Revista da UNIFA
revistaeletronica.fab.mil.br
https://doi.org/10.22480/revunifa.2023.36.549
Artigo de revisão
e-ISSN 2175-2567

Perfil profesional en ciberseguridad y ciberdefensa: un ejercicio exploratorio de conceptualización

Paula Alejandra Prieto Ararat 0000-0001-7864-3813
Programa de Maestría en Ciencias Militares Aeronáuticas, Escuela de Posgrados de la Fuerza Aérea Colombiana, EPFAC , Bogotá D.C., Colombia

Zully Ximena Rojas Ortiz 0000-0003-1267-9922
Programa de Maestría en Ciencias Militares Aeronáuticas, Escuela de Posgrados de la Fuerza Aérea Colombiana, EPFAC , Bogotá D.C., Colombia

Fabio Andrés Cruz Hernández 0009-0004-2644-5558
Programa de Maestría en Ciencias Militares Aeronáuticas, Escuela de Posgrados de la Fuerza Aérea Colombiana, EPFAC , Bogotá D.C., Colombia

Aida Hurtado Pantoja 0009-0004-3600-0923
Programa de Maestría en Ciencias Militares Aeronáuticas, Escuela de Posgrados de la Fuerza Aérea Colombiana, EPFAC , Bogotá D.C., Colombia

RESUMEN

En el presente documento, se desarrolla un ejercicio de exploración en literatura académica donde se abordan las temáticas relacionadas con la ciberseguridad y la ciberdefensa, particularmente se han tratado de identificar las principales características o posturas de varios autores en relación con los diferentes perfiles profesionales que puedan asociarse a este campo. No se han caracterizado únicamente funciones, disciplinas o conocimientos asociados al escenario militar, dando una perspectiva académicamente objetiva se han revisado propuestas multidisciplinarias. Para esto se han consultado documentos en bases de datos, de diferentes países donde se ha logrado establecer que el perfil profesional de ciberseguridad y ciberdefensa se relaciona con campos de las ciencias humanas y sociales de las ingenierías, de las ciencias de seguridad y de otros campos de la técnica y la técnica superior.

Palabras clave: *ciberseguridad; ciberdefensa; especialistas; tecnologías de la información.*

Professional profile in cybersecurity and cyberdefense: an exploratory exercise of its conceptualization

ABSTRACT

In this document, an exploration exercise in academic literature is developed where the issues related to cybersecurity and cyberdefense are addressed, particularly an attempt has been made to identify the main characteristics or positions of different authors in relation to the different professional profiles

that may join this field. Not only functions, disciplines or knowledge associated with the military scene have been characterized, giving an academically objective perspective, multidisciplinary proposals have been reviewed. For this, documents in different databases and from different countries have been consulted where it has been established that the professional profile of cybersecurity and cyberdefense is related to fields of the human and social sciences of engineering, security sciences and other fields of technique and superior technique.

Keywords: *cybersecurity; cyberdefens; specialists; information technologies-*

Perfil profissional em cibersegurança e ciberdefesa: um exercício exploratório de sua conceituação

RESUMO

Neste documento, apresenta-se um exercício de exploração da literatura académica onde são abordadas questões relacionadas com a cibersegurança e a ciberdefesa, justamente procurando identificar as principais características ou posições de diferentes autores em relação aos diferentes perfis profissionais que possam se relacionar como esse campo. Não só foram caracterizadas funções, disciplinas ou saberes associados ao cenário militar, propondo uma perspectiva acadêmica objetiva, se não também foram revisadas propostas multidisciplinares. Para isto, foram revisados documentos em diferentes bases de dados e de diferentes países onde foi possível estabelecer que o perfil profissional de cibersegurança e ciberdefesa está relacionado aos campos das ciências humanas e sociais, da engenharia, ciências da segurança e ciências da segurança, tanto níveis técnicos quanto os níveis técnicos superiores.

Palavras-chave: *cibersegurança; ciberdefesa; especialistas; tecnologias da informação.*

1 INTRODUCCIÓN

El ciberespacio ha tenido una evolución constante, con una proyección exitosa pero, a la vez, con un alcance indefinido que categoriza y enmarca su importancia, así como su desarrollo, llegando a ser hoy en día un factor determinante para la economía, la política, la comunicación y otro tipo de funciones sociales; se insiste que hace parte de un escenario en el que la era industrial parece superarse paulatinamente dando cabida a otro tipo de paradigmas tecnológicos y metodológicos (CUJABANTE et al., 2020).

Entre estos, la posibilidad de gobernanza sobre la internet se ha convertido en una preocupación que involucra cuestiones de infraestructura, técnica, y procesos de regulación normativa, siendo esto, impulso de tensiones y conflictos que pueden derivar en violaciones a los sistemas cibernéticos e informáticos (CRUZ, 2017), llegando al punto que en el año 2020, año conocido por el fuerte impacto mundial de la pandemia, se tuvieron ataques informáticos confirmados por la Agencia de Seguridad Nacional de los Estados unidos buscando datos secretos de las vacunas contra el COVID-19.

En el marco de estas consideraciones resulta deseable y siempre urgente que las interacciones y procesos que allí suceden puedan darse y funcionar con absoluta seguridad, razón por la cual cada vez la sociedad en general ha visto más necesario pensar en ciberseguridad y ciberdefensa. Se trata de una situación de defensa que, aunque involucra directamente a los cuerpos de seguridad nacionales, resulta útil para que distintas organizaciones a lo largo del mundo puedan asegurar su información e infraestructura tecnológica. Por lo mismo, la formación en ciberseguridad y en ciberdefensa se ha dado desde diferentes frentes y campos del conocimiento, siendo esto una oportunidad para que el perfil profesional asociado a estos campos sea diverso y pueda demandarse en diferentes sectores, todo ello con el fin de atender a las necesidades que se suscitan.

Es así como con este escrito se pretende caracterizar el perfil profesional en ciberseguridad y ciberdefensa partiendo de la revisión de documentos académicos en los últimos cinco años, primero a través de la indagación de las necesidades de contexto en las que se define el perfil profesional en ciberseguridad y ciberdefensa y segundo, explorando el concepto de perfil profesional en ciberseguridad y ciberdefensa en estos últimos cinco años, para identificar las dinámicas que sigue.

2 DESARROLLO

La exploración de literatura académica sobre perfiles profesionales en ciberseguridad y ciberdefensa se realiza a partir de la consulta de repositorios y bases de datos como Scielo, Dialnet, Redalyc, Crossref Metada, entre otros. Allí se rastrean documentos con una anterioridad no mayor a cinco años de realización. Además de la temporalidad, otro criterio de búsqueda ha sido que los documentos incluyan de manera particular en sus discusiones temas asociados al perfil profesional en ciberseguridad y ciberdefensa. Las palabras utilizadas para la búsqueda fueron: profesionales en ciberdefensa y ciberseguridad, especialistas en ciberdefensa y ciberseguridad, seguridad en el ciberespacio, trabajadores de la ciberseguridad, entre otros. Además, el grupo de literatura consultada cuenta con investigaciones realizadas en diferentes países de Europa y América, debido a que no se tiene ningún criterio de espacialidad que condicione la búsqueda.

Para el análisis se lleva a cabo un ejercicio de definición de categorías las cuales se organizan para posteriormente estructurar el presente documento. Tales categorías de análisis fueron: Contexto, para identificar el escenario en el que tiene lugar el problema abordado; perfil profesional, para determinar los tipos de profesiones, campos, disciplinas o áreas técnicas que deben tenerse en cuenta; y habilidades o funciones, buscando describir un poco más las posibilidades o responsabilidades de los distintos perfiles profesionales que lograron identificarse.

En total se revisaron treinta (30) documentos académicos, de los cuales: once (11) corresponden a la categoría de contexto, cuatro (4) puntualmente abordan perfil profesional y cuatro (4) que abordan las habilidades o funciones. Los once (11) restantes abordan de manera transversal las categorías de perfil profesional y habilidades y funciones. Por lo tanto, la categorización final se realiza de la siguiente manera: once (11) documentos correspondientes

a la categoría de contexto, siete (7) documentos referentes al perfil profesional en tecnologías de la información, seis (6) documentos donde se aborda el perfil profesional en ciber resiliencia y nueve (9) documentos sobre perfil profesional en el campo militar.

Lo anterior teniendo en cuenta que hay dos (2) documentos en los que se analizaron dos categorías, por tratarlas de manera importante para este análisis.

3 RESULTADOS

3.1 Situación actual de necesidades en ciberseguridad y ciberdefensa: breve prospectiva del profesional en ciberdefensa y ciberseguridad

El problema de seguridad informática presenta diferentes matices y preocupaciones relacionadas, por supuesto, con la situación cada vez más creciente de procesos vinculados al ciberespacio. Entre las principales destacan, naturalmente, las amenazas cibernéticas. Sobre esta situación las investigaciones de Basallo (2018) y Cano (2020) han presentado algunas consideraciones que dan luz sobre el contexto en el que el perfil profesional en ciberdefensa y ciberseguridad debe ajustarse a situaciones como dar respuesta a la sofisticación de técnicas para cometer ciberdelitos, siendo este uno de los problemas o situaciones de vulnerabilidad que más preocupan en la sociedad global. Delitos como la suplantación de identidad o los usos no autorizados de certificados bancarios son cada vez más latentes.

Por otro lado, según indican las investigaciones (CANO, 2020; CANO; ROCHA, 2019), el desarrollo de la tecnología y de la informática y la prevalencia de los delitos cibernéticos pueden conducir a la generación de lo que se ha denominado como *riesgos líquidos* (CANO, 2020). En este caso se ha proyectado que para el 2030 podrán ser de otra naturaleza los problemas de seguridad informática y su comprensión exigirá, entonces, propuestas y perfiles profesionales capaces de adaptarse a los cambios que esto supone. Como indica Cano (2020) el profesional en ciberseguridad tendrá que encontrar su motivación de aprendizaje y su inspiración en el atacante, tratando de abarcar todos los eventuales riesgos que puedan surgir durante la próxima década.

Otra de las situaciones actuales en la cual se inscriben las reflexiones sobre ciberseguridad y ciberdefensa es la escasez ampliamente reconocida de profesionales en este campo (BASALLO, 2018; DE HARO; VARELA, 2021; FURNELL, 2021; JACOB et al., 2018). A pesar de que, como se verá más adelante, existen definiciones claras sobre el tipo de habilidades y el perfil profesional que pueden encargarse de estas labores, la falta de talento se convierte en un elemento que limita la masificación de procesos efectivos en ciberseguridad y ciberdefensa. Existe un amplio conocimiento sobre la demanda de profesionales de este tipo, pues los ataques a la seguridad informática son cada vez más sofisticados y ponen de facto una necesidad de personal capacitado, pero la oferta es considerablemente reducida según indican algunos estudios (BASALLO, 2018; FURNELL, 2021).

Adicional a ello, existe una dificultad que tiene que ver con el proceso formativo de profesionales en ciberseguridad y ciberdefensa que requiere de una cierta cantidad de tiempo para adquirir la experiencia que, según indica Basallo (2018), puede ser hasta de ocho años. Sin embargo, este proceso de formación es fundamental para lograr suplir las necesidades del mercado de profesionales en áreas que aportan a la seguridad y defensa en el ciberespacio (DE HARO; VARELA, 2021).

A nivel mundial tiene relevancia tanto la ciberseguridad como el sistema de protección legislativo y normativo aplicable, que permita proteger el ciber espacio de la ciberdelincuencia civil, geopolítica y militar. Como tangible de este compromiso se puede resaltar a nivel europeo la capacidad requerida, para detectar la manera pronta así como mitigar las amenazas cibernéticas las cuales tienen una relación directa con las legislaciones regionales que protegen los derechos y libertades fundamentales de los ciudadanos de la Unión Europea (BEKERMAN, 2021), es así como en países de desarrollo como Estados Unidos y China se tienen fortalecidas las políticas en relevancia directa a su posible impacto de riesgo. Según Patiño (2021) el sector de la ciberseguridad simboliza una pieza fundamental en el marco de las relaciones competitivas de carácter gubernamental lo que permite que estas naciones cuenten con el ministerio de seguridad publica en China y el Departamento de Justicia en Estados Unidos de América trabajando en pro de políticas y normativas que sean afines a la ciberseguridad.

Otro elemento problémico asociado a la situación actual de los perfiles profesionales, y que menciona Gallardo (2020) en su investigación, tiene que ver con la carencia de destrezas y conocimientos gerenciales para que los asuntos de seguridad sean mucho más integrales en las diferentes organizaciones que puedan requerir de estas actividades. Esto tiene que ver, según la autora, con una especialización en conocimientos informáticos en los que los profesionales se estancan en una suerte de zona de confort y no actualizan o diversifican sus conocimientos. Sin embargo, otros investigadores sugieren que el perfil profesional en ciberseguridad y ciberdefensa no está estrictamente definido, reconociendo esto a partir de la idea de que la seguridad cibernética no es un elemento estandarizado (PEDLEY et al., 2018), lo que determina una situación en la que el perfil profesional asociado no tiene una definición única y exclusiva como se verá a continuación en la siguiente sección de los resultados.

La ciberseguridad ha evolucionado desde ser una problemática exclusiva de los ingenieros de sistemas o informáticos, para ser una discusión pública y en el caso de américa latina y el caribe se generan indicadores algunos como la publicación de National Cyber Security Index, elaborado por la marca reconocida en ciberseguridad e-Governance Academy Foundation de Estonia, la cual, marca un punto tangencial del nivel de preparación de los países para evitar amenazas a la ciberseguridad y la gestión de incidentes cibernéticos, en América Latina y el Caribe son incluidos once países, de los cuales, lideran el ranking Panamá, Colombia y Chile, y se identifican dos ejes temáticos que han recibido nula o escasa atención por parte de los Estados, como lo son: la protección de servicios esenciales donde se incluye la infraestructura crítica y las ciberoperaciones militares, según (ÁLVAREZ, 2018) puntos donde pese a ser referentes regionales existen vacíos críticos en ciberseguridad que pueden afectar la seguridad nacional.

Según Vergara y Trama (2018), en el análisis general de las medidas adoptadas por algunos países en cuanto a aportes militares a la ciberdefensa, aportes que son conocidos en concepto general sin llegar a la minucia, por la sensibilidad y confidencialidad de la información al ser de seguridad nacional para cada país, se reconocen algunos riesgos conocidos desde el punto militar donde se evidencia puntos de quiebre al respecto:

> "las bombas son guiadas por satélites GPS; los drones son piloteados remotamente desde cualquier parte del mundo; los aviones de combate y buques de guerra son grandes centros de procesamiento de datos; e incluso el soldado de a pie está interconectado". (VERGARA; TRAMA, 2018, p. 123).

Así, el continuo crecimiento del uso de las redes crea un ambiente más vulnerable para ataques cibernéticos y el nivel de dependencia de los sistemas aumenta el impacto posible, y aún más complejo que dependiendo del nivel ciber y tecnología disponible puede llegarse a ataques donde no es posible conocer la identidad del atacante.

Por otra parte, se puede resaltar de países como Francia que desde el 2011 creó el cargo de oficial general del ciber defensa como encargado de coordinar las acciones del ámbito, siendo un ejemplo para muchos países que hoy en día 10 años después no toman acciones concretas que reflejen la preocupación y gestión referente, de igual manera Países Bajos definió en el 2012 seis prioridades: la adopción de un enfoque integral; el fortalecimiento de las capacidades de la ciberdefensa; el desarrollo de capacidades militares cibernéticas ofensivas; el fortalecimiento de capacidades de inteligencia en el ciberespacio; el fomento, la innovación y la contratación de personal calificado; y la intensificación de la cooperación a nivel nacional e internacional. Por otra parte, un comando de ciberdefensa conjunto, creado en septiembre de 2014, dentro del ejército holandés, es el responsable del desarrollo de las capacidades cibernéticas. En España, en julio de 2012 se aprobó el "Concepto de Ciberdefensa Militar", que definió principios, objetivos y retos de la ciberdefensa en el ámbito militar; en este documento, se define la terminología, se realiza una valoración de la capacidad, se presentan las funciones y responsabilidades en esta área, y se ordena la elaboración de un Plan de Acción de Ciberdefensa Militar. Un año después se anunció el "Plan de Acción para la Obtención de la Capacidad de Ciberdefensa Militar" (PACDM), con el cual, comenzó la coordinación de los esfuerzos entre el ámbito conjunto y los específicos a partir del aprovechamiento de las estructuras existentes.

3.2 Perfil profesional en ciberdefensa y ciberseguridad: aportes desde la academia

En términos generales, se ha identificado que el perfil profesional en ciberseguridad y ciberdefensa no varía necesariamente según el país en el que se haya realizado cada estudio; esto se relaciona naturalmente con que la seguridad informática, por su característica de globalidad, puede verse vulnerada por el mismo tipo de delincuente cibernético. Posiblemente cambia el tipo de legislación y las formas normativas en que se inscriben los procesos generales, pero no necesariamente hay un perfil específico para cada país. En cambio, la especificidad del perfil profesional puede derivar de la amplia gama de áreas que hoy son asumidas como potenciales centros de formación de defensa en ciberseguridad y ciberdefensa o según el sector que demande este tipo de personal con habilidades en seguridad informática.

La primera referencia que se indica en los textos académicos sobre el perfil profesional en ciberdefensa y ciberseguridad se relaciona con los años de experiencia (GIRALDO; CABRERA, 2020), siendo este un factor importante. En la sección anterior se había enunciado ya este elemento como uno de los condicionantes para poder ejercer el tipo de labores que esta función necesita; ahora bien, Giraldo y Cabrera (2020) establecen que la experiencia debe estar relacionada directamente con el campo de la seguridad. Adicionalmente, estos autores plantean que para cumplir con estas funciones es importante establecer una serie de cargos escalados según el tiempo de experiencia, ubicando así a los profesionales con mayor claridad en temas de seguridad cibernética en roles que promuevan cada vez más la especialización en

este campo. No obstante, su visión centrada en los profesionales del campo de la seguridad puede ser muy limitada, pues, como se verá, otros estudios amplían la gama de conocimientos y perfiles que pueden aplicar a roles de ciberdefensa y ciberseguridad.

Furnell (2021), por ejemplo, aunque reconoce la importancia de los perfiles provenientes de áreas asociadas a la seguridad, especialmente a la seguridad en red y otras relacionadas como la ciencia forense, amplía un poco la perspectiva de origen de este tipo de profesionales. El autor, por supuesto, reconoce que la base disciplinaria corresponde con las áreas de conocimiento en tecnología de la información y sistemas de información, al igual que como lo reconocen de Haro y Varela (2021), quienes añaden el área de las comunicaciones; pero no se quedan allí. Estos últimos agregan que el conocimiento en ingeniería y el conocimiento en arquitectura puede ser referente de profesionales que se desempeñen en el campo de la seguridad cibernética. En otros casos, incluso, se habla de este profesional como aquel que posee habilidades interdisciplinarias que, además de integrar aquellas asociadas a la seguridad, involucran conocimientos de las ciencias sociales y humanas (BOHÓRQUEZ, 2019; FURNELL, 2021; JACOB et al., 2018).

Del campo de conocimiento de las ciencias humanas y sociales se integran las psicología, el derecho, la ciencia política y la administración o gestión de organizaciones (FURNELL, 2021; JACOB et al., 2018). Estas, como plantea Bohórquez (2019), hacen parte del abanico de conocimientos en ciberdefensa y ciberseguridad, en tanto este es un campo que no se limita de manera exclusiva al desarrollo y uso de habilidades técnicas o conocimientos de ingeniería. Por el mismo alcance y origen que pueden tener los delitos cibernéticos, ramas como la sociología, el derecho y la ciencia política pueden llegar a advertir de sus amenazas o, dado el caso, actuar como mecanismos de reacción. En general, son campos de conocimiento que permiten cubrir situaciones previas o posteriores que la mera técnica y la ingeniería pueden pasar por alto. También, se hace énfasis en la pertinencia de las ciencias administrativas, como negocios y gestión organizacional, que pueden aportar en conocimientos relacionados con la planificación en prevención de riesgos y los procesos de toma de decisiones (FURNELL, 2021).

Establecida esta amplitud de áreas que pueden aportar en la generación de conocimientos y destrezas para la ciberdefensa y la ciberseguridad, a continuación, se detalla con mayor énfasis cuáles son los perfiles profesionales que derivan de estos campos del conocimiento y de otros que aparecen implícitamente en las diferentes investigaciones y documentos académicos consultados.

3.3 Perfil profesional en ciberseguridad y ciberdefensa

Como lo indican de Haro y Varela (2021) el perfil profesional en ciberdefensa y ciberseguridad se encuentra relacionado con todos los niveles formativos y de especialización, incluyendo aquellos que son de formación técnica, técnica superior, universitaria y posgradual. En cada caso, se puede identificar de un nivel o una dimensión distinta de cualificación y de desarrollo de habilidades y conocimientos requeridos para este tipo de funciones.

Oltra e Ibáñez (2019) reconocen que es precisamente producto del devenir de la sociedad del conocimiento y de la información y del desarrollo de las TIC que la formación profesional en los diferentes niveles y áreas del conocimiento se han podido vincular a los procesos de seguridad informática y cibernética. En otrora, plantean estos autores, sería

un conocimiento, en el cual, el nivel técnico podría ser aquel que generaría los aportes necesarios, pero en la actualidad los profesionales de diferentes áreas tienen, casi que por obligación o por necesidad, que involucrarse con estos conocimientos, por lo cual, como se hizo énfasis en párrafos anteriores, el perfil profesional que se requiere puede ser buscado en las disciplinas ya enunciadas, siendo los profesionales responsables de diferentes formas de gestionar la ciberseguridad y la ciberdefensa.

Ahora bien, a pesar de que se habla de la variedad de disciplinas y de áreas del conocimiento involucradas potencialmente en la ciberseguridad, resulta natural que, de entrada, el perfil profesional imperante es aquel relacionado con las tecnologías de la información. Una gran variedad de autores consultados genera esta asociación por razones que pueden resultar más que obvias (ARMSTRONG et al., 2018; CANO; ROCHA, 2019; DE HARO; VARELA, 2021; FONSECA & ANSORENA, 2017; FURNELL, 2021; GIRALDO; CABRERA, 2020). En el nivel técnico superior se sitúan perfiles profesionales de administración de sistemas informáticos en red, en desarrollo de aplicaciones multiplataforma, en desarrollo de aplicaciones web, en sistemas de telecomunicaciones e informáticos y en mantenimiento electrónico (DE HARO; VARELA, 2021).

En este punto también se integra la administración con el área de ingeniería de sistemas, de ingeniería eléctrica y de las otras ingenierías que puedan resultar afines (GIRALDO; CABRERA, 2020). Además, están los profesionales que hacen parte del campo de las tecnologías de la información, pero que se perfilan desde el campo de la seguridad en sistemas TI, gerentes que se desempeñan en seguridad de la información, y otro tipo de profesionales que desde el campo de la gestión organizacional pueden diseñar, implementar o hacer seguimiento a los procesos de seguridad, tales como los auditores con experiencia en administración (FURNELL, 2021).

También se hace referencia en los dominios de las áreas profesionales o técnicas relacionadas con las tecnologías de la información al *hacker ético* (ARMSTRONG et al., 2018); este tiene un perfil profesional que deriva de la ingeniería de seguridad de la información. El denominado hacker ético se contempla por las oportunidades que pueda generar en materia de probador y analista de penetración de los sistemas informáticos y cibernéticos, de analista de vulnerabilidades y por sus funciones técnicas en los equipos de riesgo. En paralelo, puede situarse la figura propuesta por Cano y Rocha (2019) de arquitecto de software, un perfil profesional enfocado en brindar apoyo en seguridad para el diseño de software. En este caso, los autores hacen referencia al sistema *Knowledge & Experience - Security Recommendation* (KESER), sistema que se fundamenta en los conocimientos de los arquitectos de software quienes se encargan de tomar todas las decisiones relativas a la seguridad de los programas durante su diseño.

Otro perfil que resalta en este campo por su particularidad conceptual es el del *profesional de la ciberresiliencia* (MAILLOUX; GRIMALIA, 2018; SLAYTON, 2021); en este caso se trata de aquella persona que tiene la responsabilidad de proponer distintas soluciones de seguridad que aporten en la garantía del funcionamiento de los diferentes sistemas ciberfísicos. Es decir, el término *profesional de la ciberresilencia* hace referencia a especialistas en seguridad de infraestructura y demás puntos físicos críticos que puedan estar ante una amenaza de daños. Slayton (2021) de manera particular relaciona este perfil profesional con la Red

de información del Departamento de Defensa (DODIN' por sus siglas en inglés), que es aquel personal que tiene por obligación cumplir las funciones de seguridad, sostenibilidad y mantenimiento de la infraestructura tecnológica.

No sobra mencionar que también existen campos de formación posgradual en magister y doctorados orientados de manera directa a la ciberseguridad y a la ciberdefensa (FONSECA; ANSORENA, 2017). Estos están dirigidos a una gama amplia de profesionales de las tecnologías de la información como son los ingenieros de sistemas, ingenieros en mecatrónica, ingenieros en electrónica, ingenieros en telecomunicaciones e ingenieros industriales; por otro lado, se reciben también perfiles profesionales relacionados con algunos de los especialistas ya mencionados de las ciencias administrativas, gestión logística, de sectores de seguridad como la policía, y ciencias militares, navales aeronáuticas y demás del sector seguridad.

En el caso de otras áreas del conocimiento, particularmente asociadas a las ciencias sociales y humanas, algunas investigaciones permiten identificar elementos característicos de los perfiles profesionales que se relacionan con estos campos (GALLARDO, 2020; GIRALDO; CABRERA, 2020; PÉREZ; RAMOS, 2020). Empezando por profesionales del área administrativa, pero que no figuran en el campo de las tecnologías de la información se hace referencia a los supervisores de los procesos de las empresas; este es un perfil profesional denominado como SICO por Gallardo (2020). Por su parte, Giraldo y Cabrera (2020) ubican en el campo de la ciberdefensa y a ciberseguridad a los sociólogos, los psicólogos, los políticos y los abogados.

Los primeros como analistas de riesgos sociales, políticos y humanos que puedan derivar en ataques a los sistemas de información y a los sistemas cibernéticos, es decir, una suerte de analistas del contexto; mientras que los abogados se relacionan con funciones de seguridad de la información, protección de datos personales, acceso a la información y demás conocimientos que, desde el ámbito jurídico, garanticen estas funciones (PÉREZ; RAMOS, 2020).

Por último, se encuentran los perfiles profesionales asociados al campo militar; en este caso se trata de rangos que van desde los más bajos hasta los más altos y que por sus capacidades, conocimientos y un proceso de capacitación pueden cumplir funciones de ciberseguridad y ciberdefensa. En primer lugar, Heatherly y Melendez (2019) ubican a los oficiales, los suboficiales, los sodados enlistados y los contratistas civiles como perfiles que pueden involucrarse en la defensa cibernética. Incluso proponen la opción de que rangos más altos como los coroneles desarrollen habilidades y conocimientos para suplir necesidades supremas en este campo. Por otro lado, Baezner (2020) reconoce en los reservistas un escenario para adherir al campo de la seguridad militar lo que Laverde y Hernández (2020) denominan *ciberguerreros*. Su propuesta es una vinculación de tipo voluntaria que, por supuesto, implica un proceso formativo; se trata, entonces, de civiles que quieran adoptar un estatus militar, pero que también cuente con un perfil profesional de los que se han mencionada hasta este punto.

Conforme a la postura de Clarke (2011) quien afirmó que cada una de las instituciones encargada de la seguridad en los Estados Unidos; Marina y Fuerza Aérea, creó e implementó su departamento enfocado a la ciberguerra, esto posterior a la creación del Cibermando en los Estados Unidos. Considerando que había personal partidario de crear un mando unificado para esta tarea, el mando espacial se unió con el Mando Estratégico y pasó a ser responsable de centralizar los

recursos para la ciberguerra. Sin embargo, se presentarían rencillas internas puesto que la Fuerza Aérea quería ostentar el dominio de cualquier actividad que tuviera que ver con la defensa del ciberespacio estadounidense. Se definió entonces que todos los servicios harían parte del mando central, incluyendo a la CIA, la NSA y otros organismos de inteligencia norteamericanos, de esta manera evidenciamos como el perfil en Estados Unidos tuvo un comportamiento similar al que se espera en Colombia dejando la responsabilidad del ciberespacio a la FAC.

Si se toma como referente el campo militar de la ciberseguridad y la ciberdefensa, las funciones de los profesionales perfilados pueden orientarse al diseño y desarrollo de ciberarmas y programas de tipo ofensivo (LAVERDE; HERNÁNDEZ, 2020) o, como se ha hecho énfasis, a la defensa de los sistemas cibernéticos y al mantenimiento y sostenibilidad de la tecnología, es decir, a la infraestructura (BARARA, 2019). En el campo de la gestión de organizaciones, bien sea estas industriales, financieras o de otras ramas de la economía, debe pensarse también en la protección de bases de datos, de portales web y, en general, en la implementación de esquemas de protección contra intrusos (ARDILA, 2018).

Por otro lado, está el caso de los servicios informáticos en el cual los perfiles profesionales deben ofrecer soluciones en el desarrollo de software, en la administración de bases de datos y en el asesoramiento legal cibernético (HERNÁNDEZ; LÓPEZ, 2017; NEWHOUSE et al., 2020). Finalmente, es importante pensar también en el cumplimiento de otras funciones que involucran la inteligencia social y el pensamiento sistémico para garantizar análisis de amenazas mucho más factibles y sensibilizar en los diferentes componentes de la ciberseguridad y la ciberdefensa (DAWSON; THOMSON, 2018; HANEY; LUTTERS, 29d. C.)

4 CONCLUSIONES

El acelerado crecimiento de actividades vinculadas al ciberespacio ha alertado de manera considerable la seguridad informática, donde las amenazas cibernéticas se hacen cada vez más frecuentes con un grado de nocividad importante, materializando así los ciberdelitos, motivo por el cual, dar respuestas asertivas a esta problemática requiere de personal que ostenten un perfil profesional para la ciberseguridad y ciberdefensa, en el que se destaque además de la parte cognoscitiva, la experiencia, de tal forma, que les permitan adaptarse tanto a los cambios constantes como a los riesgos que se generan en este campo.

Así, el Perfil Profesional en Ciberseguridad y Ciberdefensa no se limita a áreas relacionadas con la tecnología e informática, sino también a diversas disciplinas que abarcan hasta la psicología, sociología, el derecho entre otras, por lo cual se dice que es multidisciplinario, esto, atendiendo a las múltiples necesidades que de allí se derivan no sólo de tipo tecnológico sino inclusive ético. Por ello, las áreas de conocimiento están llamadas a aportar desde su propia disciplina, de hecho, los estudios posgraduales en ciberdefensa y ciberseguridad están siguiendo esta dinámica, pues, están dirigidos a personal de diferentes profesiones, con el fin, de abarcar el mayor campo del conocimiento, enmarcados en la multidisciplinariedad del perfil.

Lo anterior, teniendo en cuenta que hoy en día los ciberataques o ciberguerras se han intensificado, y no se cuenta con suficientes profesionales en esta área, por eso se hace necesaria la capacitación en temas ciber para poder estar a la vanguardia de los avances tecnológicos a los que nos lleva el mundo en continua evolución, donde, las Fuerza Militares, deben tomar el protagonismo, pues, la ciberseguridad y Ciberdefensa de los Estados hace parte de la misión no sólo institucional, sino que trasciendo a l constitucional.

Es así como, la experiencia es un criterio relevante, al momento de hablar de perfil profesional para la ciberseguridad y la ciberdefensa, partiendo que la ciberseguridad ha avanzado significativamente, pasando de ser una problemática exclusiva de los ingenieros de sistemas o informáticos, para ser una discusión pública, y todo, lo que se ha aprendido a lo largo del tiempo en el área, pasa a tener un protagonismo importante para la solución de los nuevos problemas.

Informações sobre os autores:

Paula Alejandra Prieto Ararat
https://orcid.org/0000-0001-7864-3813
paula.prieto@epfac.edu.co
Politóloga de la Pontificia Universidad Javeriana de Bogotá (PUJ). Magister en Relaciones Internacionales de la Universidad de Essex (UK). Actualmente se desempeña como Profesional de apoyo a la gestión de investigación del programa de Maestría en Ciencias Militares Aeronáuticas de la Escuela de Postgrados de la Fuerza Aérea Colombiana. Ha participado en proyectos de análisis del sector defensa y ha realizado algunas publicaciones en temas de política exterior y asuntos de seguridad y defensa nacional; es miembro de la Red Latinoamericana de Seguridad Ambiental de la Fundación Konrad-Adenauer (KAS).

Zully Ximena Rojas Ortiz
https://orcid.org/0000-0003-1267-9922
zully.rojas@epfac.edu.co
Abogada egresada de la Universidad La Gran Colombia , Magister en Biociencias y Derecho de la Universidad Nacional de Colombia. Candidata a Doctora en Derecho de la Universidad Nacional de Colombia. Experiencia en investigación en las áreas de: Bioética, biomateriales, materiales, Derechos Humanos, colectivos y ambientales.
Perteneciente al Grupo De Investigación Derechos Colectivos y Ambientales (GIDCA) adscrito a Colciencias de la Universidad Nacional de Colombia y al Grupo en Ciencias Militares Aeronáuticas (GICMA) de la Escuela Marco Fidel Suarez – FAC. En lo últimos dos se ha desempeñado como docente del área de investigación de la Maestría en Ciencias Militares Aeronáuticas y como directora metodológica de Trabajo de Grado de los estudiantes de este programa. Participación con Poster en Congresos Nacionales e Internacionales, publicación de artículos en revistas nacionales e internacionales.

Fabio Andrés Cruz Hernández
https://orcid.org/0009-0004-2644-5558
fabio.cruz@emavi.edu.co
Oficial del cuerpo de vuelo, Ingeniero informático egresado de la Escuela Militar de Aviación, ha participado en algunos cursos como, instructor académico y de vuelo en la Escuela Militar de Aviación, actualmente es piloto instructor primario y básico en el equipo T-90 Calima. Ha volado en los equipos T-41, T-37, Turbocomander, Cheyenne, ATR, C-208B y T-90 acumulando más de 3.600 horas en misiones de transporte, inteligencia e instrucción de vuelo. Se ha desempeñado como: jefe de acción integral coordinada, jefe de itinerarios de Satena, comandante de la escuadrilla reconocimiento y vigilancia en CACOM-3, jefe de personal del grupo cadetes, comandante de escuadrón alfa en el grupo cadetes.

Aida Hurtado Pantoja
https://orcid.org/0009-0004-3600-0923
aida.hurtado@epfac.edu.co
Oficial del cuerpo administrativo del curso 31. Licenciada en Inglés y Francés de la Universidad de Nariño. Es Jefe de sección planeación CELEF. Se ha desempeñado en la Fuerza Aérea como: secretaria Académica en la Escuela de Suboficiales, comandante de Escuadrón y jefe del Área de Idiomas. En EMAVI fue jefe del área educativa del Programa de Ciencias Militares Aeronáuticas, jefe de sección Idiomas y Profesional Militar.

Cooperación:

La autora Paula Alejandra Prieto Ararat contribuyo con el diseño metodológico, organización de fuentes, análisis de resultados y redacción. La autora Zully Ximena Rojas contribuyo con el desarrollo de la metodología, análisis de fuentes, redacción y corrección de estilo. Los autores Capitán Cruz Hernández Fabio Andrés y Capitán Hurtado Pantoja Aida contribuyeron en el análisis y redacción de resultados. Todos los autores aprobaron el manuscrito final para publicación.

Como citar este artigo:

ABNT

ARARAT, Paula Alejandra Prieto; ORTIZ, Zully Ximena Rojas; HERNÁNDEZ, Fabio Andrés Cruz; PANTOJA, Aida Hurtado. Perfil profesional en ciberseguridad y cyberdefensa: un ejercicio exploratorio de conceptualización. **Revista da UNIFA**, Rio de Janeiro, v. 36, p. 1-15, 2023.

APA

Ararat, P. A. P., Ortiz, Z. X. R., Hernández, F. A. C. & Pantoja, A. H. (2023). Perfil profesional en ciberseguridad y cyberdefensa: un ejercicio exploratorio de conceptualización. **Revista da UNIFA**, 36, 1-15.

REFERENCIAS

ÁLVAREZ, D. Ciberseguridad en América Latina y ciberdefensa en Chile. **Revista chilena de derecho y tecnología**, v. 7, n.1, p. 1-2. 2018. DOI: https://dx.doi.org/10.5354/0719-2584.2018.50416

ARDILA, C. **La estrategia de ciberseguridad y ciberdefensa en Colombia:** una política pública en constante construcción. En Convergencia de conceptos: enfoques sinérgicos en relación a las amenazas a la seguridad del Estado colombiano. Escuela Superior de Guerra, 2018.

ARMSTRONG, M.; JONES, K.; NAMIM, A.; NEWTON, D. The Knowledge, Skills, and Abilities Used by Penetration Testers: Results of Interviews with Cybersecurity Professionals in Vulnerability Assessment and Management. In: Proceedings of the Human Factors and Ergonomics Society, p.709–713, 2018, Texas. **Proceedings** [...].

BAEZNER, M. **Study on the Use of Reserve Forces in Military Cybersecurity.** ETH zürich. 2020.

BARARA, I. Capacity Building for Fighting Cyber Wars. **Cyber Nomics**, v. 1, n. 1, p. 8–12, 2019.

BASALLO, A. Existen más puestos de trabajo en el sector de ciberseguridad que profesionales formados. **UNIR**, 2018. Disponible en: https://www.unir.net/ingenieria/revista/el-sector-de-la-ciberseguridad-necesita-trabaja dores-pero-no-encuentra-profesionales-bien-formados. Accedido em: Mayo 17, 2021.

BEKERMAN, U. Un acercamiento al enfoque trilateral de la nueva Estrategia de Ciberseguridad de la UE: An Approach to the Trilateral Focus of the New EU Cybersecurity Strategy. **Diario Suplemento Derecho y Tecnología**, n. 75 March 1, 2021.

BOHÓRQUEZ, A. **El impacto de la academia en la ciberseguridad. En La seguridad en el ciberespacio. Un desafío para Colombia.** Escuela Superior de Guerra. 2019.

CANO, J. Retos de seguridad/ciberseguridad en el 2030. **Revista Sistemas**, n.154, p. 68–79, 2020.

CANO, J.; ROCHA, Á. Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital. **Revista Ibérica de Sistemas e Tecnlogías de Informação**, n. 32, p. 7-9, 2019.

CRUZ, L. La política brasileña de ciberseguridad como estrategia de liderazgo regional. **Revista Latinoamericana de Estudios de Seguridad**, n. 20, p. 16–30, 2017.

CUJABANTE, X.; BAHAMÓN, M.; PRIETO, J.; QUIROGA, J. Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relacionas cívico-militares. **Revista Científica General José María Córdova**, v.18, n. 30, p. 357–377, 2020.

DAWSON, J; THOMSON, R. The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. **Frontiers in Psychology**, 2018.

DE HARO, F.; VARELA, Á. Curso de Especialización en Ciberseguridad, ¿están preparados nuestros docentes? Jorandas Nacionales de Investigación en Ciberseguridad. 6. 2021, España. **Proceedings** [...]. España, deposito de investigacion universidad de sevilla, 2021.

FONSECA, C.; ANSORENA, M. **La defensa cibernética. Alcances estratégicos, proyecciones doctrinarias y educativas.** Universidad de la Defensa Nacional. 2017.

FURNELL, S. The cybersecurity workforce and skills. **Computer & Security**, n.100, 2021.

GALLARDO, S. Diez años más tarde. Retos y amenazas a la seguridad y ciberseguridad en 2030. **Revista Sistemas**, n.155, p. 61-80, 2020.

GIRALDO, H.; CABRERA, F. **Estrategia Nacional de Ciberdefensa y Ciberseguridad.** Opciones Gráficas Editores Ltda, 2020.

HANEY, J; LUTTERS, W. Cybersecurity Advocates: Discovering the Characteristics and Skills of an Emergent Role. **Information and Computer Security,** v. 29, n. 3 (29d. C.).

HEATHERLY, C; MELENDEZ, I. Every soldier a cyber warrior: the case for cyber education in the United States Army. **The Cyber Defense Review**, v. 4, n.1, p. 63–74. 2019.

HERNÁNDEZ, G; LÓPEZ, A. Perfil y competencias del analista de información en el ámbito de la seguridad pública. **BID: textos universitarios de biblioteconomia i documentació**, n. 38, 2017.

JACOB, J; WEI, W; SHA, K., DAVARI, S; YANG, A. Is The NICE Cybersecurity Workforce Framework (NCWF) Effective For A Workforce Comprised Of Interdisciplinary Majors? Int'l Conf. **Scientific Computing**, 2018.

LAVERDE, R; HERNÁNDEZ, M. Ciberseguridad y Ciberdefensa en Colombia. **Revista Avenir**, v. 4, n.2, p. 25–36, 2020.

MAILLOUX, L.; GRIMALIA, M. Advancing Cybersecurity: The Growing Need for a Cyber-Resiliency Workforce. **IT Professional**, v. 20, n.3, p. 23–30, 2018.

NEWHOUSE, W.; KEITH, S.; SCRIBNER, B.; WITTE, G. National Initiative for Cybersecurity Education (NICE). **Cybersecurity Workforce Framework**. National Institute of Standars and Technology, v. 100, 2020.

OLTRA, J; IBÁÑEZ, R. Ciberseguridad y bibliotecas: apuntes para una propuesta de formación sobre riesgo tecnológico en bibliotecas. **Métodos de Información**, v.10, n.19, p. 75–126, 2019.

PATIÑO, G. A. Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos (Chinese and American Cyber Security Models: A Comparative). **OASIS**, n. 34, May 13, 2021.

PEDLEY, D.; MCHENRY, D.; MOTHA, H.; SHAH, J.;BUTTON, M.; WANG, V. **Understanding the UK cyber security skills labour market Research report for the Department for Digital, Culture, Media and Sport**. En Social Researcha Institute. 2018.

PÉREZ, W; RAMOS, M. Propuesta política de ciberseguridad para las fuerzas armadas. **DSpace Repository**, 2020.

VERGARA, E; TRAMA, G. **Operaciones militares cibernéticas: Planeamiento y Ejecución en el Nivel Operacional**. Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, 2018.

SLAYTON, R. What Is a Cyber Warrior? The Emergence of US Military Cyber Expertise, 1967–2018. **Texas National Security Review**, v. 4, n.1, 2021.

Recebido: 28 Out 2022

Aceito: 13 Jan 2023