Revista **Ciberespacio, Tecnología e Innovación**
Volumen 1, número 1, enero-junio 2022 (pp. 107-109)
Bogotá, D.C, Colombia

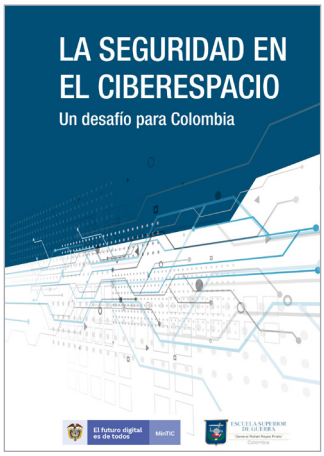
EDITORIAL **ESDEG**

Reseña de libro. La seguridad en el ciberespacio: Un desafío para Colombia

Book review. Security in cyberspace: A challenge for Colombia

DOI: https://doi.org/10.25062/2955-0270.4780

Henry Andrés Buchheim Duarte
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia



Editores del libro: **Jairo Andrés Becerra, Marco Emilio Sánchez Acevedo, Carlos Castañeda M., Alejandro Bohórquez Keeney, Rafael Vicente Páez Méndez, Arístides Baldomero Contreras, Ivonne Patricia León**
Editorial: Editorial Planeta Colombiana S.A.
Año: 2020
ISBN impreso: 978-958-42-8892-9
Páginas: 222

El propósito del libro es concientizar al lector acerca de la importancia que reviste para las organizaciones desde el ámbito académico, militar, empresarial y público, el uso adecuado del ciberespacio y la responsabilidad que tiene el Estado de preservar sus intereses y proteger la infraestructura de los nuevos riesgos que se vislumbran en el campo de la ciberseguridad y la ciberdefensa.

El libro, en una introducción hace acápite a la seguridad en el ciberespacio como un desafío para Colombia, expresa en los cinco (5) capítulos siguientes, donde se abarcan temas relacionados con la resiliencia, la investigación como eje fundamental de una política de seguridad digital en Colombia; así mismo, exponen la relevancia de la gestión de riesgos en el entorno de la Fuerza Pública y en el Sector Privado.

Entre los temas tratados, se plantea la dependencia de los flujos seguros de información para el correcto funcionamiento de las organizaciones empresariales y la operación del gobierno. De igual forma, la importancia que reviste la información y como los ataques cibernéticos se perciben como una amenaza de seguridad nacional e internacional, haciendo que los Estados manifiesten la necesidad de proteger sus redes de información, en especial las de seguridad nacional y las infraestructuras críticas.

Es así, como las sociedades están experimentando una transformación digital, basada en un mundo más interconectado, con nuevas tecnologías y, por consiguiente, nuevos riesgos que requieren la evolución de la política pública colombiana y mecanismos de cooperación en materia de delitos cibernéticos entre países. El autor define conceptos básicos como resiliencia, ciberseguridad, gestión de riesgos y como se relacionan entre ellos.

El primer capítulo hace un ejercicio académico enfocado a describir de forma detallada y clara el contexto del CONPES 3854 de 2016 entendido como una política base de seguridad digital colombiana, de esta manera disgregan las cinco dimensiones estratégicas sobre las que se adopta el enfoque de seguridad digital. Así mismo, se hace una adecuada conceptualización mediante diferentes referentes bibliográficos acerca de conceptos relevantes como ciberespacio, ciberdefensa, seguridad digital, ciberdefensa. De igual forma, el autor introduce los conceptos de las diferentes organizaciones que tienen responsabilidad de gestionar la seguridad y defensa a nivel cibernético en el país.

El segundo capítulo presenta una conceptualización general, buscando evidenciar las diferentes problemáticas que enfrenta la sociedad en el marco de la cuarta revolución industrial y como las nuevas tecnologías han generado una transformación en las actividades diarias y disminución en el tiempo para hacer las cosas, que se traduce en la reducción de costos y respuestas ágiles que generan transparencia y acceso oportuno a la información. Dentro de esta modernización aparece como eje fundamental el internet, siendo el actor principal en la globalización, ya que es el articulador en las comunicaciones e interacción digital entre personas y objetos.

Según indica el autor, la globalización y las nuevas tecnologías han hecho que los Estados se vean limitados por nuevas instituciones o actores no estatales, cuyo carácter dinámico no logra ser regulado por marcos judiciales nacionales. Por último, se describe y diferencian los conceptos de *Hacktivista, Hacker* y *Cracker,* lo cual se hace una contextualización de cómo gestionar los riesgos a nivel global y nacional con base a las nuevas amenazas, producto del carácter dinámico de las tecnologías y su acelerado ritmo de cambio.

El tercer capítulo definen los alcances académicos frente a la seguridad digital, de igual forma se realiza una interesante revisión bibliográfica, incluyendo dentro de estas,

las principales políticas públicas en materia de ciberseguridad de los actores regionales y de Estados Unidos, Israel, Estonia y Corea del Sur, lo anterior con el propósito de revisar cómo se ha llevado a cabo la ejecución de las políticas públicas en seguridad digital y la importancia de la academia en este entorno. De forma general, se abre un abanico de posibilidades para que desde la academia se genere conciencia y regulación en torno al ciberespacio. Finalmente, se ejecuta un paneo respecto al papel del sector académico en cuanto a la proyección a futuro en el área de ciberseguridad y las amenazas que se vislumbran.

El cuarto capítulo se observa cómo el autor hizo una exhaustiva comprobación de la estrategia de gestión de riesgos en seguridad digital de países europeos, así como de Estados Unidos y Canadá, con el fin de dar a conocer de una forma sucinta los avances en el tema. De igual manera, indica cómo Colombia ha avanzado para hacer frente a las amenazas latentes en el ciberespacio, generando como conclusión la importancia de involucrar a todos los actores a nivel gobierno para implementar políticas y procedimientos en la gestión de riesgos en materia de seguridad digital.

El quinto capítulo se enfoca en dar a conocer estadísticamente cómo los riesgos para la ciberseguridad han aumentado en prevalencia y potencial desestabilizador en las grandes empresas del sector público y privado. En esta investigación, el autor hace una recopilación hasta el año 2018 de las acciones adelantadas por los países latinoamericanos en relación con la implementación de políticas de seguridad digital, haciendo la claridad que se requieren mayores esfuerzos en ciberseguridad, esto en relación con que cada cuatro de cinco países carecen de estrategia de ciberseguridad.

En conclusión, el libro es una ayuda para conocer la importancia por parte de cada uno de los sectores sobre medir y mitigar los riesgos digitales, así como la necesidad de una mayor integración entre la ciberseguridad y modelos de desarrollo de resiliencia, partiendo de la premisa de que ningún sistema es cien por ciento seguro y para esto es necesario comprender la amplia gama de vectores de amenazas cibernéticas, generar conciencia y sensibilización en todos los niveles bajo el liderazgo del sector académico, que permita generar conocimiento en torno al tema.

Autor de la reseña

Henry Andrés Buchheim Duarte. Capitán de Corbeta de la Armada Nacional de Colombia. Especialista en Política y Estrategia Marítima, Escuela Naval del Cadetes "Almirante Padilla", Colombia. Ingeniero Electrónico, Escuela Naval del Cadetes "Almirante Padilla", Colombia.

ORCID: https://orcid.org/0009-0005-9784-9039

Contacto: henry.buchheim@armada.mil.co