Análisis de capacidades cibernéticas de la Fuerza Aérea Colombiana[1]

Mayor Adrián Fernando Muñoz Usa[2]
Escuela Superior de Guerra General "Rafael Reyes Prieto"

1. Resumen

La llegada de nueva tecnología ha representado una mejora evidente en diferentes actividades y procesos al interior de las Fuerzas Militares con celeridad, eficiencia y disponibilidad desde el ciberespacio; sin embargo, al mismo tiempo representa un mayor desafío para la defensa, seguridad y soberanía nacional, considerando que mientras haya mayor conectividad, el acceso a la información será más disponible y vulnerable.

Por tal motivo, es importante entender los efectos que un ataque cibernético a gran escala puede producir en el campo político, militar, económico y psicosocial, donde la protección de activos estratégicos e Infraestructura Crítica (IC) física y cibernética del país requiere de gran atención mediante unas capacidades robustas y fortalecidas, las cuales sólo son posibles por medio de una constante actualización y evolución, direccionadas desde el más alto nivel, que establezca una gobernanza que integre de manera transversal la gestión de la ciberseguridad y ciberdefensa.

De esta manera, el análisis de capacidades cibernéticas de la Fuerza Aérea Colombiana (FAC), se realiza con la metodología de análisis cualitativo, obteniendo datos, que se convierten en información de la situación actual, permitiendo evidenciar un diagnóstico a través de un marco comparativo, teniendo como referentes el modelo de capacidades DOMPI y modelo de madurez en ciberseguridad (CMM).

---

[1] Capítulo de libro resultado de investigación realizado en colaboración entre los siguientes proyectos: a) "Análisis de capacidades cibernéticas de la Fuerza Aérea Colombiana". El proyecto se encuentra adscrito y financiado por la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia.

[2] Estudiante de maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Ingeniero Mecánico de la Escuela Militar de Aviación "Marco Fidel Suárez". Contacto: munozaf@esdegue.edu.co. Código ORCID: https://orcid.org/0000-0003-4485-8845

La investigación permite identificar y proponer a la FAC, cuáles deberían ser las capacidades cibernéticas disuasivas reales, permanentes y sostenibles, para proteger sus activos cibernéticos y responder ante potenciales amenazas, contribuyendo a la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional desde y a través del ciberespacio.

2. Introducción

El constante y vertiginoso desarrollo de nuevas tecnologías ha cambiado el mundo, una mayor interacción de los sistemas y la búsqueda de la información ha llevado a la humanidad que el acceso a internet sea una necesidad, tanto así que cosas de la vida diaria ya sólo son posibles a través de este medio. La pandemia generada por el COVID-19 aceleró este proceso, que tal vez muchos no veían tan cercano; aun así, esto representó para muchos un reto o una oportunidad para reinventarse frente a esta nueva era de digitalización (WEF, 2022).

Aunque la llegada de nueva tecnología ha representado una mejora evidente en diferentes actividades y procedimientos de las Fuerzas Militares (FF.MM) con celeridad, eficiencia y disponibilidad desde el ciberespacio, representa al mismo tiempo un mayor desafío, considerando que mientras existe una mayor conectividad, el acceso a la información estará más disponible y sin duda con un mayor nivel de exposición a ser vulnerable; donde la interacción de los funcionarios en diferentes plataformas, aplicaciones, y en general lo que se denomina el internet de las cosas (IoT) por sus siglas en inglés (Internet of Things), se encuentran expuestos a nuevas amenazas que pueden ser fatales para la seguridad y defensa nacional, situación que obliga a que el grado de alfabetización digital (Organización de Estados Americanos, 2021) sea una actividad permanente y continua para estar a la vanguardia en materia de ciberseguridad y ciberdefensa.

No obstante, aunque el tema del ciberespacio y todo lo que éste representa, evoluciona de manera tan rápida que las tecnologías que hoy están vigentes, pasarán a un estado de obsolescencia en cuestión de poco tiempo. En este sentido, hablar de capacidades cibernéticas al interior de la Fuerza Aérea Colombiana no es nuevo, por ende, se debe entender que la doctrina debe cambiar, y ésta debe ser direccionada desde el más alto nivel para que se articule con las políticas y marcos legales vigentes.

Es así que, para alcanzar los fines de Estado consagrados en la constitución, es necesario un ambiente de seguridad interna y externa desde el ciberespacio, con el concurso de las ramas del poder público, de los órganos de control del Estado y, por supuesto, de todos los colombianos. (FF-MM-3-43,1996)

> Por tal motivo, las Fuerzas Militares, requieren abordar el ciberespacio como un ámbito estratégico, operativo y táctico, para organizar, entrenar y equipar a sus hombres, con el fin de aplicar medidas de prevención, disuasión, contención, protección y reacción, que permitan fortalecer las capacidades de Ciberdefensa, para enfrentar las amenazas o ataques cibernéticos que puedan afectar la infraestructura crítica cibernética del país, así como causar daños masivos, debilitar la economía, y/o dañar la moral pública y la confianza. (Realpe y Cano, 2020, p. 2)

De este modo, es prioritario profundizar en el conocimiento de las tecnologías de la información, de las comunicaciones y la operación; con el fin de crear estrategias, que permita actualizar la normatividad vigente, modernizar software, hardware, fortalecer protocolos de comunicación, acceso y autenticación; así como articular las entidades de orden nacional e internacional, que permita la transformación y futuro de la FAC mediante una estructura que se caracterice por su adaptabilidad, modularidad y sostenibilidad en el tiempo.

En consecuencia, el entendimiento de esta dinámica actual permite al comandante tener esa visión que le permita identificar o proponer cuáles deben ser las capacidades cibernéticas con una proyección multidominio, es decir, desde el ciberespacio propender por la defensa y derecho a la información, sin poner en riesgo la gestión de operaciones aéreas en un ambiente virtual ambiguo, incierto, complejo y cambiante.

Por lo anterior, se plantea la siguiente tesis, la Fuerza Aérea Colombiana tiene incorporado dentro de su doctrina, el ciberespacio como un nuevo dominio y no desconoce la importancia que este reviste en el entorno global, así que la protección de activos estratégicos e infraestructura crítica requiere de unas capacidades más fortalecidas, las cuales sólo son posibles a través de una constante actualización y evolución para hacer frente a esas nuevas amenazas. En ese sentido, con el diagnóstico cibernético, mediante el modelo DOMPI adoptado por el Ministerio de Defensa Nacional a través de la guía metodológica de planeamiento por capacidades – CAPÂCITAS - ((i) Doctrina y documentos que soportan la capacidad, (ii) Organización, (iii) Material y Equipo, (iv) Personal, e (v) Infraestructura, servirá como base para identificar el estado actual de la FAC.

Posteriormente, tomando como base un modelo de madurez de capacidad de Seguridad Cibernética (CMM), desarrollado conjuntamente por la Organización de los Estados Americanos, el Banco Interamericano de Desarrollo y la Universidad de Oxford, fundamentado en cinco categorías de actividad: (i) Políticas y estrategia nacional de seguridad cibernética; (ii) Cultura cibernética y sociedad; (iii) Educación, formación y competencias en seguridad cibernética; (iv) Marco jurídico y reglamentario, y (v) Normas, organizaciones y tecnologías, proporcionan un punto de referencia de los métodos, prácticas o procesos que permita guiar el desempeño de los esfuerzos nacionales en ciberseguridad.

En efecto, la Fuerza Aérea Colombiana siguiendo en su proceso evolutivo fortalecerá sus capacidades para contribuir desde el ciberespacio a la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional, de forma innovadora, polivalente, interoperable, líder y preferente regional, con alcance global y con capacidades disuasivas reales, permanentes y sostenibles.

3. Diagnóstico de las capacidades cibernéticas de la Fuerza Aérea Colombiana bajo el modelo DOMPI.

A medida que la tecnología avanza de manera vertiginosa y el continuo cambio de procesos, actividades, escenarios y fortalecimiento del dominio ciberespacial, es necesario prepararse y adaptarse a los nuevos desafíos, de esta manera a partir del 26 de marzo de 2018 mediante resolución ministerial No. 1014 de fecha 19 de febrero de 2018, se reestructura la organización de la Fuerza Aérea Colombiana, a través de un proceso de transformación que requirió de un equipo de trabajo, que planeó y analizó rigurosamente los procesos y procedimientos para lograr finalmente la estructuración en el nivel estratégico, de tres comandos y un estado mayor (Fuerza Aérea Colombiana, 2018).

Esta revisión y modernización de procesos de planeación estratégica y presupuestal corresponde al proceso de transformación y futuro de la Fuerza Pública liderada por el Ministerio de Defensa Nacional (MDN). Tal iniciativa tiene como objetivo diseñar un modelo de Fuerza que se caracterice por su adaptabilidad, modularidad y sostenibilidad en el tiempo (Ministerio de Defensa Nacional, 2014). Así, la planeación del futuro de la Fuerza Pública debe basarse en el uso sostenible y eficiente de los recursos públicos, donde se eliminen las duplicidades y se garantice la modernización integral de las Fuerzas Militares y la Policía Nacional (Ministerio de Defensa Nacional, 2015).

Como resultado, el MDN a través de la Resolución 7144 de 2018, puso en marcha el Modelo de Planeación y Desarrollo de Capacidades de la Fuerza Pública -CAPÂCITAS-, "como un esfuerzo para garantizar un marco coherente para la toma de decisiones respecto a la estructura de fuerza futura, de acuerdo con el direccionamiento estratégico de largo plazo, las restricciones presupuestales existentes, la doctrina y los conceptos operacionales" (Mindefensa, 2018, p. 6).

Basado en lo anterior, CAPÂCITAS define una capacidad "como la habilidad de realizar una tarea, bajo ciertos estándares (como tiempo, distancia, simultaneidad, etc.), a través de una combinación de sus respectivos componentes: Doctrina, Organización, Material y Equipo, Personal e Infraestructura (DOMPI)" (p. 30). De este modo, una capacidad puede interpretarse en función de unos componentes DOMPI debidamente articulados:

$$Capacidadt = f(Dt\ ,\ Ot,\ Mt\ ,\ Pt\ ,\ It\ )$$

Por lo tanto, basado en este desarrollo metodológico y los criterios definidos, se realiza el siguiente diagnóstico mediante unas visitas de campo, desarrollo de entrevistas, recopilación de información, donde se evidencia cuáles son las capacidades cibernéticas actuales de la FAC como se desarrolla a continuación:

Doctrina y documentos que soportan la capacidad: Entendiéndose "como el conjunto de saberes, principios, instrucciones, enseñanzas y normas, que guían los procesos y procedimientos para el cumplimiento de la misión constitucional de las Fuerzas Militares y la Policía, en aspectos operativos, administrativos y organizacionales" (Mindefensa, 2018, p. 30).

La Fuerza Aérea Colombiana (FAC) a través de los años ha venido en una constante actualización y evolución, y alineado a esa proyección, en el año 2020 cambió su misión así: "*Volamos, entrenamos y combatimos para vencer y dominar el espacio y el* ***[ciberespacio]***…" y por otro lado, su visión: "*Para ejercer el dominio en el aire, el espacio y el* ***[ciberespacio]****, la*

Fuerza Aérea será innovadora, polivalente, interoperable, líder y preferente regional…", así qué, todos sus procesos y actividades están encaminadas al "desarrollo del Poder Aéreo y Espacial de la Nación (interoperabilidad, desarrollo tecnológico y cooperación internacional), augurando para la Fuerza no solo ser líder como autoridad de aviación militar, sino también como líder en los diversos entornos del ciberespacio" (FAC, 2020, p. 29).

Por lo anterior, es de vital importancia tener en consideración los documentos doctrinarios al interior de la Fuerza, pasando desde su primera edición en el año 1975 con el nombre de Manual de Doctrina Aérea, la cual tuvo una revisión y su segunda edición en 1995; no obstante, en la tercera y cuarta edición de los años 2010 y 2013, se adoptó el nombre de Manual de Doctrina Básica Aérea y Espacial (MABDA), marcándose un hito importante en la evolución de la doctrina, lo que le llevaría a entender que su proyección de poder aéreo no sólo se da en la parte física, sino que trasciende al espacio y ciberespacio respectivamente, logrando su más reciente publicación en el año 2020, conocido como el manual de Doctrina Básica Aérea, Espacial y Ciberespacial (DBAEC).

Es de esta forma que, la FAC adopta e introduce desde el más alto nivel y como resultado del proceso de transformación, los conceptos generales del Poder Aéreo, Espacial y Ciberespacial (PAEC), entendiendo su alcance global y aplicable a todo el Rango de Operaciones Militares (ROM), definiendo el poder ciberespacial de acuerdo al DBAEC (2020) como "la capacidad virtual de aplicar, controlar y aprovechar el ciberespacio para contribuir, a través de efectos en este y otros dominios" (p. 7-1), la defensa de los derechos a la información y comunicación, a saber:

> El desarrollo de este poder requiere de la conjunción de tres áreas de acción, a saber:
>
> CONCIENCIA SITUACIONAL: busca conocer y entender el grado de superioridad o paridad que se tiene en el ciberespacio -usando inteligencia artificial o natural-, a la vez

que evalúa si se requiere algún tipo de acción para alcanzar el nivel de libertad esperado.

CIBERSEGURIDAD: siempre está operando y busca mantener un nivel apropiado de protección de las infraestructuras críticas frente a las amenazas en el ciberespacio.

CIBERDEFENSA: está relacionada con la respuesta a amenazas y el ataque en el ciberespacio. (DBAEC, 2020, p. 7-2)

Por lo tanto, la FAC desarrolla operaciones de contrapoder ciberespacial ofensivo como ciberdefensa y ciberespacial defensivo como ciberseguridad "mediante el uso de capacidades cibernéticas para alcanzar objetivos desde y a través del ciberespacio; incluye las operaciones de red, además de las actividades para operar, asegurar y defender la infraestructura crítica de la nación" (DBAEC, 2020, p. 10-3).

Figura 1. Misiones típicas y operaciones para dominar el aire, el espacio y el ciberespacio

Función	Misión Típica	Código	Anexo MOAEC	Operación
Dominar el aire, el espacio y el ciberespacio	Contrapoder Aéreo	Alfa	ACOAE FAC-3.0.1-O	Contrapoder Aéreo Ofensivo
				Contrapoder Aéreo Defensivo
	Contrapoder Espacial	Bravo	ACOES FAC-3.0.2-O	Contrapoder Espacial Ofensivo
				Contrapoder Espacial Defensivo
				Acceso al Espacio
				Explotación de Activos Espaciales
	Contrapoder Ciberespacial	Charlie	ACOCI FAC-3.0.3-O	Contrapoder Ciberespacial Ofensivo
				Contrapoder Ciberespacial Defensivo

Fuente: DBAEC (2020).

Así mismo, desarrolla operaciones de Inteligencia, vigilancia y reconocimiento (IVR) ciberespacial, para obtener una visión temprana que ayuda en el proceso de toma de decisiones "en el nivel estratégico, operacional y táctico; esta función permite observar las acciones del

enemigo con el fin de determinar sus dependencias, vulnerabilidades y fortalezas" (DBAEC, 2020, p. 10-5).

Figura 2. Misiones típicas y operaciones para gestionar IVR

Función	Misión Típica	Código	Anexo MOAEC	Operación
Gestionar IVR (Inteligencia Vigilancia Reconocimiento)	IVR Aérea	Delta	AIVRA FAC-3.0.4-O	Inteligencia Aérea
				Vigilancia Aérea
				Reconocimiento Aéreo
	IVR Espacial	Eco	AIVRE FAC-3.0.5-O	Inteligencia Espacial
				Vigilancia Espacial
				Reconocimiento Espacial
	IVR Ciberespacial	Foxtrot	AIVRI FAC-3.0.6-O	Inteligencia Cibernética
				Vigilancia Cibernética
				Reconocimiento Cibernético
	Contrainteligencia Aérea	Golf	ACONT FAC-3.0.7-O	Procedimientos Especializados de Contrainteligencia

Fuente: DBAEC (2020).

Respecto a la doctrina operacional, la FAC en el año 2015 publica el Manual de Ciberdefensa y Ciberseguridad O-MACIB, el cual establecía la misión y responsabilidades de la institución, enmarcando la función, misión típica y operaciones tipo a desarrollarse en el Ciberespacio. Posteriormente, en el año 2016 el Comando General de las Fuerzas Militares, a través del Comando Conjunto Cibernético, emite el Manual Básico de Doctrina de Ciberdefensa Conjunta (FF.MM 3-38 Restringido), configurándose como el documento de mayor jerarquía para las Fuerzas Militares, en este se establecen conceptos generales, características, limitaciones, principios, para el planeamiento, conducción y ejecución de las operaciones conjuntas en el ciberespacio, así mismo definiendo los roles y responsabilidades de acuerdo a la naturaleza y misión de cada fuerza.

Organización: Definido en CAPÂCITAS (2018) como "estructura funcional y espacial de las unidades, mediante la cual los componentes de las FF. MM y la Policía Nacional, interactúan

coordinadamente para lograr su misión. Este componente incluye funciones, estructura, protocolo organizacional, mando, coordinación y comunicación" (P. 31).

Actualmente, mediante Disposición FAC No. 048 del 10 de diciembre de 2020: "*Por la cual se reestructura parcialmente la organización de las dependencias de la Fuerza Aérea Colombiana, se reasignan las respectivas Tablas de Organización y Equipo (TOE), se modifican parcialmente la Disposición No. 014 del 7 de mayo de 2015 expedida por el Comandante de la Fuerza Aérea Colombiana, aprobada por Disposición No.042 del 28 de septiembre de 2015, proferida por el Comandante General de las Fuerzas Militares y esta a su vez aprobada mediante Resolución Ministerial No. 11443 del 15 de diciembre del 2015 y la Disposición No. 061 del 22 de diciembre de 2017 expedida por el Comandante de la Fuerza Aérea Colombiana, aprobada por Disposición No.060 del 28 de diciembre de 2017, proferida por el Comandante General de las Fuerzas Militares y aprobada mediante Resolución Ministerial No. 1014 del 19 de febrero del 2018*".

Como fruto de la experiencia, adaptación y modificación de la doctrina de la FAC, en el área de ciberseguridad y ciberdefensa, la FAC tiene dentro de su jerarquía, organización y equipo las siguientes dependencias dentro de la Jefatura de Inteligencia Aérea (JEINA) orgánica del Comando de Operaciones Aéreas y Espaciales (COAES) de acuerdo a lo estipulado en la tabla de organización y equipo TOE código No. 4-03-08-20 así: Dirección Cibernética Aérea y Espacial (DICAE), Subdirección Ciberseguridad Aérea (SUCSA), Subdirección Ciberdefensa Aérea (SUCDA), Área Operaciones Especiales Cibernéticas (AOPEC), Área Operaciones Ofensivas Cibernéticas (AOPOC).

De manera conjunta con las unidades cibernéticas de las demás Fuerzas y el Comando Conjunto Cibernético, estas dependencias tienen entre sus funciones y responsabilidades

implementar una estrategia de ciberdefensa para el país, basado en personal, tecnologías y procesos. Así mismo, desarrollar capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la seguridad y defensa nacional; por último, contribuir a la Ciberdefensa de la infraestructura crítica del país en el ámbito cibernético, incluida la del sector defensa (Comando Conjunto Cibernético, n.d.)

Material y equipo: según CAPÂCITAS (2018), **"**corresponde a los elementos necesarios para desarrollar, mantener y sostener las actividades encaminadas al cumplimiento de la misión constitucional. A su vez, contempla todo el ciclo de vida del material y equipo" (p. 31).

En ese sentido, hablar de material y equipo en el ciberespacio, corresponde al ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios (Resolución CRC 2258 de 2009), Es importante resaltar como tras el inicio de la pandemia en el año 2020, se impulsó de manera anticipada el uso de aplicativos, plataformas, software y equipos tecnológicos, donde el internet se convirtió en una necesidad tanto en los hogares como en las instituciones; al mismo tiempo, esta situación permitió a la FAC adaptarse a esta nueva realidad, empleando de una mejor manera las Tecnologías de Información y las Comunicaciones (TIC), para que los diferentes procesos al interior de la Fuerza se continuaran realizando de forma ininterrumpida a través del ciberespacio, optimizando tiempo y recursos cumpliendo a cabalidad la misión institucional.

Como resultado de lo anterior, "se alcanzó el mantenimiento eficaz de los activos aéreos, espaciales y ciberespaciales, la integración estandarización del sistema de comando y control de la institución con la Fuerza Pública y la actualización de equipos de inteligencia" (EDAES 2042, 2022, p. 55), esto se traduce en la adquisición de equipos, licencias, software, ampliación de redes

y conectividad, también se incrementó el uso de servicios en la nube, para que los funcionarios pudieran ejercer sus actividades laborales en dispositivos móviles personales; esto exigió un trabajo profundo y concienzudo orientado al fortalecimiento e implementación de las políticas de seguridad de la información, así como las capacidades en ciberseguridad y ciberdefensa de manera integrada entre la Jefatura de Tecnologías de la Información (JETIC) y la Dirección Cibernética Aérea y Espacial DICAE en la parte administrativa y operativa, de los diferentes procesos de la FAC.

Personal: Como lo define CAPÂCITAS (2018), es "el conjunto de individuos uniformados y civiles requeridos para el cumplimiento de las tareas asignadas" (p. 31). Es decir, aquí se incluye el liderazgo individual, así como la incorporación, capacitación, formación, entrenamiento y desarrollo de los individuos.

En este sentido, con una visión de futuro y entendiendo el auge de la tecnología e innovación, la FAC desde el año 2003 incluyó dentro de su pensum académico en la Escuela Militar de Aviación (EMAVI) el programa de ingeniería informática, graduando sus primeros oficiales ingenieros en el año 2008 e incorporándolos a las diferentes especialidades (Pilotaje, logística aeronáutica y de los servicios, Defensa Aérea, Seguridad y Defensa de Bases). Por otro lado, la Escuela de Suboficiales CT. Andrés M. Diaz, a través del programa de Tecnología en Inteligencia Aérea, sus egresados han logrado integrar sus conocimientos técnicos en comunicaciones, inteligencia y computación para que, desde sus unidades ubicadas a lo largo y ancho del territorio colombiano, contribuyan de manera determinante al progreso y desarrollo de la FAC en el ámbito del ciberespacio y sus operaciones.

En el área de ciberseguridad, actualmente se ha capacitado personal de oficiales a nivel de postgrado, especializaciones y maestría en áreas afines a seguridad de la información,

ciberseguridad y ciberdefensa en instituciones educativas a nivel nacional e internacional como la universidad de los Andes, la Escuela Superior de Guerra y la Universidad de Tecnología de Tallin en Estonia; de la misma forma, el personal de suboficiales ha recibido capacitaciones técnicas y operacionales para el desarrollo de operaciones cibernéticas, fortaleciendo así cada una de las dependencias desde su conocimiento y experticia aportando al reciente proceso de transformación de la FAC.

No obstante, aunque el entrenamiento y la capacitación del personal ha sido una política integral y constante a través de los años, no ha llegado a involucrar a la mayoría de los funcionarios, evidenciándose un bajo grado de alfabetización digital; que de acuerdo a la UNESCO "este tipo de aprendizaje se encuentra en permanente construcción y que incorpora a nuestros comportamientos y actitudes respecto a las nuevas tecnologías y, al mismo tiempo, a nuestros derechos y obligaciones" (UNESCO, 2020). De esta forma es importante entender que todos hacen parte fundamental para la seguridad de la información en el ciberespacio, pues deben estar preparados para identificar potenciales amenazas contribuyendo a mitigar su propagación y posible escalamiento, desarrollando mejores estrategias preventivas a través de la educación, herramientas digitales, uso correcto del internet y conciencia de seguridad cibernética por parte de cualquier persona.

De esta manera, la visión de las FF.MM y la aplicación del PAEC frente a esta nueva realidad debe corresponder a los desafíos generados desde el ciberespacio en todos los ámbitos del poder nacional, en el entendido como lo describe Realpe y Cano (2020), que desde el ciberespacio se pueden producir daños masivos, debilitamiento de la economía, y/o daño de la moral pública y la confianza. Por tal razón:

> Requieren abordar el ciberespacio como un ámbito estratégico, operativo y táctico, para organizar, entrenar y equipar a sus hombres, con el fin de aplicar medidas de prevención, disuasión, contención, protección y reacción, que permitan fortalecer las capacidades de Ciberdefensa, para enfrentar las amenazas o ataques cibernéticos que puedan afectar la infraestructura crítica cibernética del país. (p. 2)

Infraestructura: "corresponde al conjunto de bienes inmuebles, redes de servicios e instalaciones necesarios para el desarrollo de capacidades asignadas. Este componente incluye infraestructura en propiedad o en tenencia" (CAPÂCITAS, 2018, p. 31).

La actualización del material y equipo, ha requerido también una infraestructura necesaria para el óptimo desarrollo de las operaciones de contrapoder ciberespacial. Como ya se ha mencionado anteriormente, el proceso de transformación permitió tener y adecuar las instalaciones actuales para el desarrollo de estas actividades, con el fin de garantizar y mantener los diferentes servicios a los usuarios.

Lo anterior, permitió materializar en el año 2016 la finalización y "entrega del Laboratorio de Seguridad Cibernética dotado con los componentes tecnológicos tanto de hardware y software que permitirán a la FAC continuar con el desarrollo de capacidades en materia de ciberdefensa y ciberseguridad, en un entorno seguro" (FAC, 2020, p. 41).

Estas políticas institucionales, han permitido proyectar y asignar recursos para adecuar las instalaciones necesarias en el desarrollo de las funciones de la Dirección Cibernética Aérea y Espacial DICAE y sus dependencias anexas, viéndose reflejada la importancia de los temas cibernéticos, como la seguridad de la información y la comunicación en el empleo del PAEC, donde también recientemente se ha dispuesto la implementación y puesta en funcionamiento del Centro de Respuesta e Incidentes Cibernéticos de la FAC, siguiendo los lineamientos del Gobierno

Nacional, mediante la Resolución Número 473 de 17 de Febrero del 2022, el MINTIC adicionó al artículo 1. de la Resolución 002108 del 2020, el Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia – (ColCERT), bajo el Viceministerio de Transformación Digital, para continuar articulando y coordinando a nivel nacional los aspectos de ciberseguridad a todos los sectores públicos y privados del país.

4. Identificar el estado de madurez, desde las metodologías existentes, de las capacidades cibernéticas de la Fuerza Aérea Colombiana

Un modelo de madurez es un conjunto de características, indicadores, atributos que representan la capacidad y la progresión en una disciplina en particular (Rea-Guaman, Sánchez, Feliu, & Calvo-Manzano, 2017, p. 1). Estos modelos ejemplifican las mejores prácticas y permite evidenciar cuáles son los criterios en los que se pretende evolucionar para llegar a un estado final deseado.

Para el presente capítulo, el desarrollo del objetivo está basado en el marco de referencia de National Cybersecurity Capacity Maturity Model [Modelo Nacional del Estado de Desarrollo de Capacidad en Ciberseguridad, CMM], desarrollado por el Centro de Capacidad en 2014 e implementado en el año 2015; a través de un proceso de revisiones anuales en ciberseguridad en 11 países, lo que permitió realizar una evaluación regional para América Latina y el Caribe (conducida por la Organización de Estados Americanos con la colaboración del Banco Interamericano de Desarrollo) (GCSCC, 2016, p.2).

En general, los modelos de madurez en ciberseguridad, se abordan a través de diferentes áreas o dimensiones, entendiendo que cada dimensión no es necesariamente independiente de las otras, si no por el contrario, mantienen una estrecha relación para determinar “un punto de referencia con el que una organización puede evaluar el nivel actual de capacidad de sus prácticas,

procesos y métodos, y establecer objetivos y prioridades para la mejora" (Rea-Guaman, Sánchez, Feliu, & Calvo-Manzano, 2017, p. 2)

De esta manera, las organizaciones pueden comparar su desempeño entre sí y superar sus falencias. En las siguientes dimensiones, abordaremos las áreas más relevantes y fundamentales del modelo de madurez común a todos los modelos de ciberseguridad: Amenazas, Atacantes, Vectores de Ataque, Incidentes, Detección, Recuperación y Respuesta, cuyo objetivo es la protección de la información, pues el propósito de un ataque es derrotar la misión de un objetivo, donde "la forma más efectiva de hacerlo es con un sistema que no sabe que fue atacado", observó el oficial militar estadounidense Michael Hayden en 2008.

La aplicación de este modelo en la FAC tiene un propósito funcional y no simplemente una revisión teórica, pues la Organización de Estados Americanos (OEA) proporcionó esta "herramienta que optimiza la accesibilidad a varios actores que participan en la revisión de ciberseguridad" (GCSCC, 2016, p. 11).

De esta forma, el modelo CMM permite la revisión actual y estado de desarrollo de la capacidad en ciberseguridad al interior de la Fuerza Aérea Colombiana. En cada caso, nos permite comprender los requisitos para lograr altos niveles de capacidad y también evidenciar cuáles áreas necesitan mayor inversión.

Cada dimensión está compuesta por un número de factores que describen lo que significa poseer la capacidad de ciberseguridad. Cada factor presenta un número de aspectos y para cada aspecto hay indicadores que describen los pasos y acciones que, una vez observados, definen el estado de madurez de dicho aspecto. Existen cinco etapas de madurez (inicial, formativo, establecido, estratégico y dinámico). La etapa inicial implica un enfoque ad hoc de la capacidad,

mientras que la etapa dinámica representa un enfoque estratégico y la capacidad de adaptarse dinámicamente o de cambiar en respuesta a consideraciones externas.

Figura 3. Dimensiones modelo CMM

Fuente: Gráfico tomado de BID y OEA (2020).

"El Modelo (CMM) utiliza la metodología de grupos de discusión, ya que ofrece un conjunto de datos más rico en comparación con otros enfoques cualitativos" (GCSCC, 2020, p. 32). Por este motivo, fue necesario realizar entrevistas al interior de la Dirección Cibernética Aérea y Espacial (DICAE) y sus dependencias anexas, pues permite una metodología interactiva en el proceso de recopilación de datos e información, ya que, en lugar de formular únicamente preguntas a los entrevistados, facilita un debate entre los participantes, alentándolos a adoptar, complementar, interiorizar, defender o criticar el presente diagnóstico. Lo anterior, dio como resultado el actual estado de madurez de la FAC como se relaciona a continuación:

Tabla 1. *Dimensión: Políticas y estrategias en seguridad*

Factor	Aspecto	Inicial (1)	Formativa (2)	Consolidada (3)	Estratégica (4)	Dinámica (5)
Estrategia Nacional en ciberseguridad	Desarrollo de la estrategia				**X**	
	Organización				**X**	
	Contenido				**X**	
Respuesta a incidentes	Identificación de incidentes			**X**		
	Organización			**X**		
	Coordinación				**X**	
	Modo de operación			**X**		
Protección de las infraestructuras críticas	Identificación			**X**		
	Organización				**X**	
	Gestión de riesgo y respuesta			**X**		
Gestión de crisis	Gestión de crisis			**X**		
Consideración de ciberdefensa	Estrategia			**X**		
	Organización			**X**		
	Coordinación			**X**		
Redundancia de comunicaciones	Redundancia de comunicaciones		**X**			

Nota: Datos tomados de entrevista DICAE – SUCSA (2022).

En esta dimensión se evidencia la capacidad de la FAC para desarrollar y adaptar estrategias en ciberseguridad, en un nivel consolidado, a través del mejoramiento o implementación de un equipo de respuesta a incidentes, gestión de crisis, redundancia de capacidades, identificación y protección de la infraestructura crítica. Así que, es importante mencionar que recientemente el gobierno nacional a través del Decreto 338 del 8 de marzo de 2022, formaliza la definición y el alcance de los Equipos de Respuesta a Incidentes Cibernéticos (CSIRT), dirigido a todas las entidades que conforman la administración pública. Los entes de regulación podrán evaluar la necesidad de expedir normativa sectorial para la protección de infraestructuras críticas cibernéticas. Por otro lado, los particulares que tengan a su cargo

infraestructuras críticas cibernéticas o presten servicios esenciales, podrán facultativamente aplicar las disposiciones contenidas en el presente decreto.

De esta forma, la nueva política de seguridad digital debe propender en fortalecer aún más las capacidades de todas las partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.

> Según un informe anual de Symantec (ISTR), que realizó el análisis entre 157 países. Reveló que Colombia fue el sexto país de Latinoamérica con el mayor número de ataques en el 2017. Por todos estos casos, la ciberseguridad se ha vuelto un factor fundamental para la protección de la infraestructura computacional y todo lo relacionado de esta, especialmente la información que circula en la red. (Valoyes, 2017, p.1)

En este sentido, las entidades cuentan con mecanismos de articulación suficientes para tener una relación óptima con los actores de la seguridad digital de Colombia, donde el empleo del PAEC contribuye de manera significativa en la ciberseguridad y protección de infraestructuras críticas cibernéticas.

Tabla 2. *Dimensión: Cibercultura y sociedad*

Factor	Aspecto	Inicial (1)	Formativa (2)	Consolidada (3)	Estratégica (4)	Dinámica (5)
Mentalidad en ciberseguridad	Gobierno				**X**	
	Sector privado				**X**	
	Usuarios			**X**		
Confianza y seguridad en internet	Confianza y seguridad de los usuarios en internet			**X**		
	Confianza y seguridad de los usuarios en línea del gobierno		**X**			

	Confianza y seguridad de los usuarios en los servicios de comercio en línea		**X**
Conocimiento del usuario sobre la protección de información personal en línea	Conocimiento del usuario sobre la protección de información personal en línea		**X**
Mecanismos para denunciar	Mecanismos para denunciar	**X**	
Medios de comunicación y redes sociales	Medios de comunicación y redes sociales		**X**

Nota: Datos tomados de entrevista DICAE – SUCSA (2022)

Esta segunda dimensión se encuentra en un nivel consolidado, contempla los elementos de una cultura en ciberseguridad, como el nivel de riesgos en la sociedad, gobierno en línea, el nivel de confianza en los servicios de internet y servicios comerciales en línea. De esta forma, la concientización de los usuarios sobre la protección de información personal en línea es fundamental, ya que esta información estaría vulnerable debido al factor humano, pues siempre está inmerso en la interacción constante de muchos procesos que se realizan en el ciberespacio.

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) tiene desplegado a nivel nacional y territorial el Modelo de Seguridad y Privacidad de la Información, para apoyar la gestión e implementación de buenas prácticas y estándares para proteger los activos críticos de información, infraestructura tecnológica, y sistemas de información y comunicaciones, fomentando la mejora continua, donde la FAC siguiendo estos lineamientos, pone en conocimiento la existencia de mecanismos de denuncia que operan como canales para que los usuarios denuncien actividades maliciosas o que puedan generar afectación al interior de la Fuerza. Así mismo, se

revisa el rol de los medios de comunicación y redes sociales, su implicación e impacto en el área de valores, actitudes y comportamiento en ciberseguridad (CMM, 2016)

Tabla 3. *Dimensión: Educación, capacitación y habilidades en ciberseguridad*

Factor	Aspecto	Inicial (1)	Formativa (2)	Consolidada (3)	Estratégica (4)	Dinámica (5)
Campañas de sensibilización	Programas de sensibilización			**X**		
	Sensibilización ejecutiva			**X**		
Marco para educación	Provisión			**X**		
	Administración		**X**			
Marco para capacitación profesional	Provisión		**X**			
	Asimilación		**X**			

Nota: Datos tomados de entrevista DICAE – SUCSA (2022)

Esta dimensión se encuentra entre un nivel formativo y consolidado, basado en los programas de sensibilización en ciberseguridad tanto para el alto mando o directivos, como para los usuarios finales a todo nivel en la FAC.

Es por eso que, a través de grandes iniciativas cuyo origen surgen precisamente de la academia, desde el año 2017 se desarrolló un juego formativo para aportar a la concienciación en ciberseguridad al personal de la Escuela Militar de Aviación (EMAVI) “Marco Fidel Suárez”.

> Con lo cual se busca minimizar los riesgos para la seguridad de la información cuando se usa conexión a Internet, tales como robo de información, robos de claves de tarjetas bancarias, bullying, y secuestro de información. Si los ataques se dan, es necesario que los usuarios conozcan los planes de recuperación de desastres y resiliencia. El propósito de la concienciación a los empleados es aconsejar sobre seguridad de la información a través de la divulgación de las mejores prácticas en materia de seguridad (ISO 27000) para que adopten pautas de comportamiento

seguro en los diversos contextos en los que desempeñan su actividad profesional, extendiéndolas a su ámbito personal (Correa, Páez y Castiblanco, 2017, p. 266).

Por eso la educación, capacitación y habilidades en ciberseguridad debe estar enfocada a promover, mejorar y mantener un óptimo nivel de cultura en ciberseguridad "así como para lograr la concienciación de todos los funcionarios y terceros que interactúan en el sector defensa para minimizar la ocurrencia de incidentes de seguridad de la información y para que hagan un uso responsable de las nuevas tecnologías" (Correa, Páez y Castiblanco, 2017, p. 268).Así que la disponibilidad, calidad y captación de ofertas en educación y capacitación en áreas de ciberseguridad ha venido en crecimiento al interior de la FAC desde el año 2016, reflejado en el número de egresados profesionales a nivel de posgrado y capacitados en habilidades prácticas en esta área (FAC, 2016).

Tabla 4. *Dimensión: Marco Regulatorio y legal*

Factor	Aspecto	Inicial (1)	Formativa (2)	Consolidada (3)	Estratégica (4)	Dinámica (5)
Marco legal	Marcos legislativos para la seguridad TIC			**X**		
	Privacidad, libertad de expresión y otros derechos humanos en línea			**X**		
	Legislación de protección de datos			**X**		
	Protección de menores en línea					
	Legislación de protección al consumidor		**X**			
	Legislación sobre propiedad intelectual		**X**			
	Legislación sustantiva en ciberdelincuencia			**X**		

	Legislación procesal de ciberdelincuencia			**X**		
Sistema de justicia penal	Fuerzas del orden			**X**		
	Fiscalía		**X**			
	Tribunales		**X**			
Marcos de cooperación formal e informal para combatir la ciberdelincuencia	Cooperación formal			**X**		
	Cooperación informal		**X**			

Nota: Datos tomados de entrevista DICAE – SUCSA (2022)

Esta dimensión se encuentra entre un nivel formativo y consolidado, examina la capacidad del gobierno para diseñar y aprobar directa o indirectamente legislación nacional relacionada con la ciberseguridad; también se encuentran tópicos de seguridad, privacidad y asuntos relacionados con la ciberdelincuencia, los cuales si bien no aplican directamente para la FAC pueden llegar a tener incidencia en los niveles de exposición a riesgos y potenciales amenazas; por lo cual, los mecanismos de comunicación y coordinación con dependencias externas adquieren un valor relevante, donde se hace evidente mejorar los mecanismos de cooperación informal y formal, tanto a nivel nacional como transfronterizo, pues ese conocimiento, cooperación e intercambio de información permitirá fortalecer ese marco regulatorio y normativo para la aplicación del PAEC.

Tabla 5. *Dimensión: Normas, organizaciones y tecnologías*

Factor	Aspecto	Inicial (1)	Formativa (2)	Consolidada (3)	Estratégica (4)	Dinámica (5)
Cumplimiento de normas	Normas de seguridad de las TIC		**X**			
	Normas en adquisición		**X**			
	Normas en el desarrollo de software			**X**		
Resiliencia de la infraestructura de internet	Resiliencia de la infraestructura de internet			**X**		

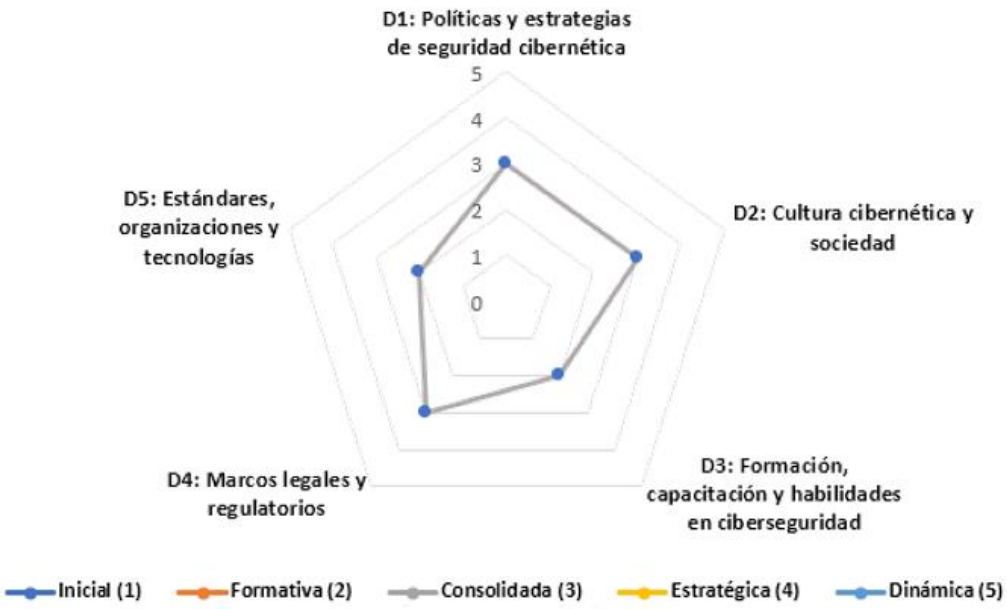
Calidad de software	Calidad de software	**X**
Controles técnicos de seguridad	Controles técnicos de seguridad	**X**
Controles criptográficos	Controles criptográficos	**X**
Mercado en ciberseguridad	Tecnologías en ciberseguridad	**X**
	Seguro cibernético	**X**
Revelación responsable	Revelación responsable	**X**

Nota: Datos tomados de entrevista DICAE – SUCSA (2022)

Esta dimensión que se encuentra en un nivel formativo, aborda el uso de la tecnología en ciberseguridad para proteger a las personas, organizaciones e infraestructura crítica. Así mismo, examina la implementación de normas y buenas prácticas en ciberseguridad, donde las operaciones conjuntas, coordinadas e Inter agenciales en el ciberespacio a través del Centro Cibernético de la Policial (CECIP), Comando Conjunto Cibernético (CCOCI), Equipo de Coordinación de Emergencias Cibernéticas de Colombia (ColCERT) y Equipos de Respuesta a Incidentes Cibernéticos (CSIRT) sectoriales, permitan una adecuada integración e implementación de procesos y controles, así como un adecuado flujo de información para el desarrollo de tecnologías y productos que permitan reducir los riesgos en ciberseguridad.

El análisis y tratamiento de los datos recopilados, permitió hacer la tabulación, ponderación y graficación del estado de madurez FAC, basado en los factores y aspectos que se lograron evidenciar a través de un enfoque comparativo mediante la aplicación de los instrumentos y/o herramientas del DOMPI y el CMM como se relaciona en la figura 4 y 5.

Figura 4. Estado actual de madurez FAC



Fuente: Elaboración propia, a partir de los datos proporcionados por DICAE (2022) con base en CMM.

Figura 5. Consolidado estado de madurez FAC por dimensiones

D1		D2		D3		D4		D5	
Factor	EM	Factor	EM	Factor	EM	Factor	EM	Factor	EM
Estrategia Nacional	4	Mentalidad en ciberseguridad	4	Campañas de sensibilización	3	Marco legal	2,7	Cumplimiento de normas	2,3
Respuesta a incidentes	3,3	Confianza y seguridad en internet	2,7	Marco para educación	2	Sistema de justicia penal	2,3	Resiliencia de la infraestructura de internet	4
Protección de las IC	3,3	Conocimiento del usuario sobre la protección de información personal en línea	3	Marco para capacitación profesional	2	Marcos de cooperación formal e informal para combatir la ciberdelincuencia	3	Calidad de software	2
Gestión de crisis	3	Mecanismos para denunciar	2	2,3		2,5		Controles técnicos de seguridad	2
Consideración de ciberdefensa	3	Medios de comunicación y redes sociales	3					Controles criptográficos	2
Redundancia de comunicaciones	2	2,9						Mercado en ciberseguridad	2
3,1								Revelación responsable	2
								2,3	
2,6									

Fuente: Elaboración propia, a partir de los datos proporcionados por DICAE (2022) con base en CMM.

5. Recomendaciones para la identificación y fortalecimiento de capacidades cibernéticas de la Fuerza Aérea Colombiana.

Después de revisar en detalle las capacidades cibernéticas mediante el modelo DOMPI y establecido el nivel de madurez actual de la FAC entre nivel formativo y consolidado con un promedio de 2,6 como se evidencia en la figura 5, este resultado se puede comparar con el obtenido en el reporte de ciberseguridad del año 2020, donde el nivel de madurez cibernética en promedio de la región está entre 1 y 2.

Sin embargo, el resultado del análisis del modelo CMM, permitió identificar en cuáles factores y aspectos la FAC debe enfocar sus esfuerzos para el cumplimiento de objetivos que permita fortalecer sus capacidades cibernéticas y le permita alcanzar un nivel superior de madurez. En ese sentido, se realizaron cinco (05) recomendaciones que influyen de manera directa y transversal en otras dimensiones y/o factores como se relaciona a continuación:

Primero, aunque Colombia fue el país con mayor desarrollo en seguridad cibernética de Suramérica particularmente en las dimensiones de "Política y estrategia" y "Cultura y sociedad" según lo estableció el reporte de ciberseguridad del año 2020 (BID y OEA, 2020), es importante considerar que se han emitido políticas y lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital mediante el más reciente decreto No. 338 del 8 de marzo de 2022, estos avances no dejan de ser una política de gobierno, así que es prioritario continuar con las gestiones pertinentes y los grupos interdisciplinarios necesarios para elevar estas iniciativas como políticas de Estado mediante una norma superior o ley, porque se deben involucrar todos los poderes del Estado (Militar, Económico, Político y Psicosocial) que permita interiorizar y fortalecer los lineamientos en materia de ciberseguridad -

ciberdefensa y cómo esta se articula con la Estrategia de Seguridad y Defensa Nacional para la protección de las infraestructuras críticas (IC), entendiendo su verdadero alcance, importancia y lo que constituye, pues como describe Cybersecurity & Infrastructure Security Agency [CISA].

> La protección de estos resulta crucial debido a que la IC sustenta las capacidades nacionales de un Estado, los cuales a su vez otorgan a su población de los servicios y recursos necesarios para su subsistencia. Debido a sus efectos, la afectación a la IC de un país sería de igual modo una afectación a su soberanía e independencia, a su estabilidad política, económica y social, y a sus intereses; con posibles efectos catastróficos para la población civil, en tanto tendría efectos que debiliten la seguridad, la economía nacional, la salud pública, o una combinación de estos. (CISA, n.d.)

De los tipos posibles de ataque a una Infraestructura Crítica, la más común en la actualidad y para el futuro vendría a ser la de naturaleza netamente cibernética, debido al inmenso daño que puede ocasionar en el país, y la facilidad de acceso por el creciente uso de tecnologías digitales dedicadas a su administración, lo cual incrementa las posibilidades de que sean vulneradas por un atacante que no requiere llevar a cabo una acción física destructiva sobre ella. Es por eso que las capacidades cibernéticas deben estar a la altura y en constante evolución para la protección de la misma, pues los Estados u otros actores no siempre atacarán las IC en el marco de un conflicto, si no que está demostrado que lo hacen también en tiempos de supuesta paz (Rossi, 2021, p. 43).

Entonces, el empleo del PAEC debe enfocarse en la defensa de una IC evitando el robo de información protegida o confidencial, o la obtención de conocimiento del funcionamiento de sistemas digitales militares, de inteligencia, de operación de una IC, entre otros; a través de la

combinación de diferentes elementos y capacidades tanto físicas como de ciberseguridad, ciberdefensa y atención a las nuevas amenazas híbridas (*et, al.*).

La acertada inclusión del ciberespacio como nueva dimensión o como el quinto dominio de la guerra dentro de la doctrina de la FAC, ha traído consigo la evolución de los tradicionales conceptos de seguridad y defensa, pues pone en consideración que hay nuevas y constantes amenazas desde el ciberespacio y la cooperación o combinación de esfuerzos privados y estatales son fundamentales para generar cambios y nuevas estrategias en materia de ciberseguridad.

Segundo, "Uno de los factores que limita el progreso de nuestra región en materia de ciberseguridad es la ausencia de talento humano **[calificado]**" es una de las afirmaciones hechas por Moisés J. Schwartz Gerente de Instituciones para el Desarrollo del BID en el año 2020 (OEA y BID, 2020). Lo anterior, se traduce en la importancia que reviste la capacitación, formación y actualización en temas de ciberseguridad y ciberdefensa, esto se evidencia con el resultado arrojado en la tercera dimensión del modelo CMM con una ponderación de 2,3 (figura 5); no obstante, en una de las capacidades distintivas que establece el DBAEC en el numeral 8.2.16 correspondiente a la Interoperabilidad Regional con Proyección Internacional, viene implícito un gran alcance que permitiría fortalecer las capacidades cibernéticas de la FAC, bajo una integración de estándares OTAN y ONU.

En ese sentido, es necesario contar con un plan de carrera y proyección del personal de oficiales, suboficiales y personal civil para que participen de manera activa con acceso a capacitación de nivel gerencial, técnico y asistencial, en los diferentes programas que ofrecen estas entidades, pues el desconocimiento y las tecnologías disruptivas hace que la actualización deba ser un proceso permanente y constante, pues es de vital importancia poner en conocimiento y ser

multiplicadores de la siguiente información con el objetivo de aprovechar estos temas que benefician no sólo a la Fuerza sino al país.

Colombia como miembro de la ONU, es partícipe en los temas de ciberseguridad e indirectamente, los de amenazas híbridas relacionados a la ciberseguridad, a través de la Oficina de las Naciones Unidas de Lucha Contra el Terrorismo (OLCT), su creación es parte de la implementación de la Estrategia Global de las Naciones Unidas en Lucha contra el Terrorismo a través del Programa de Ciberseguridad y Nuevas Tecnologías, cuyo objetivo es:

> Mejorar la capacidad de los Estados Miembros y las organizaciones privadas para que prevengan y mitiguen el uso indebido de los avances tecnológicos por los terroristas y los extremistas violentos. Esto implica contrarrestar la amenaza de los ataques cibernéticos que llevan a cabo los agentes terroristas contra la infraestructura vital, al igual que fomentar el uso de los medios sociales para recabar información de código abierto y pruebas digitales a fin de luchar contra el terrorismo y el extremismo violento en línea, a la vez que se respetan los derechos humanos. (UNCCT, n.d.).

Por su parte, dentro de la estrategia de alineación de criterios y estándares OTAN y siendo consecuente a la política de gobierno en el área de relaciones internacionales, Colombia como socio estratégico (partnership) en Latinoamérica, más allá de la alianza, es importante conocer que OTAN desde el 2008 cuenta con un Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE), el cual es un centro de ciberdefensa multinacional e interdisciplinario cuya misión “es apoyar a países miembros y a la OTAN con una experiencia interdisciplinaria única en el campo de la investigación, el entrenamiento y los ejercicios de ciberdefensa que cubren las áreas de enfoque de tecnología, estrategia, operaciones y derecho” (CCDCOE, n.d).

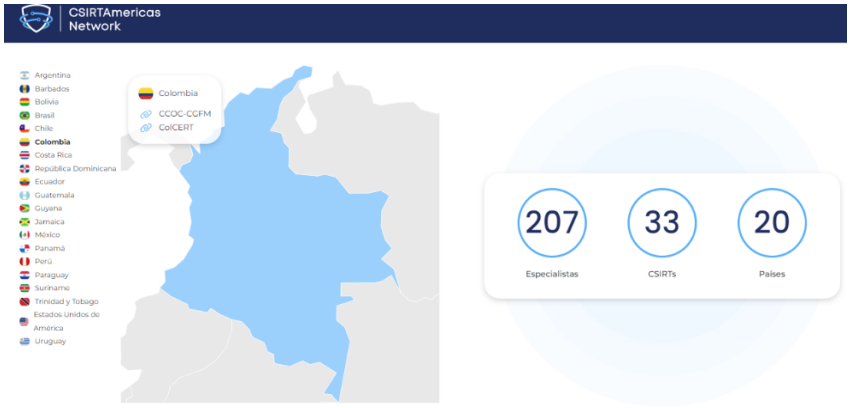
Desde 2010, el CCDCOE organiza anualmente el ejercicio internacional de ciberdefensa con fuego real más grande y complejo del mundo, A partir de enero de 2018, CCDCOE es responsable de identificar y coordinar soluciones de educación y capacitación en defensa cibernética para todos los organismos de la OTAN y desde el 2020, en una docena de años, el CCDCOE ha crecido y se ha expandido, uniendo ya a 28 países miembros, tanto aliados de la OTAN como socios afines más allá de la Alianza, De esta manera, la FAC puede acceder a constante capacitación, entrenamiento, acceso a nuevos recursos y tecnologías que permita fortalecer e innovar en sus capacidades futuras.

A nivel regional, la Organización de Estado Americanos (OEA) a través del Comité Interamericano contra el Terrorismo (CICTE), cuenta con un Programa de Ciberseguridad con más de 15 años de experiencia, siendo el líder regional en la provisión de ayuda a los Estados miembros "en el desarrollo de capacidades de ciberseguridad a nivel técnico y de políticas públicas. Sus iniciativas y actividades apuntan a garantizar un ciberespacio abierto, seguro y resistente en todo el hemisferio occidental" (CICTE, n.d.). De la misma manera, se han realizado estudios conjuntos con otras entidades como el Banco Interamericano de Desarrollo (BID) (GCSCC, 2016, p.2), que evalúan la situación de la ciberseguridad en la región, la cual ha sido objeto del presente trabajo para medir el estado de madurez al interior de la FAC.

En ese sentido, el programa trabaja en tres actividades principales: En primer lugar, el desarrollo de políticas; donde la FAC puede profundizar, aprovechar y ahondar más en estos temas para fortalecer el empleo del PAEC, así como una constante actualización y revisión de políticas a nivel regional bajo la modalidad de cooperación e interoperabilidad que ayude a mantener actualizada la doctrina y empleo de capacidades para afrontar las nuevas amenazas.

En segundo lugar, la creación de capacidades del programa de Ciberseguridad busca establecer y desarrollar las capacidades de los CSIRTs existentes en la región, si bien esta iniciativa se enfoca en cuatro objetivos compartidos: la promoción de la colaboración y compartir información sobre ciberataques, patrones de amenazas y análisis sobre herramientas de respuesta ante incidentes para los CSIRTs; la promoción de la creación de más CSIRTs y el apoyo a los que han sido recientemente establecidos; y el diseño de proyectos técnicos que apuntan a mejorar los servicios ofrecidos por los CSIRTs existentes.

Figura 6. Red CSIRT de las Américas



Fuente: Gráfico tomado de: https://csirtamericas.org/es

Aunque la FAC tiene su propio CSIRT haciendo parte de esa gran red hemisférica, lo más importante es promover una adecuada integración y cooperación entre las diferentes entidades estatales y privadas, para que no sean esfuerzos aislados y que contribuyan de manera eficiente y unificada frente a las amenazas cibernéticas de todo tipo, que pueda afectar la infraestructura crítica, recibiendo asistencia técnica personalizada y oportunidades de ejercicio para fortalecer las instituciones u organizaciones nacionales y regionales.

En tercer lugar, la investigación y divulgación desarrolla documentos técnicos, herramientas e informes para orientar a los responsables de la formulación de políticas, los CSIRT, los operadores de infraestructura, las organizaciones privadas y la sociedad civil, destacando los

desarrollos actuales e identificando problemas y desafíos clave de ciberseguridad en la región (CICTE, n.d.).

Tercero, fortalecer la DICAE en talento humano e infraestructura, pues el personal que allí labora no es suficiente para contrarrestar las amenazas actuales. Según el ESET Security Report para el año 2021 en Latinoamérica arrojó las siguientes estadísticas:

> Los códigos maliciosos (34%) son los principales responsables de los incidentes de seguridad en las empresas de la región, seguidos por los ataques de Ingeniería Social (20%) y los accesos no autorizados (16%). Las empresas en Brasil fueron las más afectadas por malware con el 19%, seguidas por México (17,5%), Argentina (13,3%), [**Colombia (10,6%)]** y Perú (8,9%). Por otro lado, 39% de los participantes afirmaron no haber padecido ningún tipo de incidente de seguridad en sus organizaciones. (p. 13)

Figura 7. Incidentes de Seguridad de la Información en las empresas de Latinoamérica.

Fuente: Datos tomados de las encuestas realizadas por ESET a empresas durante 2020.

> Los países con mayor cantidad de detecciones de *Ransomware* a nivel empresas fueron Perú (30%), seguido por México (14.9%), Venezuela (13.2%), Brasil (11.3%) y **[Colombia (7.9%)]** El caso más representativo de la Ingeniería Social es el phishing, una amenaza comúnmente utilizada para el robo de información sensible. De acuerdo con los datos, las empresas en Brasil fueron las más afectadas por casos de phishing con el 26,4%, seguidas por Perú (22,8%), México (12%), **[Colombia (9,1%)]** y Argentina (7,1%). (p. 9 -20).

De esta manera, es evidente que no sólo basta con capacitar al personal, sino que haya suficientes funcionarios que realicen de manera óptima las operaciones de contrapoder ciberespacial, pero eso requiere una adecuada administración del talento humano, que permita desempeñarse dentro de la institución en diferentes cargos, siguiendo un plan de carrera que, proporcione un desarrollo personal y profesional, encaminado a disminuir la tasa de retiros o fuga de personal calificado a entidades privadas, considerando la necesidad laborar a nivel mundial, pues "mientras los ataques de los ciberdelincuentes aumentan en cantidad y sofisticación, el mundo enfrenta una escasez de mano de obra capacitada en ciberseguridad. En tres años habrá 3,5 millones de empleos en ciberseguridad en el mundo" (Microsoft, 2022). Afirmando lo anterior, según el International Information System Security Certification Consortium (ISC):

> Actualmente hay más de tres millones de vacantes de trabajo en ciberseguridad sin cubrir a nivel mundial. Solo en las Américas hay una escasez de más de 900.000 trabajadores calificados en ciberseguridad. El programa "Creando una Trayectoria Profesional en Ciberseguridad" (Pathways to Progress) es una iniciativa que está trabajando para cerrar la brecha de habilidades técnicas en América Latina y el

> Caribe mediante el empoderamiento de jóvenes de entornos económicos diversos y el fomento de preparación profesional en la región.
>
> Entre 2017 y 2020, el programa "Creando una Trayectoria Profesional en Ciberseguridad" ha capacitado a 140 alumnos en Colombia y más de 600 en toda la región de las Américas. (OEA, 2021)

Cuarto, con base a la Estrategia para el Desarrollo Aéreo y Espacial de la FAC (EDAES 2042), esta apunta a ser un preferente regional en el tema espacial y ciberespacial, proyectando a la FAC con el empleo del PAEC dentro como fuera de sus fronteras en favor de sus intereses y contra potenciales adversarios. Es por ello que se recomienda que esa visión a largo plazo se revalúe como mínimo cada 4 años, pues las dinámicas humanas, procesos institucionales y el cambio de tecnología, ayude a reorientar la estrategia en materia de ciberseguridad y ciberdefensa que permita tener una retroalimentación de cómo continuar fortaleciendo capacidades cibernéticas que permita evolucionar y alcanzar el nivel de madurez deseado.

Quinto, según Ortiz (2021) "para la ciberdefensa no hay modelos definidos" (p. 7), donde la mayoría de los modelos de madurez de capacidad cibernética está enfocada únicamente a ciberseguridad. No obstante, la FAC desarrolla operaciones de contrapoder ofensivo (ciberdefensa); por lo tanto, los aportes realizados por este autor, permite emplear conceptos y hallazgos del trabajo de investigación "Modelo de evaluación de madurez de capacidades de ciberdefensa" para que en futuros análisis se articulen objetivos, procedimientos y operaciones ofensivas de manera conjunta desde el ciberespacio, ajustando el modelo a nuestras necesidades y amenazas actuales.

6. Conclusiones

Como resultado del presente trabajo de investigación, se pudieron extraer las siguientes conclusiones sobre el análisis de capacidades cibernéticas de la FAC como se relaciona a continuación:

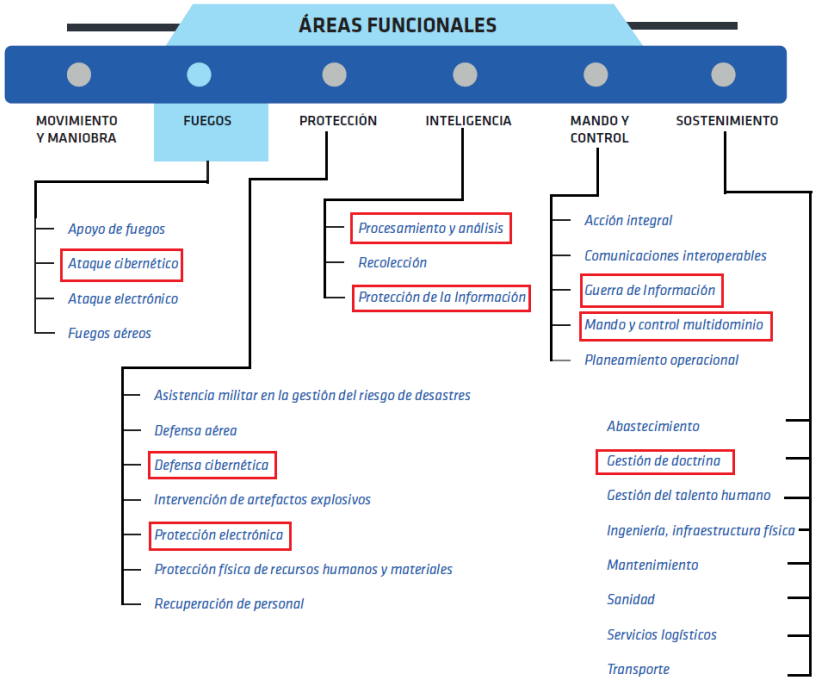
Primero, a través del diagnóstico de las capacidades cibernéticas bajo el modelo DOMPI, se evidenció qué, a través del proceso de transformación al interior de la FAC, el dominio del ciberespacio quedó incluido dentro de la misión y visión de la institución; dando un alcance y proyección en las operaciones multidominio con el empleo del PAEC; actualmente la FAC desarrolla operaciones de Contrapoder Ciberespacial – ACOCI ANEXO - FAC-3.0.3-O e Inteligencia, Vigilancia y Reconocimiento Cibernético – AIVRI - ANEXO - FAC-3.0.6-O y también tiene identificadas 3 capacidades distintivas enfocadas al ciberespacio, entendiendo la realidad presente y futura que incluye este nuevo dominio.

Segundo, el liderazgo de la DICAE, sus dependencias y personal que la conforma, han fortalecido progresivamente estas capacidades a través del tiempo, logrando así un importante grado de sinergia con las otras fuerzas y entidades Estatales a través de cooperación con el CCOCI, ColCERT, CECIP, CSIRT propio y sectoriales para destacarse a nivel de Suramérica como una de las "Fuerzas Armadas mejor capacitadas para realizar ciberoperación son las de Perú, Colombia, Argentina y Brasil" (Aguilar, 2021, p. 189), donde la identificación y protección de infraestructura crítica, ataques informáticos, información sensible o confidencial, pese a las amenazas híbridas y llegada de tecnología disruptiva, ha permitido en la actualidad aplicar el PAEC, respondiendo de manera oportuna a los fenómenos que deterioran la estrategia de Seguridad Nacional.

Tercero, el Modelo de Planeación y Desarrollo de Capacidades de la Fuerza Pública (CAPACITAS), permitió la identificación y caracterización de ocho (8) capacidades operacionales

y organizacionales enfocadas al ciberespacio (ver figura 8); con base en la Estrategia de Desarrollo Aeroespacial EDAES al año 2042, esto permitió la construcción de un marco conceptual común que facilita la interpretación y lectura detallada de las tareas que debe realizar y fortalecer la FAC.

Figura 8. Agrupación de capacidades bajo el Modelo de Planeación Sectorial



Fuente: Elaboración propia, a partir de los datos proporcionados por EDAES 2042 (2020).

Cuarto, con base en el modelo de madurez de capacidad de Seguridad Cibernética (CMM), desarrollado conjuntamente por la Organización de los Estados Americanos, el Banco Interamericano de Desarrollo y la Universidad de Oxford, se identificó que la FAC se encuentra en un estado de madurez entre formativo y consolidado con un valor de 2,6. Este resultado es comparable con el obtenido en el reporte de ciberseguridad del año 2020, donde los países del cono sur tienen un promedio entre 2 y 3; es decir, los resultados son congruentes y consecuentes al desarrollo de la región.

Quinto, es importante considerar que varios aspectos han comenzado a crecer y formularse, otros se encuentran instalados y funcionando; no obstante, falta considerar la asignación de recursos, donde se han tomado decisiones de compromiso acerca de los beneficios con respecto a la inversión relativa, aunque la etapa es funcional y se encuentra definida. Así mismo, se evidenció cuáles áreas necesitan mayor inversión (ver figura 4) en especial las dimensiones de "Formación, capacitación y habilidades en ciberseguridad", "Estándares organizaciones y tecnologías", donde se requiere una mayor atención para formular estrategias con el fin de alcanzar el nivel de madurez esperado en correspondencia con los roles y funciones de la FAC.

Sexto, la FAC definió sus preferencias sobre qué indicadores y hoja de ruta a seguir desde el alto mando a través del EDAES 2042, para afrontar las amenazas futuras y en qué áreas se debe fortalecer capacidades cibernéticas (ver figura 7), esto se constituye en el primer avance importante para continuar al siguiente nivel de madurez como el estratégico, donde el entendimiento de la sofisticación tecnológica, conflicto global o cambio significativo en un ámbito de interés, reasignación de recursos y la atención constante al entorno debe corresponder a la creciente interconectividad en la presente era de la Cuarta Revolución Industrial, brindando a los comandantes las herramientas necesarias para mejorar el proceso de toma de decisiones frente a vulnerabilidades, ataques o intrusiones cibernéticas e híbridas.

Séptimo, los modelos de madurez existentes están enfocados a la ciberseguridad y han sido el resultado de adaptaciones de otros modelos; sin embargo, la mayoría de ellos, toman como referencia el modelo CMM; por lo anterior, la FAC puede adaptar este modelo de acuerdo a sus necesidades puntuales donde quede establecido el empleo del PAEC que involucre de manera

integral las operaciones de contrapoder ciberespacial (ofensivo: ciberdefensa y defensivo: ciberseguridad) e IVR.

Finalmente, el diagnóstico a través del DOMPI y nivel de madurez del CMM permitió proponer cinco (05) recomendaciones para la identificación y fortalecimiento de las capacidades cibernéticas de la FAC que permitan evolucionar hacia los siguientes niveles, enfocadas al fortalecimiento de las instituciones con una política de Estado definida y transversal a todos los sectores (Política, Militar, Económico y Psicosocial), generando mecanismos de gobernanza, cooperación en la respuesta de incidentes informáticos, planes y estrategias, administración del talento humano y capacitación.

7. Referencias

Aguilar Antonio, J. M. (2021). *Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior*. Estudios internacionales (Santiago), 53(198), 169-197.

Becerra, J., León, I., & Medina, G. (2019). *La Seguridad en el Ciberespacio. Un desafío para Colombia*. Escuela Superior de Guerra “General Rafael Reyes Prieto” Recuperado de https://esdeguelibros. edu. co/index. php/editorial/catalog/view/42/48/741-1.

Benito Reina, W. A. Fuerza aérea colombiana, un análisis de su transformación organizacional de cara a los nuevos desafíos de la institución.

BID (Banco Interamericano de Desarrollo) y OEA (Organización de los Estados Americanos). 2020. Reporte ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. Washington, D.C.: BID. Disponible en: https://publications.iadb.org/

publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el- Caribe.pdf.

CCDCOE. (s.f.). *Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN*. Obtenido de https://ccdcoe.org/about-us/

CICTE. (s.f.). *Comité Interamericano contra el terrorismo*. Obtenido de https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

CISA. (s.f.). *Cybersecurity & infraestructure security agency*. Obtenido de https://www.cisa.gov/infrastructure-security

Comando Conjunto Cibernético. (s.f.). Obtenido de https://ccoci.mil.co/noticias/2/14

Consejo Nacional de Política Económica y Social. (2011). CONPES 3701 de 2011 – *Lineamientos de política para la Ciber-seguridad y Ciber-defensa*. Bogotá D.C.

Consejo Nacional de Política Económica y Social. (2016). CONPES 3854 de 2016 – *Política Nacional de Seguridad Digital*. Bogotá D.C.

Correa, J. A., Paez, L. O., & Castiblicanco, N. P. (2017). Desarrollo de un Juego Formativo para Aportar a la Concienciación en Ciberseguridad al Personal de la Escuela Militar de Aviación (Emavi)"Marco Fidel Suárez" de la Fuerza Aérea Colombiana en la ciudad de Cali. *Ciencia y Poder Aéreo*, 12(1), 264-275.

Cotino Hueso, L., & Sánchez Acevedo, M (2021). *Guía de ciberseguridad para ciudades inteligentes.*

DBAEC. (2020). *MANUAL DE DOCTRINA BÁSICA AÉREA, ESPACIAL Y CIBERESPACIAL FAC-0-B PÚBLICO*. 5ª Edición (2020)

DNP. (14 de julio de 2011). CONPES 3701. Obtenido de Departamento Nacional de Planeación: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

DNP. (11 de abril de 2016). CONPES 3854. Obtenido de Departamento Nacional de Planeación: https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y

Espitia Cubillos, A. A., Agudelo Calderón, J. A., & Buitrago Suescún, Ó. Y. (2020). Innovaciones tecnológicas en las fuerzas militares de los países del mundo: una revisión preliminar. *Revista Científica General José María Córdova*, 18(29), 213-235.

Fuerza Aérea Colombiana. (29 de julio de 2016). Obtenido de: https://www.fac.mil.co/es/noticias/capacitacion-en-seguridad-cibernetica

Fuerza Aérea Colombiana. (Septiembre de 2020). *HISTORIA, ESTRUCTURA, ROLES Y DOCTRINA DE LA FUERZA AÉREA COLOMBIANA.* Obtenido de https://www.fac.mil.co/sites/default/files/linktransparencia/informacioninteres/informescomision/historia_estructura_roles_y_doctrina_de_la_fuerza_aerea_colombiana.pdf

Fuerza Aérea Colombiana. (Agosto de 2020). *LA HISTORIA TRANSVERSAL DEL CONFLICTO: TRANSFORMACIONES DE LA FUERZA AÉREA COLOMBIANA EN CONTEXTO.* Obtenido de https://www.fac.mil.co/sites/default/files/linktransparencia/informacioninteres/informescomision/la_historia_transversal_del_conflicto_transformaciones_de_la_fuerza_aerea_colombiana_en_contexto_0.pdf

Garantivá Ortiz, E. M. (2015). Retos de seguridad informática y seguridad de la información (Bachelor's thesis, Universidad Piloto de Colombia).

Global Cyber Security Capacity Centre (GCSCC). (2020). *Revisión de capacidades de ciberseguridad. Oxford: Organización de los Estados Americanos*. Obtenido de

http://www.oas.org/es/sms/cicte/docs/ESP-Revision-de-capacidades-de-Ciberseguridad.pdf

Hathaway, M. (2018). Gestión del Riesgo Cibernético Nacional. Organización de los Estados Americanos. Obtenido de https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf

Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la Investigación. 6ta edición McGRAW-HILL. Educación, México.

ISO (Organización Internacional de Normalización). 2012. ISO/IEC 27032:2012: Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad. Ginebra: ISO. Disponible en: https://www.iso.org/standard/44375.html.

KPMG S.A.S. y KPMG Advisory, Tax & Legal S.A.S. (2022). *KPMG global organization*. Obtenido de https://home.kpmg/co/es/home.html: https://home.kpmg/co/es/home/services/advisory/risk-consulting/cyber-security/modelo-de-madurez-de-ciberseguridad.html

Ley 1928 de 2018, por medio de la cual se aprueba el "Convenio sobre la ciber-delincuencia" adoptado el 23 de noviembre de 2001 en Budapest

Ley Estatutaria 1621 de 2013 "la cual expide normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones".

Linares Lizarazo, Y. (2018). ¿¿Cómo estamos en ciberseguridad nacional e internacional, su gestión de riesgos y tendencias?

Microsoft. (25 de marzo de 2022). *News Center Microsoft Latinoamérica*. Obtenido de https://news.microsoft.com/es-xl/para-cerrar-la-brecha-de-habilidades-en-ciberseguridad-microsoft-expande-sus-esfuerzos-a-veintitres-nuevos-mercados-incluida-colombia-2/

Mindefensa. (2018). *Guía Metodológica de Planeamiento por Capacidades-CAPÂCITAS-*. Obtenido de http://capacitas.mindefensa.gov.co/storage/biblioteca/Tomo%202%20-%20Proceso%202.pdf

MINTIC (Ministerio de Tecnologías de la Información y las Comunicaciones). 2021. Modelo de Seguridad y Privacidad de la Información, v. 4.0. Bogotá: MINTIC. Disponible en: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/.

Mundial, F. E. (2022). Reporte de ICG. Recuperado de http://reports. weforum. org/global-competitiveness-index-2017-2018.

NIST (Instituto Nacional de Estándares y Tecnología). 2008. Guide for Mapping Types of Information and Information Systems to Security Categories. Special Publication 800-60 Volume I, Revision 1. Gaithersburg, MD: NIST. Disponible en: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152106.

OEA. (28 de junio de 2021). *Organización de Estados Americanos*. Obtenido de Comunicado de prensa: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-067/21

Rea-Guaman, Á. M., Sánchez-García, I. D., San Feliu Gilabert, T., & Calvo-Manzano Villalón, J. A. (2017). *Modelos de Madurez en Ciberseguridad: una revisión sistemática*.

Realpe, M. E., & Cano, J. (2020). *Amenazas Cibernéticas a la Seguridad y Defensa Nacional*. Reflexiones y perspectivas en Colombia.

República de Colombia. (1991). *Constitución política de Colombia*. Bogotá, Colombia: Leyer, 1.

Rossi Lévano, G. (2021). La Seguridad y Defensa en la era de la Cuarta Revolución Industrial: Elementos para una propuesta de estrategia de política exterior para el fortalecimiento de las capacidades del Perú en materia de ciberdefensa y amenazas híbridas.

Saldarriaga-Arenas, A. F., Jiménez-Navia, B., Villa-Enciso, E. M., Bermúdez-Hernández, J., Castellanos-Domínguez, Ó. F., & Jiménez-Hernández, C. N. (2019). La gestión de la tecnología y la innovación en Fuerzas Navales: un análisis comparativo entre Estados Unidos, España, Colombia.

Trama, G. A. (2017). *Operaciones Cibernéticas: su naturaleza, propósito y conducción*, Argentina, Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Valoyes Mosquera, A. (2019). Ciberseguridad En Colombia.

UNCCT. (s.f.). *Oficina de lucha contra el terrorismo*. Obtenido de https://www.un.org/counterterrorism/es/cct/programme-projects/cybersecurity

UNESCO. (8 de septiembre de 2020). Obtenido de https://es.unesco.org/news/nuevos-desafios-alfabetizacion

US Army; TRADOC Pamphlet 525-7-8; Cyberspace Operations Concept Capability Plan 2016-2028; 22 February 2010; Disponible en: https://fas.org/irp/doddir/army/pam525-7-8.pdf"

Uzal, Roberto – Conferencia en la EST / AFCEA – C.A.B.A. – 27 de junio de 2013 Defensa Cibernética: Panorama global, singularidades del marco regional y propuestas de lineamientos en el ámbito nacional.