REVISTA INCLUSIONES
REVISTA DE HUMANIDADES Y CIENCIAS SOCIALES M.R.

ISSN 0719-4706
Volumen 12 Número 3
Julio - Septiembre 2025
Páginas 1-20
https://doi.org/10.58210/ri3639

Inteligencia Artificial y Ciberseguridad: Transformación Digital de la Seguridad Nacional en el Siglo XXI
/
Artificial Intelligence and Cybersecurity: Digital Transformation of National Security in the 21st Century

Eduardo Herrera Guzmán
Colegio de defensa nacional, México
eduardohg1970@gmail.com
https://orcid.org/0009-0007-1226-3253

Fecha de Recepción: 19 de marzo de 2025
Fecha de Aceptación: 14 de junio de 2025
Fecha de Publicación: 15 de septiembre de 2025

Financiamiento:
Se financió con recursos propios.

Conflictos de interés:
Los autores declaran no presentar conflicto de interés.

Correspondencia:
Nombres y Apellidos: Eduardo Herrera Guzmán
Correo electrónico: eduardohg1970@gmail.com
Dirección postal: Calz México-Tacuba 305, Santo Tomás, Miguel Hidalgo, 11400 Ciudad de México, CDMX, México

Resumen: El presente estudio analiza la transformación digital de la Seguridad Nacional mediante la integración de inteligencia artificial y sistemas de ciberseguridad avanzados. La investigación examina cómo las tecnologías emergentes redefinen los paradigmas tradicionales de seguridad nacional, centrándose en la implementación de sistemas autónomos de defensa y la evolución de amenazas cibernéticas.
La metodología incluye análisis prospectivo de escenarios futuros, evaluación del marco regulatorio internacional, y examen de las capacidades tecnológicas del Estado mexicano. Se identifican oportunidades estratégicas para el fortalecimiento de la infraestructura de ciberdefensa nacional y la adopción de tecnologías de vanguardia en el ámbito de la seguridad.

Palabras clave: Inteligencia Artificial; Ciberseguridad Nacional; Transformación Digital; Sistemas Autónomos; Ciberdefensa; Amenazas Cibernéticas.

Abstract: *This study analyzes the digital transformation of National Security through the integration of artificial intelligence and advanced cybersecurity systems. The research examines how emerging technologies redefine traditional national security paradigms, focusing on the implementation of autonomous defense systems and the evolution of cyber threats.*

The methodology includes prospective analysis of future scenarios, evaluation of the international regulatory framework, and examination of the technological capabilities of the Mexican State. Strategic opportunities are identified for strengthening national cyberdefense infrastructure and adopting cutting-edge technologies in the security domain.

Keywords: *Artificial Intelligence; National Cybersecurity; Digital Transformation; Autonomous Systems; Cyberdefense; Cyber Threats*

Introducción

En el estudio de la Seguridad Nacional el impacto del campo tecnológico reviste una importancia vital que trasciende las fronteras coloquiales y se extiende a todas las esferas de la vida nacional. Actualmente, la tecnología no solo es una herramienta, sino un componente fundamental del poder nacional de un Estado. Por ello las potencias que acceden a tecnologías avanzadas y que poseen la capacidad de desarrollarlas e innovar vertiginosamente, son más propensas al desarrollo tecnológico, incrementar su poder y potencial como nación en un escenario global cada vez más competitivo y complejo.

El objetivo central del presente capítulo es proporcionar información al lector para comprender diversos conceptos generales de la cultura de Seguridad Nacional, y la forma en que se ha visto impactada mediante la tecnología, además se hace un

breve análisis prospectivo del uso de los Sistemas de Armas Autónomos (SAAS), planteando posibles escenarios.

1 La tecnología en la Seguridad Nacional

Inicialmente, es necesario precisar que los elementos de un Estado son población, territorio y gobierno, con un sistema jurídico y un poder soberano que encausa los esfuerzos para alcanzar un bien común. Este organismo vivo entendido como Estado, se ve constantemente expuesto a una serie de antagonismos que pueden impedir la consecución de sus aspiraciones, intereses y objetivos nacionales.[1] Por tal motivo, el Estado debe emplear el poder nacional para asegurar la protección de su integridad territorial, independencia, soberanía, estado de derecho, así como su estabilidad política, económica y social.[2] Estas condiciones son necesarias para garantizar la seguridad y el desarrollo nacionales.

Aunado a lo anterior y con la finalidad de dar coherencia y sentido al estudio es necesario considerar que el poder nacional se puede definir como “el conjunto de factores materiales y espirituales que otorga a la nación la capacidad de expresar su voluntad por conseguir y mantener los objetivos nacionales, aún en situaciones adversas”,[3] de tal manera que la integración de los diferentes componentes de este poder, doctrinariamente se denominan campos del poder, que de conformidad con el Glosario de Términos Unificados de Seguridad Nacional son: el político, económico, social, militar, tecnológico y diplomático.[4]

La coordinación efectiva de los campos del poder permite que un Estado movilice sus recursos para alcanzar y preservar sus intereses y objetivos nacionales. En el contexto político, una estrategia bien articulada puede fomentar la estabilidad y la gobernabilidad, mientras que, en el ámbito económico, la colaboración entre sectores puede impulsar el crecimiento nacional y la competitividad internacional. Socialmente, la integración de políticas puede mejorar la cohesión y el bienestar de la población. Militarmente, la coordinación asegura la Seguridad y la Defensa Nacionales, y en el campo tecnológico, promueve la innovación y el desarrollo sostenible. Diplomáticamente, la cooperación y la coherencia en las relaciones internacionales refuerzan la posición y la influencia de un país en el escenario mundial.

---

[1] Raúl Ramírez Medrano, “El Sistema de Seguridad Nacional y los objetivos nacionales permanentes tutelados por la Constitución Política Mexicana”, Los Servicios de Inteligencia en el nuevo siglo, (México, Revista de Administración Pública No 101, Instituto Nacional de Administración Pública, 2000): 175-203., 177. http://historico.juridicas.unam.mx/publica/librev/rev/rap/cont/101/pr/pr17.pdf

[2] SEDENA, SEMAR (Secretaría de la Defensa Nacional, Secretaría de Marina). Glosario de términos unificados de Seguridad Nacional. (Ciudad de México: Colegio de Defensa Nacional, Centro de Estudios Superiores Navales, 2018).

[3] Vizarretea, Emilio. *Repensar México una introducción a la Seguridad y Defensa Nacionales*. (Ciudad de México: Secretaría de Marina, Armada de México, 2020).

[4] SEDENA, SEMAR. Glosario de Términos Unificados, p. 4.

Para SEDENA-SEMAR (2018), el Glosario de Términos Unificados en Seguridad Nacional, expresa que la Seguridad Nacional: "[…] es una condición necesaria que proporciona el Estado para garantizar la prevalencia de su integridad territorial, independencia, soberanía, estado de derecho, su estabilidad política, social y económica y la consecución de sus Objetivos Nacionales".[5]

De manera particular y para profundizar en el tema, el campo tecnológico se define como un "componente del poder nacional integrado por la capacidad científica y desarrollo tecnológico, que impulsa de manera importante el desarrollo nacional del país, para coadyuvar al logro y mantenimiento de los objetivos nacionales",[6] además, en el campo tecnológico es conveniente considerar la capacidad de innovación.

En este sentido, el término de ciencia se refiere al conjunto de conocimientos sistemáticos y comprobables que estudian y explican los fenómenos sociales, artificiales y naturales. El conocimiento científico se obtiene de manera metodológica mediante la investigación, observación y experimentación en campos de estudio específicos. Por lo tanto, la ciencia es un proceso riguroso que busca comprender las leyes y principios que rigen la realidad, con el objeto de mejorar la vida humana y estimular el desarrollo en diversos aspectos.[7]

Asimismo, para Paula Roldán, la tecnología es el conjunto de conocimientos y técnicas que se aplican de manera ordenada para alcanzar un determinado objetivo o resolver un problema.[8] La tecnología es una respuesta al deseo del hombre de transformar el medio y mejorar su calidad de vida. Incluye conocimientos y técnicas desarrolladas a lo largo del tiempo que se utilizan de manera organizada con el fin de satisfacer alguna necesidad.

Es preciso señalar que como innovación tecnológica se entiende al cambio de índole técnico o científico que se introduce al bien o servicio, así como a los procesos que se desarrollan dentro de una empresa u organización. Esto con el fin de alcanzar mayor competitividad. Las innovaciones tecnológicas que se implementan en una empresa u organización provienen de la investigación y el desarrollo. Este término hace referencia a la inversión en conocimientos científicos y tecnológicos para conseguir nuevos productos, materiales o procesos.[9]

Por lo que se refiere al marco normativo internacional el campo tecnológico del Estado mexicano se guía de manera voluntaria por el Manual de Oslo, que fue

---

[5] SEDENA, SEMAR. Glosario de Términos Unificados, p. 23.
[6] SEDENA, SEMAR. Glosario de Términos Unificados, p. 5.
[7] Peiró, Rosario. "¿Qué es la ciencia?" Economipedia. https://economipedia.com/definiciones/ciencia.html (consultado el 21 de mayo de 2024).
[8] Roldán, Paula. "Tecnología: Qué es, usos y ejemplos". Economipedia. https://economipedia.com/definiciones/tecnologia.html (Consultado el 25 de enero de 2024).
[9] Westreicher, Guillermo. Innovación tecnológica. Economipedia. https://economipedia.com/definiciones/innovacion-tecnologica.html (Consultado el 1 de mayo de 2020).

elaborado por la Organización para la Cooperación y Desarrollo Económico (OCDE) y la Oficina Europea de Estadística (EUROSTAT), y representa el marco metodológico de referencia internacional para medir la innovación. El Manual define cuatro tipos de innovaciones: 1) producto; 2) proceso; 3) mercadotecnia; y 4) organización. Se aplica tanto a la industria como a los servicios, incluyendo los servicios públicos.[10]

En el mismo sentido, el manual de Bogotá, elaborado por la Organización de Estados Americanos (OEA) y la Red Iberoamericana de Indicadores de Ciencia y Tecnología (RICYT) auxilia a la elección de indicadores. Es un marco conceptual que permite conocer la estructura y las características del proceso de innovación y sus implicaciones en el diseño de políticas. Fue inspirado en el manual de Oslo y propone pautas para la normalización de indicadores de innovación tecnológica en América Latina y el Caribe.[11]

Asimismo, el manual de Frascati, establecido por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), es una guía reconocida en el plano internacional para la recopilación y presentación de estadísticas sobre investigación y desarrollo experimental. Proporciona un marco estandarizado que permite la comparación de datos de investigación y desarrollo a nivel internacional, facilitando así el análisis y la comprensión del impacto y la distribución de los esfuerzos entre países y dentro de distintos sectores.[12]

Richard Clarke, en su obra, *Guerra cibernética; la próxima amenaza para la Seguridad Nacional y qué hacer al respecto*, describe la forma en que la tecnología sustancialmente juega un papel determinante en la economía de un país. La capacidad de innovar y adaptarse a los avances tecnológicos puede impulsar el crecimiento económico, aumentar la productividad y mejorar la competitividad en el orden internacional.[13]

Aunado a lo anterior, la capacidad tecnológica se considera un factor primordial para la Seguridad Nacional, la cual significa protección a los valores básicos de una sociedad y ausencia de temor al riesgo de que estos valores sean atacados, en esta lógica el ciberespacio ha impuesto un replanteamiento del concepto de seguridad, que se relaciona con el grado en que el Estado puede volverse inmune a la amenaza de ataque a las instalaciones de infraestructura vital.[14] De ahí que las Fuerzas Armadas necesiten de instrumentos sofisticados para cumplir con la misión de

[10] OECD / Eurostat. Oslo Manual 2018: Guidelines for collecting, reporting and using data on innovation 4th edition. The Measurement of Scientific, Technological and Innovation Activities. (Paris: OECD publishing / Luxembourg: Eurostat, 2018).
[11] OEA. Manual de Bogotá: Normalización de Indicadores de Innovación Tecnológica en América Latina y el Caribe. (Washington, D.C.: Organización de los Estados Americanos, 2001).
[12] OCDE. Manual de Frascati 2015: Guía para la recopilación y presentación de información sobre la investigación y el desarrollo experimental. (París: OCDE Publishing, 2015).
[13] Clarke, Richard. Guerra cibernética: La próxima amenaza para la seguridad nacional y qué hacer al respecto. (Nueva York: Penguin Press, 2020).
[14] Alkharman, Jamal Awwad, et al. “Cyber Attacks and its Implication to National Security: The Need for International Law Enforcement”. Pakistan Journal of Criminology 16, no. 3 (2024): 851-864. 852.

Defensa y Seguridad Nacionales, esto implica desde armas convencionales hasta sistemas de armas autónomas (SAAS) que son operados con inteligencia artificial. Por lo tanto, para Clarke, la inversión en investigación, desarrollo y adquisición de tecnología militar se ha convertido en una prioridad para muchos Estados que buscan salvaguardar su Seguridad Nacional.[15]

Con base en Goodman, se afirma que la tecnología es un habilitador clave del poder nacional en el mundo contemporáneo; su capacidad para impulsar la economía, fortalecer las fuerzas armadas y mejorar la calidad de vida de los ciudadanos, convirtiéndola en un factor fundamental en la determinación del éxito y la seguridad de un país en el escenario global.[16] Por lo tanto, entender y aprovechar el potencial de la tecnología es esencial para garantizar la Seguridad Nacional; ejemplo de lo anterior está representado por los siguientes casos:

a). La República Popular China ha liderado en las últimas décadas inversiones significativas en investigación y desarrollo tecnológico, consolidándose como un referente global en campos como la inteligencia artificial y la tecnología 5G. Lo anterior, es un claro indicador que ha fortalecido su posición como actor influyente a nivel mundial.

b). En el mismo sentido, Estados Unidos cuenta con las fuerzas armadas más poderosas del mundo, en enorme medida debido a su elevada inversión, experiencia y desarrollo, lo cual se traduce en una clara ventaja tecnológica; cuenta con acceso a tecnologías de vanguardia, por lo cual el ejército estadounidense tiene una ventaja significativa en el campo de batalla.

c). Se puede inferir que el futuro tecnológico de México dependerá en gran medida de su capacidad para abordar de manera efectiva los antagonismos identificados y cerrar las brechas existentes en áreas críticas; por lo tanto, la mejora de la situación tecnológica requerirá un enfoque holístico que incluya inversiones sostenidas en infraestructura, educación y formación especializada, así como políticas que fomenten la innovación y reduzcan la dependencia tecnológica. Además, será crucial fortalecer los marcos regulatorios para combatir la ciberdelincuencia y la delincuencia organizada, al tiempo que se promueva un entorno propicio para el desarrollo tecnológico autónomo.

El éxito en estos esfuerzos podría posicionar a México como un actor más competitivo en el escenario tecnológico global, impulsando su desarrollo económico y social a largo plazo.

En otro orden de ideas, el marco normativo nacional, sin lugar a duda, es la Constitución Política de los Estados Unidos Mexicanos (CPEUM), la que, en diversos artículos, señala aspectos relacionados con el campo tecnológico, por ejemplo, el artículo 3/o. fracción V establece que “el Estado apoyará la investigación e

[15] Clarke, Richard. Guerra cibernética: La próxima amenaza para la seguridad nacional y qué hacer al respecto.

[16] Goodman, Marc. Los delitos del futuro. Todo está conectado, todos somos vulnerables y qué podemos hacer al respecto. (Barcelona: Ariel, 2015).

innovación científica, humanística y tecnológica, y garantizará el acceso abierto a la información que derive de ella, para lo cual deberá proveer recursos y estímulos suficientes, conforme a las bases de coordinación, vinculación y participación que establezcan las leyes en la materia".[17]

Por su parte el artículo 73 Constitucional menciona que el Congreso tiene facultad para dictar leyes sobre la promoción de transferencia de tecnología y la generación, difusión y aplicación de los conocimientos científicos y tecnológicos que requiere el desarrollo nacional, así como para legislar en materia de ciencia, tecnología e innovación, estableciendo bases generales de coordinación entre la Federación, las entidades federativas, los Municipios y las demarcaciones territoriales de la Ciudad de México, además de la participación de los sectores social y privado de la economía, con el objeto de consolidar el Sistema Nacional de Ciencia, Tecnología e Innovación.[18]
Con respecto a la asignación de recursos y la legislación aplicable, para favorecer el desarrollo y la promoción de estas áreas esenciales, el Congreso de la Unión promovió la nueva Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación, publicada en el Diario Oficial de la Federación, el 8 de mayo de 2023, en la cual establece que el gobierno tiene la "obligación de fomentar, realizar y apoyar actividades de investigación humanística y científica, desarrollo tecnológico e innovación que redunden en el bienestar de la población".[19]

La inversión en ciencia, tecnología e innovación repercute en la calidad y el alcance de la educación en estas disciplinas. En este sentido, para el año 2024 se destinó el 0.6% del PIB para estas actividades lo que representa el mayor incremento en los últimos años. Asimismo, ha sido notable el interés del Estado mexicano al elevar la categoría del Consejo Nacional de Humanidades, Ciencia y Tecnología (CONAHCYT) a Secretaría de Ciencia, Humanidades, Tecnología e Innovación (SECIHTI), entrando en funciones el 1 de enero de 2025, con base en el decreto por el que se reforman, adicionan y derogan diversas disposiciones de la ley Orgánica de la Administración Pública Federal, lo cual traerá aparejado el incremento de proyectos estratégicos vinculantes a mencionadas áreas del conocimiento.[20]

Ahora bien, el índice de Innovación Global 2023, presenta las tendencias recientes en innovación a nivel mundial, donde se revela la clasificación de las economías más innovadoras de la actualidad, seleccionadas entre 132, y destaca los principales

---

[17] Cámara de Diputados del Honorable Congreso de la Unión. Constitución Política de los Estados Unidos Mexicanos (CPEUM). https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf (Consultado el 15 de mayo de 2019).
[18] Cámara de Diputados del Honorable Congreso de la Unión. Constitución Política de los Estados Unidos Mexicanos (CPEUM).
[19] Periferia. "México: La inversión en ciencia y tecnología llegará al 0,6% del PBI, en 2024". https://periferia.com.ar/latinoamerica/mexico-la-inversion-en-ciencia-y-tecnologia-llegara-al-06-del-pbi-en-2024/ (Consultado el 27 de septiembre de 2023).
[20] Guarneros, Fernando (10 de abril de 2021). La educación de ciencia y tecnología en México todavía enfrenta profundos retos. Expansión. https://expansion.mx/tecnologia/2021/04/10/la-educacion-stem-en-mexico-todavia-enfrentan-profundos-retos (Consultado el 10 de abril de 2021).

centros de innovación en ciencia y tecnología en el orbe, situando a México en el lugar 58 y a nivel Región de Latinoamérica y el Caribe en el lugar 3, con ingresos medianos altos (WIPO, 2023).[21] Del mismo índice de Innovación Global 2023, se realizó una comparación del total de solicitudes de patente (presentación directa y entradas en la fase nacional del PCT), del 2018 al 2022, entre México y la República de Corea, como se muestra en la Tabla 1.

Tabla 1. *Total de solicitudes de patente 2018-2022*

País	2018	2019	2020	2021	2022
México	16,424	15,941	14,312	16,161	16,605
República de Corea	209,992	218,975	226,759	237,998	237,633

Fuente: Elaboración propia con datos estadísticos de la WIPO.

Como se puede apreciar en la Tabla 1, en el período de comparación, Corea tuvo un incremento en el número de solicitudes de patente de 2018 a 2021, y en 2022 registró una ligera disminución. Sin embargo, sus niveles se mantuvieron muy superiores a los de México, lo anterior es el resultado de que Corea, por citar un ejemplo, en el año 2020 destinó el 4.8% del PIB, mientras que México en el mismo año únicamente asignó el 0.3%.[22]

Castells analiza la forma en que la Ciencia y la Tecnología constituyen pilares fundamentales para el logro de cualquier objetivo estratégico en el ámbito nacional e internacional.[23] No solo impulsan la competitividad en el escenario global, sino que también catalizan cambios sociales, políticos y económicos que pueden presentar desafíos significativos para la Seguridad Nacional de cualquier Estado. Por lo tanto, es esencial examinar detenidamente el papel que la Ciencia y la Tecnología desempeñan en la Seguridad Nacional, así como explorar las oportunidades que los avances científicos y tecnológicos actuales ofrecen para la realización de los objetivos estratégicos del país.

En la situación actual del Estado mexicano, la tecnología es una condición crítica que debe ser fortalecida para asegurar que la Seguridad Nacional no sea vulnerada. Las políticas dirigidas hacia el ámbito de la Defensa Exterior, deben de considerar amenazas emergentes, en particular actores no estatales, que intentan atacar especialmente al campo de poder económico, que al encontrarse integrado plenamente a los circuitos comercial y financieros internacionales, son más vulnerables a diversos antagonismos, pero también el país presenta características geográficas complejas que para lograr su plena vigilancia requiere de mayor sofisticación en sus instrumentos operativos y la inteligencia artificial puede ser la

[21] World Intellectual Property Organization (WIPO). Global Innovation Index 2023: Innovation in the face of uncertainty. (Geneva: WIPO, 2023).
[22] Banco Mundial. Gasto en investigación y desarrollo (% del PIB) México 2024. https://datos.bancomundial.org/indicador/gb.xpd.rsdv.gd.zs?locations=mx (consultado el 20 de enero de 2025).
[23] Castells, Manuel. La sociedad red: una visión global (Madrid: Alianza Editorial, 2020).

respuesta, así también para el combate de la delincuencia organizada, se necesitan innovaciones tecnológicas que brinden ventajas a las fuerzas de seguridad del país.

Para Márquez de la Rubia (2025), China no solo lidera en tecnología militar, sino también en ocho campos clave de la industria energética, incluyendo la generación de electricidad a partir de hidrógeno, supercapacitores, baterías eléctricas, energía fotovoltaica, gestión de residuos nucleares, biocombustibles, energía nuclear y tecnología de energía directa (láseres, microondas y ondas de sonido).[24] Aunque Estados Unidos sigue siendo líder en computación cuántica, China ya lo ha superado en criptografía cuántica, comunicaciones y sensores cuánticos. La estrategia de contención de Estados Unidos es una respuesta directa a esta realidad y a la creciente amenaza en otros sectores.

La ciencia y la tecnología pueden desempeñar un papel fundamental en la promoción del desarrollo económico y social de México, lo que a su vez contribuye con la Seguridad Nacional. La inversión en investigación y desarrollo impulsa la creación de empleo, fomenta la competitividad empresarial y promueve la diversificación de la economía, reduciendo así la dependencia de sectores vulnerables a fluctuaciones económicas globales. Igualmente, la aplicación de tecnologías innovadoras en áreas como la salud, la educación y la infraestructura pueden mejorar la calidad de vida de la población mexicana y fortalecer la cohesión social, reduciendo los riesgos de conflictos internos y tensiones sociales que podrían afectar la estabilidad del país.

Para Pardo de Santayana, desde el punto de vista estratégico, en este momento, solo hay dos superpotencias de IA: Estados Unidos y China, son los únicos países con el talento, las instituciones de investigación y la capacidad de computación masiva necesaria para entrenar los modelos de IA más sofisticados.[25] Estos son los protagonistas de la película, aunque en la guerra de Ucrania haya una implicación muy desigual por ambas partes.

Cabe señalar que antes del inicio de este conflicto armado, la IA ya había desencadenado un cambio vertiginoso de la seguridad que apenas estaba empezando a desarrollarse. Las Fuerzas armadas de los Estados Unidos utilizaban la IA para optimizar todo, desde el mantenimiento de los equipos hasta las decisiones presupuestarias. Los analistas de inteligencia confiaban en la IA para escanear con rapidez montañas de información e identificar patrones relevantes que les permitieran tomar mejores decisiones y hacerlo más aceleradamente.[26]

Por lo antes expuesto, es una prioridad que México desarrolle sus capacidades tecnológicas y asuma con rapidez los nuevos avances científicos que existen en el área militar y de seguridad, pero sobre todo asegurar el desarrollo nacional a partir

[24] Márquez de la Rubia, Francisco. “La batalla por la supremacía tecnológica. EE. UU. vs China”. Documento de Análisis IEEE 23/2025 (Madrid: Instituto Español de Estudios Estratégicos, 2025).
[25] Pardo de Santayana, Javier. La inteligencia artificial y la guerra de Ucrania. Documento de Análisis IEEE 81/2024 (Madrid: Instituto Español de Estudios Estratégicos, 2024).
[26] Flournoy, Michele A. “AI Is Already at War: How Artificial Intelligence Will Transform the Military.” Foreign Affairs 102, no. 6 (noviembre – diciembre 2023): 56-69.

de ser vanguardia global, no solo en la producción de insumos para la industria de tecnologías avanzadas, sino ser creador de patentes, que garanticen la autosuficiencia y soberanía de insumos para las Fuerzas Armadas y las áreas de Seguridad Nacional, esto implica que desde las universidades, sectores económicos y el gobierno se promueva la innovación en el campo de la ciberseguridad y la inteligencia artificial.

Por otra parte, las principales amenazas emergentes que enfrenta México según la INTERPOL, son las siguientes:

> El phishing, el ransomware y las violaciones de la seguridad de los datos son solo algunos ejemplos de las actuales ciberamenazas, eso sin contar que continuamente están surgiendo nuevos tipos de ciberdelitos. Los ciberdelincuentes son cada vez más ágiles y están mejor organizados, como demuestra la velocidad con que explotan las nuevas tecnologías y el modo en que adaptan sus ataques y cooperan entre sí de forma novedosa.[27]

Esta visión de la Interpol es compartida por el Centro Nacional de Inteligencia (CNI) del Estado mexicano, que señala que la ciberdelincuencia abarca una amplia gama de actividades ilícitas, que van desde el robo de datos personales y financieros hasta la proliferación de contenido ilegal en línea y el sabotaje de sistemas informáticos. Estas actividades no solo representan una amenaza para la seguridad económica y financiera del país, sino que también pueden socavar la confianza en las instituciones y afectar la estabilidad social.[28]

La cooperación internacional es esencial para abordar la naturaleza transfronteriza de la ciberdelincuencia y garantizar que los responsables rindan cuentas por sus acciones. La colaboración en el intercambio de información, el desarrollo de normas y estándares de ciberseguridad y la aplicación de leyes y regulaciones internacionales, son pasos importantes para proteger los intereses nacionales en el ciberespacio.[29]

2 Amenazas tecnológicas de la delincuencia organizada.

La delincuencia organizada en la era digital ha experimentado una transformación significativa, aprovechando las herramientas y plataformas tecnológicas para llevar a cabo sus actividades ilícitas de manera sofisticada, eficiente y globalizada. Los grupos criminales mediante una evolución vertiginosa de la tecnología han diversificado sus operaciones y negocios inicuos, expandiendo su alcance y ocultando sus actividades detrás de un velo de anonimato en el ciberespacio.

---

[27] INTERPOL. La ciberdelincuencia traspasa fronteras y evoluciona a gran velocidad. https://www.interpol.int/es/Delitos/Ciberdelincuencia (Consultado el 20 de noviembre de 2024).

[28] Centro Nacional de Inteligencia. Informe del estado que guarda la ciberseguridad de México. (Ciudad de México: Gobierno de México, 2023).

[29] Kaku, Michio. Física de lo imposible: ¿Podremos ser invisibles, viajar en el tiempo y teletransportarnos? (Madrid: Editorial DeBolsillo, 2010).

Este panorama presenta nuevos y desafiantes escenarios para el Estado mexicano en su lucha contra la delincuencia organizada. Las estrategias tradicionales de prevención, investigación y persecución del delito se ven desafiadas por la complejidad y la rapidez de las operaciones criminales en el entorno digital. La falta de fronteras en el ciberespacio, junto con la capacidad de los delincuentes para operar desde cualquier lugar, dificulta los esfuerzos de las autoridades para afrontar eficazmente el crimen organizado.

Por otro lado, la naturaleza transnacional de muchas organizaciones criminales obliga a una intensa cooperación internacional y coordinación entre diferentes agencias gubernamentales y fuerzas del orden de distintos países. Esto plantea desafíos adicionales en términos de compartir información, coordinar investigaciones y llevar a cabo acciones conjuntas para desmantelar redes criminales que operan en múltiples jurisdicciones.

En este sentido, el Estado mexicano se enfrenta a la necesidad de desarrollar y adoptar estrategias integrales y multidisciplinarias que aborden tanto los aspectos tradicionales como los nuevos desafíos del crimen organizado en la era digital. Esto incluye el fortalecimiento de las capacidades de ciberseguridad y la aplicación de tecnologías avanzadas para la recopilación y análisis de inteligencia, así como la mejora de la cooperación internacional y la colaboración entre diferentes organismos encargados de hacer cumplir la ley.

3 Oportunidades de la tecnología que garanticen la Seguridad Nacional del Estado mexicano.

Con base en Nye,[30] la tecnología no solo plantea desafíos para la Seguridad Nacional de México, sino que también ofrece una amplia gama de oportunidades para fortalecerla y proteger los intereses nacionales. El uso de sistemas de vigilancia avanzados, el análisis de datos y la inteligencia artificial, pueden revolucionar las capacidades del Estado mexicano para implementar sistemas que le permitan identificar el origen para prevenir y aminorar las amenazas como el crimen organizado, el terrorismo y la migración irregular con modelos y estrategias más efectivas y eficientes.

Los sistemas de vigilancia avanzados, en especial las cámaras de circuito cerrado, los drones y los satélites de observación, proporcionan a las autoridades una visión panorámica en tiempo real de las áreas vulnerables y los puntos críticos de interés. Esto no solo facilita la detección temprana de actividades sospechosas, sino que también permite una respuesta rápida y coordinada ante posibles amenazas, mejorando así la capacidad de las fuerzas de seguridad para proteger a la población y salvaguardar la integridad del territorio nacional.[31]

Además, el análisis de datos juega un papel crucial en la identificación de patrones y tendencias que podrían referir la presencia de actividades delictivas o la planificación

[30] Nye, Joseph S. El futuro del poder. (Barcelona: Ediciones Deusto, 2011).
[31] Rid, Thomas. La guerra cibernética ya ha comenzado. (Madrid: Turner, 2020).

de ataques. Para Bruce Schneier, el uso de algoritmos y técnicas de análisis avanzadas permite a las autoridades examinar grandes volúmenes de información, como registros de llamadas telefónicas, transacciones financieras y actividad en redes sociales, para identificar conexiones ocultas entre organizaciones delictivas, ubicando posibles puntos de vulnerabilidad y prevenir incidentes antes de que ocurran.[32]

Por otro lado, la inteligencia artificial ofrece capacidades aún más avanzadas para mejorar la Seguridad Nacional de México. Los algoritmos de aprendizaje automático pueden analizar datos en tiempo real y detectar anomalías o comportamientos sospechosos, lo que permite a las autoridades anticipar y responder de manera proactiva ante amenazas potenciales. Además, la mencionada inteligencia artificial también puede ser utilizada para optimizar la eficiencia de los procesos y procedimientos avanzados en materia de seguridad, optimizando la asignación de recursos y reduciendo los tiempos de respuesta en situaciones de emergencia.

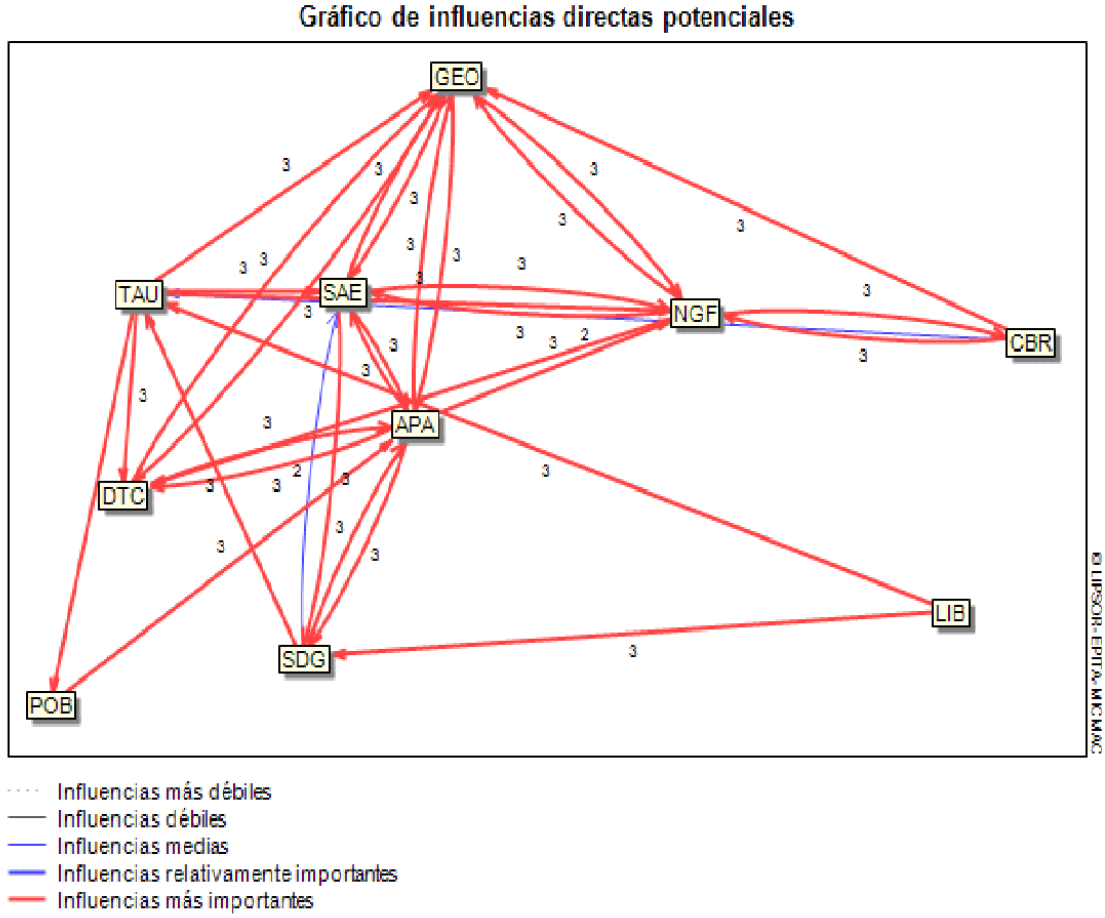
4 Sistemas de Armas Autónomas (SAAS)

Un tema relevante de actualidad a considerar por el Estado mexicano es el de los Sistemas de Armas Autónomas (SAAS), los cuales se inscriben en un escenario complejo donde una serie de fuerzas y tendencias globales entre las que destacan: 1) Acelerado proceso de automatización y uso de inteligencia artificial en todos los aspectos de la vida humana (mundo autónomo) (APA); 2) Sociedades más demandantes ante los gobiernos (SDG); 3) Mayor sofisticación de las amenazas emergentes del Estado (SAE); 4) Profundización del orden biopolítico (POB); 5) Confrontación de grandes potencias por la hegemonía mundial (Nueva Guerra Fría) (NGF); 6) Lento crecimiento económico de las regiones periféricas de la economía sistema-mundo (LIB); 7) Conflictos bélicos de índole regional (CBR); 8) Desarrollo de tecnología cuántica (DTC); 9) Competencia geopolítica por recursos naturales para el impulso de la tecnología (GEO); 10) Tendencias autoritarias vs. democracia (TAU). Las cuales, al intervenir en un estudio prospectivo, existe alta probabilidad de que influyan de manera determinante en el aumento de poder de las SAAS, especialmente aquellas integradas por la inteligencia artificial.

Una vez determinadas estas tendencias, se analizaron bajo el método de Matriz de Impactos Cruzados Multiplicación Aplicada a la Clasificación (MICMAC), en particular con la matriz de influencias directas potencias (MIDP) la cual arrojó que en el corto plazo cuatro tendencias tendrán fuerte influencia sobre las SAAS y son los conflictos geopolíticos por la obtención de los recursos; la competencia por la hegemonía, global; la sofisticación de las amenazas emergentes; y el acelerado proceso de automatización de la vida humana. Cabe señalar que el método MICMAC es una herramienta y programa desarrollado por Michel Godet,[33] para el desarrollo de

[32] Schneier, Bruce. Datos y Goliath: Los enfrentamientos ocultos para recopilar tus datos y controlar tu mundo. Madrid: Capitán Swing, 2022.
[33] Godet, Michel. La caja de herramientas de la prospectiva estratégica. (París: Instituto Europeo de Prospectiva y Estrategia, 2000).

estudios prospectivos. En esta lógica los datos y ponderaciones con los cuales se alimentó la matriz, fue a partir de la opinión de tres expertos, a los cuales se les preguntó el nivel de influencia que las variables tienen entre sí, siendo el valor de tres como alta influencia; dos, influencia media; uno, influencia baja; y cero, ninguna influencia. Los resultados fueron ingresados al programa el cual desarrolló el gráfico de influencias potenciales, donde se muestran las variables que influirán directamente en el fenómeno estudiado.



Fuente: con base en los datos obtenidos en análisis MICMAC. Elaboración propia.

Con base en los resultados de la MICMAC que ubicó las cuatro condicionantes claves del sistema y su potencialidad (a futuro) se procedió a construir bajo el sistema de prospectiva con lógica intuitiva cuatro escenarios, el tendencial, el optimista, el pesimista; el contrastado y se propone un escenario apuesta ideal. Estos escenarios son exploraciones del futuro, no son predicciones, tampoco implican condiciones estáticas, son guías para el porvenir.

Escenario tendencial
El desarrollo de SAAS sigue creciendo bajo el auspicio de las grandes potencias y de la industria militar global. Provocando tanto avances en la seguridad como en capacidades bélicas de los poseedores de esta tecnología, generando una

nueva carrera armamentista, la cual trae incertidumbre y nuevos equilibrios en el sistema internacional. La inteligencia artificial tiene un papel preponderante en el mantenimiento de la Seguridad Nacional de los Estados-Nación y forma parte sustantiva de los elementos constituyentes del poder nacional. La confrontación hegemónica se ha intensificado la cual ha generado la expansión de las SAAS a otros países involucrados de manera directa y los recursos naturales que son insumos para el desarrollo tecnológico son sumamente valorados y les da una posición competitiva a los países poseedores de estos.

México posee tecnología de SAAS bajo severas restricciones para su uso que está confinado a tareas exclusivamente de Seguridad Nacional, lo cual le permite a las Fuerzas Armadas tener mayor eficiencia y el aumento de sus capacidades operativas para mitigar y controlar a las posibles amenazas emergentes, así como los riesgos que se le presentan al Estado.

Escenario Optimista

El uso de los SAAS a nivel global está plenamente regulado por el sistema jurídico internacional y sólo se utiliza para fines defensivos por parte de los Estados-Nación. No existen armas autónomas que omiten totalmente el control humano. La confrontación hegemónica continúa, pero no ha generado una carrera armamentista.

La venta de los SAAS está fuertemente restringida a los agentes no estatales, esto disminuye que las posibles amenazas emergentes utilicen este tipo de tecnología. No hay incidentes o accidentes provocados por las SAAS donde se ve involucrado personal civil.

Los recursos naturales que se utilizan para el impulso de la industria tecnológica son abundantes y son explotados con racionalidad y se intercambian con ventajas sociales para los países poseedores, por lo que los conflictos geopolíticos se reducen sustantivamente.

México tiene desarrollados SAAS que usa para la Defensa Nacional, especialmente para optimizar acciones en el fortalecimiento de la Seguridad Nacional, lo cual reduce costos a las Fuerzas Armadas, pero también cuenta con el desarrollo de una industria de defensa vinculada a los diversos sistemas tecnológicos de vanguardia que permite mantener su crecimiento y expansión y con ello se incrementa el poder nacional del Estado mexicano.

Escenario pesimista

Los SAAS han proliferado sin control y esto ha provocado que se generen conflictos con actores tanto estatales como no estatales, que utilizan de manera constante e indiscriminada estas armas, provocando numerosas bajas entre la población civil, también las amenazas emergentes se han vuelto más sofisticadas porque han adquirido y operan esta tecnología, la cual la utilizan para desestabilizar a los Estados-Nación, especialmente grupos terroristas y de subversión de tipo interestatal.

La confrontación hegemónica ha desarrollado una industria de los SAAS con acelerado crecimiento, lo cual ha generado grandes ganancias a esta, pero también

ha provocado que se presenten fuertes tensiones entre las superpotencias y con ello se ha colocado al mundo al borde de una conflagración global.

México no cuenta con tecnologías de las SAAS, lo cual lo coloca en desventaja con otros países de la región, por lo que su Seguridad Nacional se encuentra vulnerada por amenazas emergentes, especialmente la delincuencia organizada, por lo que el Estado realiza mayores esfuerzos para mantener la condición de Seguridad Nacional en el país.

Escenario Contrastado

Las SAAS son prohibidas en su totalidad por el orden jurídico global, sin embargo, como no hay capacidad vinculante, siguen siendo usadas por diversos Estados y agentes no estatales, lo cual genera tensiones que tienen como consecuencia conflictos regionales de impacto reducido en regiones periféricas del mundo. La industria militar ha dirigido sus investigaciones y desarrollo nuevamente a las armas nucleares que ahora serán manejadas por inteligencia artificial. Los conflictores geopolíticos por los recursos naturales que impulsan el desarrollo tecnológico han cesado y se prevé un gran acuerdo para la repartición justa de insumos que garanticen prosperidad para todos.

México utiliza SAAS a pesar de la prohibición del sistema jurídico internacional, debido a que las necesita para afrontar a la delincuencia organizada, la cual se encuentra debilitada por la acción conjunta de todos los sectores de la sociedad mexicana.

Escenario apuesta

El sistema jurídico internacional tiene una amplia normatividad vinculatoria en materia del uso de las SAAS, las cuales están orientadas a uso defensivo exclusivamente y cuentan con un amplio control humano, la inteligencia artificial es utilizada en ellas, pero siempre hay la preponderancia de la decisión humana sobre estas. La competencia por la hegemonía global se ha concentrado en el tema económico y la industria militar de las armas autónomas, solo se ha extendido hacia ramas del aspecto logístico.

México cuenta con SAAS, que están plenamente reguladas y en constante supervisión tanto por instancias nacionales como internacionales y se usan con eficacia contra la delincuencia organizada, que tiene sus capacidades sumamente reducidas. También tiene una industria de defensa con amplio nivel de desarrollo armonizado que produce armas autónomas que le garantizan autosuficiencia y obtención de recursos financieros.

El país aseguró con las SAAS un medio eficaz de amplio expectro que le permita el fortalecimiento de la Seguridad Nacional, así como su integridad territorial.

Desde el punto de vista del desarrollo de la industria de defensa, existen amplias posibilidades que la innovación tecnológica enfrentará un proceso complejo y significativo para que se garantice el desarrollo de las SAAS, lo cual representará la clave de la supremacía con el uso y operación de sistemas basados en la inteligencia artificial, lo cual implica que se destinen los fondos financieros correspondientes,

mediante una planeación estratégica integral con incidencia en el desarrollo nacional.

Conclusiones

Un pilar fundamental del poder nacional del Estado mexicano, es sin duda el campo tecnológico el cual tiene la capacidad de fortalecer a los otros campos del poder: político, económico, social, militar y diplomático; sin embargo, para detonar el desarrollo nacional es conveniente sumar la voluntad de los actores estratégicos e impulsar una política pública que promueva la cultura y educación científica, tecnológica e innovación.

La situación tecnológica nacional revela la importancia de contar con regulaciones adecuadas para promover el desarrollo y la adopción de tecnologías, pero hasta ahora es imperante fomentar el desarrollo tecnológico del país; en este sentido, se enfrentan diversos desafíos políticos, económicos y sociales que pueden afectar la capacidad del Estado para fortalecer su poder tecnológico.

México muestra avances significativos con respecto a la situación tecnológica de áreas específicas como conectividad e infraestructura, pero enfrenta desafíos críticos en ciberseguridad, innovación y desarrollo de capital humano especializado, detectándose que existe una marcada disparidad regional en el acceso y desarrollo tecnológico, con una concentración de capacidades en zonas urbanas que limita las oportunidades de crecimiento en áreas urbanas y semiurbanas.

Un país con mayores fortalezas en el ámbito de la ciencia, tecnología e innovación tendrá mayor capacidad para incrementar su productividad, no sólo por el efecto directo que genera cualquier innovación, sino sobre todo porque estará mejor preparado para enfrentar las incertidumbres generadas por el actual entorno de competencia global.

Para el Estado mexicano es preciso contar con un gran potencial de recursos humanos y materiales, que le permitan considerar la posibilidad de que se implementen y apliquen políticas públicas como las de Corea u otras potencias emergentes para promover la cultura y la educación científica, tecnológica y humanística, en beneficio del Desarrollo Nacional, aspecto que es posible, ya que la actual administración, ha denotado un cambio proactivo basado en las políticas en materia de ciencia y tecnología.

Un impacto trascendental para tomar en consideración a partir del análisis de la situación tecnológica nacional y los antagonismos identificados evidencia la necesidad de políticas públicas que impulsen la independencia tecnológica y fomenten la innovación propia en México. Al promover el desarrollo de tecnología propia, con un enfoque en áreas como la ciberseguridad, resultará prioritario para proteger la soberanía y garantizar la estabilidad social, política y económica del país.

Abordar estos antagonismos de manera integral y reforzar los bienes tutelados

permitirá avanzar hacia una seguridad nacional sólida y una posición competitiva en el ámbito tecnológico global.

Las tecnologías para la Seguridad Nacional de México son claves, debido a que las amenazas son más complejas, con amplios recursos y se desarrollan en una red global que les permiten mayor operatividad, alcance y efectividad, de ahí la necesidad de su uso.

México enfrenta una serie de amenazas emergentes especialmente de ciberataques cometidos por todo tipo de delincuentes que pretenden vulnerar a las instituciones del Estado y a la población en general, por tal motivo se requiere promover políticas proactivas de índole integral que puedan controlar o mitigar la acción nociva del uso ilícito que se hace de la tecnología.

Es innegable el hecho de que las amenazas emergentes que se presentan desde el ciberespacio y la alta tecnología son una realidad que requiere de medidas urgentes por parte del Estado mexicano, estas acciones deben abarcar varios rubros: 1) la seguridad en el ciberespacio y las instalaciones estratégicas virtuales y físicas; 2) el implemento de tecnología operado con inteligencia artificial que impulse el desarrollo nacional; 3) el uso de las SAAS en las tareas de las Fuerzas Armadas para garantizar la Defensa Nacional y 4) la prevención ante la innovación tecnológica de la delincuencia organizada y los grupos terroristas . Estos cuatro rubros llevarán a la consecución de los objetivos nacionales y la salvaguarda de los bienes tutelados por la Seguridad Nacional.

Para México, es importante entender y aprovechar el impacto de la tecnología para fortalecer el desarrollo nacional, sus capacidades defensivas y salvaguardar los intereses del país. En este sentido, es transcendental identificar áreas de oportunidad que permitan aprovechar al máximo los beneficios que la tecnología puede ofrecer en términos de Seguridad Nacional, por lo cual se recomienda lo siguiente:

a). Destinar parte del presupuesto federal a la inversión en tecnología avanzada; Esto significa asignar mayores recursos a la investigación, desarrollo y adquisición de tecnología para el desarrollo y la seguridad nacional, infraestructura en comunicaciones y sistemas de vigilancia de última generación.

b). Colaboración en Investigación y Desarrollo, mediante la subvención entre los sectores público y privado y las instituciones académicas para impulsar la innovación y el desarrollo tecnológico en el ámbito de la Defensa Nacional. Esto permitirá aprovechar al máximo los avances científicos y tecnológicos disponibles para abordar los desafíos de Seguridad Nacional.

c). Fortalecimiento de Capacidades en Ciberseguridad operados con inteligencia artificial, dada la creciente amenaza de ciberataques y ciberdelincuencia, por lo que se deberán fortalecer las capacidades en ciberseguridad. Esto incluye la capacitación y el desarrollo profesional del personal, la implementación de medidas de seguridad robustas y la colaboración con diversos organismos especializados encargados de la seguridad cibernética.

d). Aplicación de Tecnologías de Vigilancia Avanzada, aprovechando las tecnologías específicas de última generación como cámaras de circuito cerrado, drones y satélites de observación, para optimizar la vigilancia de áreas vulnerables y puntos críticos de interés. Esto facilitará la detección temprana de actividades sospechosas y una respuesta rápida ante posibles amenazas.

e). Uso de la inteligencia artificial en Seguridad Nacional, mediante el uso de plataformas y algoritmos de aprendizaje automático, lo que permitirá analizar datos en tiempo real para detectar anomalías y prevenir amenazas de manera proactiva, así como optimizar la asignación de recursos y reducir los tiempos de respuesta en situaciones de emergencia.

Bibliografía

Alkharman, J., Drawsheh, S., Al-Khataybeh, M., BaniYounes, Z., Darawsheh, N. Alrashdan, H. (2024). Cyber attacks and its implication to national security: The Need for international law enforcement. Pakistan Journal of Criminology, 16(3), 851-864. https://doi.org/10.62271/pjc.16.3.851.864

Banco Mundial. (2024). Gasto en investigación y desarrollo (% del PIB) - Mexico. Obtenido de datos.bancomundial.org: https://datos.bancomundial.org/indicador/gb.xpd.rsdv.gd.zs?locations=mx

Castells, M. (2020). La sociedad red: una visión global. Alianza Editorial.

Centro Nacional de Inteligencia . (2023). Informe del estado que guarda la ciberseguridad de México. Gobierno de la República.

Clarke., R. A. (2020). Guerra Cibernética: La Próxima Amenaza para la Seguridad Nacional y Qué Hacer al Respecto. Penguin Press.

CPEUM. (15 de Mayo de 2019). Constitución Política de los Estados Unidos Mexicanos. Obtenido de la Cámara de Diputados del H. Congreso de la Unión: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Flournoy, M. A. (2023). AI Is Already at War. How Artificial Intelligence Will Transform the Military. Foreign Affairs.

Godet, M. (2000). La caja de herramientas de la prospectiva estratégica. Instituto Europeo de Prospectiva y Estrategia.

Goodman, M. (2015). Future Crimes: Todo está conectado, todos somos vulnerables y qué podemos hacer al respecto . Paidós .

Guarneros, F. (10 de Abril de 2021). La educación de ciencia y tecnología en México todavía enfrenta profundos retos. Obtenido de Expansión: https://expansion.mx/tecnologia/2021/04/10/la-educacion-stem-en-mexico-todavia-enfrentan-profundos-retos.

INTERPOL. (2024). La ciberdelincuencia traspasa fronteras y evoluciona a gran velocidad. Lyon: INTERPOL. https://www.interpol.int/es/Delitos/Ciberdelincuencia

Kaku, M. (2017). Física de lo imposible: ¿Podremos ser invisibles, viajar en el tiempo y teletransportarnos? Editorial DeBolsillo.

Lozano, D. (2023). La nueva oportunidad de México. Fondo de cultura económica.

Nye, J. S. (2021). El futuro del poder. Ediciones Deusto.

Márquez de la R. (2025). La batalla por la supremacía tecnológica: EE. UU. vs. China. Documento de Análisis IEEE 23/2025. enlace web IEEE y/o enlace bie3 (consultado

27/Abr./2025

OCDE. (2015). Manual de Frascati 2015. Obtenido de Guía para la recopilación y presentación de información sobre la investigación y el desarrollo experimental: https://www.oecd-ilibrary.org/docserver/9789264310681-es.pdf?expires=1717000928&id=id&accname=guest&checksum=474ACD53AE255F57F38ACD3C86C225F7

OEA. (Marzo de 2001). Manual de Bogotá. Obtenido de Normalización de Indicadores de Innovación Tecnológica en América Latina y el Caribe: https://oei.int/downloads/disk/eyJfcmFpbHMiOnsibWVzc2FnZSI6IkJBaDdDRG9JYTJWNVNTSWhOVEJyWTNOMlkyaDVlV3MxYkc4eWFHWTViMnMzWXpaamJERnJPQVk2QmtWVU9oQmthWE53YjNOcGRHbHZia2tpWEdsdWJHbHVaVHNnWm1sc1pXNWhiV1U5SWsxaGJuVmhiQ0JrWlNCQ2IyZHZkR0V1Y0dSbUlqc2dabWxzWlc1aGJX

OECD/Eurostat. (2018). Oslo Manual 2018: Guidelines for collecting, reporting and using data on innovation 4th edition. Obtenido de The Measurement of Scientific, Technological and Innovation Activities: El Manual define cuatro tipos de innovaciones: Producto, proceso, marketing y organización.

PapaEsceptico. (2024). Biografía Juan Manuel Lozano Gallegos. Obtenido de papaesceptico.com: https://papaesceptico.com/oxytam-es-oxigeno-liquido-o-peroxido-de-hidrogeno-y-un-fraude/biografia-juan-manuel-lozano-gallegos/

Pardo de Santayana, J .(2024). La inteligencia artificial y la guerra de Ucrania. Documento de Análisis IEEE 81/2024. enlace web IEEE y/o enlace bie3 (consultado 1/mayo/2025)

PECITI. (28 de diciembre de 2021). Programa Especial de Ciencia, Tecnología e Innovación 2021-2024. Obtenido del Consejo Nacional de Ciencia y Tecnología: https://www.siicyt.gob.mx/index.php/normatividad/nacional/programa-especial-de-ciencia-tecnologia-e-innovacion-peciti/programa-especial-de-ciencia-tecnologia-e-innovacion-peciti-2/4965-programa-especial-de-ciencia-tecnologia-e-innovacion-peciti-2021-2024/

Peiró, R. (21 de mayo de 2024). *¿Qué es la ciencia?* Obtenido de https://economipedia.com/definiciones/ciencia.html

Periferia. (26 de septiembre de 2023). *México: La inversión en ciencia y tecnología llegará al 0,6% del PBI, en 2024*. Obtenido de https://periferia.com.ar/latinoamerica/mexico-la-inversion-en-ciencia-y-tecnologia-llegara-al-06-del-pbi-en-2024/

Ramírez, R. (2021). *El sistema de Seguridad Nacional y los objetivos nacionales permanentes tutelados por la Constitución Política Mexicana.* Obtenido de Revista de

Administración Pública. Instituto de Investigaciones Jurídicas: https://revistas-colaboracion.juridicas.unam.mx/index.php/rev-administracion-publica/article/view/19061/17170

Rid, T. (2020). *La guerra cibernética ya ha comenzado.* Turner.

Roldán, P. (25 de enero de 2024). *Tecnología: Qué es, usos y ejemplos*. Obtenido de https://economipedia.com/definiciones/tecnologia.html

Schneier, B. (2022). *Datos y Goliath: Los enfrentamientos ocultos para recopilar tus datos y controlar tu mundo.* Capitán Swing .

SEDENA-SEMAR. (2018). *Glosario de Términos Unificados de Seguridad Nacional.* CODENAL-CESNAV.

Vizarretea, E. (2020). *Repensar México una introducción a la Seguridad y Defensa Nacionales.* Ciudad de México: Secretaría de Marina.

Westreicher, G. (1 de mayo de 2020). *Innovación tecnológica*. Obtenido de https://economipedia.com/definiciones/innovacion-tecnologica.html

WIPO. (2023). *World Intellectual Property Organization*. Obtenido de Índice de Innovación Global 2023: https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2023-en-main-report-global-innovation-index-2023-16th-edition.pdf

REVISTA INCLUSIONES M.R.

CUADERNOS DE SOFÍA EDITORIAL