EDITORIAL ESDEG

Revista
Ciberespacio, Tecnología e Innovación
Volumen 2, número 4, julio-diciembre 2023
Bogotá, D.C, Colombia
ISSN: 2955-0270 • eISSN: 3028-3310
Página web: https://esdegrevistas.edu.co/index.php/rcit

Reseña del libro. Ciberseguridad, una estrategia informático/militar

Book review. Cybersecurity, a computer/military strategy

Viviana Pilar Fuquen Flautero

CITACIÓN APA:

Fuquen Flautero, V. P. (2023). Reseña de libro. Ciberseguridad, una estrategia informático/militar. *Ciberespacio, Tecnología e Innovación, 2*(4), 209-212. https://doi.org/10.25062/2955-0270.4818

Publicado en línea: **Diciembre 30 de 2023**

Enviar un artículo a la Revista

Revista **Ciberespacio, Tecnología e Innovación**
Volumen 2, número 4, julio-diciembre 2023 (pp. 209-212)
Bogotá, D.C, Colombia

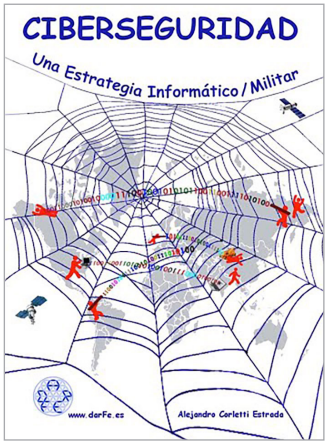
EDITORIAL **ESDEG**

Reseña del libro. Ciberseguridad, una estrategia informático/militar

Book review. Cybersecurity, a computer/military strategy

DOI: https://doi.org/10.25062/2955-0270.4818

Viviana Pilar Fuquen Flautero
Corporación Universitaria del Meta, Villavicencio, Colombia



Autor del libro: **Alejandro Corletti Estrada**
Editorial: DarFe Learning Consulting S.L
Año: 2017
Páginas: 245
ISBN: 978-84-697-7205-8

El libro *Ciberseguridad, una estrategia informática/militar,* es una reflexión sobre la importancia de la ciberseguridad mediante la recopilación de información y experiencias. Este trabajo se compone de 10 capítulos.

Primer capítulo, es una aproximación conceptual y de contexto sobre la ciberseguridad, en este apartado se explica las definiciones que se comprenden por ciberseguridad y ciberdefensa, reconociendo que estos dos campos resultan ser importantes para la defensa del Estado en un ambiente cibernético. La importancia es identificar que existen nuevas ciberamenazas vigentes que han explotado las ventajas tecnológicas, lo que les ha permitido abrir su accionar criminal en el ciberespacio, por ello es relevante

defenderse ante ciberataques organizados y generados desde estructuras que pueden llegar a ser mafiosas. En esta medida, se propone adoptar la resiliencia entendida como una capacidad de proceder y proteger, como parte de la estrategia para la defensa de las redes y sistemas.

Segundo capítulo, se escribe la importancia de las estrategias de seguridad en las redes, afirmando la necesidad, desde el punto de vista militar, de planear cursos de acción que permitan la relación-beneficio. En este capítulo se reconoce la existencia de emplear una buena metodología y soporte especializado con recursos tecnológicos suficientes, acompañado también de analistas para reconocer el pensamiento de las amenazas. Lo importante de este ejercicio en planeación estratégica es generar operaciones ofensivas y defensivas y desarrollar una doctrina concentrada en el desarrollo de capacidades operacionales y estratégicas en los diferentes niveles (estratégico, táctico, y operacional).

Tercero capítulo, para el autor es fundamental desarrollar una estrategia a defensa en profundidad y en altura. En este apartado y bajo esta afirmación, se establece que deben existir un orden, una misión y un desarrollo secuencial y planeado para dar cumplimiento a un objetivo final. Desde una perspectiva militar, y aplicando conceptos como la maniobra, la defensa en profundidad y deposición, la identificación de zonas claves, se establece un análisis comparado sobre lo que se debe comprender en el ciberespacio, estableciendo, por ejemplo, los espacios físicos, la gestión y servicio de las redes de comunicación.

Cuarto capítulo, en este apartado el autor aborda la importancia de los procesos en la ciberseguridad. Se establece un análisis descriptivo sobre la comprensión de los procesos tales como la de producción, gestión de cambios, gestión de accesos, configuraciones e inventario, gestión del backup, gestión de incidencias, supervisión y monitorización, gestión de logs. Bajo este análisis se establece la necesidad del registro de una auditoría que identifique las facilidades y prioridades en las plataformas, reconociendo que bajo el concepto de sistema todos tus aspectos resultan ser interdependientes y lo que permitiría a largo plazo reducir los incidentes informáticos.

Quinto capítulo, un aspecto esencial es comprender que existe un espacio virtual y uno digital, y frente al escenario físico y tangible, existen plataformas e infraestructuras de seguridad en la red, deben gestionarse, supervisarse y defenderse. Para el autor es importante establecer una secuencia, detección, prevención y mitigación.

Sexto capítulo, profundizando el análisis, establece que en el escenario mundial las redes resultan ser un eje principal para la comprensión de la ciberseguridad. En este apartado se analiza la forma en que está configurada la interconexión a nivel mundial y destacando la existencia de redes "tubos" (fibras ópticas, cables de cobre y enlaces

de radio) lo cual le permite el funcionamiento de la internet y demás actividades a nivel mundial.

Séptimo capítulo, en un aspecto técnico, se analiza el empleo de NOC (Network Operation Center) y SOC (Security Operation Center), lo cual le permite generar disponibilidad y alertas tempranas para fortalecer la ciberdefensa. La NOC, se encuentra centrada en el control de la red y se caracteriza por la convergencia de la supervisión, monitorización y alarmas de la red en infraestructuras. Lo característico de este procedimiento es que establece y prioriza las infraestructuras como a plataformas, dispositivos, redes y sistemas que serán monitorizados. La SOC se concentra en el capital humano y recursos disponibles, manteniendo como característica la monitorización, detección, análisis, prevención y seguimiento de eventos de seguridad en las redes. Según el autor, los dos diferentes enfoques a nivel estratégico generan una serie de servicios que dependiendo de la actividad desarrollada pueden generar un costo de beneficio mayor.

Octavo capítulo, en este apartado se establece la relevancia del registro de auditoría (LOGS). Mediante un análisis conceptual se establece que los registros son una serie de huellas que se pueden detectar en los diferentes procesos de los sistemas de información, lo característico de este ejercicio es reconocer dichos registros con el objetivo de categorizarlos y priorizarlos. Estos registros hacen parte del concepto de resiliencia que se caracteriza por el resguardo y la recuperación ante ciberincidentes, adicionalmente se trata de un cuidado que es estar sincronizado.

Noveno capítulo, establece y abordó un concepto militar, los juegos de guerra, esta vez relacionados con la ciberguerra. Para este apartado se establece que existir una metodología de evaluación como auditoría y acción que mejore la respuesta ante incidentes, por lo cual los juegos de guerra tienen una serie de características como las de capacitar al personal, comprobar los planes y preparar al personal para el desarrollo de capacidades. En esta medida, el autor propone que los juegos de guerra deben considerar una serie de elementos para que sean desarrollados en el ciberespacio y entre los cuales debe existir como aspecto fundamental el desarrollo de una doctrina, es decir, una normativa que regule los temas de seguridad, redes e incidentes en la organización

Décimo capítulo, finalmente en este apartado se aborda una recopilación de nuevos conceptos, metodologías y desafíos. Para el autor es importante considerar que, en dicha transformación a nivel mundial generada por el ciberespacio, las instituciones deben centrarse en tres conceptos cruciales como las redes, nodos y zonas, señalando que estos conceptos son los que se abordarán a largo plazo y de manera transversal por las diferentes dinámicas sociales en las diferentes instituciones. Adicionalmente, es relevante señalar que existen desafíos que cada vez van a ser más complejos si no se desarrollan protocolos de seguridad en la red, por lo cual la resiliencia será un concepto importante en la defensa desde el ciberespacio.

Autora

Viviana Pilar Fuquen Flautero. Ingeniera Industrial, Corporación Universitaria del Meta, Colombia. Especialista en Administración en Seguridad y Salud en el Trabajo, Corporación Universitaria del Meta, Colombia. Técnica en Asistencia, Análisis y Producción de Información Administrativa con énfasis Contable del CENACAP, Colombia. Técnica profesional en Planificación para la Creación y Gestión de Empresas, Servicio Nacional de Aprendizaje, Colombia.

Orcid: https://orcid.org/0000-0002-0714-7895

Contacto: viviana.fuquen@academia.unimeta.edu.co

Referencia

Corletti, A. (2017). *Ciberseguridad, una estrategia informático/militar.* DarFe Learning Consulting S.L.