneidad y la competencia del personal en consonancia con el riesgo para la infraestructura crítica y los objetivos organizacionales de la ARC. Dado esto por la gran cantidad de información que permite procesar y analizar los SOC de 5G que permitirán mostrar al mando naval la necesidad de contar permanentemente con personal capacitado y entrenado en las unidades, para así lograr responder y gestionar los incidentes que se detecten y que podrían afectar las infraestructuras críticas navales. Para consolidar la capacidad se establecen cinco (05) objetivos que deben ser desarrollados por la institución.

1. Asignar responsabilidades de seguridad cibernética al personal.
2. Controlar el ciclo de vida del personal en los procesos de administración de sistemas críticos en las unidades.
3. Desarrollar las capacidades cibernéticas del personal de Ciberseguridad y Ciberdefensa
4. Aumentar la concienciación situacional de riesgos del personal de Ciberseguridad y Ciberdefensa.
5. Desarrollar actividades de gestión que evidencien el entrenamiento y las capacidades del personal de Ciberseguridad y Ciberdefensa.

6.4. Conciencia situacional

A través de talleres y entrenamiento, se buscan establecer y mantener actividades y tecnologías para recopilar, analizar, alarmar, presentar y utilizar información operativa y de ciberseguridad, incluyendo información de estados, para formar una imagen operativa común. Igualmente, implica el desarrollo de conocimiento en tiempo real de un entorno operativo dinámico a través de herramientas UEBA que utiliza el ISOC y que generan valor a la entidad. Esta capacidad se logra a través del registro y monitoreo de servicios de TI y activos de infraestructura de comunicaciones esenciales (sistemas de comunicaciones navales). Así mismo, es importante mantener el conocimiento de eventos de ciberseguridad relevantes y actuales externos a la ARC. La capacidad de cambiar de un estado predefinido a otro puede permitir una respuesta más rápida y eficaz a eventos de ciberseguridad.

Para consolidar la capacidad se establecen cuatro (04) objetivos que deben ser desarrollados por la institución a través de la correcta gestión que se den de los recursos que conformarían el ISOC de la ARC

1. Realizar registro de Log's de activos críticos.
2. Realizar monitoreo Continúo de activos críticos.
3. Establecer y mantener una imagen operativa de disponibilidad
4. Desarrollar actividades de gestión que permitan medir el estado de conciencia situacional del personal en la institución.

Igualmente el ISOC permitirá elevar los niveles de conciencia situacional en todos los niveles de la ARC, a través de los productos que se generen en el mismo, los cuales estarán

*Oficina de Seguridad de la Información de la Armada Nacional

*Comando Conjunto Cibernético FEMM, COLCER, Centro Cibernético Policial

enmarcados en boletines, alertas y expedientes, cada uno dependiendo a quien se dirija y el tipo de información que contenga.

6.5. Intercambio de Información y Comunicaciones

Por intermedio de las capacidades que permite generar el ISOC se busca establecer y mantener relaciones con entidades internas (OSI's ARC⁹) y externas (CCOC, COLCERT, CCP y entidades privadas)¹⁰ para recopilar y proporcionar información sobre ciberseguridad y ciberdefensa, incluyendo amenazas y vulnerabilidades, para reducir riesgos y aumentar la resiliencia operacional, proporcional al riesgo para la infraestructura crítica y los objetivos organizacionales.

Para consolidar la capacidad se establecen dos (02) objetivos que deben ser desarrollados por la institución.

1. Compartir información de Ciberseguridad.
2. Desarrollar actividades de gestión que evidencien las actividades de información compartida con otras entidades.
3. Establecer convenios institucionales.

6.6. Gestión de amenazas y vulnerabilidades

Teniendo presente las capacidades que generan el ISOC y las herramientas de análisis de grandes volúmenes de información, se buscan establecer y mantener planes, procedimientos y

⁹ Oficiales de Seguridad de la Información de la Armada Nacional.

¹⁰ Comando Conjunto Cibernético FFMM, COLCERT, Centro Cibernético Policial

tecnologías para detectar, identificar, analizar, gestionar y responder a las amenazas de ciberseguridad. Además a la gestión de vulnerabilidades de acuerdo al riesgo para los objetivos de la infraestructura de la organización (Por ejemplo, infraestructuras críticas informáticas y operacionales).

Para consolidar la capacidad que brinda el ISOC se establecen tres (03) objetivos que deben ser desarrollados por la institución.

1. Identificar y responder a las amenazas cibernéticas.
2. Reducir las vulnerabilidades de ciberseguridad de los activos estratégicos de la institución.
3. Efectuar actividades de gestión que permitan medir las actividades de reducción de amenazas de ciberseguridad en los activos estratégicos de la ARC.
4. Gestionar la identificación, cambio y configuración de activos

6.7. Respuesta a eventos e incidentes, continuidad de operaciones y restauración de servicios

Con la implementación del ISOC, se busca establecer y mantener planes, procedimientos y tecnologías para detectar, analizar y responder a eventos de ciberseguridad y mantener las operaciones a lo largo de un evento de ciberseguridad, en conformidad con los riesgos para la infraestructura crítica y los objetivos organizacionales. Por tanto un evento de ciberseguridad en un sistema o red es cualquier ocurrencia observable relacionada con una afectación de uno de los principios de la seguridad de la información (confidencialidad, integridad o disponibilidad de activos).

Para consolidar la capacidad se establecen cinco (05) objetivos que deben ser desarrollados por la institución para garantizar que el ISOC contribuya a cerrar la brecha ante los eventos e incidente de seguridad.

1. Detectar eventos de ciberseguridad y efectuar reporte en mesa de ayuda institucional.
2. Escalar los eventos de ciberseguridad y declarar los incidentes de acuerdo a la determinación de que es evento y que es un incidente.
3. Responder a incidentes y eventos escalados de ciberseguridad de acuerdo a procesos implementados y catalogación de prioridad.
4. Implementar un Plan de Continuidad determinando el proceso definido para identificación, manejo, comunicación, coordinación y cierre de un incidente.
5. Efectuar actividades de gestión donde se evidencie con lecciones aprendidas y la documentación el proceso desarrollado para la respuesta y continuidad de las operaciones ante un evento o incidente de ciberseguridad.

6.8. Gestión de Riesgos

Con la implementación del SOC de 5G en la ARC, se busca establecer, operar y mantener un programa de gestión de riesgos de ciberseguridad para identificar, analizar y mitigar los riesgos de ciberseguridad para la organización, incluyendo sus unidades de negocio, infraestructura interconectada relacionada y partes interesadas. Los riesgos de ciberseguridad se definen como un riesgo para las operaciones de la organización (La misión, las funciones, la imagen y la reputación), y los recursos debido al potencial de acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados de información. El ISOC permitirá reducir los riesgos y minimizar el

impacto que se pueda presentar por la ocurrencia o materialización. Para consolidar el dominio o la capacidad se establecen tres (03) objetivos que deben ser desarrollados por la institución.

1. Establecer una estrategia de gestión de riesgos de ciberseguridad.
2. Gestionar los riesgos de ciberseguridad.
3. Desarrollar actividades de gestión que permitan evidenciar la forma como se están gestionando los riesgos de ciberseguridad en la institución.

Conclusiones

La evolución tecnológica causada por las TICs no solo permite un desarrollo eficiente para el mundo, sino que también producen grandes retos e incertidumbres para garantizar la seguridad de las organizaciones. Por lo tanto, para lograr una defensa con altos niveles de seguridad en las organizaciones es necesario contar no solo con herramientas y soluciones que se complementen (ISOC), sino que también es necesario efectuar un análisis por capacidades que se oriente a cada uno de los requerimientos que se desean fortalecer, como son para el caso de la Ciberseguridad y Ciberdefensa los componentes de Doctrina y personal.

Para el caso de Análisis de este documento se cree que la aplicabilidad de una arquitectura de referencia de un ISOC en la ARC permitirá tener un grado de innovación en los procesos organizacionales de la institución en el área de la gestión y administración del dominio del Ciberespacio, la Ciberseguridad y la Ciberdefensa, direccionada especialmente por la Dirección Cibernética Naval como ente regulador y estructurador en la institución.

Se logró determinar de los resultados obtenidos de las entrevistas realizadas al personal de TI y la Dirección Cibernética de la institución, que las capacidades en Ciberseguridad y Ciberdefensa requeridas por la ARC, deben ir enmarcadas bajo un modelo de seguridad proactiva que trabaje bajo un enfoque integral que permita identificar y gestionar los riesgos que amenazan las plataformas críticas navales y sus tripulantes, además que se encuentre impulsada y orientada desde el alto mando naval bajo una estrategia de fortalecimiento del dominio del ciberespacio.

Del análisis efectuado para determinar los componentes requeridos en las variables de personas, procesos y tecnología para el ISOC, se evidenció que es necesario efectuar un establecimiento del mismo por fases, empezando por crear una estrategia que incluya el fortalecimiento de las capacidades que conforman un ISOC (Personas, Procesos y Herramientas

tecnológicas) e identificar los objetivos deseados en cada uno de los componentes, lo que permitirá una mayor comprensión de las principales metodologías, operaciones y procedimientos de seguridad y ataques actuales al usar las colaboraciones brindadas por los centros de inteligencia de amenazas.

El apoyo del modelo propuesto del ISOC al modelo de capacidades de Ciberseguridad de la Armada Nacional, se definió con base a la arquitectura de modelos por dominios del departamento de energía de los Estados Unidos, escogiendo como fase de inicio para el ISOC de la institución siete (07) dominios que son la base para garantizar un proceso eficiente y efectivo en la correcta gestión de riesgos e incidentes cibernéticos y que permitirán generar valor en ciberseguridad a la institución.

Recomendaciones

Para fortalecer el componente de personas que conformarían el ISOC, es necesario establecer una coordinación dirigida entre el alto mando naval, el cual incluye la Jefatura de talento humano, la Dirección de incorporación y reclutamiento, la Dirección cibernética naval y la Dirección de tecnologías de la información, en el que se cree un plan de carrera para el personal de oficiales y suboficiales que tripularan el área del ISOC y además que desde el planteamiento de necesidades de personal institucional se contemplen la incorporación y asignación de personal a las áreas de Ciberseguridad y Ciberdefensa de la institución.

Igualmente es necesario efectuar un análisis de responsabilidades en la ARC que permita determinar la mejor ubicación dentro la estructura organizacional de la institución a la cual debería pertenecer la Dirección Cibernética y el ISOC, esto dado desde el concepto del dominio del ciberespacio, orientado según las capacidades y operaciones de ciberdefensa que se deseen establecer, así mismo dado por las connotaciones de generar la DICIB como un bastión para el desarrollo de operaciones cibernéticas que contribuyan al cumplimiento de la misión constitucional y el fortalecimiento del poder Naval de la nación, debería poder considerarse que esta capacidad perteneciera a la Jefatura de Operaciones Navales.

Referencias Bibliográficas

- Álvaro Hernández Gerente PROSEGUR Colombia. (julio de 2016).
<http://colombiaempresarial.com.co/2016/07/08/el-centro-global-de-operaciones-de-seguridad-soc-responde-ante-los-retos-de-seguridad-digital/>.
- Ariel Pontón CEO Telefonica Colombia. (Marzo de 2016).
<http://www.siliconweek.com/security/security-management/66199-66199#ymObVPh5qVRh7TVt.99>.
- Armada Nacional de Colombia, A. (2015). *Plan Estratégico Naval 2015 - 2018*. Bogotá D.C.
- Castro, H. (noviembre de 2015). <https://www.linkedin.com/pulse/microsoft-y-sus-salas-inteligentes-de-guerras-herminia-castro>.
- Cezary Prokopowicz Regional Manager SEE HP Enterprise Security Products. (2014). *Hewlett-Packard*. Obtenido de <http://docplayer.net/7600383-Security-operation-centre-5th-generation.html>
- Chiavenato, I. (1986). *Introducción a la teoría General de la Administración*. Bogotá.: M. G. Hill. Ed.
- cisco Lab. Talos Security Intelligence and Research. (12 de 2015). *CISCO.COM*. Obtenido de Informe anual de seguridad de Cisco:
https://www.cisco.com/c/dam/global/es_es/assets/pdf/asr_final_os_ah_es.pdf
- Comando General Fuerzas Militares Colombia. (2015). *Las Fuerzas Militares y de Policía se preparan para nuevos escenarios de 2030*. p. 8. Obtenido de
<http://cgfm.mil.co/documents/10197/341108/PDF+LAS+FUERZAS+%23+36.pdf/102867bd-61ec-40c5-836d-adb219629d7e>
- Committee on National Security Systems. (2010). "CNSS Instruction No. 4009," Ft. Meade, 2010.
- CONPES 3854. (2016). *Política Nacional de Seguridad Digital*. Obtenido de
<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>
- Cuellar, G. (2013). *Concepto de Planeación por capacidades*. Obtenido de
<http://fccea.unicauca.edu.co/old/tgarf/tgarfse60.html>
- Cybersponse. (2016). *Cybersponse Seguridad adaptativa*. Obtenido de <https://cybersponse.com/>
- DATALERT Varonis. (2017). *Varonis DATALERT*. Obtenido de
<https://www.varonis.com/es/products/datalert/>

- David Chismon, Martyn Ruks. (26 de Noviembre de 2016). *MWR info security*. Obtenido de <https://www.mwrinfosecurity.com/assets/Whitepapers/Threat-Intelligence-Whitepaper.pdf>
- David Emm, Andrey Nikishin, Alexander Gostev. (3 de 12 de 2015). *Securelist, Kaspersky Security Bulletin 2015. Principales incidentes de seguridad*. Obtenido de <https://securelist.lat/kaspersky-security-bulletin-20152016-die-top-security-stories/82250/>
- Dr. Boiney, L., Connolly, J., Dr. Skorupka, C., Krueger, S., & Dr. Summers, A. (2015). *Cyber Operations Rapid Assessment*. Obtenido de MITRE: https://www.mitre.org/sites/default/files/publications/pr_15-2853-cyber-operations-rapid-assessment-state-of-methodologies.pdf
- Dutta, A. McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, 45(1), 67-87.
- esmartcity.es. (2014). <https://www.esmartcity.es/articulos/centro-inteligente-de-operaciones-para-gestion-de-la-ciudad>. Obtenido de Centro Inteligente de Operaciones para gestión de la ciudad,.
- Gallego, Á. (Abril de 2013). <http://www.redseguridad.com/actualidad/info-tic/s2-grupo-inaugura-isoc-su-centro-de-operaciones-de-ciberseguridad-industrial>.
- Guardicore. (2016). <https://www.guardicore.com/>.
- H. Jara; F. G. Pacheco. (2012). *Ethical Hacking 2.0*. Buenos Aires. Red users, 2012.
- Hewlett-Packard . (2015). *HP ESP Security Intelligence and Operations Consulting Services*. Recuperado el noviembre de 2016, de <https://ssl.www8.hp.com/ww/en/secure/pdf/4aa4-6539enw.pdf>
- HP Enterprise. (Julio de 2016). *Intelligent security operations*. Recuperado el 26 de Noviembre de 2016, de <https://www.hpe.com:https://www.hpe.com/h20195/V2/GetPDF.aspx/4AA6-6440ENW.pdf>
- IBM. (2015). http://www.ibm.com/expressadvantage/mx/downloads/IBM_Intelligent_Ops_Center_Solution_Brief_SPA.pdf.
- IBM Resilient Incident Response Platform Standard*. (2017). Obtenido de <http://www-03.ibm.com/software/products/es/resilient-incident-response-platform-standard>
- Israel Martínez Lacabe, Josep Castells Rafel, José Antonio Castrillo. (Octubre de 2016). *Ciberseguridad. Una guía de supervisión. En Principales técnicas de ataque y vulnerabilidades*. Obtenido de https://auditoresinternos.es/uploads/media_items/guia-supervision-ciberseguridad-fabrica-pensamiento-iai.original.pdf
- Joanne, C. (2005). How to staff a SOC. *Network World*, 22(11), 1. Retrieved from <http://search.proquest.com/docview/215987840?accountid=143348>.

- Kelly M. Kavanagh, Oliver Rochford, Toby Bussa. (10 de Agosto de 2016). *Gartner*. Recuperado el 2017, de <https://www.gartner.com/doc/reprints?id=1-3EG4GVX&ct=160810&st=sb>
- León, O. P. (2009). Operación y Servicios SOC. Telefónica del Perú S.A.A.
- Manuel Pérez Cortés. (2013). *CIBERDEFENSA: RETOS Y OPORTUNIDADES PARA EL SECTOR DE LA DEFENSA Y LA SEGURIDAD*. . Obtenido de Paper presented at the Semana Naval de la Armada.: http://www.armada.mde.es/mardigital/biblioteca-digital/jornadas-tecnologicas-iii-snm/04_jornadas-tecnologicas-manuel-perez-cortes.pdf
- Mnemo, Roberto Peña. (octubre de 2016). <http://www.channelbiz.es/2016/10/07/mnemo-presenta-intellsoc-para-ofrecer-seguridad-inteligente/>. Obtenido de <https://www.mnemo.com/ciberseguridad/>.
- Neil MacDonald, Peter Firstbrook. (28 de Enero de 2016). *MacDonald, N., & Firstbrook, P. (2014). Designing an adaptive security architecture for protection from advanced attacks.*
- NIARA, Larry Lunetta. (2016). <https://www.niara.com>. Obtenido de <https://www.niara.com/products/niara-security-analytics-platform/>
- NIST Special Publication 800-53. *Security and Privacy Controls for Federal Information Systems*. (s.f.). Obtenido de <http://dx.doi.org/10.6028/NIST.SP.800-53r4>
- Nizry, G. (2015). *Ayehu Software Technologies*. Recuperado el 2016, de <http://ayehu.com/wp-content/uploads/2015/09/5-Reasons-You-Should-Automate-Cyber-Security-Incident-Response-By-Gabby-Nizri-Ayehu1.pdf>
- Oliver Rochford, Neil MacDonald. (02 de Noviembre de 2015). *Gartner*. Recuperado el 24 de Noviembre de 2016, de <http://www.gartner.com/home>
- Pequerul, C. (2013). <https://www.esmartcity.es/articulos/control-inteligente-de-emergencias>. Obtenido de Control inteligente de emergencias.
- Puig M., M. (2015). *Planificación y Diseño de la Fuerza Militar por Capacidades: La Importancia de una Correcta Comprensión y Aplicación*. Cuaderno de Trabajo, 17, 28. Obtenido de <http://www.asociacioncolegiosdefensaiberoamericanos>
- Renaud, B. (2005). <http://iv2-technologies.com/SOCConceptAndImplementation.pdf>. (S. o. implementation., Ed.) Recuperado el 25 de Noviembre de 2016, de <http://www.iv2-technologies.com>
- Samir_Kapuria. (26 de Septiembre de 2014). *Symantec Official Blog*. (A. P. Next Generation Security Operations Center in Sydney, Editor) Obtenido de <https://www.symantec.com/connect/blogs/next-generation-security-operations-center-sydney-australia-positions-symantec-closer-global-c>
- Siemplify. (2017). Obtenido de <https://www.siemplify.co>

- splunk.com. (2017). *splunk.com*. Obtenido de Splunk® User Behavior Analytics:
https://www.splunk.com/es_es/products/premium-solutions/user-behavior-analytics.html
- Sqrrl Enterprise*. (2017). Obtenido de <https://sqrrl.com/media/Overview-Datasheet.pdf>.
- The Department of Energy (DOE). (2014). *Cybersecurity Capability Maturity Model (C2M2)*.
 Obtenido de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf
- TN. Julián D. Aponte D. (2014). TFM Proyecto para la creación del Comando de Ciberseguridad y Ciberdefensa de la Armada Nacional de la República de Colombia. pag. 38. Madrid.
- Zimmerman, C. (2014). Ten strategies of a world-class cybersecurity operations center. MITRE corporate communications and public affairs. Appendices.

Figura 5 Modelo de Ciberseguridad OTAN	35
Figura 6 Modelo de Ciberseguridad OTAN	36
Figura 7 Resultado estadístico Respuesta preguntas en el componente Personas	37
Figura 8 Resultado estadístico Respuesta preguntas en el componente Doctrina/Procesos	38
Figura 9 Resultado estadístico Respuesta preguntas en el componente Material y Equipo / Tecnologías	38
Figura 10 Comparación de Componentes Doctrina, Personal, Material y Equipo para brindar Capacidades a un ISOC (Elaboración Propia a partir de resultados de entrevista realizada personal TI y Seguridad de ARC, 2017)	39
Figura 11 Capacidades generales de ciberdefensa CTN, Julián D. Aponte D., 2014	45
Figura 12 Organización ISOC ARC	52
Figura 13 Proceso Operación y Gestión Incidentes en ISOC ARC	52
Figura 14 Arquitectura de seguridad adaptativa (Neil MacDonald, Peter Firstbrook, 2016)	59
Figura 15 Modelo de operación ISOC (Neil MacDonald, Peter Firstbrook, 2016)	61
Figura 16 Cuadrante Mágico SIEM (Gartner, 2016)	64

Listado de Figuras

Figura 1 Módulos Funcionamiento SOC (Renaud, 2005)	19
Figura 2 Arquitectura SOC (Renaud, 2005)	22
Figura 3 Roles en un SOC (Zimmerman, 2014)	24
Figura 4 Eventos de interés 1G-SOC (Hewlett-Packard, 2015)	26
Figura 5 Modelo de Ciberseguridad (Dutta, A. McCrohan, K., 2002)	35
Figura 6 Modelo de Ciberseguridad OTAN	36
Figura 7 Resultado estadístico Respuesta preguntas en el componente Personas	37
Figura 8 Resultado estadístico Respuesta preguntas en el componente Doctrina/Procesos	38
Figura 9 Resultado estadístico Respuesta preguntas en el componente Material y Equipo / Tecnologías	38
Figura 10 Comparación de Componentes Doctrina, Personal, Material y Equipo para brindar Capacidades a un ISOC (Elaboración Propia a partir de resultados de entrevista realizada personal TI y Seguridad de ARC, 2017).....	39
Figura 11 Capacidades generales de ciberdefensa (TN. Julián D. Aponte D., 2014).....	45
Figura 12 Organigrama ISOC ARC.....	52
Figura 13 Proceso Operación y Gestión Incidentes en ISOC ARC	52
Figura 14 Arquitectura de seguridad adaptativa (Neil MacDonald, Peter Firstbrook, 2016)	59
Figura 15 Modelo de operación ISOC (Neil MacDonald, Peter Firstbrook, 2016).....	63
Figura 16 Cuadrante Mágico SIEM (Gartner, 2016)	64

Listado de Tablas

Tabla 1 Preguntas para Conocer el Estado de Capacidades Cibernéticas	39
Tabla 2 Perfil del Personal	49
Tabla 3 Modelo organizacional ISOC en ARC	50
Tabla 4 Soluciones Implementación ISOC en ARC	54
Tabla 5 Capacidades de los ISOC	64

BIBLIOTECA CENTRAL DE LAS FF.MM.
"TOMAS RUEDA VARGAS"



201002336