

Seguridad y defensa cibernética en Venezuela: riesgos científicos y tecnológicos

Douglas Enrique Torres Dugarte
Centro de Investigación y Postgrado UNEFA
Centro de Investigaciones Postdoctorales CIPOST - UCV
torres.douglas@gmail.com, dtorres@unefa.edu.ve

La presente investigación estudia la situación problema derivada de la utilización extensa e intensa de Tecnologías de Información y Comunicación (TIC) y su impacto en la seguridad de la información en Venezuela. Ataques e incidentes cibernéticos sobre organizaciones y ciudadanos son frecuentes y peligrosos, y pueden orientarse hacia instalaciones de infraestructura crítica de la nación. La situación problema se sustenta teóricamente desde el paradigma sistémico, y la realidad se estudia, como si fuese un sistema. Teorías de: sistemas, información; cibernética; redes; derecho penal; seguridad, defensa son algunos de los soportes teóricos. La Metodología de los Sistemas Suaves (MSS) para el abordaje de situaciones problema se empleó para el tránsito entre la realidad observada y el mundo de sistemas, donde emerge un Modelo Estratégico de Seguridad y Defensa Cibernética (MESDCI), propuesto como un componente de la estrategia de seguridad, defensa y desarrollo integral. El modelo conceptual prevé cinco subsistemas y 36 actividades mínimas. El sistema de actividades humanas propuesto, prevé la interacción con el ambiente donde se inserta y con el cual interactúa promoviendo el ámbito cibernético como nueva dimensión en el entorno operativo de la República Bolivariana de Venezuela. La investigación considera que la seguridad y defensa cibernética es un asunto de la sociedad y del Estado, por tanto es seguridad de la Nación.

Palabras clave: Cibernética, Modelo estratégico, Seguridad, Defensa, Desarrollo integral, Sistemas suaves.