RIS
Revista de Inteligencia y Seguridad

Claves y definiciones: crisis internacional, investigación policial y ciberseguridad ante los desafíos para la seguridad nacional

Número 2
(JULIO-DICIEMBRE 2024)

ISSN 2992-7455
www.inap.mx/ris

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

69 AÑOS
Laboratorio de Excelencia Académica
1955-2024

RIS

Revista de Inteligencia y Seguridad

Número 2
(julio-diciembre 2024)

Claves y definiciones: crisis internacional, investigación policial y ciberseguridad ante los desafíos para la seguridad nacional

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

69 AÑOS
Laboratorio de Excelencia Académica
1955-2024

Revista de Inteligencia y Seguridad, No. 2, julio-diciembre 2024, es una publicación semestral digital (www.inap.mx/ris), editada por el Instituto Nacional de Administración Pública, ubicado en Km. 14.5 Carretera México-Toluca No. 2151, Col. Palo Alto, C.P. 05110, Alcaldía de Cuajimalpa, Ciudad de México. Teléfono (55) 5081 2657. www.inap.mx
contacto@inap.org.mx

Editor responsable: José Rafael Martínez Puón.
Reserva de Derechos al Uso Exclusivo No. 04-2023-032713274000-102, otorgado por Instituto Nacional del Derecho de Autor.
ISSN: 2992-7455

Consejo Directivo 2023-2026

Luis Miguel Martínez Anzures
Presidente

Olga Sánchez Cordero
Vicepresidenta

Carlos Eduardo Flota Estrada
Vicepresidente para los IAPs de los Estados 2023-2024

CONSEJEROS
Rina Aguilera Hintelholher
Eber Omar Betanzos Torres
Esther Nissán Schoenfeld
David Villanueva Lomelí
Susana Libién Díaz González
Gerardo Felipe Laveaga Rendón
Luis Humberto Fernández Fuentes
Laura Enríquez Rodríguez

Selene Lucía Vázquez Alatorre
Secretaria del INAP

Rafael Martínez Puón
Director de la Escuela Nacional de Profesionalización Gubernamental

Ricardo Corral Luna
Director de Consultoría

Luis Armando Carranza Camarena
Director de Administración y Finanzas

CONSEJO DE HONOR
Luis García Cárdenas
José Natividad González Parás
Alejandro Carrillo Castro
José R. Castelazo
Carlos Reta Martínez

IN MEMORIAM
Gabino Fraga Magaña
Gustavo Martínez Cabañas
Andrés Caso Lombardo
Raúl Salinas Lozano
Ignacio Pichardo Pagaza
Adolfo Lugo Verduzco

FUNDADORES

Francisco Apodaca y Osuna
José Attolini Aguirre
Enrique Caamaño Muñoz
Antonio Carrillo Flores
Mario Cordera Pastor
Daniel Escalante Ortega
Gabino Fraga Magaña
Jorge Gaxiola Zendejas
José Iturriaga Sauco
Gilberto Loyo González
Rafael Mancera Ortiz
Antonio Martínez Báez
Lorenzo Mayoral Pardo
Alfredo Navarrete Romero
Alfonso Noriega Cantú
Raúl Ortiz Mena
Manuel Palavicini Piñeiro
Álvaro Rodríguez Reyes
Jesús Rodríguez y Rodríguez
Raúl Salinas Lozano
Andrés Serra Rojas
Catalina Sierra Casasús
Ricardo Torres Gaitán
Rafael Urrutia Millán
Gustavo R. Velasco Adalid

REVISTA DE INTELIGENCIA Y SEGURIDAD

Número 2 (julio-diciembre 2024)

CLAVES Y DEFINICIONES: CRISIS INTERNACIONAL, INVESTIGACIÓN POLICIAL Y CIBERSEGURIDAD ANTE LOS DESAFÍOS PARA LA SEGURIDAD NACIONAL

Director del Número: Mtro. Severino Cartagena

REVISTA DE INTELIGENCIA Y SEGURIDAD

Número 2 (julio-diciembre 2024)

ÍNDICE

Presentación 8
Luis Miguel Martínez Anzures

Introducción 11
Severino Cartagena Hernández

Policrisis y Multilateralismo fallido en el siglo XXI 15
María Cristina Rosas

Claves del análisis criminal en México 31
Mario Vignettes

Conflictos de Cuarta Generación (4GW) entre Cárteles de la Droga y sus Proxys: Impacto en la inversión del Nearshoring en el sureste de México 50
Eduardo Zerón García

Ciberseguridad orquestable: tendencias de IA para ciberdefensa proactiva y ciberinteligencia automatizable 80
Carlos Estrada Nava

Agua y Seguridad Nacional: El hackeo de la Comisión Nacional del Agua en México 99
Erick Alejandro Rafael Aguilar Obregón

Transformación de la Gobernanza Pública en la Protección Ciudadana Post COVID-19: Desafíos y Oportunidades para la Seguridad en México 117
Guadalupe Rivero Rodríguez

La Inteligencia para la Seguridad Nacional como Elemento de Tutela de los Derechos Humanos 143
Alejandro Toledo Utrera

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

PRESENTACIÓN

A partir de la gran aceptación que recibió la Revista de Inteligencia y Seguridad dentro de nuestra comunidad en general, así como del público especializado en la materia, el Instituto ha continuado con este compromiso. Por lo tanto, en este número, se abordan desafíos contemporáneos que impactan a México y al mundo, desde temas novedosos como la "policrisis" y el debilitamiento del multilateralismo, hasta las amenazas del crimen organizado, los ciberataques y la necesidad de una gobernanza pública adaptada a la era post-COVID-19.

El número inicia con María Cristina Rosas, quien nos invita a reflexionar sobre la "policrisis" que define el siglo XXI, un escenario de crisis múltiples y simultáneas que dificultan la toma de decisiones y la gobernanza global. En este contexto, el multilateralismo se ve debilitado, lo que agrava aún más la incertidumbre y la complejidad del panorama internacional.

En el ámbito de la seguridad pública, Mario Vignettes explora la figura del analista criminal en México, destacando la importancia del análisis para la generación de inteligencia y proponiendo un catálogo de productos analíticos esenciales.

La expansión de los cárteles de la droga y sus actividades ilícitas en el sur de México son analizadas por Eduardo Zerón García, quien examina el impacto de los Conflictos de Cuarta Generación (4GW) en la viabilidad del *nearshoring*. A pesar de la violencia y la percepción de inseguridad, el autor concluye que, por el momento, estos factores no son determinantes para el desarrollo económico de la región, aunque se requiere un control efectivo a mediano y largo plazo.

La ciberseguridad se ha convertido en una preocupación global, y Carlos Estrada Nava aborda la necesidad de una "ciberseguridad orquestable" que integre la inteligencia artificial para una ciberdefensa proactiva y una ciberinteligencia automatizable. En un contexto de creciente sofisticación de los ciberataques, México se encuentra en una posición vulnerable, lo que hace esencial la adopción de estrategias innovadoras y la cooperación internacional. El hackeo a la Comisión Nacional del Agua (Conagua) en 2023, expuesto por Erick Alejandro Rafael Aguilar Obregón, ilustra la vulnerabilidad de la

infraestructura crítica de México ante los ciberataques. El autor destaca la necesidad de fortalecer la ciberseguridad como un elemento fundamental de la seguridad nacional, especialmente en un mundo donde el ciberespacio se ha convertido en un nuevo teatro de operaciones.

La pandemia de COVID-19 ha transformado la gobernanza pública, y Guadalupe Rivero Rodríguez analiza los desafíos y oportunidades para la seguridad ciudadana en el contexto post-pandemia. El estudio revela una brecha entre la teoría y la práctica en las políticas de seguridad, lo que debilita la confianza en las instituciones y exige un enfoque más integral y colaborativo. Para cerrar, Alejandro Toledo Utrera explora la relación entre la inteligencia para la seguridad nacional y la protección de los derechos humanos. El autor destaca cómo los productos de inteligencia pueden contribuir a salvaguardar derechos fundamentales como la vida, la libertad, la seguridad de los datos y la privacidad, elementos esenciales para la gobernanza y la paz.

Aprovecho la ocasión para reconocer la labor realizada por el Mtro. Severino Cartagena, quien diligentemente ha conducido los trabajos de coordinación de este número, con el apoyo de siete destacados especialistas, quienes nos dan una muestra del amplio manejo de los temas sobre los que trabajan.

En conjunto, los artículos de este número de la Revista de Inteligencia y Seguridad ofrecen una visión panorámica de los desafíos y oportunidades que enfrenta México en materia de seguridad. La publicación se consolida como un espacio de reflexión y debate plural, donde expertos de diversas disciplinas comparten sus conocimientos y perspectivas para construir un futuro más seguro y próspero.

Dr. Luis Miguel Martínez Anzures
Presidente del INAP

Introducción

Claves y definiciones: crisis internacional, investigación policial y ciberseguridad ante los desafíos para la seguridad nacional

En este número participan tanto profesores de larga experiencia en sus diversas especialidades, como egresados tanto de la Maestría y la Especialidad en Inteligencia para la Seguridad nacional como del Doctorado en Administración Pública del INAP. Sus aportes buscan establecer definiciones claras; arrojar luz sobre problemáticas que ameritan atención en el momento actual de la inteligencia y la seguridad, aplicando en el estudio y valoración de las diversas situaciones que abordan estos trabajos, metodologías de utilidad que respondan a los problemas que se han orecido para la crítica y la reflexión.

En "Policrisis y multilateralismo fallido en el siglo XXI", la Dra. María Cristina Rosas desarrolla, con base en el término policrisis, un sólido argumento en torno a la multiplicación de las amenazas vitales que se amplifican y retroalimentan al grado de que en su conjunto es más que la suma de sus partes. El enrarecimiento consecuente de las relaciones internacionales, la presencia de dos guerras que amenazan la estabilidad mundial, y el serio menoscabo de la cooperación multilateral, debilitándola, ha tenido incluso el efecto de extrañar la misma guerra fría y el orden mundial al que dio forma. Se trata de una crisis que no sólo ha socavado los mecanismos multilaterales por excelencia, empezando por el sistema de Naciones Unidas, sino que se ha internalizado a través de expresiones políticas y proyectos de gobierno desapegados de los marcos institucionales, en momentos en que la hegemonía del antaño "único país indispensable" acusa signos de reformulación, cuando no de retroceso. La autora se pronuncia por ver los problemas de frente y rescatar con decisión el sistema multilateral y la cooperación internacional.

El trabajo del Dr. Mario Vignettes del Olmo, "Claves del Análisis Criminal en México" ofrece una metódica disección del marco jurídico a nivel federal que define y habilita al analista criminal. Con base en la distinción entre información

e inteligencia, el autor se aboca a revisar con espíritu crítico el papel que el marco normativo confiere al analista en las dimensiones estratégica y táctica de la inteligencia criminal; su aporte al propio ciclo de inteligencia; las herramientas necesarias para realizar su trabajo, además de su participación en los diversos procesos relacionados con la investigación policial y su conducción ministerial. El documento añade una reflexión en torno al perfil de la persona analista criminal, de valor apreciable para visibilizar su condición actual, a fin de elevar su categoría y mejorar su participación como parte de la tetralogía de la investigación en el sistema penal acusatorio. La propuesta busca enfocar el reclutamiento y la formación de personal, así como la actualización de las competencias que tanta falta hacen para fortalecer la figura del analista criminal a nivel federal y en las entidades federativas.

Eduardo Zerón aborda en "Conflictos de Cuarta Generación (4GW) entre Cárteles de la Droga y sus Proxys: Impacto en la inversión del *Nearshoring* en el sureste de México", los posibles efectos de la inseguridad en la restricción de oportunidades que orece el nearshoring como estrategia de desarrollo. Como las guerras de cuarta generación socavan la capacidad del Estado para ejercer la dominación frente a la dinámica de formación, multiplicación, pero también la diferenciación y conflictos violentos entre las organizaciones del crimen organizado, hasta qué punto las evidentes consecuencias para la sociedad pudieran podrían hacerse extensivos en la inversión productiva. Con base en un aparato estadístico enfocado al corredor transístmico, que incluye los estados de Veracruz, Oaxaca y Chiapas, el artículo concluye que el impacto de la violencia no parece frenar el flujo de inversión, al menos no directamente, lo que obliga a revisar los supuestos económicos que sostienen las argumentaciones habituales con relación a los efectos perniciosos de la violencia y la seguridad, sin subestimar el drama de la violencia en el tejido social y comunitario.

Carlos Estrada Nava, en "Ciberseguridad orquestable: tendencias de IA para ciberdefensa proactiva y ciberinteligencia automatizable" ofrece al público interesado los componentes de un intrincado panorama de componentes, riesgos y amenazas que comprende la expansión de la frontera de la ciberseguridad a la luz de la inteligencia artificial. Consciente de que se trata de un arma de doble filo, inicia con las acechanzas más relevantes que han sufrido importantes sistemas informáticos de nuestro país, para explorar las posibilidades de la inteligencia artificial, lo que deriva en un planteamiento de "ciberseguridad orquestable", en tanto capacidad para coordinar e integrar los sistemas y procesos ante los desafíos recientes a la ciberseguridad a través de la implementación de plataformas de gestión estratégica de amenazas y riesgos, facilitando la interoperabilidad entre diferentes soluciones, agilizando la toma de decisiones efectivas para aislar dispositivos e interrumpir el flujo de tráfico

malicioso, con el resultado de mejorar la velocidad y precisión de la respuesta ante incidentes.

Con el fin de explorar las condiciones de la ciberseguridad en el país, Erick Alejandro R. Aguilar Obregón, propone en el artículo "Agua y Seguridad Nacional: El hackeo de la Comisión Nacional del Agua en México", un interesante estudio de caso que ilustra cómo fallas a nivel de la gobernanza, que incluyen el desorden administrativo e introducen notas de corrupción, pueden derivar en una seria afectación a los sistemas de gestión y control del agua en nuestro país. Los hechos, ocurridos en 2023, consistentes en el encriptamiento de información afectando a 12 mil personas, perfilaron una situación de seguridad nacional por su impacto en el funcionamiento de la infraestructura hídrica y la operación de sus servicios. Previamente, la advertencia derivada de haber soslayado diversas pruebas, diagnósticos y una auditoría informática constituyen el antecedente más significativo del grado de vulnerabilidad ante cualquier ataque, lo que plantea la necesidad de generar un sistema de inteligencia que reduzca riesgos y mantenga un elevado nivel de gobernanza de una entidad tan importante para el bienestar de la población.

"Transformación de la Gobernanza Pública en la Protección Ciudadana Post COVID-19: Desafíos y Oportunidades para la Seguridad en México", de Guadalupe Rivero Rodríguez, se propone una exploración de la forma como la pandemia de Covid 19, pudo haber incidido en el marco normativo e institucional en materia de seguridad nacional, seguridad interior, seguridad pública y seguridad ciudadana, para luego analizar las posibles correlaciones entre la incidencia de la enfermedad y los factores relacionados con la seguridad. El artículo añade los resultados de una encuesta empírica que recoge los principales ecos de lo que puede ser una agenda que atienda algunas asignaturas pendientes, tales como la activación de los cuerpos de seguridad pública para mejorar la atención sanitaria comunitaria, la capacitación, adiestramiento y certificación en la materia, el desarrollo de protocolos específicos, así como el monitoreo de salud, además de la incorporación del enfoque intercultural y de derechos humanos. Todo lo cual puede hacerse extensivo a la prevención de otras enfermedades y a la incidencia de comorbilidades, así como él diseño de políticas y la gobernanza de la seguridad a la luz de la cuestión sanitaria.

Finalmente, en su artículo "La Inteligencia para la Seguridad Nacional como Elemento de Tutela de los Derechos Humanos" Alejandro Toledo Utrera, egresado de la Especialidad en Inteligencia para la Seguridad nacional, aborda desde tres enfoques: la filosofía política, el derecho de los derechos humanos y las diferentes experiencias jurídicas derivadas de procesos y sentencias en materia de derechos humanos, las complicaciones que enfrenta la relación entre la inteligencia y los derechos humanos. Entendida como inveterado

instrumento al servicio del poder, la inteligencia se ha encontrado con situaciones que atañen a los derechos humanos que el autor documenta de manera puntual con el propósito de iluminar algunos de los factores que debe tener en cuenta la armonización de la práctica del poder con las garantías fundamentales. El artículo concluye con una referencia a la inteligencia artificial, cuya irrupción complica el panorama.

Con el deseo de que esta colección de artículos aliente la reflexión y dirija la atención a aspectos críticos de nuestra vida en comunidad, además de fortalecer las capacidades del Estado en los diversos ámbitos que se abordan, se incorpora este número al acervo de recursos académicos y de investigación que, además de la consulta, buscan propiciar en el ánimo de la comunidad INAP el interés de seguir colaborando en esta expresión del conocimiento de lo público.

Severino Cartagena Hernández

Coordinador del número

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

Policrisis y Multilateralismo fallido en el siglo XXI

María Cristina Rosas *

Síntesis

Luego del término de la Guerra fría, la escena internacional enfrenta una crisis múltiple, simultánea y en extremo compleja. A este fenómeno se le denomina "policrisis". Aunque tales crisis son diferentes por su naturaleza, el hecho es que la interacción entre ellas crea una percepción de incertidumbre, lo que acentúa las presiones que recaen sobre los gobiernos para generar soluciones. Mientras los tomadores de decisiones cuentan con menos tiempo para procesar elevados volúmenes de información en tiempos de infodemia, gobiernos e instituciones enfrentan dificultades derivadas de las preocupaciones en torno a su legitimidad y efectividad. Así, la policrisis y el deterioro del multilateralismo complican en extremo la gobernanza en el mundo de hoy.

Palabras clave: Policrisis, Multilateralismo, Incertidumbre, Riesgos Globales.

Abstract: After the end of the Cold War, the international scene faces multiple, sumultaneous and extremely complex crisis. Although these crisis are different in nature, they interact between themselves and create a perception of incertitude, thus, putting pressure on Governments to provide solutions. Today, Policy makers have less time to process large amounts of information,

* Presidenta del Centro de Análisis sobre Paz, Seguridad y Desarrollo Olof Palme A. C. Profesora e investigadora de la Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México. Su libro más reciente se titula *Desarme y seguridad internacional: la agenda olvidada* (México, Centro de Análisis e Investigación sobre Paz, Seguridad y Desarrollo Olof Palme A. C./Universidad Nacional Autónoma de México, 2024, 670 pp.). Correo electrónico: mcrosas@unam.mx Twitter: @mcrosasg. Facebook: María Cristina Rosas. Página electrónica: http://mariacristinarosas.mx ORCID: 0000-0001-9230-8502.

at a time of fake news. Governments and institutions face difficulties due to legitimacy and effectiveness concerns. Thus multiple crisis and the shortcomings of multilateralism make very difficult Global Governance in today's World.

Keywords: Policrises, Multilateralism, Uncertainty, Global risk

Introducción

Tras la conclusión de la guerra fría, en el mundo se ha acentuado un escenario de crisis múltiples, simultáneas y de gran complejidad. Las crisis, aunque distintas en su naturaleza, se retroalimentan unas a otras de manera que propician la incertidumbre en las sociedades y el reclamo hacia gobiernos e instituciones para dar una cabal respuesta a los desafíos. Dado que gobiernos e instituciones enfrentan igualmente dificultades para operar e incluso para ser vistos como actores legítimos, la percepción de complejidad y falta de rumbo se combinan para hacer muy difícil la construcción de escenarios de gestión, planeación y prevención

Estados Unidos emergió como el vencedor de la confrontación Este-Oeste, pero al paso del tiempo pareciera que ha perdido capacidades para conducir al mundo por los senderos de la prosperidad y la seguridad. Su cruzada contra el terrorismo ha tenido un alto costo con resultados a todas luces, fallidos, abriendo frentes para que prosperaran múltiples flagelos -*i. e.* además del terrorismo, la delincuencia organizada, la crisis ambiental, las epidemias y pandemias, la polarización social, el auge de la migración indocumentada, la crisis energética, las hambrunas- sin que se les pueda gestionar de manera adecuada. En Estados Unidos, el auge del nacionalismo visto en especial durante la primera administración de Donald Trump bajo la consigna de *Make America Great Again* (MAGA) o *hacer a Estados Unidos grande otra vez* ha sido replicado en diversas partes del mundo, haciendo muy difícil la cooperación internacional para enfrentar problemas que trascienden las fronteras nacionales y que, a todas luces, un sólo Estado no podrá resolver. Donald Trump está de vuelta en medio de una transición hegemónica, donde el retraimiento de la Unión Americana sugiere una ausencia de liderazgo, al menos en Occidente, que abre las puertas para que otros gestores - ¿la República Popular China? ¿Rusia? ¿ambos? o ¿los BRICS?[1]- tomen o no la estafeta, lo que genera un pronóstico reservado para el mundo.

[1] Acrónimo propuesto en 2001 por Goldman Sachs conforme a la premisa de que Brasil, Rusia, India y la República Popular China (RP China) serían las economías dominantes en las siguientes décadas. El grupo BRICS se reunió por vez primera en 2009 y en 2011 se sumó Sudáfrica para integrar el acrónimo actual. En 2023 se amplió a Emiratos Árabes Unidos, Egipto, Etiopía e Irán. Argentina también fue admitida pero el nuevo gobierno de Javier Milei declinó la invitación. Arabia Saudita también fue invitada, pero a la fecha no ha aceptado la invitación.

El fin de la guerra fría: de la certeza a la incertidumbre

Cuando la Unión Soviética dejó de existir a principios de la década de los 90 del siglo pasado, el triunfalismo emanado de la percepción de que Estados Unidos era el ganador de la guerra fría y de que no se perfilaba en el horizonte una amenaza equivalente al comunismo soviético, prevaleció al menos hasta que terminó ese decenio. Discursos como el del nuevo orden mundial de George Bush padre en noviembre de 1990, o el de Madeleine Albright quien, también en 1990 calificó sin empacho alguno a Estados Unidos como la *única nación indispensable* -frase retomada en varias ocasiones por el presidente William Clinton- (Rupérez, 27 de noviembre de 2014) se tornaron cada vez más frecuentes y dejaban entrever esa percepción de que el mundo sería "aburrido" en términos de desafíos estratégicos para la Unión Americana, como lo anticipó Francis Fukuyama, porque al final prevalecería la democracia liberal en todas partes, si bien no a un mismo tiempo (Fukuyama, 1992: 78).

> Después de la guerra fría se ha recuperado al hombre en su integridad. Esto sólo ha sido posible por el hundimiento del comunismo y el triunfo de la democracia liberal. Aunque la democracia liberal es la forma política más avanzada de la sociedad humana, ésta no está exenta de obstáculos para su implantación y permanencia. Sin embargo, al no poseer en su seno contradicciones fundamentales, está llamada a extenderse por todo el mundo. El comunismo, por el contrario, fracasó, además de ser incapaz de adaptarse a los cambios tecnológicos, por no otorgar el reconocimiento que necesitaba el individuo para sentirse satisfecho (Hueso García, s/f: 205).

Si todo había resultado como Estados Unidos quería -o como convenía a sus intereses-, entonces parecería que no había razón para preocuparse. Empero, el fin de la guerra fría dificultó dilucidar cuál era la información relevante que debía ponerse a consideración de los tomadores de decisiones: determinar qué era importante y más aún cuáles eran los flagelos por enfrentar dio pie a un *impasse* que terminó el 11 de septiembre de 2001. En ese *impasse* no ayudó la falta de claridad de los tomadores de decisiones, que mayormente tendieron a actuar de manera reactiva y con una visión de corto plazo. Otro problema más es que ante la proliferación de más y más información, muchos tomadores de decisiones encontraron difícil distinguir entre la información de calidad y veraz, y la *pseudo* información. Incluso con frecuencia se ha visto que los tomadores de decisiones han dado por sentado la fiabilidad de la información y no en pocas ocasiones han debido reconocer que "se equivocaron." Peor aún es que numerosos tomadores de decisiones han creado *noticias falsas* para fines instrumentales particulares. El lector podría pensar que el caso que mejor

ejemplifica esta situación es Donald Trump. Empero, mucho antes que él, el recurso a desinformar es una práctica de larga data, empleada en tiempos de guerra y en tiempos de paz. Se recuerda, a principios del presente siglo, cómo la administración de George W. Bush y su vicepresidente Dick Cheney se confrontaron con la comunidad de inteligencia, descalificando a la Agencia Central de Inteligencia (CIA), en ese tiempo presidida por George Tenet, debido a su "incapacidad" para encontrar armas prohibidas en Irak (Tenet, 2008; Blix, 2004; Ritter, 2009).[2] La narrativa sobre las armas de destrucción en masa que supuestamente poseía Saddam Hussein llevó a que, contra la opinión de la mayor parte de la comunidad internacional Estados Unidos, acompañado de unos cuantos aliados, incursionara en el país árabe. Por cierto, la posterior ocupación y devastación de Irak empoderó a su vecina Irán, a la vez que posibilitó el surgimiento de *Daesh* -emanado de la guardia republicana iraquí-, de manera que los errores de cálculo y de un dimensionamiento apropiado de las consecuencias geopolíticas de las acciones bélicas de Washington, pueden considerarse como parte de la explicación de la compleja crisis que aqueja a Medio Oriente en el momento actual.

> … [E]l caso de Irak pasará a la historia por ser una decisión política al margen de la información o en un claro ejemplo de acomodo informativo a los intereses políticos… las protestas por parte de los miembros de los servicios de inteligencia británicos a causa de la forma en que se presentó la información en el Reino Unido no han hecho sino avivar esta sospecha hasta convertirse en un escándalo político mayúsculo. Lo que parecían conjeturas se convirtieron en verdades demostradas una vez puestas en marcha las comisiones de investigación en Estados Unidos y el Reino Unido. Una mayor contundencia en la crítica actuación del MI6 británico en los prolegómenos de la guerra de Irak se ha visto reflejada en el informe

[2] George Tenet fue una figura central en esta crisis. Investido como director de la CIA en 1995 durante la administración Clinton, permaneció en el cargo hasta el 11 de julio de 2004, cuando presentó su renuncia por "razones personales." Tenet fue cuestionado por los ataques terroristas del 11 de septiembre de 2001, pese a lo cual, conservó el cargo. Con todo, aparentemente su postura en torno a Irak no fue bien recibida por el vicepresidente Cheney, lo que aceleró su renuncia.

Otro caso que ponderar es el del estadunidense Scott Ritter, quien fuera inspector de Naciones Unidas en Irak de 1991 a 1998 y quien criticó fuertemente la postura de E.E.U.U de hacerle la guerra a ese país. Él destacó la importancia de que hubiera mayor rendición de cuentas de parte de los servicios de inteligencia, por ejemplo, ante el Congreso, lo cual podría disminuir la discrecionalidad del presidente, del vicepresidente y de otros miembros del gabinete (Ritter, *Ibid.*). Ritter fue arrestado en varias ocasiones por cargos de pedofilia y entre 2012 y 2014 pasó año y medio en prisión en Pensilvania. Él siempre ha argumentado que estas acusaciones son represalias políticas por sus revelaciones.

> Butler (julio de 2004). Este informe elaborado por Lord Butler, John Chicot, Ann Taylor, Michael Mates y el ex jefe del estado mayor entre 1994 y 1997, Lord Inge, constituye una prueba más de la controvertida actuación o utilización del trabajo de inteligencia con fines políticos. Es curioso observar las similares conclusiones a las que se llega en estos informes dejando en una posición comprometida a la CIA y el MI6. De la lectura del informe Butler se desprende que el servicio exterior británico de inteligencia no contrastó las fuentes, sobrevaloró sin datos fiables la amenaza de las armas de destrucción en masa y fueron presentados como hechos irrefutables lo que parecían meras hipótesis a contemplar. Todos estos fueron registrados en los ya célebres *dossiers* sobre la amenaza de ataque en 45 minutos (…) El resultado fueron documentos de inteligencia sesgados, defectuosos, apresurados en su elaboración y poco fiables (Navarro Bonilla, s/f: 54).

Así las cosas, la añoranza por la guerra fría no sorprende. En los tiempos de la confrontación Este-Oeste, era relativamente sencillo anticiparse a las acciones del adversario -claro, esto visto desde Estados Unidos o la URSS. El principio de que *a toda acción corresponde una reacción* propició una moderación estratégica que se tradujo en compromisos para contener la amenaza nuclear y para librar las batallas que fuesen necesarias en otros países, es decir, *guerras proxy*. Dichos conflictos operaban como ollas de presión, liberando tensiones que evitaban ataques directos entre Washington y Moscú. Así, por ejemplo, si el Congo belga desarrollaba un movimiento de liberación nacional, se sabía que tanto E.E.U.U como la URSS y quizá el "aliado" de alguno de ellos, en este caso, Bélgica, intervendría para propiciar un resultado "favorable" a su causa. Claro que cuando terminó la guerra fría, los conflictos pasaron de la internacionalidad a ser más locales y con actores antaño ampliamente ignorados que aprovecharon la ausencia de aquellas grandes potencias para impulsar sus agendas. La hoy República Democrática del Congo -el ex Congo belga- es un polvorín, pero carece de la centralidad geopolítica de la guerra fría debido a que las potencias ahora son más selectivas y jerarquizan sus zonas de interés -*i. e.* Ucrania para Rusia; Taiwán para la RP China; Israel para E.E.U.U- en tanto el declive de algunos poderes -*i. e.* Francia en el Sahel o el Reino Unido en la Mancomunidad Británica- abre también frentes para actores como *Daesh* u otros.

Joseph Nye subrayaba que, tras el fin de la guerra fría, había tenido lugar un incremento en la relación de misterios a secretos en las cuestiones para las que los centros políticos de toma de decisiones necesitan respuesta. Un secreto, sostiene Nye, es algo concreto que puede ser sustraído y decodificado al adversario, mientras que un misterio es un rompecabezas abstracto para el que nadie puede estar seguro de tener respuestas (Nye, 2011). De ahí que la inteligencia actualmente deba analizar y anticipar, más allá de actividades

militares y/o actividades políticas, temas más complejos como el poder, las comunicaciones, el ciberespacio y la tecnología, todo ello en un entorno globalizado e interdependiente (Saavedra, November 2, 2015: 77-78).

Policrisis e incertidumbre

Justo tras el fin de la guerra fría Edgar Morin y Anne-Brigitte Kern en un libro denominado *Terre-Patrie* introdujeron el concepto de *policrisis* (Morin y Kern, 2010). Aquí los autores afirman que no existe un problema vital exclusivo, sino muchos problemas vitales, y es esta interacción y simultaneidad de problemas la que da pie a antagonismos, crisis, procesos incontrolados y la debacle general del planeta cuya existencia se encuentra en entredicho. En la actual sexta extinción masiva no debe perderse de vista que, a diferencia de las anteriores, la que el mundo enfrenta hoy es enteramente de origen antropogénico.

Morin es considerado como uno de los artífices de los planteamientos y estudios sobre la complejidad.[3]

> Desde la perspectiva del pensamiento complejo, Edgar Morin propone comprender la complejidad en términos organizacionales. Se trata de pasar de una noción de objeto esencial/sustancial a una noción de objeto relacional, es decir, de totalidades organizadas compuestas por elementos heterogéneos en interacción. La idea de organización remite así la idea de una totalidad relativa, no cerrada, sino abierta, histórica y contextualizada. Morin destaca que la organización es algo común al mundo físico, biológico y antroposocial y propone pensar la idea de organización a partir de un marco concepto que denomina bucle tetralógico, con el cual busca dar cuenta de la relación complementaria-concurrente y antagonista entre los conceptos de orden-desorden-interacciones (encuentros)-organización: "para que haya organización es preciso que haya interacciones: para que haya interacciones es preciso que haya encuentros, para que haya encuentros, es preciso que haya desorden (agitación, turbulencia) (Rodríguez Zoya y Leónidas Aguirre, 2011).

[3] Sin embargo, el concepto de *complejidad organizada* fue acuñado por Warren Weaver (1948) en un artículo publicado bajo el emblemático título "Science and Complexity" , y que puede considerarse con justicia, como una de las contribuciones fundacionales del campo, en la que se emplea por primera vez el término complejidad de modo deliberado y explícito. No es exagerado decir que, con el texto de Weaver, el 'significante' complejidad irrumpe en el vocabulario científico, lo que permitirá, décadas más tardes, dotar de identidad, a un conjunto de teorías formuladas en distintas disciplinas y ciencias. La idea de la *complejidad organizada* sugiere que lo complejo no es anárquico o caótico, sino que su existencia es necesaria ante las crisis. Una existe porque la otra existe.

Por su parte, Adam Tooze, en una reflexión similar a la de Morin y Kern pero más reciente, explica a la policrisis como una situación que acontece de cara a múltiples crisis pero también en la que el conjunto es todavía más peligroso que la suma de las partes (Tooze, 2019).

Desde la óptica de la policrisis, las crisis generan efectos que se amplifican y retroalimentan. Sin embargo, este argumento podría generar una suerte de parálisis al propiciar valoraciones no del todo adecuadas. Por ejemplo, una mirada al gráfico 1 sobre los riesgos globales para 2024, muestra las posibles interconexiones entre problemáticas de tipo económico, ambiental, geopolítico, social y tecnológico. La intención de la encuesta que año con año publica el Foro Económico Mundial y que elabora con académicos, empresarios, tomadores de decisiones y líderes de opinión, entre otros, es poner en la mesa de análisis los temas que tienen la posibilidad de influir negativamente en el curso de los acontecimientos globales. Los riesgos pueden ser altos, medios y bajos. Por ejemplo, en la categoría económica, el mayor riesgo que anticipa el Foro Económico Mundial es una recesión. Le siguen las disrupciones de infraestructuras críticas y la actividad económica ilícita. En el terreno ambiental se considera que la escasez de recursos naturales constituye el mayor riesgo. En un plano más secundario se menciona al cambio climático, a la contaminación y a la pérdida de biodiversidad. No deja de ser interesante que en el terreno tecnológico se considera que el mayor riesgo proviene de la desinformación, seguido de lejos por la inseguridad cibernética, la censura y vigilancia, la inteligencia artificial y la concentración del poder tecnológico en unas pocas manos. En el terreno geopolítico la violencia interestatal se impone a la violencia intraestatal, a los ataques terroristas, a los riesgos nucleares, químicos y biológicos y a la confrontación geoeconómica. En el terreno social se acusa a la polarización de las sociedades como el riesgo mayúsculo, por encima de la falta de oportunidades económicas, la migración involuntaria, el desempleo y las enfermedades infecciosas y crónicas.

Gráfico 1
Informe de riesgos globales en 2024

Fuente: Encuesta de Percepción de Riesgos Globales del Foro Económico Mundial 2023-2024.

Como se puede inferir, el panorama de riesgos globales del Foro Económico Global permite identificar riesgos que pueden o no interconectarse en distintas proporciones, pero el análisis debe ser más detallado.[4] Una escalada nuclear no parece que sea resultado de la contaminación o de la escasez de mano de obra. La recesión económica, no parece que dependa tanto de la desinformación o de la vulneración de los derechos humanos. La vinculación entre ataques terroristas y eventos climáticos extremos no se aprecia tan directa. La censura y vigilancia no está tan relacionada con la pérdida de biodiversidad.

Ahora bien, aun cuando a primera vista los riesgos enumerados en el gráfico 1. no se vinculen directa y claramente entre sí, la policrisis se produce de cara a la simultaneidad. Si, por ejemplo, la polarización social ocurre al mismo tiempo que la desinformación, la recesión económica y la migración involuntaria, se torna en extremo difícil dar respuesta a todos los flagelos.

[4] Este estudio del Foro Económico Mundial reúne las opiniones de casi 1 500 expertos del mundo académico, empresas, gobiernos, la comunidad internacional y la sociedad civil.

Súmese a ello la ausencia de la cooperación y el auge del nacionalismo, por lo que la gestión multilateral es endeble, con instituciones carentes de credibilidad.

Desde la óptica del Foro Económico Mundial los riesgos globales se pueden medir por impacto o bien por probabilidad. Los primeros se desarrollarían en el corto plazo, en tanto los segundos tendrían lugar en el mediano plazo. En el cuadro 1. se puede visualizar que hay algunos riesgos globales presentes tanto en el corto como en el mediano plazo, destacando los de carácter ambiental, social y tecnológicos. Empero, queda la sensación de que se tiende a privilegiar a la inmediatez sobre las causas de los riesgos globales. Llama profundamente la atención, por ejemplo, que las epidemias y pandemias ya no figuren, pese a que la globalización, la crisis ambiental, la urbanización creciente, los viajes internacionales, etcétera, coadyuvan al surgimiento y/o propagación de enfermedades cuya gestión, como se pudo observar entre 2020 y 2022 para el caso del SARS-CoV2, se torna muy difícil de cara a la ausencia de cooperación internacional, la falta de liderazgo y la crisis de las instituciones.

Crisis del multilateralismo y policrisis

Es evidente que lo que es presentado como matriz de riesgos globales por el Foro Económico Mundial y autores como Morin, Kern y Tooze, no surgió súbitamente, como tampoco es un *cisne negro.* Parte del problema en la gestión de esos riesgos globales es que se les mira en sus efectos, no en sus causas, lo que lleva a articular, en el mejor de los casos, medidas paliativas coyunturales. La desinformación, por otra parte, puede generar la percepción de *cisnes negros*. En la pandemia del SARS-CoV2, sin ir más lejos, era frecuente escuchar tanto de autoridades como de la sociedad en general que la enfermedad era inexistente o bien, que era parte de un plan para controlar a la población.

Sumado a lo anterior tómese en cuenta que los liderazgos de hoy no sólo enfrentan la disyuntiva entre la democracia y el autoritarismo. Gran parte de la narrativa se suele centrar en los peligros que entraña para el mundo el autoritarismo cuando, en los últimos años se ha podido constatar que es en las urnas donde regímenes "democráticos" como el de Trump, Bukele, Netanyahu, Modi y Milei, para citar algunos de los casos más conocidos, han sido encumbrados. Ello ha llevado a Levistky y Ziblatt a documentar la muerte de las democracias, la cual se consuma en las urnas -Hitler, sin ir más lejos, llegó al poder por el voto popular (Levitsky y Ziblatt, 2022).

Las democracias también mueren por el desprecio que personajes como los referidos y otros más tienen hacia las instituciones. Si sirven a sus intereses, las emplean, si no, las defenestran. Pero ¿por qué importan las instituciones? Para comenzar, desempeñan una amplia variedad de tareas esenciales, tanto dentro de los países como a nivel internacional. A nivel interno, posibilitan que los gobernantes gestionen y generen las condiciones que garanticen el funcionamiento óptimo de las sociedades. Son un mecanismo

de diálogo y gestión entre gobernantes y gobernados. Protegen a estos últimos de los abusos del poder. A nivel internacional, las instituciones posibilitan el desarrollo de las relaciones internacionales, mitigando las tensiones que se producen entre las naciones, evitando o reduciendo conflictos potencialmente devastadores que pudieran destruir al mundo.

Cuadro 1
Los 10 riesgos globales más importantes en los siguientes dos y 10 años

Posición	En los siguientes dos años	En los siguientes 10 años
1	Mala información y desinformación	Eventos climáticos extremos
2	Eventos climáticos extremos	Cambios críticos en los sistemas de la Tierra
3	Polarización social	Pérdida de biodiversidad y colapso de los ecosistemas
4	Ciber inseguridad	Escasez de recursos naturales
5	Conflictos armados interestatales	Mala información y desinformación
6	Falta de oportunidades económicas	Consecuencias adversas de las tecnologías con inteligencia artificial
7	Inflación	Migración involuntaria
8	Migración involuntaria	Ciber inseguridad
9	Estancamiento económico	Polarización social
10	Contaminación	Contaminación

Fuente: Foro Económico Mundial.

Douglass North, ganador del Premio Nobel de Economía en 1993, señala que las instituciones son reglas formales e informales en una sociedad y que son pensadas a efecto de regular la interacción entre individuos, ya sea a nivel político, social o económico. North, fundador de la nueva economía institucional, postula que las instituciones importan porque permiten que existan el orden, la certidumbre, el estado de derecho, un sistema de justicia imparcial, y una democracia participativa con poderes equilibrados. Las reglas formales son, por ejemplo: leyes, normas, ordenanzas; mientras que las reglas informales se refieren a la cultura, las tradiciones, los usos y las costumbres, etcétera (North, 1990).

La Red Liberal de América Latina (RELIAL) que produce el índice de calidad institucional, el cual mide qué tan cerca o tan lejos están los países de alcanzar un orden que permita que las libertades económicas y políticas de los individuos sean respetadas, reconoce que el cambio institucional -en un sentido positivo- toma tiempo. El índice, que se publica desde hace varios años, muestra casi siempre a los mismos países con mejor calidad institucional con

variaciones pequeñas en el curso de los años. En el índice correspondiente a 2024, los 10 países con mejor calidad institucional son Dinamarca, Suiza, Finlandia, Nueva Zelanda, Países Bajos, Suecia, Noruega, Luxemburgo, Irlanda y Canadá, en tanto los 10 países con la más deficiente calidad institucional son Afganistán, Somalia, Myanmar, Sudán del Sur, Sudán, Eritrea, Venezuela, Siria, Yemen y Corea del Norte -México figura en la 96ª posición entre 183 países evaluados en tanto E.E.U.U está en el 18º lugar (Krause, 2024).

Gráfico 2
La buena calidad de las instituciones produce un círculo virtuoso

Fuente: Banco de España.

El Premio Nobel de Economía en 2024 ha sido otorgado a los profesores Daron Acemoglu, Simon Johnson y James A. Robinson, por sus estudios sobre cómo las instituciones económicas y políticas se desarrollan y determinan la prosperidad de las naciones y la desigualdad entre ellas. Estos autores son conocidos por documentar el fracaso de las naciones (Acemoglu y Robinson, 2013). Este galardón reviste enorme importancia en momentos en que la calidad institucional parece estancarse en un creciente número de países (Alberola y Sanz, 14/10/2024).

La aportación de Acemoglu, Johnson y Robinson es que en sus análisis plantean, en esencia, que los países fracasan por la mala calidad de sus instituciones. Al respecto, en un análisis histórico acerca de la colonización

europea a partir del siglo XVI comparan los modelos de colonización y su impacto en el desarrollo económico. Así, caracterizan dos tipos de instituciones, a saber:

- Las instituciones inclusivas, que se fundamentan en el respeto al estado de derecho, y que suelen estar asociadas a sociedades democráticas. En estas instituciones, las élites apoyan que las personas alcancen sus objetivos económicos y sociales y las personas, de su lado, participan, exigen y ejercen sus derechos. De este modo, este tipo de institución incentiva los comportamientos que facilitan el buen funcionamiento de la economía, la creación de riqueza y el desarrollo de la sociedad civil. Y una sociedad civil fuerte demanda mejores instituciones, con lo que se genera un círculo virtuoso de crecimiento económico, progreso social y mejora continua de las instituciones.

- Las instituciones extractivas, donde se suprimen derechos básicos y no hay seguridad jurídica. Aunque son más comunes en regímenes autocráticos, también pueden estar presentes en democracias. En este caso, las élites dilapidan y se apropian de los recursos del resto de la sociedad para su propio beneficio. Este contexto limita el incentivo de la sociedad para generar riqueza, emprender e innovar y menoscaba el desarrollo social además de que fractura, divide y polariza. En lugar de incentivar la participación lleva a evadir la ley y el orden y fortalece a la delincuencia organizada y a las "actividades sombra" al margen de la licitud (Acemoglu y Robinson, *Ibid.*).

¿Y en el terreno multilateral? El deterioro vivido por las instituciones en muchos de los países del mundo contribuiría a explicar, al menos en parte, la crisis del multilateralismo, el cual depende de la voluntad política de los miembros de la comunidad internacional para llegar a buen puerto en las tareas que se les encomiendan. Las instituciones multilaterales, al final del día, son lo que sus miembros desean que sean. Posiblemente el caso más ilustrativo de una institución multilateral en crisis sea la Organización de las Naciones Unidas (ONU), la cual cumplirá, en 2025, ocho décadas de existencia. Si bien la ONU fue creada tras uno de los conflictos armados más devastadores en la historia moderna, y se propuso objetivos loables y cruciales -i. e. mantener la paz y la seguridad internacional, promover el desarrollo y garantizar el disfrute y promoción de los derechos humanos- la encomienda no ha sido cumplida o lo ha sido parcialmente.

Es frecuente que se mencione a la crisis del multilateralismo como explicación respecto a las tareas aun inconclusas de la ONU, cuyos éxitos en diversas esferas, simplemente no llegan a los titulares de los medios de comunicación. Hay que partir también de que los éxitos no son noticia, además

de que siempre es preferible culpar a alguien por los problemas existentes y la ONU se ha convertido así, en un objetivo de ataque, menosprecio y denostación, amén de que se insiste en que su mantenimiento es costoso y su burocracia ineficiente. Pero ¿es la ONU una institución de *buena calidad*? Hay cosas que deberían cambiar, pero también se debería reforzar aquello que funciona. Por otro lado, con un presupuesto tan reducido para cumplir con las tareas encomendadas hoy muchos programas, organismos especializados y agendas de Naciones Unidas dependen mayormente de la filantropía, donaciones y recursos aportados por el sector privado, lo cual tiene un efecto no necesariamente positivo en la institución. Por ejemplo, si para un magnate es fundamental que la Organización Mundial de la Salud (OMS) combata la tuberculosis, y, para ello, entrega recursos importantes para ese fin, el riesgo es que el tratamiento integral de la salud se ve comprometido porque la OMS deberá complacer al donante asigna fondos contra la tuberculosis, no así a otras enfermedades, tanto las crónico-degenerativas como las infecciosas. En el ejemplo señalado, la dependencia hacia donaciones, el sector privado y la filantropía tienen lugar porque los Estados miembros de la ONU no cumplen con sus obligaciones financieras -el caso más conocido es el de Estados Unidos, responsable del 22 % del presupuesto total de Naciones Unidas. Por otra parte, la reforma de la ONU ahora es reclamada también por los actores no estatales, dado que, si contribuyen financieramente a los programas de la institución, desearían tener capacidad decisoria en el organismo multilateral más importante del orbe.

Gráfico 3

La crisis del multilateralismo es multifactorial y obedece no sólo a fallos que la ONU ciertamente tiene, sino sobre todo a que los países han optado por tomar decisiones al margen de la institución. En ello tiene que ver el ya citado

nacionalismo rampante, y el rechazo a que los conflictos sean gestionados globalmente, sea mediante sanciones, operaciones de mantenimiento de la paz o el uso de la fuerza. Siempre se ha cuestionado, por ejemplo, la composición del Consejo de Seguridad de Naciones Unidas, cuyos miembros permanentes tienen prerrogativas que los miembros electos no poseen. La parálisis del Consejo de Seguridad ante la guerra de Rusia contra Ucrania -donde el primero veta cualquier posible resolución sobre el tema- o de cara a las acciones de Israel en la Franja de Gaza -donde Estados Unidos objeta cualquier medida contra su estratégico aliado-, ilustran esa parálisis, si bien la cantidad de resoluciones aprobadas por el Consejo en torno a una amplia variedad de temas debería ser difundida. El Consejo decide sobre sanciones a países y regímenes; decide la continuación o el fin de las misiones de paz desplegadas en el mundo; sugiere acciones en torno a temas tan diversos como epidemias y pandemias, mujeres y violencia, cultura de paz, construcción y consolidación de la paz, la asistencia humanitaria, los objetivos de desarrollo sostenible, y junto con la Asamblea General, el Secretario General, la Corte Internacional de Justicia y el Consejo Económico y Social aborda prácticamente la totalidad de tópicos que son del interés no sólo de sus 193 miembros, sino de actores no gubernamentales como la sociedad civil, corporaciones, etcétera. Agendas como la seguridad humana, la ambiental, mujeres y niños, telecomunicaciones, salud, derechos de los trabajadores, la alimentación, el espacio ultraterrestre, el desarme, el desarrollo, los derechos humanos, etcétera, son sólo algunas que son desarrolladas en el seno de la ONU. Para ello se requiere no sólo el voluntarismo o el querer hacer, sino también recursos financieros que algunas naciones regatean a la institución.

Consideraciones finales

Las narrativas sobre la policrisis acaparan en estos momentos la atención de las comunidades académicas y políticas, y si bien ayudan a visualizar las agendas globales, su principal desafío radica en que podrían coadyuvar a la parálisis al generar un desánimo ante *problemas tan variados* que además son *demasiado complejos*.

Si bien desde los estudios de la complejidad se cuenta con herramientas para abordar el estudio de fenómenos complejos como la auto-organización, la emergencia, la no-linealidad, etcétera, la abstracción de riesgos a los que no se mira en sus causas es, para decir lo menos, peligroso. Sugerir, como hace el planteamiento de la policrisis, premisas supuestamente neutrales, dejando la responsabilidad ética, social y humana de su aplicación a tomadores de decisiones cada vez más preocupados por el corto plazo y el beneficio personal o de los grupos de poder a los que pertenecen, no es apropiado.

La respuesta a los flagelos del mundo de hoy parecen reposar más en la identificación de las causas de los conflictos y del trabajo permanente, más allá de los ciclos de gobiernos y/o las coyunturas políticas, todo ello inmerso en un proyecto o proyectos de nación. El multilateralismo, por su parte, puede ser un valioso instrumento para estimular tanto el debate como la cooperación internacional, por lo que su importancia es hoy mayor que nunca. Superar las narrativas catastrofistas que convocan a la parálisis, sólo podrá empeorar las cosas.

Bibliografía

Acemoglu, Daron y James A. Robinson 82013), *Why Nations Fail. The Origins of Power, Prosperity and Power,* New York, Crown Currency.

Alberola, Enrique y Carlos Sanz (14/10/2024), *Premio Nobel 2024: la calidad de las instituciones potencia el crecimiento económico,* Madrid, Banco de España, disponible en https://www.bde.es/wbe/es/noticias-eventos/blog/premio-nobel-economia-2024.html

Blix, Hans (2004), *Disarming Iraq,* New York, Pantheon Books.

Fukuyama, Francis (1992), *The End of History and the last man,* New York, Free Press.

Hueso García, Vicente (s/f), *Francis Fukuyama. El fin de la historia y el último hombre. Una visión optimista de la evolución de la historia,* disponible en https://dialnet.unirioja.es/descarga/articulo/4553618.pdf

Krause, Martín (2024), *Índice de calidad institucional 2024,* Red Liberal de América Latina, disponible en https://relial.org/wp-content/uploads/2024/07/ICI-2024_web.pdf

Levitsky, Daniel y Steven Ziblatt (2022), *Cómo mueren las democracias,* Madrid, Paidós.

Mizrahi, Ilan (2016), "Strategic Intelligence Challenges in the 21st Century", en Shashi Jayakumar (Editor), *State, Society and National Security. Challenges and Opportunities in the 21st Century,* Singapore, World Scientific.

Morin, Edgar y Anne-Brigitte Kern (2010), *Terre-Patrie,* Paris, Points.

Navarro Bonilla (s/f), *El ciclo de inteligencia y sus límites,* Madrid, Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol no. 48, disponible en https://dialnet.unirioja.es/descarga/articulo/2270935.pdf

North, Douglass C. (1990), *Institutions, Institutional Change and Economic Performance,* Cambridge, Cambridge University Press.

Nye Jr., Joseph S. (2011), *The Future of Power,* New York, Public Affairs.

Ritter, Scott (2009), *Iraq Confidential. The Untold Story of America's Intelligence Conspiracy,* New York, I. B. Tauris.

Rodríguez Zoya, Leonardo G. y Julio Leónidas Aguirre (2011), "Teorías de la complejidad y ciencia sociales. Nuevas estrategias epistemológicas y metodológicas", en *Nómadas. Critical Journal of Social and Judicial Sciences,* vo. 30, núm 2, disponible en https://www.redalyc.org/pdf/181/18120143010.pdf

Rosas, María Cristina (2020), "Cultura, patrimonio y seguridad", en María Cristina Rosas (ccordinadora), *La seguridad extraviada. Apuntes sobre la seguridad nacional de México en el siglo XXI,* México, Universidad Nacional Autónoma de México, Centro de Análisis e Investigación sobre Paz, Seguridad y Desarrollo Olof Palme A. C.

Rucker, Phillip y Robert Costa (Septiembre 10, 2020), "Trump sabía que el virus era 'mortal' y peor que la gripe, y engañó intencionalmente a los estadunidenses, según el nuevo libro de Bob Woodward", en *The Washington Post,* disponible en https://www.washingtonpost.com/es/politics/2020/09/10/trump-sabia-que-el-coronavirus-era-mortal-y-peor-que-la-gripe-y-engao-intencionalmente-los-estadounidenses-segun-nuevo-libro-de-bob-woodward/

Rupérez, Javier (27 de noviembre de 2014), "Los Estados Unidos de América: ¿todavía la nación indispensable?", en *Nueva Revista,* disponible en https://www.nuevarevista.net/cultura-comunicacion/los-estados-unidos-de-america-todavia-la-nacion-indispensable/

Saavedra, Boris (noviembre 2 de 2015), *Inteligencia estratégica en un mundo globalizado en Latinoamérica: retos y desafíos en el siglo XXI,* Washington D. C., Universidad Nacional de la Defensa, disponible en https://www.lamjol.info/index.php/RPSP/article/view/2326/2103

Tenet, George (2008), *At the Center of the Storm,* New York, Harper Perennial.

The Henry L. Stimson Center (2008), *New Information and Intelligence Needs in the 21st Century Threat Environment,* Washington D. C., The Henry L. Stimson Center, disponible en https://www.stimson.org/wp-content/files/file-attachments/SEMA-DHS_FINAL_1.pdf

Tooze, Adam (2019), *Crashed. How a Decade of Financial Crisis Changed the World,* New York, Penguin Books.

Ugarte, José Manuel (julio-agosto 2019), *Desarrollo, situación y probable evolución de la inteligencia criminal en Latinoamérica,* ponencia presentada en el X Congreso Latinoamericano de Ciencia Política, disponible en https://alacip.org/cong19/285-ugarte-19.pdf

Viamonte, Yoan Israel (5 de noviembre de 2017), "La inteligencia científico-tecnológica para el desarrollo y la seguridad geoeconómica latinoamericana", en *Revista FLACSO Andes,* disponible en https://revistas.flacsoandes.edu.ec/urvio/article/download/2850/2097?inline=1

Woodward, Bod (2020), *Rage,* New York, Simon & Schuster.

World Economic Forum (2024), *The Global Risk Report 2024,* Geneva, Zurich Insurance Group, disponible en https://es.weforum.org/stories/2024/01/informe-sobre-riesgos-globales-2024-los-riesgos-aumentan-pero-tambien-nuestra-capacidad-de-respuesta/

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

Claves del Análisis Criminal en México

Mario Vignettes*

Resumen: Bajo la premisa de que toda inteligencia surge del análisis, el presente ensayo explora la figura del analista criminal tal cual está descrita en la normatividad federal vigente. Con esa base, se define un catálogo básico de productos analíticos. También se proponen algunas definiciones centrales al tema abordado.

Palabras clave: Amenaza a la seguridad pública, análisis criminal estratégico, análisis criminal táctico, estándar de competencia, política de Estado.

Abstract: Under the premise that all intelligence arises from analysis, this essay explores the figure of the criminal analyst as described in current federal regulations. With this basis, it defines a basic catalog of analytical products. Some central definitions of the topic addressed are also proposed.

Keywords: Public security threat, strategic criminal analysis, tactical criminal analysis, competency standard, state public policy.

1. Enfoque y alcance

* Doctor en Derecho (2004) y profesor de la Facultad de Derecho de la Universidad Nacional Autónoma de México. Autor de artículos académicos sobre inteligencia publicados en revistas arbitradas de México, Argentina, Colombia, España y el Reino Unido. Practicante de inteligencia para la seguridad nacional durante 24 años. Consultor independiente.

La presente contribución enfatiza la importancia cardinal del análisis criminal para la Estrategia Nacional de Seguridad Pública5. Se estudian las atribuciones y facultades que definen su función, ahí donde la normatividad vigente regula esta figura. Especial atención reciben los productos de análisis establecidos por las normas aplicables, sean de corte estratégico o táctico.

La seguridad pública debe entenderse como el resultado (output) de múltiples procesos coordinados en un sistema. Ese sistema existe en México y se denomina «Sistema Nacional de Seguridad Pública». El anunciado sistema único de inteligencia, en el mejor de los casos, será un componente del Sistema referido como está descrito en su ley general6. De manera esquemática, el análisis criminal se organiza en táctico y estratégico. Para efectos de este ensayo, se proponen las siguientes definiciones:

Análisis Criminal Táctico: Es la delimitación y estudio de las características fundamentales de hechos criminales concretos y recientes, con el objeto de: a) generar hipótesis, estimaciones o pronósticos; b) aportar elementos de conciencia situacional7 en cualquier ambiente operativo8, c) proponer acciones policiales o penitenciarias de proximidad social, prevención y de reacción; d) establecer líneas de investigación de un hecho delictivo concreto; e) apoyar la definición de planes de investigación y la ejecución de actos de investigación y; f) definir teorías de caso, y g) proponer a fiscales, argumentos para probar hechos en un litigio penal.

Análisis Criminal Estratégico: Es la delimitación y estudio de las características fundamentales de fenómenos criminógenos9, así como categorías de delitos, con el objeto de: a) generar hipótesis, estimaciones o pronósticos; b) delimitar tendencias criminógenas; c) identificar causas evidentes y subyacentes de la dinámica criminal en comunidades, territorios y lapsos determinados; d) sugerir vías para explotar las debilidades de las organizaciones delictivas, a partir de las fortalezas de las estructuras policiales, ministeriales y penitenciarias; e) recomendar formas de acotar las debilidades de las instituciones policiales, ministeriales y penitenciarias al considerar las fortalezas de las organizaciones delictivas; f) generar agendas para fortalecer

---

5 Artículo 74 fracción XI de la Constitución Política de los Estados Unidos Mexicanos (CPEUM).

6 Ley General del Sistema Nacional de Seguridad Pública, DOF 02 de enero de 2009, en adelante LGSNSP.

7 Según el Protocolo de Investigación adoptado como anexo I en el Acuerdo 08/XLIX/2023 del Consejo Nacional de Seguridad Pública, conciencia situacional es «La capacidad de percibir y procesar posibles amenazas en el entorno». Publicado en el Diario Oficial de la Federación el 22 de diciembre de 2023.

8 Rural, semi rural, urbano y penitenciario.

9 Pueden ser de naturaleza socioeconómica, política o tecnológica, etc.

estructuralmente las funciones de proximidad social, reacción, prevención e investigación del delito y reinserción social, g) proponer conceptos estratégicos para ser incorporados a programas y estrategias, y h) evaluar los resultados intermedios de programas y estrategias, en todas las funciones propias de la seguridad pública.

2. La persona analista criminal en el Derecho Positivo Mexicano

Conviene ahora delimitar la seguridad pública según el marco normativo vigente, porque ese es el ámbito de las decisiones y acciones que debe apoyar el analista criminal. Siguiendo al artículo 21 de la Carta Magna, el servicio de seguridad pública se presta por estructuras de los tres niveles de gobierno. Lógicamente, el analista criminal debería estar presente a nivel municipal, estatal y federal. Debiese también generar productos de corte estratégico y táctico para apoyar todas las aristas de la seguridad pública. Esta última afirmación encuentra fundamento en el artículo 3º de la LGSNSP (Ley General del Sistema Nacional de Seguridad Pública), cuando señala que la seguridad pública:

> …se realizará en los diversos ámbitos de competencia por conducto de las Instituciones Policiales, de Procuración de Justicia, de las instancias encargadas de aplicar las infracciones administrativas, de la supervisión de medidas cautelares, de suspensión condicional del procedimiento de los responsables de la prisión preventiva y ejecución de penas…

A pesar de lo anterior, la realidad nacional es otra. En el ámbito ministerial, la persona analista criminal es la última en integrarse a la «tetralogía de la investigación» conformada también por policías, fiscales y peritos. Ello explica su insuficiente regulación a nivel estatal. En efecto, únicamente Baja California, Campeche, Durango, Quintana Roo y Yucatán omiten esta figura10. La regulación de las Unidades de Análisis en las Leyes Orgánicas y Reglamentos de las Fiscalías Estatales es un avance en la consolidación de la figura estudiada. Empero, hay mucho que hacer para homologar las funciones de estas unidades, así como las competencias de las personas analistas criminales en nuestro país.

---

[10] INEGI (2024), «Comunicado de prensa número 603/24» **consultado el 21 de octubre de 2024, disponible en:** https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2024/EAP_diaMP.pdf. El universo es de 75,444 trabajadores en las agencias y fiscalías del MP en el país, de los cuales el 77.9% atienden delitos estatales, es decir, 58 785 personas. Este documento refiere «analistas de información criminal» dentro de la categoría «otra función» junto con personal directivo y facilitadores. Ello justifica indirectamente este ensayo, cuyo objetivo es visibilizar y revalorar esta función cardinal en la seguridad pública.

En el ámbito policial o de la reinserción social, el analista criminal es la última figura en ser incorporada. Empero, las personas en esas funciones que ya trabajan a nivel estatal y federal lo hacen con plazas de peritos, policías o auxiliares, porque el arreglo administrativo aun no reconoce ese puesto funcional. Ello los coloca en un estado de fragilidad administrativa y laboral inaceptable, además reñido con el marco jurídico que los rige.

En ese orden de ideas, dado el grado de impunidad que priva en México11, es imprescindible incorporar el análisis criminal a la operación cotidiana de cuerpos de policía, de secretarías de seguridad pública y al sistema penitenciario nacional. Las conferencias nacionales de secretarios de Seguridad Pública Estatal y del Sistema Penitenciario tienen las atribuciones para lograrlo, con base en los artículos 29 y 31 respectivamente de la LGSNSP.

Si bien es recomendable el examen exhaustivo de las atribuciones y facultades del analista criminal en las 27 legislaciones estatales que lo prevén; este ensayo se enfoca en estudiar solo la legislación federal, como muestra representativa. En ese sentido, las diecisiete fracciones del artículo 45 de la Ley de la Fiscalía General de la República (LFGR) se agrupan para su comentario en cinco núcleos funcionales: a) recolección de información; b) administración de información; c) análisis; d) control y supervisión; e) desarrollo y capacitación.

2.1. Atribuciones de recolección de información

Según la fracción XIII del artículo 45 de la LFGR, la persona analista criminal debe,

> …Contribuir en la captación, recuperación, control, análisis y compilación de información delincuencial, así como para la estandarización de procesos de trabajo y la elaboración de bases de colaboración con instituciones públicas y privadas…

Esta fracción agrupa tres tareas distintas. La primera, es propiamente la labor de recolección de información delincuencial, lo cual es correcto y complementario a la labor de policías de investigación, peritos y fiscales. Empero, es un error incluir el «análisis» aquí, toda vez que para ello el mismo numeral incluye siete fracciones, como se verá en el punto 2.3.

La «estandarización de procesos de trabajo», por otra parte, es una tarea de orden metodológico-administrativo que no corresponde a un analista ni por

11 Estimaciones independientes lo sitúan en el 96.3%, véase México Evalúa (2023), «Justicia, sólo en 4 de cada 100 delitos que son investigados», consultado el 01 de octubre de 2024, disponible en: https://www.mexicoevalua.org/justicia-solo-en-4-de-cada-100-delitos-que-son-investigados/.

jerarquía ni función, sino al titular de la Fiscalía General de la República según la fracción IX del artículo 19 de la LFGR.

Algo parecido debe argumentarse de la tercera tarea, es decir, la «elaboración de bases de colaboración». Corresponde al titular de la FGR conforme a la fracción XV del numeral recientemente citado que prevé la colaboración institucional nacional y en la fracción XVI la internacional.

2.2. Atribuciones de administración de información

De conformidad con las fracciones VII, X y XV del artículo 45 de la LFGR, el analista criminal debe,

> …Implementar y administrar bancos de datos y sistemas de información delincuencial que permitan la consulta, integración y clasificación adecuada de los elementos que fortalezcan las investigaciones, así como la investigación y persecución de delitos; …Alimentar y actualizar los bancos de datos y sistemas de información delincuencial; …Enviar la información que corresponda a las bases de datos de los Sistemas Nacional y Estatal de Seguridad Pública…

Las tareas señaladas son de una importancia cardinal en términos institucionales en particular y para el funcionamiento del Sistema Nacional de Seguridad Pública, en los términos de la fracción IX del artículo 7º de la LGSNSP. La alimentación diaria y verificada de datos a esos bancos, registros y sistemas es uno de los insumos de la generación de inteligencia policial o ministerial.

2.3. Atribuciones analíticas

Éstas se describen en las fracciones I, II, III, V, VI, IX y XVII del artículo 45 de la LFGR ya citado. Así, la persona analista criminal debe,

> …Realizar el análisis de información estratégica, a través de la elaboración de productos de inteligencia que permita a las personas agentes del Ministerio Público de la Federación contar con elementos de información integral para una efectiva integración de los indicios, datos y medios de prueba suficientes que fortalezcan las investigaciones a cargo de la Institución…

La redacción de la fracción I es deplorable. En primer término, lo «estratégico» es el análisis y no la información. En segundo lugar, la locución «contar con elementos de información integral» hace pensar erróneamente que el análisis criminal no aporta nada. Hubiese sido más técnico señalar «contar con hipótesis» porque ese es el meollo del esfuerzo analítico en todos los ámbitos donde se produce inteligencia. Por otra parte, el éxito de una investigación

ministerial es conformar y defender en juicio la «teoría del caso» que no es otra cosa que la hipótesis mejor apoyada en la evidencia recopilada.

> …Analizar los contenidos de los expedientes de las investigaciones para sugerir líneas de investigación para el esclarecimiento de los hechos y la probable autoría o participación de las personas…

La redacción de la fracción II es práctica. Es acertado consignar «expedientes de las investigaciones» y no carpetas de investigación, porque estás últimas cumplen requisitos formales para poderlas compartir con víctimas, presuntos responsables y sus representantes, así como para su presentación formal en juicio. La persona analista criminal trabaja «tras bambalinas» por así decirlo, con los elementos de información de toda fuente, que luego de su procesamiento podrían llegar a integrarse a una carpeta de investigación en calidad de «antecedente de investigación»; es decir, «todo registro incorporado en la carpeta de investigación que sirve de sustento para aportar datos de prueba».12

> …Realizar análisis de contexto sobre fenómenos criminales, reiterados o emergentes para contribuir a la política de persecución penal…

La fracción III refiere a una clase específica de productos de corte estratégico que se comenta en el punto 3.2. Empero, se debe enfatizar la referencia a la «política de persecución penal» que se interpreta en este ensayo como los criterios prácticos, generales y permanentes para presentar en un juicio específico (persecución penal) una teoría del caso (investigación del delito) que explique un hecho criminal en términos de intención, medios y oportunidad.

> …Realizar reportes estratégicos sobre criminalidad nacional, trasnacional o internacional a efecto de identificar patrones, estructuras, organizaciones, modos de operación, así como cualquier otra información que se considere necesaria, oportuna o útil para la formulación, seguimiento, evaluación y replanteamiento del Plan Estratégico de Procuración de Justicia y la investigación de los delitos…

La fracción V que se transcribe, identifica una clase específica de producto analítico que se asocia al Plan Estratégico institucional a que se refiere el párrafo primero del artículo 88 de la LFGR. La evolución de las metodologías y de los avances tecnológicos aplicados al procesamiento de información cruda es permanente. Si México va a adoptar aplicaciones de Inteligencia Artificial

12 Artículo 260 del Código Nacional de Procedimientos Penales (CNPP).

generativa a la seguridad pública como ya lo hacen en otras latitudes13, lo hará únicamente apoyado en su fuerza de tarea analítica, así como en las bases de datos actualizadas que ya están previstas en el marco normativo vigente14.

> …Analizar la información derivada de los sistemas de comunicación inherente a las investigaciones relacionadas con delitos cometidos por organizaciones delictivas…

La fracción VI se enfoca en una fuente técnica explotada mediante el acto de investigación denominado «intervención de comunicación privada», regulada prolijamente en México.15 Es importante someter esa información a análisis, porque de esa forma se acotan sesgos y errores de la que adolece toda la información cruda que viene de las tareas de recolección. Sin análisis apropiado, la información de esta fuente tiene utilidad táctica a un alto costo de seguridad operativa y nula aplicación estratégica.

> …Clasificar la información, así como integrar fichas técnicas y elaborar mapas delincuenciales para la compilación de datos de carácter sensible que permitan vincular e integrar los indicios existentes que fortalezcan las investigaciones…

La fracción IX hace referencia a etapas intermedias del procesamiento como lo son la compilación y clasificación de información. Menciona productos «intermedios» como fichas y mapas, que suelen ser anexos a productos analíticos sofisticados. Es lamentable que omita el análisis cronológico expresado en «líneas de tiempo», el análisis de asociación que se concreta en «redes de vínculos», o el análisis decisional que sustenta «árboles de decisiones». Todas ellas, técnicas de uso generalizado en otros países y útiles en el esclarecimiento de hechos concretos.

---

13 Guo Jun y Zhang Xiaomin (2024), «*'AI police' improve rate of solving crime*», *China Daily*, 23 de octubre, consultado el 25 de octubre de 2024, disponible en: https://www.chinadaily.com.cn/a/202410/23/WS6718580ca310f1265a1c9146.html

14 Entre otros: Banco de Datos de Órdenes de Protección, Base de Datos de las Operaciones del Centro Federal de Protección a Personas, Base Nacional de Datos sobre Casos de Violencia contra las Mujeres, Base Nacional de Información Genética, Registro Nacional de Personal de Seguridad Pública, Registro Nacional de Personas Desaparecidas y No Localizadas, Registro Nacional de Personas Fallecidas No Identificadas y No Reclamadas, Registro Nacional de Prestadores de Servicios de Seguridad Privada, Registro Nacional de Víctimas, Registro Público Vehicular, Sistema de Información Criminal, Sistema Estadístico Nacional de Procuración de Justicia, Sistema Informático Nacional Interoperable, Sistema Nacional de Información Estadística Penitenciaria.

15 Artículo 16 párrafos décimo tercero y décimo quinto de la CPEUM; artículos 252 fracción III, 291 párrafo primero, 293 y 299 del CNPP; párrafo primero del artículo 28 de la Ley Federal contra la Delincuencia Organizada (LFCDO); fracciones XVI a XIX, XXVI y XXVIII del artículo 161 del Estatuto Orgánico de la Fiscalía General de la República (EOFGR), entre otros.

> …Las demás que determinen las disposiciones aplicables, las que deberán ser compatibles con las atribuciones constitucionales y legales de la Fiscalía General…

La fracción XVII permite vincular este apartado con los puntos 3.1 y 3.2 que identifican productos analíticos mencionados en los materiales legales consultados.

Una observación común a todas las fracciones que expresan atribuciones y facultades de corte analítico es que ninguna hace mención del plan de investigación, lo cual es un error importante. «Los planes de investigación enunciarán las diligencias, actos o técnicas de investigación e intervenciones periciales estrictamente necesarias para el esclarecimiento de los hechos que la ley señale como delitos»16. El plan debe modificarse o actualizarse de conformidad con el avance logrado en la investigación inicial o complementaria.

Su elaboración no es opcional. Es una tarea necesaria para el éxito de una investigación criminal profesional. Si bien elaborar un plan de investigación es tarea del fiscal que debe cumplimentar en las primeras 48 horas siguientes al inicio de la carpeta de investigación17, el analista criminal puede asistirlo en su elaboración y en su actualización, máxime en investigaciones de casos complejos que pueden durar meses. Éste se beneficia del conocimiento del plan porque así tendrá conciencia de las fuentes de información que se tocarán, y con ello conformará un «marco referencial» útil para evaluar y contrastar datos derivados de la información cruda, recopilada vía actos de investigación programados en el plan. En esta línea de pensamiento, el «Protocolo de Investigación» vigente señala en su punto 3.2.9:

> Para garantizar que se realicen investigaciones centradas y de buena calidad, los supervisores deben asignar las investigaciones adecuadamente, estableciendo y acordando un plan de investigación claro…18.

Entonces, el apoyo del analista criminal al fiscal no debe ser discrecional y episódico, sino permanente. El plan debe ser revisado de forma programada mediante supervis de coordinación19. Es prudente que el analista criminal asignado al caso se integre siempre a dichas supervis.

2.4. Atribuciones de control y supervision

16 Artículo 217 del EOFGR.
17 Fracción XV del artículo 223 del EOFGR.
18 Véase el Protocolo de Investigación citado en la nota 4.
19 Artículo 219 del EOFGR.

Por su parte, las fracciones IV, VIII, XI y XII del artículo 45 de la LFGR, señalan que la persona analista criminal debe,

> …Llevar el control y seguimiento de resultados del análisis de la información con el fin de establecer el vínculo correcto de las investigaciones relacionadas con organizaciones delictivas…

La fracción IV se refiere a un necesario trabajo de correlación entre casos diversos seguidos en contra de una misma organización delictiva o de un indiciado en particular. Ello, con la pretensión de que los resultados de dichas correlaciones sirvan a los fiscales asignados para tener un contexto cada vez más amplio de la evolución de actores y estructuras delictivas. Es una tarea de análisis táctico, pero con el tiempo debe ofrecer valiosos hallazgos de corte estratégico.

> …Efectuar el mantenimiento y control documental de los bancos de datos y de los sistemas de información delincuencial para generar y procesar información relacionada con las investigaciones y persecución de delitos…

Esta fracción refiere una labor elemental pero valiosa, usualmente asignada a los analistas más jóvenes. Así, comprenderán la estructura lógica de los bancos de datos que alimenten y los criterios para integrar o no datos a dichos bancos. Es errónea la redacción cuando asume que un banco de datos «genera información» (sic). Todo lo contrario. Con base en los datos que constituyen el banco, el analista criminal debe generar conjeturas, convertirlas en hipótesis, verificarlas20 y derivar de ello una ventaja[21].

> …Registrar los casos en que se haya optado por alguna de las vías de solución alterna de conflictos… [y] Llevar el control de la información sensible almacenada en el banco de datos, así como en otros medios de acuerdo con las políticas establecidas…

Las labores de estas últimas fracciones son más administrativas que analíticas. Empero, pueden dar pauta de las estrategias de litigación de los abogados defensores de los indiciados y revelar circuitos de apoyo e influencia entre ambos conjuntos de personas. Sirve también a la correcta clasificación de datos bajo los criterios de la normatividad federal de transparencia y acceso a la información vigente. Clasificación con implicaciones de contrainteligencia, ya

[20] En realidad, «falsearlas» en la terminología de Popper. Para una explicación asequible, véase Popper, Karl (2005), Conocimiento Objetivo, 4ª ed., Tecnos, Madrid, p. 83; y Bunge, Mario (1999), Buscar la Filosofía en las Ciencias Sociales, Siglo XXI, México, p. 133.

[21] Vignettes Del Olmo, Mario, (2022) «Ventaja Legítima en el Análisis de Inteligencia», Revista de Inteligencia y Seguridad, Instituto Nacional de Administración Pública A.C., No. 1, ps. 29 a 49.

que debe servir para reforzar las medidas de seguridad física y cibernética que prevengan filtraciones.

2.5. Atribuciones de Desarrollo y capacitación

Finalmente, pero no menos importante, las fracciones XIV y XVI del artículo 45 de la LFGR asignan al analista criminal lo siguiente,

> …Colaborar en el diseño de metodologías para la custodia, seguridad y análisis de información ministerial relacionada con cateos y aseguramientos de bienes relacionados con las investigaciones… Apoyar en la elaboración de metodologías que permitan la consulta de bases de datos nacionales e internacionales para la obtención y vinculación de información criminal o delincuencial…

Es acertado involucrar a los analistas criminales en el diseño y evolución de metodologías. Desafortunadamente, se quedan cortas en señalar el universo al que puede contribuir el analista. Se mejorará el desempeño de las fiscalías, cuando los analistas criminales aporten perfiles de víctimas, perfiles de autores materiales e intelectuales, perfil de entorno, criterios para analizar tatuajes, «narcomantas», grafitis, redes sociales y otras fuentes abiertas, etc. y cuando se sistematice todo ello en banco de datos accesibles desde cualquier punto de la geografía nacional.

3. Productos de Inteligencia Criminal

Este apartado identifica productos analíticos nombrados expresamente en la normatividad vigente. Para su comentario se agrupan en tácticos y estratégicos. Se asume aquí que toda unidad analítica debería poder generar, al menos, el siguiente elenco de productos.

3.1. Productos de corte táctico

Análisis de contexto[22]: Evalúa la información recolectada de forma preliminar relacionada con un hecho delictivo en particular, para determinar las circunstancias específicas que rodearon el evento o fenómeno. De ahí su carácter retrospectivo y táctico. Pero tienen la finalidad primordial de apoyar la formación de «planes de investigación congruentes» para que se coordinen «equipos o unidades de investigación y litigación» que continúen y concluyan la investigación complementaria. Es un acierto hacer depender la ejecución de los actos de investigación de un análisis de contexto. Ello ahorra recursos materiales y humanos, acota el lapso de investigación y, lo más importante,

[22] Artículo 29, Ley de la Fiscalía General de la República (LFGR).

ordena y focaliza el ejercicio de atribuciones y facultades que ejercerán policías, peritos y fiscales.[23]

Análisis de modus operandi[24]: Este es un clásico del análisis criminal. Aquí, la persona analista debe identificar y describir con detalle «los modos de operación de las organizaciones delictivas». Este conocimiento nuevo y ventajoso debe ser compartido por los canales del Sistema Nacional de Seguridad Pública para que se comparen y corrijan en una base de datos nacional que hoy no existe. Cuando se alcance este nivel de cooperación interinstitucional, esta clase de análisis mostrará su mejor faceta, la predictiva. Con ello se elevará la eficacia en la reacción, la prevención e investigación de los hechos delictivos que coincidan con las categorías de comportamientos descritos. Generar y mantener actualizada tal base de datos, será un avance estructural en la institucionalización y profesionalización de la investigación criminal en México.

Análisis para apoyar el ejercicio de la Extinción de Dominio[25]: Esta es una especie del género «análisis de contexto». Es un acierto que la normatividad haga partícipe al analista criminal y al perito, del ejercicio de una facultad tan severa, por parte del fiscal. Este producto imprime objetividad y eficacia a la medida cautelar. De la redacción del numeral citado, la intervención del analista parecería ser potestativa del fiscal, pero en nuestra opinión debe ser obligatoria. Análisis para apoyar el ejercicio del Criterio de Oportunidad[26]: Esta también es una especie del género «análisis de contexto». La interpretación sistemática de los numerales pertinentes a esta figura, arroja que la aplicación del criterio de oportunidad debe realizarse motivado en un «análisis objetivo de los datos» derivados de la investigación realizada. Para que el criterio de oportunidad otorgue ventaja a la autoridad investigadora frente las organizaciones delictivas; debe realizarse una evaluación de costo-beneficio, un análisis de las consecuencias en términos de la promoción de la seguridad pública, que pudiese arrojar la información cruda obtenida por esta vía. La objetividad demandada por el articulado sólo puede lograrse mediante la aplicación de técnicas analíticas estructuradas[27], cuyo dominio corresponde a las personas analistas.

---

[23] Artículo 45 fracción III de la LFGR.
[24] Artículo 34 fracción VII del Reglamento de la Guardia Nacional (RGN).
[25] Artículo 190 párrafo primero de la Ley Nacional de Extinción de Dominio (LNED).
[26] Artículos 221 párrafo quinto y 256 párrafo primero del Código Nacional de Procedimientos Penales (CNPP).
[27] Véase Heuer J., Richards Jr y Randolph H. Pherson (2015), *Structured Analitic Tehcniques for Intelligence Analysis*, 2ª ed., SAGE, Los Ángeles, passim.

Análisis para Líneas de Investigación[28]: Este producto es toral. La persona analista ministerial está facultada para sugerir líneas de investigación a partir del estudio de los expedientes. Pero para que este ejercicio sea significativo, es necesario que el analista genere conjeturas e hipótesis, y que las valide por métodos lógicos reconocidos. Lo anterior atendiendo al conocido axioma «no hay inteligencia sin hipótesis». En el contexto de la investigación de un hecho delictivo, ya se dijo líneas arriba, la hipótesis mejor sustentada con indicios se convierte en «teoría del caso». Hasta que se internalice este axioma, no habrá mejoría en los índices de justicia penal en México29. La práctica de acudir a «videntes» o las carpetas de investigación con miles de fojas, evidencia lastimosamente que ningún fiscal involucrado se tomó la molestia de generar y validar hipótesis.

Los productos identificados son también útiles para apoyar la toma de decisiones y las acciones de proximidad social, prevención del delito, reacción y reinserción social. Por cierto, no es necesario que alguna ley o reglamento lo ordene, basta la voluntad y el conocimiento especializado de los titulares de las dependencias y entidades que deben desempeñar esas especialidades de la seguridad pública.

3.2. Productos de corte estratégico

Estudio Criminógeno[30]: Aquí se identifica y analizan factores personales, sociales, económicos, ambientales, etc. que prohíjan la comisión de cierta clase de delitos en una comunidad determinada. Así, la persona analista en consenso con criminólogos, debe discernir «causas estructurales, tendencias históricas y patrones de comportamiento»[31] para actualizar y perfeccionar la política criminal y de seguridad pública,[32] pero también para emprender acciones adecuadas a cada entorno y comunidad, así como en los ámbitos policiales, ministeriales o penitenciarios, en caso de que hayan sido cooptados por actores delincuenciales.

Al elaborar esta clase de producto, el analista criminal debe considerar el parecer de «las autoridades, ciudadanos y comunidades organizadas» y evaluar sus recomendaciones sobre «medidas y acciones que permitan mitigar

---

[28] Artículo 45 fracción II de la LFGR.

[29] México ocupa el lugar 134 de 142 en este factor específico del Índice de Estado de Derecho, *World Justice Project* (2024) «*Rule of Law Index. México*», consultado el 13 de octubre de 2024, disponible en: https://worldjusticeproject.org/rule-of-law-index/country/2024/Mexico/Criminal%20Justice/

[30] Artículo 128 fracción XIV y 161 fracción XI de EOFGR

[31] Lo hace a través del Centro Nacional de Prevención del Delito y Participación Ciudadana según el artículo 12 fracción XVIII, del Reglamento del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (RSESNSP).

[32] Idem.

el fenómeno de la delincuencia».[33] Una variante de este género analítico es el que se enfoca en «das causas que originan la comisión de conductas antisociales en adolescentes».34 En este punto, el Centro Nacional de Prevención del Delito y Participación Ciudadana, del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública es el punto de contacto con los tanques de pensamiento y las organizaciones no gubernamentales, nacionales y extranjeras, enfocadas en la seguridad pública[35]. La sociedad civil organizada es aliada, no adversaria, en el esfuerzo honesto de las instancias de seguridad pública cuando se desempeñan en un Estado democrático de derecho.

Estudio de Mercados Criminales[36]: La comprensión profunda de las organizaciones delictivas demanda entender el funcionamiento y la dinámica de los mercados negros que crean y sostienen. Generar esta clase de productos estratégicos corresponde legalmente a la fiscalía general de la República a través de la Agencia de Investigación Criminal. Empero, nada obsta para que se realicen en otras dependencias federales, estatales o municipales, porque son necesarias en todas las especialidades de la seguridad pública. En este punto la Unidad de Inteligencia Financiera cuenta con atribuciones específicas[37] para apoyar este esfuerzo.

Estudio Geodelictivo[38]: Referenciar una clase específica de hechos criminales a su contexto geográfico, es esencial para varias tareas estratégicas; por ejemplo: comprender la ocupación y disputa de territorios, revelar las vías de suministros de personas, vehículos, armas, municiones, precursores, sistemas de comunicación, drones, etc.; así como los circuitos de lavado de activos, entre otras. Dichos productos también deben sugerir el emplazamiento de efectivos con el perfil operativo adecuado e incluso los límites de uso de la fuerza. Los componentes del Sistema Nacional de Seguridad Pública o las unidades administrativas de su Secretariado Ejecutivo, deberían poder realizar esta clase de producto, directamente o mediante consultores[39].

Específicamente en materia de secuestro, el Centro Nacional de Prevención y Participación Ciudadana del Secretariado Ejecutivo, es el punto de coordinación para que las instituciones de los tres órdenes de gobierno

---

[33] Artículo 3º fracción II del Reglamento de la Ley General para la Prevención Social de la Violencia y la Delincuencia (RLGPSVD).

[34] Artículo 257, Ley Nacional del Sistema Integral de Justicia Penal para Adolescentes (LNSIJPA).

[35] Artículo 12 fracción XIV del RSESNSP) y artículo 35 del RLGPSVD.

[36] Artículo 128 fracción XIV y 161 fracción XI de EOFGR.

[37] Artículo 15 fracciones VI, XII, XIII, XVII y XXII del Reglamento Interior de la Secretaría de Hacienda y Crédito Público (RISHCP).

[38] Artículo 128 fracción XIV y 161 fracción XI de EOFGR.

[39] Artículo 12 fracción XVIII, del RSESNSP.

interpreten la información geodelictiva vinculada con «factores que generan las conductas antisociales […] con la finalidad de identificar las zonas, sectores y grupos de alto riesgo, así como sus correlativos factores de protección»[40].

Estudio prospectivo[41]: Las instituciones de los tres niveles de gobierno se pueden beneficiar de esta clase de producto, porque son insumo para «programas de prevención social de la violencia y la delincuencia». En la medida en que el análisis criminal se suponga ajeno a estos programas, la acción gubernamental será reactiva y nunca proactiva, con lo cual el posicionamiento estratégico de las autoridades será débil.

Evaluación de amenaza de seguridad pública[42]: Esta clase de reportes tiene la finalidad de «Detectar los factores que incidan en las amenazas o en los riesgos que atenten contra la preservación de las libertades de la población, el orden y la paz públicos y proponer medidas para su prevención, disuasión, contención y desactivación». La intención es loable, pero la redacción es desafortunada. Confunde amenaza con riesgo lo cual es común en el medio mexicano. Este error conceptual tiene repercusiones negativas que van desde lo presupuestal hasta lo táctico.

Para efectos de este ensayo entendemos aquí por amenaza a la seguridad pública un «fenómeno dañoso de origen humano o natural, que dificulta o impide a un Estado desempeñar funciones de proximidad social, reacción, prevención del delito, investigación del delito o reinserción social, en una comunidad determinada». Por otra parte, riesgo a la seguridad pública es la «probabilidad de que en un lapso determinado se actualicen daños cuantificables al orden público de una comunidad determinada». Por lo tanto, la amenaza es un fenómeno, en tanto que el riesgo es una razón en términos aritméticos. Entonces, es absurdo confundir un fenómeno con una idea.

Ahora bien, para que la evaluación de amenazas sea completa, además de caracterizar cada fenómeno dañoso, se requiere sugerir principios de política pública que enmarquen e identifiquen decisiones y acciones concretas a adoptarse en días y horas determinados. Hacerlo así convierte un simple diagnóstico en una agenda estratégica para promover el orden público. Una muestra de tales principios rectores incluye: la resolución pacífica de conflictos, el respeto a los derechos humanos, la promoción de la cultura de la paz, el trabajo social comunitario y el contacto permanente con los actores sociales y comunitarios.[43] La Estrategia Nacional de Seguridad Pública que debe aprobar

---

[40] Artículo 21 fracción II de la Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro (LGPSDMS).
[41] Artículo 257 fracción IV de la LNSIJPA.
[42] Artículo 33 fracción XII del RGN.
[43] Artículo 3º fracción VIII de la Ley General de Prevención Social de la Violencia y la Delincuencia (LGPSVD).

el Senado[44], ser formulada por la Secretaría de Seguridad y Protección Ciudadana y aplicada por la Guardia Nacional[45]; debe cimentarse en esos principios para ser coherente con el orden jurídico y administrativo nacional. Pero las estrategias son por naturaleza mudables. La verdadera expresión de voluntad política se plasma en el Programa Sectorial de Seguridad Pública sexenal46 que debe publicarse en el Diario Oficial de la Federación, como seguramente lo será.

Evaluación de Impacto Comunitario[47]: Es un producto enfocado en «identificar los problemas que pueden afectar a la confianza de la comunidad en la capacidad de las instituciones de procuración de justicia y de seguridad pública para responder eficazmente a sus necesidades». Si bien su naturaleza es estratégica, su utilidad táctica es también evidente. Las personas analistas criminales deben ser creativas al momento de concebir, diseñar y sugerir respuestas gubernamentales mejoradas para modular dichos impactos. Claramente, este género analítico debe elaborar a partir de los resultados arrojados por la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE), la Encuesta Nacional de Seguridad Pública Urbana (ENSU), la Encuesta Nacional de Calidad e Impacto Gubernamental (ENCIG), pero también con base en indicadores e índices generados por organizaciones de la sociedad civil con base en metodologías científicas, libres de sesgos ideológicos.

Reporte Estratégico sobre criminalidad[48]: Esta clase de producto abarca un amplio abanico de temas y ámbitos. Aquí, el analista ministerial debe «identificar patrones, estructuras, organizaciones, modos de operación» sobre «criminalidad nacional, trasnacional o internacional». Está destinado a soportar el Plan Estratégico de Procuración de Justicia de la Fiscalía General de la República. Subsidiariamente enmarca la investigación de delitos federales, pero puede ser una herramienta valiosa en otros ámbitos, incluso en la conducción de negociaciones comerciales internacionales de México. Es un logro que la legislación federal considere este género de productos. Empero, es de lamentar la redacción ya que la «identificación» es una labor primaria del análisis, necesaria sin duda, pero insuficiente para sugerir pautas de decisión y comportamiento estratégico.

Por otra parte, nada impide que esta clase de producto se redacte en las secretarías de seguridad pública estatales o en el seno de las autoridades penitenciarias. México seguirá a la saga de las organizaciones delictivas, en la

[44] Artículo 21 párrafo décimo primero, décimo segundo y décimo tercero, CPEUM.
[45] Artículo 74 fracción XI de la CPEUM.
[46] Artículo 26 apartado A de la CPEUM.
[47] Véase Protocolo de Investigación citado en la nota 4.
[48] Artículo 45 fracción V de la LFGR.

medida en que se abstenga de realizar labores de análisis criminal en los centros penitenciarios.

El cuerpo de este ensayo podría ser útil en el diseño de la Subsecretaría de Inteligencia e Investigación Policial, que se anunció como parte de la Estrategia Nacional de Seguridad Pública 2024-2030.49 La armonización de sus atribuciones con aquellas del Centro Federal de Inteligencia Criminal debe guiarse por criterios técnicos en el plano de la inteligencia y en el plano legal para evitar duplicaciones y contradicciones. El anunciado sistema único de inteligencia50 debe ser resultado de una política de Estado que concilie el programa sectorial y la estrategia en seguridad púbica.

La pieza central de la política, el programa y la estrategia, debe ser el análisis criminal. México hoy cuenta con estándares de competencia específicos. Pueden citarse, entre otros los siguientes: el EC0329 que fue el primero, el EC1588 y el más reciente, EC1599. Estas son las bases para que en un futuro se reconozca al analista criminal como un jugador clave en todos los ámbitos de la seguridad pública.

Conclusiones y recomendaciones

El orden público capturado por la actividad delictiva, la presión internacional y los índices de impunidad, evidencian la necesidad de establecer definitivamente la figura del analista criminal en la administración pública mexicana. Así se atacaría una de las causas estructurales de la violencia. Con base en lo expuesto, se ofrecen conclusiones fundadas en los materiales legales consultados y recomendaciones motivadas en el sentido común.

El ámbito de actuación del analista criminal es mucho más extenso que el delineado por la normatividad vigente, pero no está visibilizado por las autoridades federales y estatales. Implantar el análisis criminal en las funciones de proximidad social, prevención del delito, reacción, investigación del delito y reinserción social; es necesario para aumentar la eficacia en esas especialidades. Ello demanda todo un programa de homologación de leyes federales y estatales que, en las condiciones de mayoría legislativa que privan en el trienio 2024-2027, puede lograrse con celeridad.

---

49 Belmont, José Antonio y Gaspar Vela (2024), «García Harfuch anuncia creación de Subsecretaría de Inteligencia en la SSPC», Milenio, 08 de octubre, consultado el 09 de octubre de 2024, disponible en: https://www.milenio.com/policia/garcia-harfuch-anuncia-nueva-subsecretaria-de-inteligencia

50 Rosas, Sirse (2024), «Anuncia Sheinbaum creación de sistema único de inteligencia», Universal, 14 de octubre, consultado el 15 de octubre de 2024, disponible en: https://www.eluniversal.com.mx/nacion/anuncia-sheinbaum-creacion-de-sistema-unico-de-inteligencia/

Prevalece un déficit de personas analistas criminales en todo el Sistema Nacional de Seguridad Pública. Entonces, priorizar la formación de analistas criminales en todas las instancias de seguridad pública sería un avance memorable.

El arraigo del análisis criminal inicia con la estabilidad laboral de los servidores públicos que desempeñan hoy esas atribuciones. Es recomendable crear o transformar perfiles laborales y plazas para denominarlas «analista criminal» y dotarlas de su propia línea de desarrollo institucional.

El análisis criminal debe ser homologado para lograr su mayor impacto positivo. La Conferencia Nacional de Procuración de Justicia debiese emitir estándares, protocolos y guías técnicas ad hoc. Otro tanto debiesen hacer las Conferencias Nacionales de Seguridad Pública y del Sistema Penitenciario.

El examen crítico del artículo 45 de la LFGR, tomado como muestra de la normatividad vigente, arroja luces y sombras. Es recomendable entonces, proceder a la reforma de dicho numeral para clarificar y enfocar las atribuciones del analista criminal y potenciar así su impacto positivo.

En la labor ministerial, el análisis criminal se muestra disociado del Plan de Investigación. Por tanto, la asistencia del analista al fiscal en este rubro debe ser permanente.

Para evolucionar al ritmo de las estructuras criminales, conviene que todos los involucrados en la seguridad pública se actualicen regularmente. En ello, el analista criminal juega un papel central. Es aconsejable que participe en la creación y modificación de metodologías en un rango de temas más amplio que el establecido en la normatividad federal comentada.

Las fuerzas del orden seguirán a la saga de las organizaciones delictivas, en la medida en que se abstenga de realizar labores de análisis criminal en los centros penitenciarios. Es urgente institucionalizar la figura del analista criminal en el seno del Órgano Administrativo Desconcentrado de Prevención y Readaptación Social de la Secretaría de Seguridad y Protección Ciudadana, así como en las autoridades penitenciarias estatales.

El uso de Inteligencia Artificial generativa en labores de seguridad pública es inminente. Las personas analistas criminales deberán ser el punto focal de ese esfuerzo modernizador, para avanzar en la atención de las causas estructurales del fenómeno delictivo con un enfoque realmente estratégico.

Este ensayo confirma la confusión conceptual que priva en México. La unificación del léxico en materia de análisis criminal es una tarea que debe acometerse como parte de cualquier política pública en la materia.

Bibliografía

Fuentes académicas
Heuer J., Richards Jr y Randolph H. Pherson (2015), Structured Analitic Tehcniques for Intelligence Analysis, 2ª ed., SAGE, Los Ángeles, passim.
Bunge, Mario (1999), Buscar la Filosofía en las Ciencias Sociales, Siglo XXI, México, p. 133.
Popper, Karl (2005), Conocimiento Objetivo, 4ª ed., Tecnos, Madrid, p. 83.
Vignettes Del Olmo, Mario, (2022) «Ventaja Legítima en el Análisis de Inteligencia», Revista de Inteligencia y Seguridad, Instituto Nacional de Administración Pública A.C., No. 1, ps. 29 a 49.
Normatividad Federal
Constitución Política de los Estados Unidos Mexicanos (CPEUM)
Código Nacional de Procedimientos Penales (CNPP)
Ley General de Prevención Social de la Violencia y la Delincuencia (LGPSVD)
Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro (LGPSDMS)
Ley Nacional de Extinción de Dominio (LNED)
Ley Nacional del Sistema Integral de Justicia Penal para Adolescentes (LNSIJPA).
Ley de la Fiscalía General de la República (LFGR)
Ley de la Guardia Nacional (LGN)
Estatuto Orgánico de la Fiscalía General de la República (EOFGR)
Reglamento de la Coordinación Nacional Antisecuestro y Delitos de Alto Impacto (RCNADAI)
Reglamento de la Guardia Nacional (RGN)
Reglamento de la Ley General para la Prevención Social de la Violencia y la Delincuencia (RLGPSVD)
Reglamento del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (RSESNSP)
Reglamento Interior de la Secretaría de Hacienda y Crédito Público (RISHCP)
Reglamento Interior de la Secretaría de Seguridad y Protección Ciudadana (RISSPC)
Estándares administrativos
Estándar de competencia EC0329 «Analizar información para el desarrollo de productos de inteligencia»
Estándar de competencia EC1588 «Elaboración del análisis delictivo para la investigación y prevención del delito»
Estándar de competencia EC1599 «Generación de productos de análisis para la investigación criminal»
Protocolo de Investigación adoptado como anexo I en el Acuerdo 08/XLIX/2023 del Consejo Nacional de Seguridad Pública
Fuentes electrónicas

Belmont, José Antonio y Gaspar Vela (2024), «García Harfuch anuncia creación de Subsecretaría de Inteligencia en la SSPC», Milenio, 08 de octubre, consultado el 09 de octubre de 2024, disponible en: https://www.milenio.com/policia/garcia-harfuch-anuncia-nueva-subsecretaria-de-inteligencia

Guo Jun y Zhang Xiaomin (2024), «'AI police' improve rate of solving crime», China Daily, 23 de octubre, consultado el 25 de octubre de 2024, disponible en: https://www.chinadaily.com.cn/a/202410/23/WS6718580ca310f1265a1c9146.html

INEGI (2024), «Comunicado de prensa número 603/24» consultado el 21 de octubre de 2024, disponible en: https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2024/EAP_diaMP.pdf

México Evalúa (2023), «Justicia, sólo en 4 de cada 100 delitos que son investigados», consultado el 01 de octubre de 2024, disponible en: https://www.mexicoevalua.org/justicia-solo-en-4-de-cada-100-delitos-que-son-investigados/.

Rosas, Sirse (2024), «Anuncia Sheinbaum creación de sistema único de inteligencia», Universal, 14 de octubre, consultado el 15 de octubre de 2024, disponible en: https://www.eluniversal.com.mx/nacion/anuncia-sheinbaum-creacion-de-sistema-unico-de-inteligencia/

World Justice Project (2024) Rule of Law Index. México», consultado el 13 de octubre de 2024, disponible en: https://worldjusticeproject.org/rule-of-law-index/country/2024/Mexico/Criminal%20Justice/

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

Conflictos de Cuarta Generación (4GW) entre Cárteles de la Droga y sus Proxys: Impacto en la inversión del *Nearshoring* en el sureste de México

Eduardo Zerón García*

Resumen: El presente estudio analiza los Conflictos de Cuarta Generación (4GW) entre cárteles de la droga y sus *proxys* en el sur de México, mismos que podrían afectar la viabilidad del *nearshoring*. Se examinará cómo la expansión de los cárteles, sus economías criminales y su interés por controlar más territorio generan un entorno de inestabilidad, incertidumbre y una percepción negativa que a la postre podría superar los beneficios económicos y logísticos del Corredor Interoceánico del Istmo de Tehuantepec. Se estima que la violencia podría dirigirse contra actores económicos legítimos, lo que daría como resultado un clima de inseguridad persistente.

No obstante, concluiremos que, a pesar de la escalada e intensidad de este conflicto, la percepción, y la incapacidad del Estado para mitigar la influencia de los cárteles y la inseguridad en la región son componentes de relevancia, al momento, no son un factor determinante. Al correlacionar los eventos criminales y las dinámicas de confrontación entre las Organizaciones de la Delincuencia Organizada Trasnacional (DOT) en relación con factores económicos, observaremos que, los actos de violencia, a pesar de tener un impacto negativo, no son significativos. Los hallazgos indican la necesidad de tener un control efectivo a mediano y largo plazo; sin embargo, la viabilidad del *nearshoring* en el sur de México se ve comprometida por otros factores que pueden obstaculizar el desarrollo económico de esta estrategia.

Palabras clave: Conflictos de Cuarta Generación (4GW); *Nearshoring, Reshoring*[51], *Proxys*, Cárteles, Pillaje, Percepción de Riesgo, Inversionistas, Organizaciones de la Delincuencia Organizada Transnacional (DOT), Tren Interoceánico, Infraestructuras Críticas, Delincuencia Organizada.

Abstract: This study analyzes the Fourth Generation (4GW) Conflicts between drug cartels and their proxies in southern Mexico, which could affect the viability of nearshoring. It will examine how the expansion of the cartels, their criminal economies,

* Maestría en Inteligencia para la Seguridad Nacional – INAP, Licenciado en Ciencias de la Comunicación por la Universidad de las Américas de Puebla.

[51] Que busca reubicar la producción a países de origen para enfrentar tensiones geopolíticas y desafíos logísticos.

and their interest in controlling more territory generate an environment of instability, uncertainty, and a negative perception that could ultimately outweigh the economic and logistical benefits of the Tehuantepec Isthmus Interoceanic Corridor. It is estimated that violence could be directed against legitimate economic actors, resulting in a persistent climate of insecurity.

However, we will conclude that, despite the escalation and intensity of this conflict, the perception and the inability of the State to mitigate the influence of the cartels and insecurity in the region are relevant components, at the moment, they are not a determining factor. By correlating criminal events and the dynamics of confrontation between Transnational Organized Crime Organizations (TOC) in relation to economic factors, we will observe that acts of violence, despite having a negative impact, are not significant. The findings indicate the need to have effective control in the medium and long term; however, the viability of nearshoring in southern Mexico is compromised by other factors that may hinder the economic development of this strategy.

Keywords: Fourth Generation Conflicts (4GW); Nearshoring, Reshoring, Proxies, Cartels, Pillage, Risk Perception, Investors, Transnational Organized Crime Organizations (TOC), Interoceanic Train, Critical Infrastructures, Organized Crime.

1. Introducción.

Este artículo analiza cómo los Conflictos de Cuarta Generación (4GW), en los que actores no estatales, como las Organizaciones de la Delincuencia Organizada Transnacional (DOT), desafían el control del Estado mediante confrontaciones asimétricas. (Lind, Nightengale, Schmidt, Sutton, & Wilson, 1989). Estos grupos operan fuera de los ordenamientos legales, emplean tácticas no convencionales para consolidar el control territorial y las rutas de intercambio de sus economías criminales, tales como el contrabando y el narcotráfico (Robb, 2007). Este fenómeno ha alterado el contexto de seguridad en México, especialmente en el sur del país.

En los estados de Veracruz, Chiapas y Oaxaca, la violencia ha exacerbado dramáticamente. Los cárteles de la droga y sus *proxys* han establecido redes de poder que desafían la autoridad estatal, afectando gravemente la seguridad local. Su expansión no sólo intensifica la violencia y el control territorial, sino que añade una capa de complejidad, ya que estos grupos criminales emplean actores indirectos, como pandillas locales, informantes y autoridades civiles coaccionadas o cómplices, para alcanzar sus fines, a lo que denominamos *proxys* (Sullivan & Bunker, 2002, p. 45).

El sureste mexicano comienza a presentar un entorno económico dinámico impulsado por proyectos de infraestructura, como el Corredor Interoceánico. (Gobierno de México, n.d.). El Gobierno de México, para el periodo de 2018-2024, destinó 1 billón quinientos seis mil 415 millones de pesos a proyectos prioritarios; el Corredor del Istmo de Tehuantepec

representó el 2.3 % de la inversión de estos proyectos, esto es treinta y cuatro mil 655 millones de pesos, para su totalidad. Para el presente año, se prevé una designación de 21,059 millones de pesos (Centro de Investigación Económica y Presupuestaria [CIEP], 2023). Con ello incrementando los intereses gubernamentales en la región.

Paralelamente, los intereses de los grupos criminales también evolucionan, se diversifican y se adaptan en respuesta a la presión de sus antagonistas ya sea el Estado u otras organizaciones criminales, lo hacen respecto a sus economías criminales, desarrollando entramados mucho más sofisticados para sus organizaciones, en consecuencia trayendo nuevos riesgos para este tipo de desarrollos que al estar ubicado en una geografía de conflicto y enclavados en la zona de sus intereses comerciales, tienen mucho mayor vulnerabilidad, por ejemplo los productos y las mercancías que transitan por este corredor pueden convertirse en objetivos de la delincuencia, de pillaje, del sabotaje, esto gracias a diversas amenazas presentes como el cruce de migrantes o del tráfico de estupefacientes, de mercancía, de contrabando, el huachicol, etc.

El fenómeno de la violencia siempre se correlaciona con la percepción pública, el impacto de la violencia masiva puede tener efectos negativos y diversas repercusiones que pueden desalentar la inversión, precisamente cuando el *nearshoring*, que se refiere a la estrategia de reubicar actividades empresariales a países cercanos para reducir costos y optimizar las cadenas de suministro, se orienta como una estrategia que pretende perseguir el Gobierno para que sea clave para el desarrollo económico del país (Kearney, 2022).

El proyecto del Corredor Interoceánico fue desarrollado para fomentar el comercio y la conectividad, como hemos mencionado este desarrollo se enfrenta a diversas amenazas directas e indirectas por parte de estos grupos criminales, lo que pone en riesgo la seguridad de la infraestructura y podría generar desconfianza en los inversionistas. Es entonces que este artículo analizará cómo la amenaza categorizada en el conflicto entre los cárteles, junto con la ineficiencia del Estado para contenerlos, podría impactar negativamente a la atracción de inversión, creando una percepción de incertidumbre y peligro.

Correlacionaremos cómo el incremento de la actividad criminal podría influir negativamente en las decisiones de los inversionistas, se analizará la relación entre el comportamiento delictivo y las expectativas económicas, fundamentalmente la Inversión Extranjera Directa (IED). Catalogaremos, explicaremos y definiremos el tipo de violencia al que hace frente la región y daremos respuesta a nuestra pregunta de investigación: ¿los eventos de violencia masiva pueden disuadir la inversión en el sureste mexicano? Concluiremos que si bien, a medida que la criminalidad aumenta, también lo hará negativamente su percepción, la inversión solo se ve marginalmente afectada por este fenómeno, en este momento, teniendo mucha más

preponderancia otros factores. Sin embargo, esto no significa que, en adelante, de seguir escalando la criminalidad y de no disuadirse, neutralizarse o mitigarse, podría convertirse en un factor determinante, enturbiando el entorno económico, haciéndolo hostil, volátil e incierto.

2. Análisis de los Conflictos de Cuarta Generación (4GW) en la Delincuencia Organizada.

Para definir los Conflictos de Cuarta Generación (4GW) resulta necesario hacer un repaso de los conflictos armados y contempéranos. Carl von Clausewitz, define a la guerra como: "un acto de fuerza para obligar al adversario a acatar nuestra voluntad" (Clausewitz, 1832). Esta visión contiene elementos como lo son: la violencia primordial, el juego de probabilidades y el razonamiento político. Esto estructura lo que llamamos "la dinámica de los conflictos bélicos".

Los conflictos contemporáneos, especialmente en nuestro tiempo, requieren una ampliación de esta perspectiva. Mary Kaldor, en su obra *New and old wars* (1999), introduce el concepto de "nuevas guerras", en donde las explica, como: "un acto de violencia que involucra a dos o más grupos organizados (actores estatales o no estatales) enmarcados en términos políticos". Según la lógica de esta definición, la guerra podría ser una "lucha de voluntades", como implica la definición de Clausewitz, o podría ser una "empresa mutua". Estos conflictos mezclan guerra, crimen y violaciones masivas de derechos humanos. Según Kaldor, las nuevas guerras "son una forma de organizar la sociedad mediante la violencia" (Kaldor, 1999).

Esta visión refleja cómo los conflictos modernos entre los actores estatales podrían no sólo perseguir fines políticos, sino cómo lo hacen en su mayoría los actores no estatales, que su principal ambición está intrínsecamente ligada a la **economía criminal**. "La tendencia interna de tales guerras (o conflictos) no es la de una guerra sin límites, sino la de una guerra sin fin. Las guerras, definidas de esta manera, crean un interés compartido que se perpetúa a sí mismo en la guerra para reproducir la identidad política y promover intereses económicos". (Kaldor, 1999).

Las guerras modernas resultan distintas a las guerras convencionales, tanto en sus métodos como en sus tácticas en las que incorporan elementos de guerrilla, de violencia masiva y la dirigida específicamente hacia sus antagonistas y en otras a la población civil, Jolle Demmers dice que "las guerras modernas se caracterizan por la participación de actores no estatales que emplean tácticas irregulares, incluyendo la guerrilla y el terrorismo, lo que complica la distinción entre combatientes y civiles" (Demmers, 2017).

Las guerras de guerrillas por ejemplo se caracterizan por tácticas de combate irregulares, emboscadas o sabotajes, realizadas estratégicamente por

pequeños grupos armados para enfrentarse a fuerzas superiores y mejor equipadas, las guerrillas tienen un mejor conocimiento del terreno y utilizan la sorpresa como su ventaja táctica (Bolstering Ukraine's Irregular War, 2024), mientras que las guerras irregulares agrupan conflictos donde participan milicias, insurgencias y otros actores no estatales que operan al margen de las normas de combate. Estas fuerzas no mantienen una línea de batalla tradicional y tratan de pasar inadvertidas al mimetizarse con la población civil, empleando estrategias de desgaste en contra de sus antagonistas, usando métodos diversos como ataques puntuales y el control de poblaciones locales que los convierten en sus *proxys* para obtener apoyo y recursos (RAND Corporation, 2024).

as guerras asimétricas son enfrentamientos donde un actor recurre a tácticas no convencionales —como ataques sorpresa o guerra cibernética—. Esto sucede cuando el adversario cuenta con mayores y mejores medios (Modern War Institute, 2021). Mientras que las guerras híbridas combinan estrategias militares convencionales con tácticas irregulares, ciberataques y terrorismo, en Ucrania, por ejemplo, antes de 2022, Rusia empleó una mezcla de fuerzas regulares, mercenarios y ciberataques para desestabilizar al gobierno ucraniano (RAND, 2022).

En las guerras modernas, el Estado ya no mantiene el monopolio de la violencia. Actores no estatales, como insurgentes, terroristas y cárteles, mantienen una disputa con el Estado, además de sostener un conflicto entre otros grupos rivales mediante tácticas irregulares. En México, por ejemplo, podemos hablar de estos enfoques cuando hablamos de las Organizaciones de la Delincuencia Organizada Trasnacional (DOT), mismas que combaten mediante tácticas que incluyen guerrillas urbanas, narco bloqueos, ataques sorpresa, drones armados, desinformación y la infiltración de fuerzas de seguridad (Méndez, 2020; Felbab-Brown, 2019) estos conflictos no son exclusivos de los Estados, sino también entre actores no estatales.

Un método común dentro de las tácticas irregulares que emplean los grupos de la delincuencia organizada es la subvención a otros grupos locales, células, beneficiados, asociados o cárteles afines, llegando incluso a integrar a las comunidades enteras dentro de su estructura criminal para hacer frente a sus antagonistas. Estos grupos, conocidos como "Proxys", son utilizados para avanzar los intereses de sus patrocinadores externos, sin que estos últimos se involucren directamente en el conflicto, lo que les permite mantener una negación plausible de las acciones violentas en contra de sus adversarios (Moghadam, Rauta, & Wyss, 2023).

El uso de *proxys* en los conflictos o -"los conflictos por *proxys"-,* para hacer una mejor distinción provoca que "la frontera que divide a los combatientes y civiles se anule", y que los campos de batalla, o la geografía donde se desarrolla, se expanda y se diversifique dentro de sus tres niveles de confrontación: el estratégico, operacional y táctico, lo que se denomina "teatros de operación", que son espacios delimitados por fronteras tangibles (Vego,

2020) como lo pueden ser al ciberespacio, la economía entre otros. William S. Lind describe este fenómeno como "Guerras de Cuarta Generación (4GW)", que pueden involucrar tanto a actores estatales como no estatales (Lind, 1989; Moghadam, Rauta, & Wyss, 2023).

En estas conflagraciones entre actores de las Organizaciones de la Delincuencia Organizada, en contra del Estado o de otros actores no estatales, donde participan otros actores asociados o beneficiados que luchan contra enemigos comunes, se le conoce como "enfrentamiento por *proxys*" que es "una relación en la que un agente externo, ya sea estatal o no estatal, patrocina a sus representantes o beneficiarios en un conflicto, proporcionando armas, entrenamiento y financiamiento" (Moghadam, Rauta, & Wyss, 2023).

En México, aunque el principal conflicto que enfrenta el Estado es contra los grupos de la delincuencia organizada, en particular contra los cárteles de la droga, también existen conflictos paralelos entre estas organizaciones criminales. La guerra que sostienen entre los cárteles puede considerarse un Conflicto de Cuarta Generación (4GW).

Los cárteles utilizan métodos y tácticas asimétricas, como emboscadas, narcobloqueos y propaganda, lo cual va más allá de los enfrentamientos tradicionales. Además, operan de manera descentralizada para controlar territorios estratégicos. El uso de *proxys* es un sello distintivo de este tipo de Conflictos de Cuarta Generación (4GW), (Blin, 2023; Insight Crime, 2023). En este enfoque el adversario busca que el poder del Estado se vea disminuido a través de guerra psicológica, propaganda, uso de violencia masiva, y la explotación de vulnerabilidades de las autoridades tales como la corrupción y la infiltración en los niveles de poder (Lind et al., 1989; Hoffmann, 2007), es entonces que en nuestro país podríamos definir nuestro concepto de Conflicto de Cuarta Generación (4GW) de la siguiente manera:

> "Un conflicto que implica actores no estatales y sus *proxys* donde ambos utilizan tácticas irregulares de combate para el control territorial, económico y de retaliación de su adversario, a través de métodos como la violencia y la intimidación, estos grupos no solo buscan el apropio de rutas y mercados ilegales, sino también de la población para hacerla parte de su estructura y ganar su respaldo, en un tipo de conflicto no convencional que difumina las líneas entre combatientes y civiles, aprovechando el control, la propaganda, la coerción así como la narrativa para expandir su influencia".

3. Los conflictos entre los cárteles y sus economías criminales.

El conflicto entre grupos delictivos en México ha sido constante y violento, impulsado en gran parte por la búsqueda de expansión, control de territorios y de economías. Durante más de dos décadas, estas organizaciones han

diversificado sus intereses más allá del tráfico de drogas, incursionando en otras actividades como la trata de personas, el tráfico de armas, el robo de hidrocarburos y el lavado de dinero. A estas actividades se les denominan economías criminales, que pueden ser entendidas como "una actividad de una organización inmersa dentro de un ecosistema criminal que cuenta con recursos humanos y financieros en beneficio de actividades ilegales" (Guerra, Interamerican Institute for Democracy, Universidad Peruana de Ciencias Aplicadas, & Universidad de la Paz, 2024). Estas acciones han permitido que los grupos delictivos amplíen sus capacidades y progresión más allá de las fronteras nacionales, integrándose o convirtiéndose en grupos de Delincuencia Organizada Transnacional (DOT) con presencia local, nacional, hemisférica y global, así como su capacidad de operar fuera de las fronteras nacionales ha generado serias repercusiones en la estabilidad internacional, (Saviano, 2015; Shelley, 2020) y en especial en la Seguridad Multidimensional, que reconoce la interrelación económica, social y ambiental que afectan la estabilidad de una nación (OEA, 2020).

Las Organizaciones de la Delincuencia Organizada Transnacional (DOT), como los cárteles, constituyen una amenaza significativa para la paz, la estabilidad y los derechos humanos. Su impacto es devastador para la viabilidad social, la estabilidad de las instituciones y el desarrollo económico, afectando gravemente la gobernanza democrática y fomentando la corrupción en las regiones donde operan (UNODC, 2023; White House, 2023).

4. Presencia de las Organizaciones de la Delincuencia Organizada Transnacional (DOT) en México.

El Gobierno de la México ha reconocido que, en nuestro país, actualmente existen diez cárteles regionales: Cártel del Golfo, Los Arellano Félix, La Familia Michoacana, Los Rusos, Cártel de los Beltrán Leyva, Cártel del Noreste, Cártel Santa Rosa de Lima, Cártel Nueva Plaza, Cártel Jalisco Nueva Generación (CJNG) y el Cártel del Pacífico o Cártel de Sinaloa. Estos últimos se consideran las organizaciones con la mayor presencia, relevancia y dominancia geográfica (Gobierno de México, 2024, p. 17).

Carteles Regionales[52]

[52] Gobierno de México, 2024, p. 17

Para los estados como Chiapas, el Cártel Jalisco Nueva Generación (CJNG) mantiene su hegemonía y se encuentra en disputa con el Cartel de Sinaloa por los puntos de entrada y desembarque de cargamentos de estupefacientes provenientes de Sudamérica como sugiere el gráfico. Por lo que se refiere al Estado de Oaxaca, ambas organizaciones tienen un conflicto por el territorio, mientras que, en Veracruz, el Cártel Jalisco Nueva Generación (CJNG) tiene el liderazgo, sin embargo, la atomización de los *proxys* contrarios grupos locales, y la presencia del Cártel de Sinaloa hace que mantengan una constante disputa.

Cártel Jalisco Nueva Generación (CJNG) y el Cartel de Sinaloa tienen presencia en 28 y 24 estados de la república respectivamente, un artículo denominado "*Reducing cartel recruitment is the only way to lower vionlence in México"* advierte que para 2022 los cárteles contaban entre 160.000 y 185.000 personas, convirtiéndose en uno de los principales empleadores del país, reclutando entre 350 y 370 personas por semana (…) (Curiel, Capedelli, Hope, 2022).

Los 20 principales cárteles y su tamaño estimado en 2022[53]

[53] Prieto-Curiel R, Campedelli GM, Hope A. Reducing cartel recruitment is the only way to lower violence in Mexico. Science. 2023 Sep 22;381(6664):1312-1316. doi: 10.1126/science.adh2888. Epub 2023 Sep 21. PMID: 37733856.

Group	State rivals	State allies	Size
Cártel Jalisco Nueva Generación (CJNG)	77	55	28,764
Cártel de Sinaloa	19	34	17,825
La Nueva Familia Michoacana	21	13	10,736
Cártel del Noreste	16	10	8,992
La Unión Tepito	13	9	7,561
Los Chapitos	9	10	6,823
Cártel del Golfo	10	7	5,556
Los Zetas	10	6	4,697
Guerreros Unidos	13	2	3,096
Gente Nueva	4	9	4,325
Zetas Vieja Escuela	9	4	3,084
Caballeros Templarios	8	4	2,686
Fuerza Anti-Unión Tepito	7	5	2,903
Los Rojos	12	0	813
Cárteles Unidos	6	4	2,051
Los Mayas	7	3	1,824
Cártel de Tláhuac	5	4	2,050
Cártel de Caborca	4	4	2,114
Los Cabrera	3	4	2,016
Los Cuinis	0	6	2,061
Other cartels (130)	105	133	55,023
Total	358	326	175,000

Un estudio realizado por AC Consultores, con datos extraídos por el colectivo "Guacamaya *Leaks*" con datos de la SEDENA, revela que en el país actualmente operan 175 organizaciones criminales a nivel regional, estatal y municipal. Estas organizaciones están presentes en el 81 % del territorio nacional. Entre los cárteles con mayor presencia están el Cártel Jalisco Nueva Generación (CJNG), que opera en 427 municipios, y el Cártel de Sinaloa, presente en 293 municipios. (AC Consultores, 2023).

La presencia de estos grupos criminales abarca al menos 1,488 de los 2,471 municipios del país (Prieto-Curiel, Campedelli, & Hope, n.d.). Cada estado tiene al menos 9.5 grupos delictivos, con algunas regiones disputadas por múltiples cárteles. A nivel regional, se han forjado alianzas u operaciones fragmentadas de los grupos, lo que llevó a una mayor diversificación y complejidad dentro de sus estructuras y, en consecuencia, de sus conflictos. En algunos estados de la república, ciertos grupos delincuenciales luchan por mantener una hegemonía, mientras que en otros lo hacen por tenerla, entonces tenemos múltiples grupos luchando por los mismos fines en diversas dimensiones.

5. Chiapas, Oaxaca y Veracruz.

Los estados de Chiapas, Oaxaca y Veracruz concentran la mayor parte del desarrollo del denominado Corredor Interoceánico del Istmo de Tehuantepec, que comprende entre otras cosas la interconexión a las empresas concesionarias de los servicios ferroviarios (Segob, s. f.-a). Esta infraestructura comprende tres líneas, la línea "FA" que recorre los estados de Veracruz, Tabasco y Chiapas con un total de 310 km de vía férrea; la línea "K" que recorre los estados de Oaxaca y Chiapas, y tiene 472 km de vía férrea y se plantea que tenga conexión hasta Guatemala y la línea "Z" que recorre Veracruz hacia Salina Cruz, Oaxaca y cuenta con 212 km. (Segob, s. f.-b).

También considera la modernización de puertos, la construcción de carreteras, para el transporte de mercancías y el desarrollo de lo que denominan Polos de Desarrollo para el Bienestar (PODEBIS) que están concebidos como áreas geográficas delimitadas y que cuentan con las condiciones para atraer

inversión y potenciar capacidades productivas, a efecto de detonar el desarrollo económico y social en la región del Istmo de Tehuantepec. (Segob, s. f.-c)

El Desarrollo "Istmo" comprende para su programa 79 municipios para los tres Estados (Segob, s. f.-d) que se encuentran enclavados desde Veracruz hasta Oaxaca, en la geografía del desarrollo, existe la presencia de Organizaciones de la Delincuencia Organizada Transnacional (DOT), y sus *proxys* que han desarrollado sus actividades en la región que comprende estos tres estados.

El fenómeno delictivo que se presenta es diverso y complejo, en el caso del estado de Chiapas, se destaca la presencia del Cártel de Sinaloa y el Cártel Jalisco Nueva Generación (CJNG), disputándose territorios como Tuxtla Gutiérrez, San Cristóbal de las Casas, y áreas fronterizas como Tapachula y Palenque, también existen pandillas transnacionales como Mara Salvatrucha y grupos locales como Los Chamula (Insight Crime, 2023a; Martínez, 2023).

En Oaxaca, el Istmo de Tehuantepec se ha convertido en un bastión de suma importancia para organizaciones como la Banda de los Terán, Los Ántrax, y El Rilo, controlando territorios estratégicos vinculados al Corredor Interoceánico (Ramírez, 2023). Mientras que, en Veracruz, el CJNG, Los Zetas, y grupos como Grupo Sombra y el Cártel de Tuxpan tienen una fuerte presencia en ciudades importantes como Coatzacoalcos, Poza Rica, y Tuxpan, donde compiten por rutas de tráfico y control económico (Secretaría de Gobernación, 2023a; Insight Crime, 2023b).

Tabla 1. Intensidad de Conflictos por Estado y Municipio[54]

[54] Nota metodológica en apartado

Tabla 2. Grupos Criminales, zonas en Conflicto, rivalidades y Economía Criminal[55]:

Estado	Municipio	Grupo	Liderazgo	Zonas en conflicto	Vs.	Economía Criminal
Chiapas	San Juan Chamula	Cártel de los Chamula (CSJC)	Desconocido	San Cristóbal de las Casas	Cártel de los Chamula vs. Cártel de Sinaloa	Extorsión, tráfico local
Chiapas	Tuxtla Gutiérrez	Cártel de Sinaloa	Isidro & Jesús Gilberto Rivera	Tuxtla Gutiérrez, Palenque	Cártel de Sinaloa vs. CJNG	Tráfico de drogas, extorsión
Chiapas	Región Indígena	Los Rojos	Desconocido	San Cristóbal de las Casas	Cártel de Sinaloa vs. CJNG	Tráfico de drogas, extorsión
Chiapas	San Cristóbal de las Casas	Cártel de Sinaloa	Isidro & Jesús Gilberto Rivera	San Cristóbal de las Casas	Cártel de Sinaloa vs. CJNG	Tráfico de drogas, extorsión

[55] Datos de recolección en anexo.

Estado	Municipio	Grupo	Liderazgo	Zonas en conflicto	Vs.	Economía Criminal
Chiapas	Región montañosa	Los Montoneros	Desconocido	Región montañosa, Ciudad Real, específicamente en la Zona Norte, Santo Domingo	Grupos locales vs. Cártel de Sinaloa	Extorsión, actividades locales
Chiapas	Venustiano Carranza	Los Pelones	Luis Alejandro Cruz	Venustiano Carranza	Grupos locales vs. CJNG	Extorsión, contrabando
Chiapas	Tapachula	Mara Salvatrucha	Luis Alberto Ramírez 'El Chino'	Tapachula	Mara Salvatrucha vs. Cártel de Sinaloa	Tráfico de personas, extorsión
Chiapas	Chiapas-Guatemala frontera	Consejo Indígena (P2)	Desconocido	Chiapas-Guatemala frontera	Indefinido	Tráfico de drogas
Chiapas	San Cristóbal de las Casas	Sentimientos de la Nación	Desconocido	Región montañosa	Indefinido	Tráfico de armas
Chiapas - Guatemala	Región fronteriza	Cártel de Chiapas-Guatemala	Desconocido	Región fronteriza Chiapas-Guatemala	Cártel de Chiapas-Guatemala vs. Los Huistas	Tráfico de drogas, extorsión
Chiapas - Guatemala	Chiapas-Guatemala frontera	El Maíz (P1)	Desconocido	Chiapas-Guatemala frontera	El Maíz vs. Cártel de Sinaloa	Tráfico de drogas, tráfico de armas
Chiapas - Guatemala	Huehuetenango, Guatemala	Los Huistas (P1) (P2)	Desconocido	Frontera con Guatemala	Los Huistas vs. Fuerzas guatemaltecas	Tráfico de drogas, extorsión
Oaxaca	Istmo de Tehuantepec	Cártel del Istmo	Juan Terán (Detenido)	Istmo de Tehuantepec	Cártel del Istmo vs.	Tráfico de drogas,

Estado	Municipio	Grupo	Liderazgo	Zonas en conflicto	Vs.	Economía Criminal
					Grupos locales	tráfico de armas
Oaxaca	Loma Bonita	Ca□ rtel Jalisco Nueva Generaci o□ n	A través de *proxys* independie ntes y células locales	Regio□ n del Papaloapan	Alianza con células locales escindidas de Los Zetas y grupos independient es	Tráfico de drogas
Oaxaca	Región Costa	Facción Caro Quintero	Manuel Yglesias Rivas (a) "Pantera", Bogar Soto Rodríguez (a) "El Bogar"	Región Costa	Alianza con "Los Yglesias"	Tráfico de drogas vía marítima y aérea
Oaxaca	Valles Centrales, Sierra Sur, Istmo	Célula Díaz Pantoja	Desconocid o	Valles Centrales, Sierra Sur, Istmo	Conflictos con células locales de vendedores de drogas y extorsionad ores	Acopio de enervantes (goma de opio y marihuana)
Oaxaca	Valles Centrales, Istmo, Costa, Mixteca	Los Oaxaqueñ os, Los Coyunda, Los Terán, Los Chehuis	Diversos líderes locales	Valles Centrales, Istmo, Costa, Mixteca	Rivalidades internas entre las células	Extorsión, narco, menudeo, secuestro
Oaxaca	Mixteca	Los Alacranes , Los Públicos, Catapitas	Desconocid o	Región Mixteca	Rivalidades entre las bandas locales	Delitos del fuero común

Estado	Municipio	Grupo	Liderazgo	Zonas en conflicto	Vs.	Economía Criminal
Oaxaca	Valles Centrales	Hermanos Ríos Suárez	Iván Ríos Suárez (a) "Cuqui", Indira Janet Ríos Suárez (a) "La Chamaca"	Valles Centrales	Desconocido	Narcomenudeo
Oaxaca	Valles Centrales	Los Oaxaqueños (brazo armado de Díaz Pantoja)	Desconocido	Valles Centrales	Contra células locales de vendedores de drogas y extorsionadores	Ejecuciones violentas
Oaxaca	Juchitán de Zaragoza	Los Chehuis, Los Terán	José Luis Terán de la Rosa (a) "El Chehui", Juan Terán Regalado (a) "El Loco" (detenido).	Istmo de Tehuantepec	Los Chehuis vs. Los Terán	Disputa por la hegemonía en actividades delictivas
Oaxaca	Istmo de Tehuantepec, Cuenca del Papaloapan	Diversas células	Desconocido	Istmo de Tehuantepec, Cuenca del Papaloapan	Desconocido	Secuestro, robo de autos, tráfico de drogas y armas, extorsión
Oaxaca	Salina Cruz	Cártel de Sinaloa	Desconocido	Salina Cruz	Cártel de Sinaloa vs. Grupos locales	Tráfico de drogas, extorsión
Oaxaca	Matías Romero	Los Ántrax	Desconocido	Matías Romero	Los Ántrax vs. CJNG	Tráfico de drogas

Estado	Municipio	Grupo	Liderazgo	Zonas en conflicto	Vs.	Economía Criminal
Oaxaca	Juchitán de Zaragoza	Banda de El Rilo	Desconocido	Juchitán de Zaragoza	Banda de El Rilo vs. Grupos locales	Extorsión, tráfico local
Veracruz	Poza Rica	CJNG	Desconocido	Poza Rica, Tuxpan	CJNG vs. Los Zetas	Tráfico de drogas, extorsión
Veracruz	Xalapa	CJNG	Desconocido	Xalapa	CJNG vs. Grupos locales	Tráfico de drogas, extorsión
Veracruz	Coatzacoalcos	Los Zetas	Desconocido	Coatzacoalcos	Los Zetas vs. CJNG	Tráfico de drogas, extorsión
Veracruz	Veracruz	CJNG	Desconocido	Veracruz	CJNG vs. Los Zetas	Tráfico de drogas, extorsión
Veracruz	Córdoba	Grupo Sombra	Desconocido	Córdoba	CJNG vs. Grupo Sombra	Tráfico de drogas, robo de combustible
Veracruz	Tuxpan	Cártel de Tuxpan	Desconocido	Tuxpan	Cártel de Tuxpan vs. Los Zetas	Tráfico de drogas, extorsión
Veracruz	Veracruz, La Antigua	Desconocido	Daniel Arsenio Chávez Cruz (a) "El Negro"	Desconocido	Desconocido	Desconocido
Veracruz	Zona Norte	Grupo Sombra	Martín Martínez Hernández y/o Francisco Mendiola Cisneros (a) "Cmte. Mirinda", (a) "Cmte.	Zona Norte	Desconocido	Extorsión, narcomenudeo, secuestro

Estado	Municipio	Grupo	Liderazgo	Zonas en conflicto	Vs.	Economía Criminal
			Fénix", (a) "El Pelón"			
Veracruz	Cosoleacaque, Oteapan, Zaragoza, Coacotla, Jáltipan, Las Chopas	CJNG[56]	Efrén Martínez Gómez (a) "Fantasma"	Zona Sur	Desconocido	Trasiego y venta de drogas, cobro de cuota a migrantes, corrupción gubernamental, lavado de dinero
Veracruz	Tres Valles, Tierra Blanca, Los Naranjos	CJNG	Desconocido	Zona Centro	Desconocido	Desconocido
Veracruz	Ixcatepec, Cerro Azul	Cártel del Golfo	Francisco "N" (a) "Cmte." Panchito" y/o (a) "F1"	Zona Norte	Desconocido	Desconocido
Veracruz	Emiliano Zapata, Coatepec, Banderilla	35Z	Erick Manuel Lee Becerra (a) "El Güero Lee"	Zona Centro	Desconocido	Trasiego y venta de drogas
Veracruz	Zona Sur	Zetas Vieja Escuela y Nueva	Desconocido	Zona Sur	Entre Zetas Vieja Escuela y Nueva Sangre Zeta	Extorsión, tráfico de drogas, secuestro

[56] Los Liderazgos del CJNG en el Estado de Veracruz José Roberto Sánchez Cortés "Robert", El "80", El "Huevochas", "El Licenciado", Roberto Herrera Corso, Daniel Alberto Vargas Larrainza "El Fercho", Juan N "El Piraña", Hendir Barrientos Guillen "El 20", El "Jessi", "El Lobito" y/o "El Negro", Jorge Armando Hernández Vargas "Kilo", Alberto Ríos Treviño "Texano", Raúl Martínez Torreblanca (a) "El 30", "La Cuija", y/o "Raúl Torres" (Fue detenido en mayo de 2020).

Estado	Municipio	Grupo	Liderazgo	Zonas en conflicto	Vs.	Economía Criminal
		Sangre Zeta				

P1: *Proxys* del CJNG

P2:*Proxys* del Cartel de Sinaloa.

Municipio	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**	**Tasa 2018**	**Tasa 2023**	**Incremento absoluto**	**Incremento en tasa.**
San Juan Chamula	5	7	6	8	9	10	10.2	20.4	5	10.2
San Cristóbal de las Casas	20	22	25	27	30	32	12.0	19.2	12	7.2
Zinacantán	2	3	3	4	4	5	8.0	20.0	3	12.0
Tenejapa	1	1	2	2	2	3	5.0	12.5	2	7.5
San Andrés Larráinzar	1	2	2	3	3	4	5.0	10.0	3	5.0
Juchitán de Zaragoza	15	17	19	21	23	25	14.0	23.3	10	9.3 %
Salina Cruz	12	14	16	18	20	22	13.0	23.8	10	10.8
Tehuantepec	10	11	12	13	14	15	11.0	17.9	5	6.9
Matías Romero	5	6	7	8	9	10	10.0	20.0	5	10.0
Santo Domingo Tehuantepec	4	5	5	6	6	7	8.5	12.8	3	4.3
Ciudad Ixtepec	3	4	4	5	5	6	6.0	12.0	3	6.0
Oaxaca de Juárez	25	27	29	31	33	35	15.0	21.0	10	6.0
Tlacolula de Matamoros	2	3	3	4	4	5	4.0	10.0	3	6.0
Zimatlán de Álvarez	1	1	2	2	2	3	2.5	7.5	2	5.0
San Pablo Villa de Mitla	1	1	1	2	2	2	2.5	5.0	1	2.5
Ocotlán de Morelos	2	2	2	3	3	4	5.0	10.0	2	5.0
Huajuapan de León	5	6	7	8	9	10	7.0	15.0	5	8.0

Asunción Nochixtlán	1	1	1	2	2	2	2.0	4.0	1	2.0
Tlaxiaco	2	2	3	3	3	4	4.0	8.0	2	4.0
Putla Villa de Guerrero	3	3	4	4	5	5	6.0	10.0	2	4.0
San Juan Bautista Coixtlahuaca	1	1	1	1	1	1	2.0	2.0	0	0.0
Tierra Blanca	10	12	14	15	16	18	12.0	18.4	8	6.4
Tres Valles	5	6	7	8	9	10	9.0	13.5	5	4.5
Cosamaloapan	4	5	5	6	6	7	7.0	12.0	3	5.0
Tuxtepec	8	9	10	11	12	13	10.0	15.0	5	5.0
Loma Bonita	3	4	4	5	5	6	6.5	10.5	3	4.0
Poza Rica	20	22	24	26	28	30	16.0	24.0	10	8.0
Tuxpan	10	12	14	16	18	20	11.0	22.0	10	11.0
Pánuco	5	6	7	8	9	10	6.0	12.0	5	6.0
Tihuatlán	3	4	4	5	5	6	5.0	8.0	3	3.0
Álamo Temapache	2	3	3	4	4	5	3.5	6.5	3	3.0
Coatzacoalcos	30	32	34	36	38	40	18.0	24.0	10	6.0
Minatitlán	15	17	19	21	23	25	14.0	18.0	10	4.0
Acayucan	10	12	14	15	16	18	13.0	16.0	8	3.0
Cosoleacaque	5	6	7	8	9	10	10.0	12.0	5	2.0
Las Choapas	4	5	5	6	6	7	7.0	10.0	3	3.0

La violencia y la rivalidad entre estos grupos han intensificado la inseguridad en algunas subregiones (localidades y municipios) de manera focalizada, afectando tanto a la población como al desarrollo económico, en geografías cercanas al Corredor Interoceánico (Ramírez, 2023). Como principal indicador que representa el delito del homicidio doloso, el cual, se muestra representado en lo que denominamos "Zonas de Conflicto".

Tabla 3. Homicidios dolosos (2018-2023) en Zonas de Conflicto con incremento en tasa[57]

[57] Nota metodológica en anexo
Instituto Nacional de Estadística y Geografía (INEGI): Defunciones por homicidio
Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP): Incidencia Delictiva del Fuero Común

Estado	Año	Homicidio doloso	Trata de personas	Narcotráfico	Portación de arma de	Extorsión	Secuestro	Robo con violencia	Homicidio doloso. %	Trata de personas %	Narcotráfico % cambio	Portación de arma de	Extorsión % Cambio	Secuestro % cambio	Robo con violencia %
Chiapas	2018	8.5	0.2	1.5	2.0	1.0	0.5	15.0							
	2019	9.0	0.3	1.6	2.1	1.1	0.6	16.0	6.0	50.0	7.0	5.0	10.0	20.0	7.0
	2020	8.8	0.2	1.4	1.9	1.0	0.5	14.0	-2.0	-33.0	-13.0	-10.0	-9.0	-17.0	-12.0
	2021	8.2	0.2	1.3	1.8	0.9	0.4	13.0	-7.0	0.0	-7.0	-5.0	-10.0	-20.0	-7.0
	2022	7.5	0.1	1.2	1.7	0.8	0.3	12.0	-9.0	-50.0	-8.0	-6.0	-11.0	-25.0	-8.0
	2023	7.0	0.1	1.1	1.6	0.7	0.2	11.0	-7.0	0.0	-8.0	-6.0	-13.0	-33.0	-8.0
Oaxaca	2018	12.0	0.3	2.0	2.5	1.5	0.7	20.0							
	2019	13.0	0.4	2.1	2.6	1.6	0.8	21.0	8.0	33.0	5.0	4.0	7.0	14.0	5.0
	2020	12.5	0.3	2.0	2.4	1.4	0.7	19.0	-4.0	-25.0	-5.0	-8.0	-13.0	-13.0	-10.0
	2021	11.8	0.3	1.9	2.3	1.3	0.6	18.0	-6.0	0.0	-5.0	-4.0	-7.0	-14.0	-5.0
	2022	11.0	0.2	1.8	2.2	1.2	0.5	17.0	-7.0	-33.0	-5.0	-4.0	-8.0	-17.0	-6.0
	2023	10.5	0.2	1.7	2.1	1.1	0.4	16.0	-5.0	0.0	-6.0	-5.0	-8.0	-20.0	-6.0
Veracruz	2018	15.0	0.4	2.5	3.0	2.0	1.0	25.0							
	2019	16.0	0.5	2.6	3.1	2.1	1.1	26.0	7.0	25.0	4.0	3.0	5.0	10.0	4.0
	2020	15.5	0.4	2.3	2.8	1.8	0.9	24.0	-3.0	-20.0	-12.0	-10.0	-14.0	-18.0	-8.0

	2021	14.8	0.4	2.2	2.7	1.7	0.8	23.0	-5.0	0.0	-4.0	-4.0	-6.0	-11.0	-4.0
	2022	14.0	0.3	2.1	2.6	1.6	0.7	22.0	-5.0	-25.0	-5.0	-4.0	-6.0	-13.0	-4.0
	2023	13.5	0.3	2.0	2.5	1.5	0.6	21.0	-4.0	0.0	-5.0	-4.0	-6.0	-14.0	-5.0

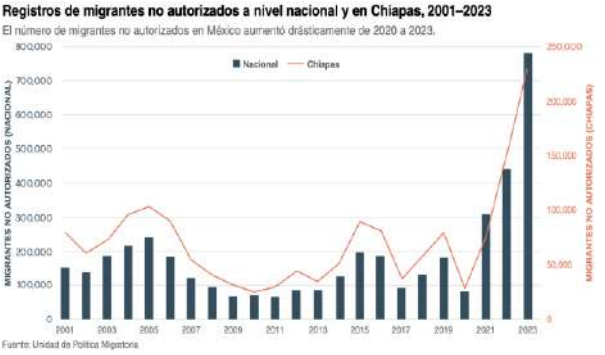
Los datos presentados advierten que el delito de Homicidio Doloso en las Zonas en Conflicto se deriva fundamentalmente de las rivalidades entre los cárteles de la droga, como el Cártel Jalisco Nueva Generación (CJNG) y el Cártel de Sinaloa, sus asociados y grupos antagonistas locales, esto está estrechamente relacionado con el aumento de la violencia en estas regiones, con las luchas por el control de territorios estratégicos: rutas de tráfico de drogas, extorsión, contrabando, robo de combustible, tráfico de migrantes; sin embargo, estas cifras englobadas por estado, no tienen una significancia importante, no contribuyen de manera sustancial en el incremento a nivel estatal y al contrario se ha encontrado una disminución, sino contundente, clara, en diversos delitos.

Tabla 4. tasas por 100,000 habitantes de delitos seleccionados en Chiapas, Oaxaca y Veracruz (2018-2023)[58]

Para el homicidio doloso, la extorsión, el secuestro, el robo con violencia, todos ellos han registrado caídas. De este modo, se pueden sugerir varios puntos de interpretación, entre otros, los cambios de las dinámicas de los grupos criminales en la región y la intervención y detección por parte del estado para su mitigación. Dos delitos podrían estar subestimados, son los relativos a la trata de personas y secuestro, que podrían sugerir subregistro.

Registros de Migrantes no Autorizados a nivel nacional y en Chiapas 2001-2023[59]

[58] Nota metodológica en anexo
[59] Índice de Paz México 2024: Identificación y medición de los factores que impulsan la paz.



El narcotráfico, la trata de personas, el contrabando de mercancías y el tráfico de armas son los principales delitos y economías criminales que impulsan la violencia en la región, los estados y sus municipios. Todas estas tendencias apuntan a una mejora en el control de ciertos delitos de alto impacto. Los números también muestran variaciones en la intensidad y frecuencia, del homicidio doloso y el robo con violencia, aunque han disminuido, siguen teniendo tasas que implican un entorno adverso, volátil y violento. En el caso de Veracruz, particularmente las cifras más altas en delitos como el homicidio y la extorsión, mientras que la portación de armas de fuego muestra una tendencia decreciente, aunque esto no necesariamente garantiza una menor capacidad de los grupos criminales para cometer actos violentos y tampoco implica una situación de seguridad estable o consolidada.

Este incremento sostenido de los homicidios dolosos entre 2019 y 2023 en estas localidades específicas, revela la creciente influencia de grupos criminales, las cuales vemos representadas directamente en su incremento porcentual delincuencial que deriva de su disputa. Se debe de apuntar que, si bien es cierto, no todos los delitos corresponden exclusivamente a una única economía criminal; algunas de ellas pueden abarcar y albergar varios tipos de delitos.

Un hallazgo que nos presentan los datos es que el desarrollo de la geografía del Corredor Interoceánico, se encuentra enclavado en el teatro de operación de la delincuencia, la amenaza de la criminalidad se actualiza de manera focalizada de forma subregional (Localidades y Municipios) a regional (Estados), cuando una economía criminal entra en pausa, las economías criminales secundarias se incrementan en apoyo de las primarias, esto sucede cuando la presencia del Estado persiste o se incrementa, pero la amenaza principal prevalece, se mantiene y muta, en espera de volverse a actualizar.

En contraste con la disminución de la violencia entre 2019 y 2024, la percepción de inseguridad y corrupción, han incrementado. Según los datos de la ENVIPE, la percepción de inseguridad en estas áreas está fuertemente

vinculada a la extorsión y otras actividades controladas por la delincuencia, lo que muestra cómo los actores no estatales en un Conflicto de Cuarta Generación (4GW) ejercen violencia irregular y tácticas asimétricas para consolidar su control sobre territorios que consideren estratégicos (*World Justice Project*, 2023; INEGI, 2023).

Tabla 5 Percepción de Inseguridad y Corrupción (2019-2023)[60]

Año	Chiapas (Percepción de Inseguridad % - ENVIPE)	Oaxaca (Percepción de Inseguridad % - ENVIPE)	Veracruz (Percepción de Inseguridad % - ENVIPE)	Corrupción - Chiapas % (Percepción - ENVIPE)	Corrupción - Oaxaca % (Percepción - ENVIPE)	Corrupción - Veracruz % (Percepción - ENVIPE)	Ranking Nacional (Estado de derecho - WJP)
2019	80.0 %	77.0 %	85.0 %	70.0 %	68.0 %	72.0 %	99 de 126
2020	82.0 %	78.0 %	86.0 %	71.0 %	69.0 %	73.0 %	104 de 128
2021	83.0 %	80.0 %	87.0 %	73.0 %	70.0 %	74.0 %	107 de 130
2022	84.0 %	81.0 %	88.0 %	74.0 %	71.0 %	75.0 %	109 de 132
2023	85.0 %	82.0 %	89.0 %	75.0 %	72.0 %	76.0 %	113 de 134

6. El Corredor Interoceánico, el *Nearshoring* y sus riesgos

México, dentro de los países de América Latina, está posicionado como uno de los más relevantes para aprovechar el auge del *nearshoring* (Forbes México, 2023), una tendencia acelerada por las disrupciones globales en las cadenas de suministro (EGADE Business School, 2023). Esta práctica, que implica reubicar operaciones de manufactura y servicios más cerca de los mercados, ha tenido grandes alicientes en un contexto geopolítico volátil, como la guerra económica y el desacoplamiento comercial entre China y Estados Unidos (France 24, 2024) y las tensiones por conflictos armados en Ucrania, Rusia, Irán y el Medio Oriente (El País, 2024; Euronews, 2024).

Según el Índice de la Paz México 2024, en su apartado "Impacto Económico de la Violencia" define esta acepción como: "el gasto y el efecto económico relacionados con contener, prevenir y afrontar las consecuencias de la violencia. Comprende el costo económico de la violencia (tanto directo como indirecto) más un efecto multiplicador" (Índice de Paz, 2024), y datos según este estudio, el impacto económico de la violencia en 2023 para Chiapas fue de 116.4 mil millones de pesos, representando el 24.3 % del PIB estatal, para Oaxaca alcanzó los 133.4 mil millones de pesos en 2023, lo que representa el 26.1 % del PIB estatal, el impacto de la violencia en Oaxaca aumentó un

[60] Nota metodológica en anexo

100.8 %, posicionándolo entre los estados con mayor deterioro en este aspecto, mientras que Veracruz experimentó un impacto económico de la violencia de 195.7 mil millones de pesos, correspondiente al 14.6 % de su PIB en 2023.

Es entonces que Chiapas: ocupa el 3er lugar entre los estados con menor impacto económico de la violencia, Oaxaca se sitúa en la 14.ª posición y Veracruz en el 11.º lugar, en el deterioro económico. El Fondo Monetario Internacional coincide con estas consideraciones en su reporte "México: Consulta y revisión del Artículo IV 2024 bajo el Acuerdo de Línea de Crédito Flexible-Comunicado de Prensa; Informe del Personal, y Declaración de la directora ejecutiva para México 1 de noviembre de 2024" advierte que:

> "El costo económico y la percepción del delito están más concentrados en el sur y varían sustancialmente entre estados e indicadores. Los delitos pueden implicar costos económicos directos, con pérdidas directas debidas al delito (por ejemplo, costos de robos y extorsiones), gastos de las empresas en seguridad y también costos indirectos, ya que las decisiones pueden tener en cuenta los costos esperados del delito, que pueden reflejar no solo el delito real, sino también la percepción de la prevalencia del delito. El gasto en seguridad en el ámbito de empresa está muy vinculado con el historial de pérdidas por delito y algo vinculado con los homicidios pasados a nivel estatal, pero no parece estar relacionado con pérdidas u homicidios posteriormente menores. Además, el delito toma formas divergentes en los estados: algunos con tasas de homicidios más altas frente a otros con más pérdidas económicas. Si bien se podría esperar que las organizaciones criminales generen tanto homicidios como costos económicos como extorsiones, **las correlaciones ligeramente negativas entre homicidios y pérdidas económicas sugieren que hay otros mecanismos en juego. Por ejemplo, cuando una organización criminal enfrenta menos disputas, puede extraer más ingresos, mientras que los homicidios pueden ser menores".** (IMF, 2024)

El organismo internacional observa que: "(…) mejorar la gobernabilidad está asociado con mayores flujos de IED; mientras el crimen está asociado con mayor emigración y un consistente aumento de las remesas al país de origen". (CITA). El objeto de nuestro estudio es comprobar o no, si la violencia es un factor que desmotive la estrategia del *nearshoring* en el país, para ello tenemos que advertir que una variable que es fundamental para representar el interés de las empresas en la inversión se refiere a la Inversión Extranjera Directa, en subsectores como el de infraestructura, empleos nuevos y reinversión, deberemos de advertir si la correlación con los datos de violencia generan

desmotivación, para ello utilizaremos una matriz de correlación entre estos factores:

7. Análisis de Estudio

El Análisis de matriz de correlación completa ha arrojado resultados de gran interés y que desmantelan ciertas suposiciones sobre el impacto de la criminalidad y la percepción de inseguridad en la inversión extranjera directa (IED). Aunque se esperaría que un contexto de inseguridad y alta incidencia delictiva como el que acontece en los estados analizados presupone una disminución en la confianza de los inversionistas en los estados de Oaxaca, Chiapas y Veracruz, los datos sugieren una relación más compleja y menos directa de lo anticipado.

En términos generales, la correlación entre las tasas de delitos violentos —incluyendo homicidio doloso, trata de personas, narcomenudeo, secuestro y la percepción de inseguridad— en relación con los flujos de IED resulta de mediana a alta para operaciones en los sectores de construcción de ingeniería civil y para la construcción de obras de suministro. Este hallazgo indica que, aunque la criminalidad pueda representar un riesgo en particular para Estados como Veracruz que sus índices de criminalidad resultan más altos, no deja de haber inversión, mientras que, para Chiapas y Oaxaca, resulta más importante la percepción que incluso la tasa de delitos, sin embargo, sus números para IED siempre han sido poco favorables.

La percepción de inseguridad, un indicador subjetivo que refleja el sentimiento general de la población sobre su entorno, también mostró una correlación mediana limitada con las cifras de inversión en estos sectores. Esto sugiere que, en estos casos, los inversionistas pueden estar más influenciados en otro tipo de factores que por los índices de seguridad pública percibida.

Es importante anotar que si bien el modelo que mide la percepción de inseguridad está diseñado para saber el sentimiento de estas amenazas al interior de las entidades federativas, esto no representa en ningún sentido las inquietudes que tienen los inversionistas extranjeros que reciben estímulos de todo tipo y que muy bien podrían, no representar la realidad objetiva de la región, más aún, estas tendencias en su mayoría son débiles y en algunas tienden a tener una correlación importante, no se advierten que exista una generalización por ejemplo, la variable secuestro pareciera no disuadir la reinversión, y en algunos casos, podrían estar asociados con un incremento en la reinversión de utilidades, lo cual pudiese interpretarse como una medida de mitigación de riesgos en donde las empresas adoptan estas estrategias para proteger sus operaciones, lo anterior se puede corroborar con las variables Secuestro (0.784) y Homicidio Doloso (0.639).

La relación entre las variables Percepción de Inseguridad (-0.499), Trata de Personas (-0.397) y Robo a Transportista (-0.626), es indicativa de que el riesgo derivado de estos incidentes afecta de manera adversa las decisiones de inversión, específicamente con las Nuevas Inversiones de manera mesurada y leve, esto no significa que no exista una criminalidad evidente y contundente en la región, como hemos explicado en este tipo de conflictos donde existen dos o más organizaciones de la Delincuencia Organizada en disputa, el teatro de operaciones se desarrolla en muchos ámbitos y en diferentes niveles.

En un análisis específico por estado y año, se observó que la inversión en sectores relacionados con la construcción y los servicios de almacenamiento y transporte no presentó una disminución consistente en años de alta criminalidad. Más aún, en algunos periodos y estados, hubo incrementos en la IED en sectores clave pese a un contexto de inseguridad elevado, lo cual puede indicar que los inversionistas priorizan las condiciones de mercado, incentivos fiscales o políticas locales de desarrollo sobre los niveles de criminalidad. Este patrón es especialmente notorio en el sector de construcción de infraestructura de transporte y almacenamiento, que mantiene una tendencia de inversión relativamente estable a pesar de las fluctuaciones en las tasas delictivas.

Estos resultados permiten formular una hipótesis alternativa, en la cual factores como el potencial de mercado, la existencia de políticas favorables, y la cercanía estratégica a corredores comerciales y proyectos de infraestructura, como el Tren Interoceánico en el caso del sur de México, podrían jugar un papel más relevante que la seguridad en la atracción de inversión extranjera. En consecuencia, la criminalidad y la percepción de inseguridad, aunque relevantes en el contexto social, no parecen ser los principales condicionantes para la toma de decisiones en los sectores de IED estudiados.

Finalmente, cabe destacar que los resultados sugieren una cierta resiliencia de la inversión extranjera en estos estados frente a condiciones de inseguridad. Este análisis indica que la IED en sectores fundamentales de infraestructura no se ve notablemente disuadida por el entorno de violencia y criminalidad en los estados del sur de México. Si bien existen fluctuaciones en los flujos de inversión, estas no parecen responder directamente a la percepción de inseguridad ni a los índices de violencia. Este fenómeno refleja una relativa independencia de la inversión en infraestructura con respecto a las condiciones de seguridad, lo que abre nuevas líneas de investigación sobre los factores que motivan o inhiben el capital extranjero en contextos de alta criminalidad.

8. Conclusiones[61].

Primero: Que la información arroja que la captación de la Inversión Extranjera Directa (IED) para las entidades de Chiapas y Oaxaca durante el periodo 2018-

[61] Posibles sesgos, en anexo.

2023 ha sido limitada en contraste con el estado de Veracruz que ocupa el cuarto lugar en el ranking nacional, este tiene mejores oportunidades por albergar mejores condiciones de infraestructura logística y de transporte, parques industriales y clústeres manufactureros lo cual da como resultado un ecosistema más atractivo.

Segundo: Los estados de Chiapas y Oaxaca ocupan dentro del ranking de Inversión Extranjera Directa (IED) Nacional posiciones muy desfavorables, que, si bien han ido mejorando, no han sido suficientes para la captación de inversión contraria a Veracruz, esto sugiere que un mejor desarrollo económico está asociado a una mayor atracción de inversión extranjera.

Tercero: El desarrollo industrial del Corredor Interoceánico y sus polos son efectivamente el catalizador para la región; sin embargo, necesita maduración y tiempo para su consolidación y, en consecuencia, para que se vuelva atractivo para los inversores.

Cuarto: Los valores indican una correlación débil entre la Inversión Extranjera Directa (IED) y los indicadores de seguridad en un entorno definido con un Conflicto de Cuarta Generación (4GW) entre diversos cárteles de la droga, en especial, el Cártel de Sinaloa contra el Cártel Jalisco Nueva Generación (CJNG) y sus *proxys* para los tres estados, aunque existe una relación inversa, **no** es lo suficientemente fuerte para afirmar que un aumento de la violencia impacta significativamente en la captación de la Inversión Extranjera Directa (IED). Los indicadores como el homicidio doloso, secuestro, narcotráfico, trata de personas, Delincuencia Organizada fueron determinados con relación a las particularidades de la definición del Conflicto de Cuarta Generación (4WG). Es entonces que la percepción que se tiene de la violencia es evidentemente negativa, el entorno de riesgo es moderado o alto, los inversionistas no ven a la inseguridad como un impedimento especialmente si las oportunidades económicas justifican los costos de operar en dichos entornos. Finalmente, la inseguridad, se puede afirmar, es un factor de relevancia, pero no determinante para la inversión, esto es si bien hay ciertas variables que resultan de interés, como por ejemplo la percepción de inseguridad que tiene una correlación negativa de -0.49 (negativa moderada) con las nuevas inversiones, entonces conforme aumente la inseguridad las nuevas inversiones también disminuyen.

9. Prospectiva[62]

[62] En Anexo

Bibliografía

Lind, W. S., Nightengale, K., Schmitt, J. F., Sutton, J. W., & Wilson, G. I. (1989). *The Changing Face of War: Into the Fourth Generation*. Marine Corps Gazette, 73(10), 22-26, http://www.mca-marines.org/files/The%20Changing%20Face%20of%20War%20-%20Into%20the%20Fourth%20Generation.pdf

Robb, J. (2008). *Brave New War: The Next Stage of Terrorism and the End of Globalization*. John Wiley & Sons.

Sullivan, John P., and Robert J. Bunker. "Drug Cartels, Street Gangs, and Warlords." *Small Wars & Insurgencies* 13, no. 2 (2002): 40-53.

Gobierno de México. (n.d.). ¿Qué hacemos? *Corredor Interoceánico del Istmo de Tehuantepec*. https://www.gob.mx/ciit/que-hacemos

Kearney. (2022). *The 2022 Kearney Foreign Direct Investment Confidence Index*. Kearney. https://www.kearney.com/foreign-direct-investment-confidence-index

Vego, M. (2020). *Joint Operational Warfare: Theory and Practice*. Naval War College Press.

Clausewitz, C. von. (1984). *On War* (M. et al., Eds. y Trans.). Princeton University Press. (Original work published 1832).

Kaldor, M. (*2001). Las nuevas guerras: la violencia organizada en la era global*. Tusquets Editor.

Bolstering Ukraine's Irregular War Against Russia. (2024). RAND Corporation.

Modern War Institute. (2021). From guerrilla to maneuver warfare: A look at the talibán's growing combat capability.

Demmers, J. (2017). *Theories of Violent Conflict: An Introduction* (2da ed.). Routledge.

Felbab-Brown, V. (2019). *Crime, conflict, and cartels: The changing dynamics of Mexico's war on drugs*. Brookings Institution. https://www.brookings.edu/research/crime-conflict-and-cartels/

Méndez, E. (2020). *El narcotráfico y la violencia en México: Estrategias y dinámicas*. Fondo de Cultura Económica.

Moghadam, A., Rauta, V., & Wyss, M. (2023). *Routledge Handbook of Proxy Wars*. Taylor & Francis.

Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP). (2024). *Incidencia delictiva y víctimas del fuero común 2024*. https://www.gob.mx/sesnsp

El Financiero. (2024). *Sexenio de AMLO cerró con récord de 199,952 asesinatos*. https://www.elfinanciero.com.mx

Guerra, Víctor Hugo, *Presentación del libro "Economías Criminales":. "Enfoques multidimensionales"* https://www.youtube.com/watch?v=nEdANT1r2C8 2024.

Saviano, R. (2015). *Gomorra: Viaje al imperio económico y al sueño de dominio de la Camorra*. Debate.

Shelley, L. (2020). *Dark Commerce: How a New Illicit Economy is Threatening Our Future*. Princeton University Press.

Organización de los Estados Americanos (OEA). (2020). *La seguridad multidimensional y su impacto en las Américas*. https://www.oas.org

White House. (2022). *National Security Strategy*. https://www.whitehouse.gov

UNODC. (2023). *Impact of Transnational Organized Crime on Stability and Development*. United Nations Office on Drugs and Crime. https://www.unodc.org

White House. (2023). *Strategy to Combat Transnational Organized Crime*. https://www.whitehouse.gov

Gobierno de México. (2024). *Estrategia de seguridad de los primeros 100 días* (p. 17). Ciudad de México: Autor.

Prieto-Curiel, R., Campedelli, G. M., & Hope, A. (n.d.). *Spanish translation of supplementary material for Science.adh2888*. Science. https://www.science.org/action/downloadSupplement?doi=10.1126%2Fscience.adh2888&file=science.adh2888_spanish_translation_aam.pdf

AC Consultores. (2023). *Estudio sobre crimen organizado en México*. Con datos recolectados por el colectivo "Guacamaya Leaks". https://shorturl.at/hcJ1Y

Blin, A. (2023). *Fourth Generation Warfare: Understanding its impact on modern conflicts*. Small Wars Journal.

Insight Crime. (2023). *How Mexico's Cartels Have Learned Military Tactics*. https://www.insightcrime.org

Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2024). *Datos abiertos de incidencia delictiva*. https://www.gob.mx/sesnsp.

Secretaría de Gobernación (Segob). (s. f.-a). *Actividades que desarrolla el Ferrocarril del Istmo de Tehuantepec S.A. de C.V.* https://www.ferroistmo.com.mx/actividades-que-desarrolla-el-ferrocarril-del-istmo-de-tehuantepec-s-a-de-c-v/

Secretaría de Gobernación (Segob). (s.f.-b). *Infraestructura.* https://www.ferroistmo.com.mx/

Secretaría de Gobernación (Segob). (s. f.-c). *Polos del Desarrollo para el Bienestar (PODEBIS).* https://www.gob.mx/ciit/articulos/polos-de-desarrollo-para-el-bienestar-podebis?idiom=es

Secretaría de Gobernación (Segob). (s. f.). *79 municipios, Istmo de Tehuantepec, CIIT*. https://www.gob.mx/cms/uploads/attachment/file/533667/79_MUNICIPIOS_ISTMO_DE_TEHUANTEPEC__CIIT_.pdf

InSight Crime. (2023a). *Chiapas: A Battleground for Mexico's Drug Cartels*. https://www.insightcrime.org/news/analysis/chiapas-battleground-mexico-drug-cartels/

InSight Crime. (2023b). *Cross-Border Criminal Dynamics in Chiapas and Guatemala*. https://www.insightcrime.org/guatemala-chiapas-criminal-collaboration

Martínez, I. (2023). *Indigenous Communities and Organized Crime in Chiapas*. Journal for Peace and Justice Studies, 33(2), 145-162.

Ramírez, M. (2023). *Control Territorial en el Istmo de Tehuantepec: Los cárteles en la región del tren interoceánico*. La Silla Rota. https://www.lasillarota.com/opinion/2023/7/16/carteles-en-oaxaca-el-control-del-istmo-313455.html

Instituto Nacional de Estadística y Geografía. (2023). *Defunciones por homicidio*. INEGI. Recuperado de https://www.inegi.org.mx/sistemas/olap/proyectos/bd/continuas/mortalidad/defuncioneshom.asp?s=est

Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2023). *Incidencia Delictiva del Fuero Común - Nueva Metodología*. SESNSP. Recuperado de https://www.gob.mx/sesnsp/acciones-y-programas/incidencia-delictiva-del-fuero-comun-nueva-metodologia

Consejo Nacional de Población. (2023). *Proyecciones de la población de los municipios de México, 2015-2030*. CONAPO.

Secretaría de Gobernación. (2023a). *Incidencia Delictiva y Control Territorial del CJNG en Veracruz*. Gobierno de México. https://www.gob.mx/sesnsp

Infobae. (2023). *Narco en Chiapas: Qué grupos criminales se disputan el territorio al sur del país*. Infobae. https://www.infobae.com/mexico/2023/09/24/narco-en-chiapas-que-grupos-criminales-se-disputan-el-territorio-al-sur-del-pais/

El Universal de México (2024, octubre). Documentos hackeados por el colectivo Guacamaya Leaks y publicados por el Periódico El Universal de México, muestran análisis delictivo en Oaxaca, Chiapas y Veracruz. https://drive.google.com/file/d/14Qq71D3_6dyRdQkiAYpWGE1b7SW03jei/view ; https://drive.google.com/file/d/1A2vnNjynNU8nLkH4koXLmWimgaSmpK0m/view

Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP). (2024). *Incidencia delictiva del fuero común*, Gobierno de México. Recuperado de https://www.gob.mx/sesnsp/acciones-y-programas/incidencia-delictiva-del-fuero-comun-nueva-metodologia

Centro de Investigación Económica y Presupuestaria (CIEP). (2023). *Presupuesto para proyectos prioritarios 2018-2024: Fortalecer la transparencia y priorizar la inversión*. Recuperado de https://ciep.mx/presupuesto-para-proyectos-prioritarios-2018-2024-fortalecer-la-transparencia-y-priorizar-la-inversion/

Lind, W. S., Nightengale, K., Schmitt, J. F., Sutton, J. W., & Wilson, G. I. (1989). *The changing face of war: Into the fourth generation. Marine Corps Gazette, 73*(10), 22-26.

Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. *Potomac Institute for Policy Studies*.

Felbab-Brown, V. (2020). *Narco-nomics: How to run a drug cartel*. Oxford University Press.

Instituto Nacional de Estadística y Geografía (INEGI). (2023). *Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE)*. https://www.inegi.org.mx/programas/envipe/

Shelley, L. I. (2020). *Dark commerce: How a new illicit economy is threatening our future*. Princeton University Press.

World Justice Project (2023). *Rule of Law Index 2023*. https://worldjusticeproject.org/our-work/research-and-data/wjp-rule-law-index

El País. (2024, 24 de junio). *El apoyo de China y Corea del Norte a la industria bélica de Rusia desata las alarmas entre EE. UU. y sus aliados*. Recuperado de https://elpais.com/internacional/2024-06-24/el-apoyo-de-china-y-corea-del-norte-a-la-industria-belica-de-rusia-desata-las-alarmas-entre-ee-uu-y-sus-aliados.html

Euronews. (2024, 12 de abril). *El precio del oro aumenta mientras se intensifica la tensión geopolítica en Oriente Medio*. Recuperado de https://es.euronews.com/my-europe/2024/04/12/el-precio-del-oro-aumenta-mientras-se-intensifica-la-tension-geopolitica-en-oriente-medio

EGADE Business School. (2023, 12 de diciembre). *El círculo virtuoso de la cadena de suministro y el nearshoring*. Recuperado de https://egade.tec.mx/es/egade-ideas/investigacion/el-circulo-virtuoso-de-la-cadena-de-suministro-y-el-nearshoring

Forbes México. (2023, 15 de agosto). *Nearshoring en México: estos son los beneficios que podría obtener el país a 2030*. Recuperado de https://forbes.com.mx/nearshoring-en-mexico-estos-son-los-beneficios-que-podria-obtener-el-pais-a-2030/

Larraín, F., & Cifuentes, G. (2024). *Nearshoring* in Latin America: Who could benefit most? *Americas Quarterly*. https://www.americasquarterly.org/article/nearshoring-in-latin-america-who-could-benefit-most/

Astorga, L. (2019). *El crimen organizado en México: Historia y reflexiones*. Fondo de Cultura Económica.

International Monetary Fund. Western Hemisphere Dept. (2024), "México: 2024 *Article IV Consultation and Review Under the Flexible Credit Line Arrangement-Press Release; Staff Report; and Statement by the Executive Director for Mexico"*, *IMF Staff Country Reports* 2024, 317 accessed November 4, 2024, https://doi.org/10.5089/9798400292620.002

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

Ciberseguridad orquestable: tendencias de IA para ciberdefensa proactiva y ciberinteligencia automatizable

Carlos Estrada Nava*

Resumen: En la era digital la ciberseguridad se ha convertido en una prioridad global que afecta significativamente a individuos y organizaciones debido al incremento de dispositivos conectados y la dependencia tecnológica. La inteligencia artificial (IA) se considera una espada de doble filo: facilita un análisis de datos más eficiente y rápido, permitiendo una detección y respuesta más avanzadas a las amenazas; pero puede ser utilizada por actores malintencionados para amplificar la sofisticación y alcance de sus ataques. México se encuentra en una posición vulnerable, siendo uno de los países más impactados en América Latina y sin una Agencia Nacional de Ciberseguridad Civil que coordine una defensa integral. La adopción de una ciberseguridad orquestable se vuelve esencial, para integrar y coordinar diversas herramientas y procesos de seguridad mediante IA, logrando una defensa cohesionada y eficiente. Esto permite una ciberdefensa proactiva, anticipando y neutralizando amenazas antes de que se materialicen, y facilita una ciberinteligencia automatizable, permitiendo la recolección y análisis continuos de inteligencia sobre amenazas con mínima intervención humana. Esto requiere mejores prácticas ante un mundo digital en rápida evolución, incluyendo cooperación internacional, actualización de marcos legales y educación.

Palabras clave: Ciberseguridad, Inteligencia Artificial, Ciberdefensa, Transformación Digital.

* Coordinador de la Especialidad de Ciberdefensa, de la Escuela Militar de Inteligencia, en el Centro de Estudios del Ejército y Fuerza Aérea (Secretaría de la Defensa Nacional); fundador del programa WomenCISO para Google (Alphabet Inc.) en América Latina; y titular de la asignatura de Ciberseguridad de la Maestría en Inteligencia para la Seguridad Nacional (INAP), de la Universidad de las Américas Puebla (UDLAP), y del Diplomado de Prospectiva del Instituto Mexicano de Estudios Estratégicos en Seguridad y Defensa Nacionales (IMEESDN). Perito de cómputo forense y consultor de ciberseguridad por 16 años (Ernst & Young, Kroll Inc., FTI Consulting), e instructor para guardia nacional, policías estatales y cámaras de comercio. Titulado como técnico en computación, en gestión y administración pública, postgrado en Business Administration por University of Phoenix (Arizona, EUA), y con estudios de ingeniería en desarrollo de software. Autor del "Atlas de riesgos para la Seguridad Nacional Cibernética en México" (Revista de Administración Pública, número 148). Correo: carlos.estrada@udlapjenkins.mx

Abstract: In the digital era, cybersecurity has become a global priority that significantly affects individuals and organizations due to the increase in connected devices and technological dependence. Artificial Intelligence (AI) is considered a double-edged sword: it facilitates more efficient and faster data analysis, allowing for more advanced threat detection and response; but it can be used by malicious actors to amplify the sophistication and reach of their attacks. Mexico finds itself in a vulnerable position, being one of the most impacted countries in Latin America and lacking a National Civil Cybersecurity Agency to coordinate a comprehensive defense. The adoption of orchestrable cybersecurity becomes essential to integrate and coordinate various security tools and processes through AI, achieving a cohesive and efficient defense. This allows for proactive cyberdefense, anticipating and neutralizing threats before they materialize, and facilitates automatable cyberintelligence, enabling the continuous collection and analysis of threat intelligence with minimal human intervention. This requires better practices that protect us in a rapidly evolving digital world, including international cooperation, updating of legal frameworks, and education.

Keywords: Cybersecurity, Artificial Intelligence, Cyberdefense, Digital Transformation.

Introducción

La pandemia de Covid19 ha sido un catalizador para acelerar la transformación digital, con lo cual hemos tenido una proliferación de dispositivos conectados, por tanto, para los cibercriminales, se ha ampliado la "superficie de ataque"[63]. A su vez, la segunda causa del crecimiento exponencial de incidentes cibernéticos en el mundo radica en las nuevas maneras en que se pueden monetizar los ataques, mediante criptomonedas.

Entre las amenazas de nueva generación se encuentran el *juice jacking* (ataques a dispositivos a través de puertos de carga USB públicos), los script kiddies (individuos sin experiencia que utilizan herramientas de auto aprendizaje), el catfishing (suplantación de identidad en línea), el doxxing (publicación de información personal sin consentimiento), los evil twins (puntos de acceso Wi-Fi falsos), las vulnerabilidades de zero-day (sin precedentes), el domain squatting (registro de dominios similares a marcas conocidas), el malware polimórfico (que cambia su código fuente), la ejecución remota de código, técnicas de living off the land (uso de herramientas legítimas

[63] Se refiere al conjunto total de puntos o caminos a través de los cuales un usuario no autorizado puede entrar o extraer datos de un entorno. Esta superficie incluye todas las áreas accesibles que podrían ser explotadas por actores maliciosos para realizar acciones no autorizadas, como acceder a información sensible, ejecutar código malicioso o alterar funciones del sistema. Los componentes de la superficie de ataque pueden incluir software, redes, e interfaces de usuario entre otros.

para actividades maliciosas) y ataques a la cadena de suministro (software) como los casos de Log4j y SolarWinds.

Microsoft (2023) señala que el número de ataques de contraseña detectados aumentó de 579 por segundo a más de 4,000 por segundo en solo dos años. Las organizaciones a menudo utilizan una colección desconectada de herramientas de seguridad fragmentadas, lo que resulta en una sobrecarga de datos, fatiga de alertas y visibilidad limitada a través de las soluciones de seguridad. Los equipos de seguridad enfrentan un desafío asimétrico: deben proteger todo, mientras que los cibercriminales solo necesitan encontrar un punto débil. Por estas razones, según McKinsey (2024) la adopción de IA por parte de las organizaciones aumentó al 72% en 2024, en diversas regiones e industrias.

En este contexto, México se ha posicionado como uno de los países más vulnerados por ataques cibernéticos en América[64]. En la transición de la Policía Federal a la Guardia Nacional, y la adscripción de ésta a la Secretaría de la Defensa Nacional (SEDENA), se ha mantenido una unidad cibernética todavía de carácter civil, condición que habrá de cambiar conforme se consoliden las nuevas atribuciones de la Secretaría de Seguridad y Protección Ciudadana, acordes a la reforma al artículo 21 Constitucional y a la Ley Orgánica de la Administración Pública Federal, aprobadas entre el 14 y el 28 de noviembre de 2024, que eventualmente fortalecerán la instancia civil con facultades en materia de ciberseguridad, incluso una Agencia Nacional de Ciberseguridad Civil, que coordine esfuerzos y políticas en esta materia. Por su parte, se espera que la Guardia Nacional haya de formar los cuadros que desempeñarán tales funciones en la Subjefatura de Investigación e Inteligencia, creada en marzo de 2024.

En el sector privado también existen rezagos. Ante el fenómeno del *nearshoring*, se debe cumplir con el programa Customs Trade Partnership Against Terrorism (CTPAT), gestionado por la Oficina de Aduanas y Protección Fronteriza de Estados Unidos (CBP). Este programa requiere, entre otras cosas, la realización de pruebas de penetración (pentesting) para asegurar la integridad de las cadenas de suministro, pero estimamos que menos del 35% de exportadoras lo cumple.

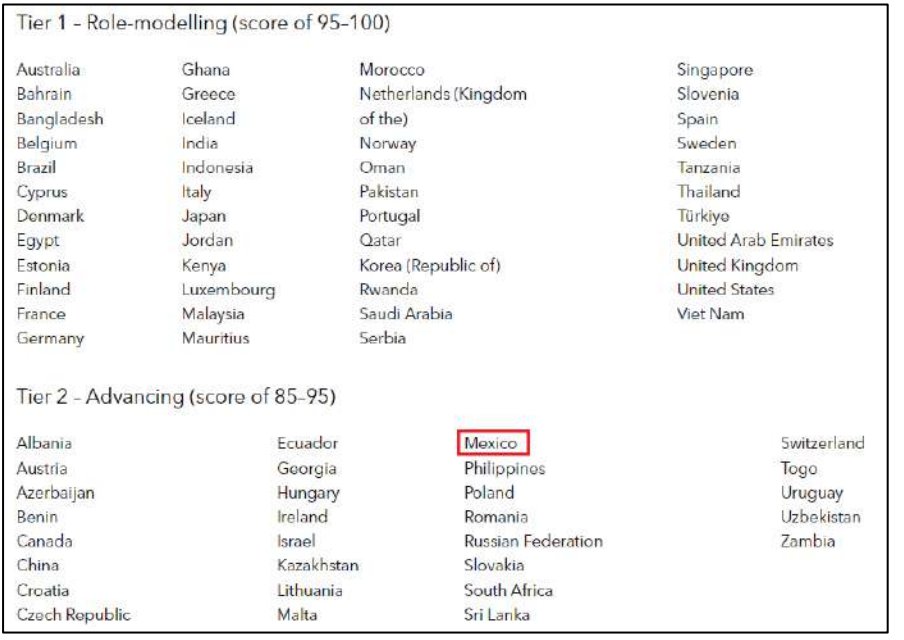
Estado crítico de la ciberseguridad en México

El Índice de Ciberseguridad Global (GCI, en el reporte original) de la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés), de la Organización de las Naciones Unidas (ONU), evalúa el compromiso de los países con la ciberseguridad en cinco pilares fundamentales: legal, técnico,

[64] Puede revisarse semanalmente la estadística desde el mayor antivirus https://cybermap.kaspersky.com/

organizativo, desarrollo de capacidades y cooperación internacional. En la edición de 2021, México ocupó el puesto 52 con una puntuación de 81.68 (en escala de 0 a 100), y aunque en la edición más reciente de 2024 mejoró ligeramente a 85.77 puntos, el país continúa en el "Tier-2", situándose fuera de los 46 principales países en ciberseguridad (véase gráfica 1).

Gráfica 1: Índice de Ciberseguridad de Naciones Unidas 2024



Tier 1 - Role-modelling (score of 95-100)

Australia	Ghana	Morocco	Singapore
Bahrain	Greece	Netherlands (Kingdom	Slovenia
Bangladesh	Iceland	of the)	Spain
Belgium	India	Norway	Sweden
Brazil	Indonesia	Oman	Tanzania
Cyprus	Italy	Pakistan	Thailand
Denmark	Japan	Portugal	Türkiye
Egypt	Jordan	Qatar	United Arab Emirates
Estonia	Kenya	Korea (Republic of)	United Kingdom
Finland	Luxembourg	Rwanda	United States
France	Malaysia	Saudi Arabia	Viet Nam
Germany	Mauritius	Serbia	

Tier 2 - Advancing (score of 85-95)

Albania	Ecuador	Mexico	Switzerland
Austria	Georgia	Philippines	Togo
Azerbaijan	Hungary	Poland	Uruguay
Benin	Ireland	Romania	Uzbekistan
Canada	Israel	Russian Federation	Zambia
China	Kazakhstan	Slovakia	
Croatia	Lithuania	South Africa	
Czech Republic	Malta	Sri Lanka	

Fuente: Global Cybersecurity Index 2024, ITU, ONU.

La clasificación en el GCI pone de manifiesto las áreas en las que México necesita fortalecer su postura de ciberseguridad[65]: adoptar tecnologías avanzadas y desarrollar marcos legales y organizativos actuales. La principal consecuencia de una deficiente postura de ciberseguridad en México implica que nuestro país ha experimentado una serie de incidentes cibernéticos de alto perfil que han afectado tanto al sector público como al privado (véase lista 1). La mayoría de los incidentes cibernéticos en México no son conocidos o su

[65] La "postura de ciberseguridad" de una organización se entiende como el estado general de su seguridad de la información y su capacidad para proteger sus activos de información y sistemas contra amenazas cibernéticas. Incluye una variedad de elementos que determinan cuán bien está preparada una organización para prevenir incidentes de seguridad, detectar amenazas, responder a ataques y recuperarse de ellos.

información se reserva hasta por 5 años por parte del gobierno federal ("Reservan datos del ciberataque a Pemex", 2020).

Lista 1: Incidentes cibernéticos de alto impacto en México

A. En 2017 en el mundo se produjo un ataque masivo del ransomware "WannaCry", y si bien los servicios del CERT de la entonces Policía Federal lo contuvieron en un principio, México padeció la constante evolución del ransomware, lo cual impactó a empresas de importancia.

B. El primer gran ataque de una Amenaza Persistente Avanzada (APT) contra México ocurrió en 2018 contra Bancomext (Banco de Comercio Exterior), robando más de 35 millones de dólares.

C. Hackers mexicanos autonombrados "Bandidos Revolution Team" atacaron al Sistema de Pagos Electrónicos Interbancarios (SPEI) administrado por el Banco de México en 2018, robando alrededor de 300 millones de pesos.

D. A inicios de noviembre de 2019, se dio a conocer que Petróleos Mexicanos (Pemex) fue blanco de un ataque cibernético por parte de un grupo de cibercriminales, bajo la modalidad de "Ransomware as a Service" llamado "DoppelPaymer".

E. En 2020, la Secretaría de Economía detectó un ataque cibernético en algunos de sus servidores; el ciberataque se atendió de inmediato por lo que no hubo consecuencias mayores.

F. En julio de 2020, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), el Banco de México (Banxico) y el Sistema de Administración Tributaria (SAT) sufrieron afectaciones en sus páginas de Internet.

G. El hackeo a la Secretaría de la Defensa Nacional fue una filtración de correos electrónicos, en septiembre de 2022, por un grupo de hackers llamado "Guacamaya", filtrando información sensible relacionada con operaciones militares contra el crimen organizado.

H. Desde 2020 hasta 2022 Foxconn en México (principal proveedor de microcomponentes de celulares y computadoras en el mundo) sufrió ataques de Ransomware, pidiendo pago de 35 millones de dólares.

I. En 2023 fue comprometida la operación del Aeropuerto Internacional de Querétaro debido a un ataque de Ransomware, donde se cobraba una extorsión por 5 millones de dólares.

J. Durante 2024 Coppel ha sido víctima de incidentes cibernéticos en su aplicación por Internet, lo cual afectó durante más de 2 semanas sus operaciones bancarias.

Fuente: Elaboración propia con base en reportes de la industria.

La magnitud de los incidentes de alto impacto pone de relieve la sofisticación creciente de los ataques cibernéticos y la vulnerabilidad de las infraestructuras críticas en México. A pesar de los desafíos referidos, en el último Plan Nacional de Desarrollo, correspondiente al periodo 2019-2024 no se menciona la palabra "ciberseguridad"[66], además de que en el periodo el Congreso terminó por no aprobar una Ley Nacional de Ciberseguridad, lo que plantea un atraso de al menos desde hace 25 años, cuando comenzaron las primeras generaciones de legislaciones cibernéticas en el mundo, lo que dificulta la implementación de una estrategia unificada y coherente. En la coyuntura actual, ya se plantea una discusión de ley en materia de inteligencia artificial. Entretanto, existen ciertas normativas y esfuerzos que abordan aspectos específicos para el sector público:

- 2010: Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información.
- 2017: Estrategia Nacional de Ciberseguridad, que busca establecer lineamientos generales, pero carece de fuerza vinculante.
- 2020: Estrategia Digital Nacional, enfocada en la transformación digital, pero con limitaciones en materia de seguridad.
- 2022: Protocolo Homologado de Respuesta a Incidentes de la Guardia Nacional, que centraliza la respuesta a incidentes a través de la figura de los aliados estratégicos, aunque no se cuenta con una perspectiva civil amplia.

APTs y crimen como desafíos estructurales en la ciberdefensa global

Como parte de la "taxonomía" de adversarios (atacantes) cibernéticos, se han establecido cuatro principales categorías, con base en la motivación del ataque[67]: "insiders" (que impactan a la organización que sufre el ataque), "hacktivistas" (quienes visibilizan una causa), cibercriminales (dinero) y las Amenazas Persistentes Avanzadas (APTs). Estas últimas representan uno de los mayores desafíos en el panorama de la ciberseguridad global, ya que conforman grupos sofisticados que llevan a cabo operaciones cibernéticas dirigidas y prolongadas, a menudo respaldadas por recursos de estados nacionales. La tabla 1 presenta una serie de APTs asociadas con diversos países, ilustrando la perspectiva global y geopolítica de estas amenazas, las cuales

[66] De consulta en el Diario Oficial de la Federación en: https://www.dof.gob.mx/nota_detalle.php?codigo=5565599&fecha=12/07/2019#gsc.tab=0

[67] Metodología del Modelo Diamante: comprender y atribuir actividades de ciberamenazas, mediante cuatro puntos clave: el adversario (quién realiza el ataque), la infraestructura (las herramientas y recursos usados), la capacidad (técnicas y habilidades del atacante) y la víctima (el objetivo del ataque).

obedecen a los objetivos geopolíticos de cada uno de sus respectivos estados-nación.

Tabla 1: APTs destacados de las 30 potencias cibernéticas

APT	País
DSIRF	Austria
UNC1151	Bielorrusia
G0033	Brasil
APT41	China
Lazarus	Corea del Norte
TA406	Corea del Sur
Stealth Falcon	Emiratos Árabes
KelvinSecurity	España
APT-C-39	EUA
APT-C-09	India
Storm-1167	Indonesia
APT33	Irán
Altahrea	Iraq
Black Cube	Israel
UNC4990	Italia

APT	País
BibiGun	Jordania
YoroTrooper	Kazajistán
G0070	Líbano
Scorpions	Libia
DragonForce	Malasia
Kasablanka	Marruecos
SilverTerrier	Nigeria
APT36	Pakistán
FIN4	Rumania
APT28	Rusia
APT-C-27	Siria
Anonymous64	Taiwán
Fallaga	Túnez
UNC1326	Turquía
APT32	Vietnam

Fuente: Elaboración propia con base en Malpedia, recurso del Instituto de la Información, Tratamiento de la Información y Ergonomía (FKIE por sus siglas en alemán) con sede en Frankfurt. RFA.

Según el más reciente informe de Microsoft (2024), es cada vez mayor la evidencia disponible respecto al apoyo de los comandos de hackers de estos gobiernos (APTs) hacia grupos de cibercriminales bajo la modalidad de franquicia conocida como "Ransomware as a Service", destacadamente los 3 países que también han participado en el conflicto militar contra Ucrania: Rusia, Corea del Norte e Irán.

En el caso de Rusia (Microsoft, 2024), se observa la subcontratación de actividades de ciber espionaje a grupos criminales. Entre junio y julio de 2023, Aqua Blizzard, grupo atribuido al Servicio Federal de Seguridad (FSB) de Rusia, "entregó" el acceso a 34 dispositivos ucranianos comprometidos al grupo criminal Storm-0593 (también conocido como Invisi-mole). Microsoft posee telemetría[68] con respecto a que Storm-0593 utilizó esta infraestructura en una campaña de spear-phishing contra sistemas militares ucranianos el año pasado, lo que indica un patrón de apoyo de Storm-0593 a los objetivos de recolección de inteligencia del estado ruso.

Otro ejemplo notable es el de los actores norcoreanos, como Lazarus (detrás del ataque contra Bancomext), que han llevado a cabo operaciones cibernéticas para robar criptomonedas, acumulando más de 3 mil millones de

[68] La recolección y transmisión remota de datos en tiempo real para monitorear y analizar el rendimiento o comportamiento de sistemas y dispositivos.

dólares desde 2017. Estos fondos se han utilizado para financiar programas nucleares y de misiles (Microsoft, 2024).

Además, se ha observado que Cotton Sandstorm, de Irán, han realizado operaciones con fines financieros, marcando un cambio en el comportamiento tradicional que se centraba en ataques destructivos contra Israel (Microsoft, 2024).

Estado del arte en investigación y tecnologías de ciberseguridad

La ciberseguridad es un campo híbrido donde concurren diversas disciplinas, desde ciencias de la computación, hasta temas legales, financieros y de psicología organizacional. Hoy en día, de acuerdo a la clasificación del instituto SANS[69], existen más de 60 subdominios de especialización, mismos que tienen sus propias herramientas y metodologías. En la siguiente lista 2 se agrupan en 10 núcleos para tener un currículo actualizado de ciberseguridad.

Lista 2: Áreas de especialización actuales en ciberseguridad

1. Seguridad de Redes y Comunicaciones
2. Defensa Cibernética (Equipo Azul)
3. Operaciones Ofensivas (Equipo Rojo)
4. Gestión de Incidentes y Respuesta a Incidentes
5. Inteligencia de Amenazas Cibernéticas y OSINT
6. Seguridad de Aplicaciones y Desarrollo de Software
7. Seguridad de Sistemas Operativos y Automatización
8. Análisis Forense y Forenses Digitales
9. Seguridad de Infraestructuras Críticas
10. Liderazgo y Gestión en Ciberseguridad

Fuente: "SANS Ultimate Recognition to Elite Cybersecurity Professionals".

Estos subdominios muestran cómo la ciberseguridad abarca desde la protección técnica de infraestructuras hasta la gestión y liderazgo estratégico. Un panorama amplio de las herramientas y tecnologías empleadas por esta industria, las cuales cubren la mayoría de los subdominios previamente desarrollados, se muestran en la siguiente lista 3.

Lista 3: Principales herramientas o tecnologías de ciberseguridad

[69] El Instituto SANS (oficialmente el Escal Institute of Advanced Technologies) es una empresa privada estadounidense con fines de lucro, fundada en 1989, que se especializa en seguridad de la información, capacitación en ciberseguridad y venta de certificados, líderes en la industria.

1. NGAV (Next-Generation Antivirus): Antivirus de nueva generación.
2. Firewall: Cortafuegos (incluyendo cortafuegos de red y de aplicaciones web).
3. SIEM (Security Information and Event Management): Gestión de información y eventos.
4. EDR (Endpoint Detection and Response): Detección y respuesta en el dispositivo.
5. CASB (Cloud Access Security Broker): Agente de seguridad de acceso a la nube.
6. SOAR (Security Orchestration, Automation, and Response): Orquestación de seguridad.
7. IDS/IPS (Intrusion Detection/Prevention System): Detección y prevención de intrusiones.
8. UEBA (User and Entity Behavior Analytics): Análisis de comportamiento de usuarios.
9. DLP (Data Loss Prevention): Prevención de pérdida de datos.
10. IAM (Identity and Access Management): Gestión de identidad y accesos.
11. Vulnerability Management Tools: Herramientas de gestión de vulnerabilidades.
12. WAF (Web Application Firewall): Cortafuegos de aplicaciones web.
13. MDR (Managed Detection and Response): Detección y respuesta gestionadas.
14. Sandboxing: Máquinas virtuales para análisis de archivos o aplicaciones sospechosas.
15. SAST/DAST (Static/Dynamic Application Security Testing): Pruebas de seguridad.

La investigación en ciberseguridad se concentra en 10 revistas académicas, destacadamente del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). De la principal publicación del IEEE, desde 2019 la mitad de los 20 artículos más citados por la comunidad académica de ciberseguridad, están enfocados a temas de IA y Machine Learning (véase tabla 2).

Tabla 2: Top 10 de artículos sobre AI y ML para ciberseguridad

Articulo (Paper) Título / Autor	Citas	Año
Exploiting Unintended Feature Leakage in Collaborative Learning	1631	2019
Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box	1498	2019
Neural Cleanse: Identifying and Mitigating Backdoor Attacks in Neural Networks	1423	2019
Machine Unlearning	609	2021
Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus	455	2020
HOLMES: Real-time APT Detection by Correlation of Suspicious Information Flows	432	2019
Plundervolt: Software-based Fault Injection Attacks against Intel SGX	382	2020

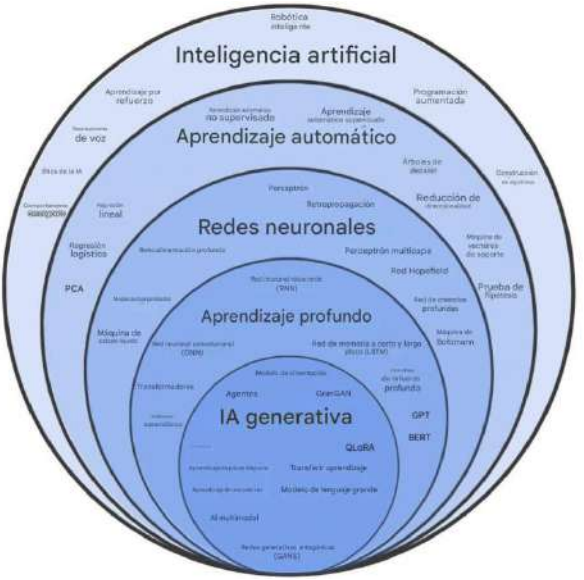
Differentially Private Model Publishing for Deep Learning	303	2019
Detecting AI Trojans Using Meta Neural Analysis	293	2021
Intriguing Properties of Adversarial ML Attacks in the Problem Space	281	2020

Fuente: Elaboración propia del top 20 de Google Scholar[70] en la subcategoría del IEEE.

Inteligencia artificial como arma de doble filo en ciberseguridad

Así como ha sucedido con la tecnología de ciberseguridad, en los últimos años la inteligencia artificial (IA) también ha experimentado un crecimiento exponencial. Definida como el campo de estudio que se enfoca en la creación de máquinas capaces de realizar tareas que normalmente requerirían inteligencia humana (Russell y Norvig, 2020, pp. 1-16), la IA engloba múltiples subdisciplinas y tecnologías que imitan el razonamiento, el aprendizaje y la percepción humanos (véase gráfica 2).

Gráfica 2: Las capas de la inteligencia artificial



[70] En Google Scholar, el h5-index es el mayor número h tal que h artículos publicados en los últimos cinco años han recibido al menos h citas cada uno; el h5-median es la mediana de citas de esos h artículos, reflejando la distribución típica de citas entre los más influyentes.

Fuente: Traducción propia de diagramas públicos basados en las obras "Artificial Intelligence: A Modern Approach" (Russell, et. al., 2020) y ""Deep Learning" (Goodfellow, et. al., 2016).

Estas capas de la IA son fundamentales para entender su aplicación en ciberseguridad.

- **Aprendizaje Automático (Machine Learning, ML):** Es la rama de la IA que permite a las computadoras aprender sin ser explícitamente programadas, utilizando algoritmos que iterativamente aprenden de los datos (Bishop, 2006, p. 23). ML analiza grandes volúmenes de datos y detecta patrones anómalos en tiempo real.
- **Redes Neuronales (Neural Networks, NN):** Sistemas de algoritmos modelados a partir del cerebro humano, diseñados para reconocer patrones y procesar datos sensoriales (Goodfellow, et al., 2016, p. 18). Las NN son cruciales para tareas como el reconocimiento de imágenes y el procesamiento del lenguaje natural.
- **Aprendizaje Profundo (Deep Learning, DL):** Subcampo del ML que utiliza redes neuronales con muchas capas, permitiendo aprender tareas complejas directamente de los datos (Goodfellow, et al., 2016, p. 14). DL ha revolucionado áreas como la visión por computadora y el análisis de texto.
- **IA Generativa (GenAI):** Tipo de IA capaz de crear contenido nuevo y realista, desde texto hasta imágenes y música, basándose en grandes conjuntos de datos (Goodfellow, et al., 2016, p. 710). Aquí se destacan los Large Language Models (LLMs), son modelos de inteligencia artificial entrenados con grandes cantidades de texto para procesar y generar lenguaje natural; GPT (Generative Pre-trained Transformer) es un tipo específico de LLM creado por OpenAI, diseñado para comprender y producir texto de manera coherente en múltiples contextos.

La integración de la IA en ciberseguridad ha dado lugar a una "**ciberdefensa proactiva**", enfoque que se centra en anticipar, identificar y neutralizar amenazas cibernéticas antes de que puedan explotar vulnerabilidades (Andress y Winterfeld, 2011, p. 169).

Por su parte, la "**ciberseguridad orquestable**" se refiere a la capacidad de coordinar y automatizar diversos sistemas y procesos de seguridad de manera integrada. La implementación de plataformas de Orquestación, Automatización y Respuesta de Seguridad (SOAR) permite a las organizaciones gestionar centralmente sus estrategias de seguridad, facilitando la interoperabilidad entre diferentes soluciones. Estas plataformas "orquestables" habilitan las funciones del ciclo OODA (Observar, Orientar,

Decidir y Actuar)[71] para la toma de decisiones y las operaciones (Kott, 2023, p. 77). Ante una amenaza, el sistema puede automáticamente aislar el dispositivo afectado, bloquear el tráfico malicioso y notificar al equipo de seguridad (Roberts y Brown, 2017, p. 198).

A su vez, la "**ciberinteligencia automatizable**" implica el uso de tecnologías y procesos que permiten la recopilación, procesamiento y análisis automatizado de grandes volúmenes de datos relacionados con la seguridad cibernética, generando inteligencia accionable (desarrollado como "data-driven cybersecurity" por Mongeau y Seeger, 2017, p. 68). Este enfoque mejora la velocidad y precisión de la respuesta ante incidentes.

Las tendencias de IA para la ciberdefensa proactiva y la ciberinteligencia automatizable (Kott, 2023, p. 14) se exploran a través del concepto de "AICA" (Autonomous Intelligent Cyber-Defense Agent). AICA es un agente de software que reside en uno o más dispositivos, percibe su entorno y ejecuta acciones para lograr objetivos de ciberdefensa.

En este contexto, el uso de telemetría, la recolección y análisis de datos sobre el estado y comportamiento de sistemas y redes, es esencial para anticipar ataques, y así tener una organización guiada por el análisis de datos (Jacobs y Rudis, 2014). Al monitorear el tráfico de red y las actividades de los usuarios, se pueden detectar intentos de intrusión o comportamientos anómalos. La IA permite procesar estos datos en tiempo real, con alertas tempranas y permitiendo acciones preventivas (Chio y Freeman, 2018).

Evolución de las amenazas cibernéticas potenciadas por IA

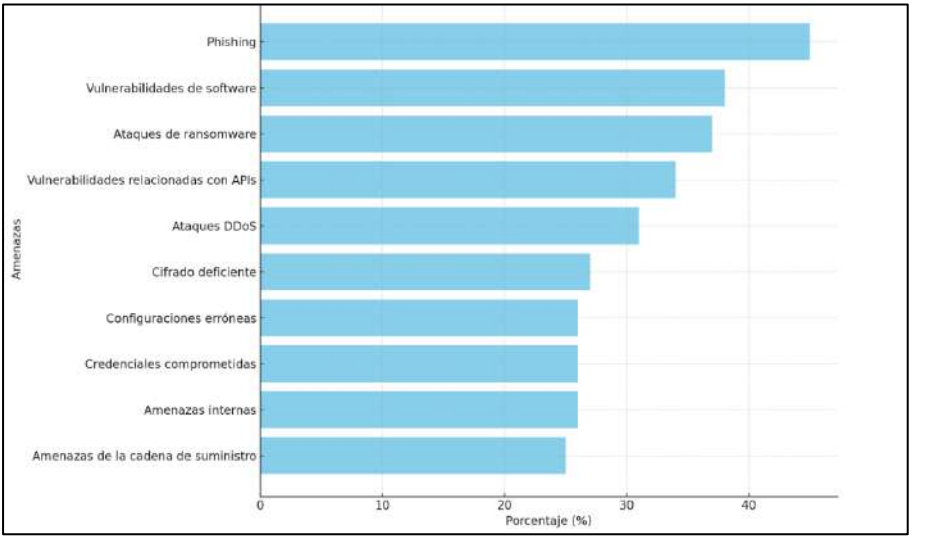
Según un informe de MIT Technology Review (2021), el 60% de los ejecutivos encuestados indicaron que las respuestas humanas a los ciberataques están quedando rezagadas frente a los ataques automatizados, subrayando la necesidad de tecnologías más avanzadas para combatir estas amenazas.

Los adversarios están aprovechando bots inteligentes y algoritmos de aprendizaje automático para automatizar y sofisticar sus ataques. Ahora los atacantes utilizan modelos avanzados de IA para generar phishing avanzado (mensajes apócrifos) y deepfakes (archivos multimedia falsos), creando contenidos altamente realistas que engañan tanto a personas como a sistemas automatizados. De esta manera, los atacantes explotan la confianza humana, y con la ayuda de la IA, esta explotación se vuelve aún más eficaz (Mitnick y Simon, 2002, p. 246). La generación automática de malware polimórfico es otra aplicación contra soluciones tradicionales.

[71] Como parte de las metodologías de "agile management", proporciona un marco dinámico para responder eficazmente contra amenazas: permite a los equipos de seguridad reaccionar rápidamente y adaptarse ante ataques cibernéticos en constante evolución.

Otro de los riesgos consiste en la manipulación de los datos de entrenamiento, conocida como "data poisoning". Los atacantes pueden introducir datos maliciosos en los conjuntos de entrenamiento, alterando el comportamiento del modelo y causando decisiones incorrectas o sesgadas.

Gráfica 3: Crecimiento en peligrosidad de ciberamenazas por IA generativa



Fuente: Elaboración propia con datos de la empresa Ivanti (2024).

Según datos presentados en el Foro Económico Mundial (Ivanti, 2024), hemos tenido un crecimiento significativo en la peligrosidad de las ciberamenazas potenciadas por IA generativa (véase gráfica 3).

Tecnologías de IA para fortalecer la ciberdefensa

El consenso en la industria (ITI, 2024) destaca áreas donde la IA fortalece la ciberdefensa[72]: detección avanzada de amenazas, respuesta automatizada a incidentes, mejora en la gestión de la exposición, y ciberinteligencia.

Un ejemplo destacado es CamoGPT (Defense News, 2024), desarrollado por el Cyber Center of Excellence del Ejército de Estados Unidos. Este sistema de IA generativa integra doctrinas, lecciones aprendidas y mejores prácticas,

[72] Considerando que la ciberseguridad se enfoca en proteger sistemas y datos de amenazas, mientras que la ciberdefensa abarca estrategias y acciones activas para detectar, responder y neutralizar ataques dirigidos contra infraestructuras críticas o intereses nacionales.

mejorando el entrenamiento y preparación de los soldados para enfrentar amenazas modernas.

En el ámbito regional, la Junta Interamericana de Defensa (JID) de la Organización de los Estados Americanos (OEA) ha impulsado desde 2024 la incorporación de la asignatura de Inteligencia Artificial en los programas y planes de estudio de los ejércitos del continente, sobre todo para las escuelas militares de ingenieros y de transmisiones. De manera similar, como indica Geers (2011, p. 30) en *Strategic Cyber Security*, del Centro de Excelencia Cooperativo de Defensa Cibernética de la OTAN (CCDCOE), abordar la seguridad cibernética desde una perspectiva estratégica es esencial para enfrentar las amenazas emergentes en el ciberespacio.

Los países con casos de éxito de la JID y del índice de ciberseguridad de la ONU coinciden en aplicar el modelo de triple hélice: la estrecha colaboración entre industria privada, universidades y gobierno. Como evolución de DARPA, el departamento de tecnología del ejército de Estados Unidos (creadores del Internet), funciona la DIU (Unidad de Innovación de Defensa). Su misión principal es conectar "Startups" tecnológicas de Silicon Valley con el Pentágono para modernizar las capacidades militares y acelerar la adopción de tecnologías comerciales innovadoras.

Ejemplos específicos de empresas respaldadas por DIU son los siguientes: ForAllSecure y Tanium, las cuales desarrollan software para proteger los sistemas de armas y otras infraestructuras críticas (Shah y Kirchhoff, 2024). Por su parte, Palantir aporta algoritmos inteligentes para tareas como el mantenimiento de flotas. Además, se creó el Proyecto Maven, una iniciativa conjunta entre DIU y empresas como Amazon, Google y Microsoft, para desarrollar software de aprendizaje automático que analice imágenes de drones, con el objetivo de proteger a las fuerzas armadas y reducir el riesgo de bajas civiles.

La IA generativa tiene un enorme potencial para revolucionar las estrategias de ciberdefensa, destacándose por su capacidad para crear datos sintéticos (Jhanjhi, 2025, p. 191) que imitan a la perfección escenarios de ataque reales mediante técnicas como las redes generativas antagónicas (GAN) y los autocodificadores variacionales (VAE). De esta manera, uno de los principales casos de uso[73] hacia 2025 se aplicará como "Detection-as-Code", con respecto a cinco principales subdominios que se concatenan para combatir las amenazas emergentes, en el nuevo teatro de operaciones de ciberguerra: *cyber intelligence*, *incident response*, *threat hunting*, *digital forensics* y *red teaming* (emulación de adversarios para simulacros de ataques en entornos controlados).

Un nuevo concepto de "confluencia panóptica", inspirado en el panóptico de Michel Foucault, sugiere la necesidad de una vigilancia integral y

[73] Escenarios específicos diseñados para identificar, monitorear y responder a amenazas o comportamientos anómalos en un entorno de red o sistema.

constante para la protección de las infraestructuras críticas. La implementación de sistemas avanzados de monitoreo, como el "Panoptic Junction" desarrollado por el Army Cyber Command (ARCYBER) de Estados Unidos, utiliza inteligencia artificial y aprendizaje automático para analizar el cumplimiento de sistemas, inteligencia sobre amenazas y datos de eventos cibernéticos a velocidades inalcanzables para los humanos (DefenseScoop, 2024).

Transformación digital y tendencias en computación

La transformación digital no sólo implica avances tecnológicos, sino también el desarrollo de competencias humanas que permitan aprovechar de manera segura y ética las oportunidades que brinda la era digital. Al respecto, el DQ Institute (2020) ha desarrollado un marco de trabajo conocido como Inteligencia Digital (DQ), aprobado por la Junta de Estándares del IEEE en 2020 como el estándar IEEE 3527.1.

Esta inteligencia digital se refiere a un conjunto integral de competencias técnicas, cognitivas, metacognitivas y socioemocionales que permiten a los individuos enfrentar los desafíos y aprovechar las oportunidades de la vida digital. Estas competencias están fundamentadas en valores morales universales y abarcan áreas críticas como identidad digital, uso responsable de la tecnología, seguridad en línea, empatía digital, alfabetización digital, comunicación y derechos digitales. Esto es desarrollado también por Sadiku y Musa en la obra *A Primer on Multiple Intelligences* (2021, pp. 95-105).

Por su parte, la transformación digital ha impulsado el desarrollo de sistemas cada vez más complejos y autónomos. En el ámbito de la ciberseguridad, esto ha dado lugar a la creación de sistemas autogestionados y autorreparables, capaces de adaptarse y responder dinámicamente a amenazas emergentes sin intervención humana constante. Estos sistemas se basan en arquitecturas de **sistemas multiagente**: conjuntos de agentes inteligentes que interactúan entre sí, compartiendo información y coordinando acciones para resolver problemas complejos (Russell y Norvig, 2020, pp. 42-43).

Como antecedente, la obra *Society of Mind* (Minsky, 1986, p. 23), propuso que la mente humana, y la inteligencia en particular, consiste en un conjunto de agentes simples que interactúan, idea que ha influido en el desarrollo de sistemas multiagente. Esta teoría es aplicable a la ciberseguridad autonómica, donde la suma de agentes individuales contribuye a una defensa robusta y adaptable: 2 GPT3 suelen tener mejor desempeño que 1 GPT4.

A su vez, la computación de próxima generación está emergiendo con tecnologías que prometen revolucionar la forma en que procesamos, manejamos y protegemos la información (Global Information, Inc., 2023):

- **Bio-Computing:** Utiliza moléculas biológicas para realizar cálculos y almacenar información, abriendo posibilidades para resolver problemas complejos de manera eficiente.
- **Interfaces cerebro-computadora:** Permiten la comunicación directa entre el cerebro humano y dispositivos externos, facilitando el control tecnológico mediante señales neuronales.
- **Computación de alto rendimiento:** Involucra el uso de supercomputadoras y procesamiento paralelo, esencial para manejar grandes volúmenes de datos y realizar análisis complejos.
- **Nanocomputación:** Se centra en el desarrollo de dispositivos a escala nanométrica, permitiendo una miniaturización extrema y nuevas capacidades en procesamiento.
- **Computación neuromórfica:** Emula la arquitectura del cerebro humano, mejorando la eficiencia energética y la capacidad de aprendizaje de las máquinas.
- **Computación sin servidor:** Modelo en la nube donde el proveedor gestiona la infraestructura, permitiendo a los desarrolladores centrarse en el código sin preocuparse por la administración de servidores.
- **Computación en enjambre:** Basada en la colaboración de múltiples agentes o dispositivos que trabajan de manera coordinada, inspirándose en comportamientos colectivos observados en la naturaleza.
- **Computación cuántica:** Utiliza principios de la mecánica cuántica para procesar información, ofreciendo una capacidad de cálculo exponencialmente superior.

Estos desarrollos presentan tanto oportunidades como desafíos en el campo de la ciberseguridad, requiriendo una adaptación continua y estrategias innovadoras para proteger la información. Por ejemplo, uno de los aportes principales de ML a ciberseguridad han sido algoritmos para cifrado, análisis predictivo y detección de intrusiones, como son: Regresión Logística, Árboles de Decisión, Redes Neuronales Artificiales, Random Forest y Gradient Boosting (Shekokar, et. al., 2024, p. 182). No obstante, la computación cuántica tendrá la posibilidad de romper todos estos cifrados, por lo cual se requieren soluciones de criptografía post-cuántica (PQC), que se refiere a algoritmos criptográficos diseñados para ser resistentes a estos nuevos tipos de ataques.

El mundo actual se caracteriza por entornos VUCA (Volatilidad, Incertidumbre, Complejidad y Ambigüedad) y BANI (Frágil, Ansioso, No lineal e Incomprensible), que describen las condiciones dinámicas y a menudo impredecibles en las que operan las organizaciones. En estos entornos, es fundamental desarrollar capacidades de resiliencia y adaptabilidad, así como

habilidades para aprender rápidamente nuevas competencias (*upskilling*, *reskilling*). La creatividad asistida por IA será cada vez más relevante, permitiendo a los individuos y organizaciones innovar y resolver problemas de manera eficaz.

Conclusiones y agenda pendiente para México

Nick Bostrom (2014) explora los posibles riesgos asociados con el desarrollo de una inteligencia artificial que supere la capacidad cognitiva humana, argumentando que una superinteligencia podría actuar de manera autónoma y perseguir objetivos que no necesariamente se alineen con los intereses humanos, lo que podría resultar en consecuencias catastróficas, incluso peores que una bomba atómica.

Además, existen riesgos asociados con sesgos inherentes y la falta de "explicabilidad" en los modelos de IA. Como destaca, quizá el autor más citado en ciberseguridad, Schneier (2000, p. 255) confiar ciegamente en la tecnología sin entender sus limitaciones puede llevar a una falsa sensación de seguridad. Los modelos de IA opacos dificultan la identificación de errores o manipulaciones, lo que puede ser aprovechado por atacantes para evadir sistemas de seguridad o dirigirlos hacia objetivos erróneos.

Debido a que los conflictos modernos se están trasladando al ciberespacio (Clarke y Knake, 2010, p. 69), resulta imperativo que las naciones desarrollen políticas y estrategias gubernamentales robustas para fortalecer la defensa cibernética. Por ello en Estados Unidos, su gobierno federal acaba de emitir un memorando de seguridad nacional sobre IA (octubre de 2024). México tiene la oportunidad de aprender de estas iniciativas y desarrollar políticas propias que refleje nuestras necesidades y doctrina de ciberdefensa.

Como se ha enlistado, en noviembre de 2019 Pemex sufrió un ataque de ransomware que afectó sus sistemas y operaciones, evidenciando las vulnerabilidades en infraestructuras críticas nacionales. Una de las maneras en que se pudo haber evitado el ataque a Pemex es mediante la IA y la ciberseguridad orquestable: con la implementación de sistemas de detección basados en reglas YARA, las cuales son herramientas que permiten crear alertas para identificar malware mediante patrones textuales o binarios. Destacadamente, la alerta por el tipo de ataque sufrido (por el grupo ruso de cibercriminales DoppelPaymer) era del conocimiento de la industria cuando menos 7 meses antes del incidente (Kremez, 2019).

Para quien desee profundizar sobre estos temas, puede tomar el curso gratuito "Generative AI for Cybersecurity Professionals Specialization", impartido por ingenieros de IBM mediante la plataforma Coursera, disponible desde la elaboración del presente documento.

Bibliografía principal

Andress, J., y Winterfeld, S. (2011). *Cyber warfare: Techniques, tactics and tools for security practitioners*. Syngress.

Bishop, C. M. (2006). *Pattern recognition and machine learning*. Springer.

Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford University Press.

Chio, C., y Freeman, D. (2018). *Machine learning and security: Protecting systems with data and algorithms*. O'Reilly Media.

Clarke, R. A., y Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. HarperCollins.

Defense News. (2024, octubre 28). "From CamoGPT to life skills, the Army is changing how it trains troops". https://www.defensenews.com/land/2024/10/16/from-camogpt-to-life-skills-the-army-is-changing-how-it-trains-troops/

DefenseScoop. (2024, octubre 30). "Cybercom seeing successes with Panoptic Junction artificial intelligence capability". https://defensescoop.com/2024/10/30/cybercom-army-cyber-command-panoptic-junction-artificial-intelligence/

DQ Institute. (2020). *Digital Intelligence (DQ) framework*. https://www.dqinstitute.org/

Geers, K. (2011). *Strategic cyber security*. NATO Cooperative Cyber Defence Centre of Excellence.

Global Information, Inc. (2023, enero 30). *Next generation computing market*. https://www.giiresearch.com/report/min1205924-next-generation-computing-market-bio-computing.html

Goodfellow, I., Bengio, Y., y Courville, A. (2016). *Deep learning*. MIT Press.

Information Technology Industry Council (ITI). (2024). *AI security policy principles*. https://www.itic.org/documents/artificial-intelligence/ITI_AI-Security-Principles_102124_FINAL.pdf

International Telecommunication Union (ITU). (2024). *Global Cybersecurity Index 2024*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Ivanti. (2024, octubre 17). *AI cybersecurity best practices: Meeting a double-edged challenge*. https://www.ivanti.com/blog/ai-cybersecurity-best-practices-meeting-a-double-edged-challenge

Jacobs, J., y Rudis, B. (2014). *Data-driven security: Analysis, visualization and dashboards*. Wiley.

Jhanjhi, N. Z. (Ed.). (2025). *Utilizing generative AI for cyber defense strategies*. IGI Global.

Junta Interamericana de Defensa. (2024). *Desarrollo de políticas cibernéticas y aplicaciones de inteligencia artificial para la defensa*. https://jid.org/jid-participa-en-cyberai-2024/

Kott, A. (Ed.). (2023). *Autonomous intelligent cyber defense agent (AICA)*. Springer.

Kremez, V. (2019, noviembre 11). *YARA hunting for code reuse: DoppelPaymer ransomware & Dridex families*. SentinelOne. https://www.sentinelone.com/blog/yara-hunting-for-code-reuse-doppelpaymer-ransomware-dridex-families/

McKinsey & Company. (2024, mayo 30). *The state of AI in early 2024: Gen AI adoption spikes and starts to generate value*.

https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

Microsoft. (2023, noviembre 15). *The future of security with AI*. https://www.microsoft.com/en-us/security/blog/2023/11/15/microsoft-unveils-expansion-of-ai-for-security-and-security-for-ai-at-microsoft-ignite/

Microsoft. (2024). *Microsoft Digital Defense Report 2024*. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Minsky, M. (1986). *The society of mind*. Simon & Schuster.

MIT Technology Review. (2021, abril 8). "Preparing for AI-enabled cyberattacks". https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyberattacks/

Mitnick, K. D., y Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Wiley.

Mongeau, S., y Seeger, A. (2017). *Cybersecurity data science: Machine learning and data analytics for cyber risk management*. Springer.

Roberts, S. J., y Brown, R. (2017). *Intelligence-driven incident response: Outwitting the adversary*. O'Reilly Media.

Russell, S., y Norvig, P. (2020). *Artificial intelligence: A modern approach*. Pearson.

Sadiku, M. N. O., y Musa, S. M. (2021). "Digital intelligence". En *A primer on multiple intelligences*. Springer.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. Wiley.

Shah, R. M., y Kirchhoff, C. (2024). *Unit X: How the Pentagon and Silicon Valley are transforming the future of war*. Scribner.

Shekokar, N. M., Vasudevan, H., Durbha, S. S., Michalas, A., & Nagarhalli, T. P. (2024). *Intelligent approaches to cyber security*. CRC Press.

White House. (2024, octubre 24). *Memorandum on advancing the United States' leadership in artificial intelligence; harnessing AI to fulfill national security objectives*. https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/

"Reservan datos del ciberataque a Pemex". (2020, febrero 8). En *El Sol de México*. https://www.elsoldemexico.com.mx/mexico/sociedad/reservan-datos-del-ciberataque-a-pemex-4807474.html

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

Agua y Seguridad Nacional: El hackeo de la Comisión Nacional del Agua en México

Erick Alejandro Rafael Aguilar Obregón*

Resumen: El presente artículo expone el caso del hackeo en México, en el año 2023, a la Comisión Nacional del Agua (Conagua), como organismo responsable de la administración del agua de la nación. Desde 2015, algunas subdirecciones de la Conagua ostentan el rango de Instancias de Seguridad Nacional dada la importancia crítica de sus funciones para el Estado mexicano. Pese a lo anterior en 2023, un el grupo de cibercriminales BlackByte logró penetrar y secuestrar alrededor de 15 años de información de la entidad.

Las ciberamenazas cada vez ocupan el principal riesgo para los Estados en tanto el teatro de operaciones ha pasado del mundo físico al ciberespacio. La ciberseguridad es un concepto que debe tener al momento de hablar de Seguridad Nacional. El caso de la Conagua no es aislado, México ha sido sujeto de múltiples ciberataques dirigidos contra organizaciones privadas y públicas como los más conocidos: *guacamaya leaks* y *chilango leaks*.

Así, se busca exponer los avisos previos que por años se documentaron e ignoraron y que tuvieron como trágico desenlace la irrupción en lo que internacionalmente se cataloga como infraestructura crítica.

Palabras clave: Agua; Seguridad Nacional; Conagua; Blackbyte; ciberseguridad; México.

Abstract: This paper exposes the case of the 2023 hack of the Comisión Nacional del Agua (Conagua) -National Water Commission- in Mexico. Conagua is the institution

* Investigador posdoctoral en la Facultad Latinoamericana de Ciencias Sociales sede México en el marco de los Programas Nacionales Estratégicos (ProNacEs) del Conahcyt para agua. Miembro del Sistema Nacional de Investigadores. Ha colaborado como ponente en la Especialidad de Ciberdefensa en el Centro de Estudios del Ejército y la Fuerza Aérea (Secretaría de la Defensa Nacional). Ha sido especialista invitado para temas de agua y sociedad tanto en la Cámara de Diputados como en la Cámara de Senadores. Licenciado en Sociología por la UNAM. Maestro en Administración Pública por el INAP. Maestro en Ciencias en Estudios Ambientales y de la Sustentabilidad. En proceso de titulación de la maestría en Inteligencia para la Seguridad Nacional por el INAP y Doctor en Investigación en Ciencias Sociales con mención en Sociología por la Flacso sede México. Ha realizado estancias de investigación en la Universidad de Salamanca, España y en la Universidad General Sarmiento en Buenos Aires, Argentina.

responsible for the administration of the nation's water. Since 2015, some administrative areas of Conagua have held the rank of National Security Instances given the critical importance of their functions for the Mexican State. Despite the above, in 2023 a group of BlackByte cybercriminals managed to penetrate and kidnap around 15 years of Conagua's information.
Cyber threats increasingly occupy the main risk for States as the theater of operations has moved from the factical world to cyberspace. Cybersecurity is a concept that should run together with National Security. The case of Conagua is not isolated, Mexico has been subject to multiple cyberattacks directed against private and public organizations such as the best known: guacamayaleaks, chilangoleaks. and so on.
This paper seeks to expose previous warnings that were documented and ignored for years and that had the tragic outcome of breaking into what is internationally classified as critical infrastructure.

Keywords: Water, National Security, Conagua, Blackbyte, Cybersecurity, México.

Introducción

En México, el ente administrativo responsable del tema hídrico es la Comisión Nacional del Agua[74] (Conagua), la cual fue constituida formalmente el 16 de enero de 1989 como un órgano desconcentrado de la Secretaría de Agricultura y Recursos Hidráulicos (SARH). En diciembre de 1994, la Conagua fue sectorizada a la Secretaría de Medio Ambiente, Recursos Naturales y Pesca, actualmente llamada Secretaría de Medio Ambiente y Recursos Naturales (SEMARNAT) (Conagua, s/f).

En términos jurídicos, de acuerdo con el artículo 9° de la Ley de Aguas Nacionales[75] (LAN), la Comisión Nacional del Agua tiene como principales ordenamientos jurídico-administrativos:

1. La Ley de Aguas Nacionales.
2. La Ley Orgánica de la Administración Pública Federal (LOAPF).
3. El Reglamento Interior de la Comisión Nacional del Agua (RICNA).

Amén de lo establecido por la LAN como los principales ordenamientos jurídico-administrativos a los cuales la Conagua debe ceñirse, existen otros ordenamientos cuyas temáticas son transversales a la Conagua.

---

[74] El rubro de la administración del agua ha sido clave para el Estado Mexicano. A lo largo del siglo XIX se crearon distintos entes administrativos responsables de las aguas nacionales: La Dirección de Aguas, Tierras y Colonización (1917); la Comisión Nacional de Irrigación (1926-1946), la Secretaría de Recursos Hidráulicos (1946-1975), la Secretaría de Agricultura y Recursos Hidráulicos (1976-1988) (CONAGUA, s/f; Durand, 2016; INAP, 2015).

[75] Que a la letra dice:
"ARTÍCULO 9. "La Comisión" es un órgano administrativo desconcentrado de "la Secretaría", que se regula conforme a las disposiciones de esta Ley y sus reglamentos, de la Ley Orgánica de la Administración Pública Federal y de su Reglamento Interior." (LAN, art 9, fr. I)

Ordenamiento jurídico-administrativo	Apartados o artículos pertinentes	Fecha de creación	Temática abordada
Bases de Colaboración que en el marco de la Ley de Seguridad Nacional celebran la Secretaría de Gobernación y la Secretaría de Medio Ambiente y Recursos Naturales	Antecedentes fracción IV +Declaración 2.4, 3.1 +Bases: Primera fracción IV; Segunda; Quinta	26 febrero 2015	Agua y Seguridad Nacional
Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP)	Artículo 69 fracción VII (inciso "*e*" al "*h*")	9 de mayo 2016	Transparencia y rendición de cuentas
Lineamiento para el impulso, conformación, organización y funcionamiento de los mecanismos de participación ciudadana en las dependencias y entidades de la Administración Pública Federal	Lineamiento cuarto, fracción V	11 agosto 2017	Referente al mecanismo establecido en la Ley de Aguas Nacionales para incorporar la participación ciudadana en la toma de decisiones sobre el agua

Cuadro 1. Otros ordenamientos jurídico-administrativos transversales a la Conagua más allá de los dispuestos en la LAN. Elaboración propia a partir de DOF (2015, 2017), LFTAIP (2016), SEGOB (2018).

Con respecto a lo que atañe a la Seguridad Nacional, conviene hacer mención del documento intitulado *Bases de Colaboración que en el marco de la Ley de Seguridad Nacional celebran la Secretaría de Gobernación y la Secretaría de Medio Ambiente y Recursos Naturales* publicado en 2015. En dicho documento se establecieron como Instancias de Seguridad Nacional -que a su vez participan en la Red Nacional de Información- a las siguientes áreas de la Conagua:

> *"+Oficina de la Dirección General;*
> *+ Las Subdirecciones Generales de Agua Potable, Drenaje y Saneamiento; Técnica; y de Infraestructura Hidroagrícola;*
> *+ Las Coordinaciones Generales de Atención de Emergencias y Consejos de Cuenca; y del Servicio Meteorológico Nacional;*
> *+ Los Organismos de Cuenca Aguas del Valle de México, Frontera Sur, Golfo Centro, Golfo Norte, Noroeste, y Río Bravo, y*
> *+ La Dirección Local Tabasco."* (DOF, 2015)

Por su parte, en la Ley de Seguridad Nacional (LSN), se definen como amenzas a la Seguridad Nacional:

"I. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional;
II. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano;
III. Actos que impidan a las autoridades actuar contra la delincuencia organizada;
IV. Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;
V. Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada;
VI. Actos en contra de la seguridad de la aviación;
VII. Actos que atenten en contra del personal diplomático;
VIII. Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva;
IX. Actos ilícitos en contra de la navegación marítima;
X. Todo acto de financiamiento de acciones y organizaciones terroristas;
XI. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia;
XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos, y
XIII. Actos ilícitos en contra del fisco federal a los que hace referencia el artículo 167 del Código Nacional de Procedimientos Penales." (LSN, art. 4).

Resalta el hecho de que la fracción XII hace alusión a los *actos tendentes a destruir o inhablititar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos*. Es en la anterior fracción en donde se encuentra el vínculo entre agua –entendida como servicio público- la cual es proveida a través de complejas redes de infraestructura. Y es esa misma infraestructura la que por su importancia, cobertura y función adquiere la calidad de indispensable para efectos de seguridad nacional. Sin embargo, ¿es suficiente constreñir el binomio de Seguridad Nacional y agua a una cuestión de meros *tubos*?

1. Hackeo a Conagua

En marzo de 2019 en las oficinas centrales de la Conagua en Insurgentes Sur se reportó un incendio que consumió seis pisos del edificio. Si bien no hubo pérdida de vidas, abundantes datos, información, archivos físicos y documentos pertenecientes a la Coordinación General de Recaudación y Fiscalización se perdieron, así como muchos otros datos del Registro Público de Derechos de Agua (REPDA) (Soto, 2023). No sería la primera gran pérdida de información de la Conagua en la presente administración.

La mañana del jueves 13 de abril de 2023, como cada día, los poco más de 2,000 empleados que laboran en las oficinas centrales de Conagua llegaron puntuales a su lugar de trabajo (Conagua, 2019). Una vez en frente a sus equipos de cómputo, los prendieron y en sus monitores apareció algo muy similar a la imagen 1.

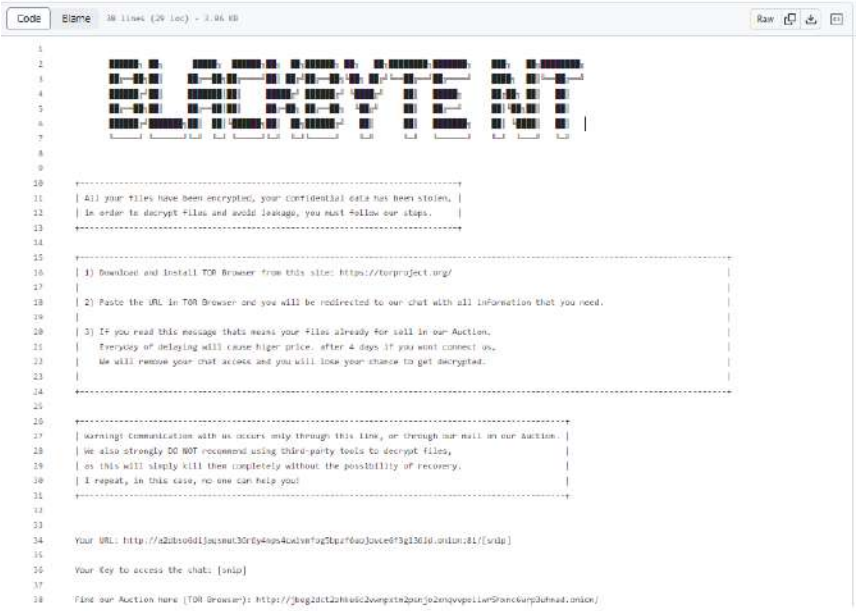


Imagen 1. Pantalla de aviso de robo de información con instrucciones sobre contacto y pago con el grupo BlackByte. Tomado de Github (2023)

La traducción del mensaje dice:

"Todos tus archivos han sido encriptados, tus datos confidenciales han sido robados; para poder descifrar archivos y evitar fugas, debes seguir nuestros pasos.

1) Descarga e instala el navegador TOR desde este sitio: https://torproject.org/

2) Pega la URL en el navegador TOR y serás redirigido a nuestro chat con toda la información que necesitas.

3) Si lees este mensaje significa que tus archivos ya están a la venta en nuestro sitio de subasta. Cada día de retraso provocará un precio más alto. Después de 4 días si no nos contactas, eliminaremos tu acceso al chat y perderás la oportunidad de desencriptar tu información.

¡Advertencia! La comunicación con nosotros se produce
únicamente a través de este enlace, o a través de nuestro correo en
nuestro sitio de subastas.
De igual forma NO TE recomendamos el uso de herramientas de
terceros para descifrar archivos, ya que esto simplemente los
eliminará por completo sin posibilidad de recuperación.
Repito, en este momento ¡nadie puede ayudarte!"

¿Cómo es que la Conagua llegó a este punto? ¿Cómo es que sus más de 12 mil trabajadores a nivel nacional se quedaron sin acceso a los sistemas internos expuestos en el segundo capítulo de la presente investigación? ¿Cómo es que los portales de OSINF de la Conagua se quedaron de pronto en blanco? ¿Fue de improviso o hubo indicios que, por incapacidad, desconocimiento o incluso sabotaje de personal de la Conagua se dejaron pasar y que en ese cabalístico 13 de abril de 2023 por fin se conjuraron bajo la forma de un ciberataque? Intentaremos responder estas preguntas en el siguiente apartado.

1. 1. Señales y avisos

En 2023, la Auditoria Superior de la Federación (ASF), publicó el documento intitulado *Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2022-5-16B00-20-0075-2023*, que se realizó en Conagua con motivo de la fiscalización Superior de la Cuenta Pública 2022.

Desde el inicio de la actual administración federal en el año 2018 hasta el año 2022 la Conagua había invertido más de $3,200 millones de pesos totales (ver cuadro 2)

RECURSOS INVERTIDOS EN MATERIA DE TIC
(Miles de pesos)

Año	2018	2019	2020	2021	2022	Total
Monto	779,201.2	581,458.4	702,419.9	611,174.3	591,906.1	3,266,159.9

Cuadro 2. Histórico de montos invertidos en Tecnologías de la Información y Comunicación por Conagua. Tomado de ASF (2023).

La Gerencia de Tecnologías de la Información y Comunicaciones, dependiente de la Subdirección General de la Administración de la Conagua erogó $ 583,785,100 pesos en materia de contrataciones de Tecnologías de la Información y Comunicación (TIC) y $9,627,100 pesos en el rubro de materiales y suministros relacionados con TIC durante el ejercicio fiscal de 2022. Así, el monto total ejercido en materia de TIC durante el año 2022 fue de $591,906,100 pesos (ver cuadro 3).

RECURSOS EJERCIDOS EN CONTRATACIONES RELATIVAS A LAS TIC
EN LA CONAGUA DURANTE 2022
(Miles de pesos)

Capítulo	Descripción	Ejercido	Ejercido Contratos TIC	%
2000	Materiales y Suministros	9,267.1	8,732.3	1.5
3000	Servicios Generales	582,639.0	575,052.8	97.2
	Total	**591,906.1**	**583,785.1**	**98.6**

Cuadro 3. Descripción de montos ejercidos en materia de TIC. Tomado de ASF (2023: 3)

Del monto asignado a contrataciones –es decir de los $ 583,785,100 pesos- la ASF tuvo como muestra auditada $227,773,200 pesos. Dicha muestra se integra por contratos y convenios relacionados con:

I) El servicio de cómputo y bienes informáticos
II) El servicio atención y administración de requerimientos tecnológicos
III) El servicio de ciberseguridad

Cabe resaltar que la última fila del cuadro 15 muestra el proceso de contratación –adjudicación directa- a la empresa Scitum para efectos de ciberseguridad. Si bien sería un error considerar que Scitum –o cualquier otra empresa- es la única responsable de la falla de ciberseguridad en la Conagua en tanto que la compra de equipos nuevos es un elemento que afecta a la ciberseguridad, o bien el uso de software con licencia es otro factor, etc. el análisis de las líneas subsecuentes se centra en el contrato con Scitum por considerarlo el más emblemático dada su relación directa con la ciberseguridad.

La vigencia del contrato con Scitum empezó en octubre de 2021 y terminaría en diciembre de 2024. Hasta el año 2022, se le habían pagado $39,957,200 pesos por el concepto específico de ciberseguridad.
El objetivo del servicio amparado en el ya mencionado contrato CNA-GRM-044-2021 con la empresa Scitum fue según lo auditado:

> *Contar con un servicio de Ciberseguridad que incluyera los componentes tecnológicos y las mejores prácticas para proteger la seguridad en los sistemas y la información tanto en las oficinas a nivel nacional, direcciones locales, organismos de cuenca y la Coordinación General del Servicio Meteorológico Nacional; al término de la vigencia del contrato, la totalidad de la infraestructura y licenciamiento bajo el alcance del servicio quedará en propiedad de la CONAGUA a título gratuito.* (ASF, 2023: 13)

MUESTRA DE CONTRATOS CON PAGOS REALIZADOS DURANTE 2022
(Miles de pesos)

Proceso de Contratación	Contrato / Convenio	Proveedor	Objeto	Vigencia		Monto		Ejercido 2022
				De	Al	Mínimo	Máximo	
Licitación Pública Electrónica Nacional	CNA-GRM-022-2020	Mainbit, S.A. de C.V., en participación conjunta con Innovation, Business and Infraestructures in Technology, S.A. de C.V.	Servicio de equipo de cómputo y bienes informáticos, Lotes 1, 6, 7 y 8.	13/06/2020	12/06/2023	190,409.6	353,557.2	75,894.0
Licitación Pública Electrónica Nacional	CNA-GRM-023-2020	Servicio Administrados BSS, S.A. de C.V., en participación conjunta con Centro de Productividad Avanzada, S.A. de C.V.	Servicio de equipo de cómputo y bienes informáticos, Lotes 2, 3, 4 y 5.	13/06/2020	12/06/2023	32,065.1	60,086.5	24,592.0
Licitación Pública Nacional	CNA-GRM-COLAB-002-2022	INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación	Servicio de Atención y Administración de Requerimientos Tecnológicos 2022.	01/04/2022	28/02/2023	120,052.1	144,062.5	88,330.0
Adjudicación Directa	CNA-GRM-044-2021	Scitum, S.A. de C.V.	Servicio de ciberseguridad para la CONAGUA.	30/10/2021	29/12/2024	97,956.5	284,943.1	38,957.2
					Total	440,483.3	842,649.3	227,773.2

Cuadro 4. Pagos y contratos realizados por Conagua en materia de TIC en 2022. Tomado de ASF (2023: 4).

Dicho contrato generaría beneficios como:

"• Establecer y mantener programas, controles y políticas con la finalidad de mantener la confidencialidad, integridad y disponibilidad de los activos de información.

• Minimizar las vulnerabilidades y amenazas de la información.

• Fortalecer la continuidad operativa de los servicios mediante el empleo de componentes tecnológicos de última generación." (ASF, 2023: 13)

Y los alcances del servicio serían:

"Servicios de instalación, configuración, mantenimiento, administración, monitoreo, soporte, atención, respuesta y mitigación de incidentes, actualizaciones, bajas y cambios, alertas, notificación, documentación, reportes, mediante la operación de todos los componentes del servicio…" (ASF, 2023: 13)

Para lograr dichos alcances los componentes del servicio incluirían:

"1. Firewall de Nueva Generación y Sistema de Prevención de Intrusos (IPS)

2. Filtrado de Correo

3. Resolución de Nombres de Dominio (DNS)

4. Correlacionador de Eventos (SIEM) y Monitoreo

5. Filtrado de Contenido Web

6. Monitoreo" (ASF, 2023: 14)

La Conagua erogó $38,957,200 pesos por concepto de servicios prestado por Scitum de enero a julio de 2002. En la revisión de la ASF, ésta detectó:

"El concepto de la cuenta por pagar certificada no se corresponde con los servicios objeto del contrato.
Las cantidades facturadas no concuerdan con las métricas registradas por el proveedor para todos los servicios entregados durante 2022." (ASF, 2023: 14)

Como se observa, empieza a gestarse el escenario sobre el cual se realizaría el ciberataque de abril de 2023 a la Conagua. Pero antes de llegar a él sigamos la ruta hacia el desastre, plasmada por los hallazgos de la ASF de los cuales, o por lo menos de los más obvios y evidentes, Conagua tenía conocimiento desde el año 2022.

De los seis servicios citados líneas arriba, se encontró que los servicios 2. Filtrado de correo, 3. Resolución de dominio y 5. Filtrado de contenido web cumplieron con lo requerido por la Conagua. Para los otros tres: el resto -1. Firewall de Nueva Generación y Sistema de Prevención de Intrusos (IPS), 4. Correlacionador de Eventos (SIEM) y Monitoreo y 6. Monitoreo- se observó lo siguiente:

"I. Servicio de firewall de nueva generación y Sistema de prevención de intrusos (IPS)

Se identificó que no se dio la totalidad de los servicios, por lo que se estiman pagos no procedentes por 6,366.0 miles de pesos por los servicios prestados en 2022 y 4,547.2 miles de pesos pagados con recursos del ejercicio fiscal de 2023. Al respecto, en el transcurso de la auditoría mediante oficio número DGATIC/414/2023 de fecha 6 de octubre de 2023 se solicitó la intervención de la instancia de control competente.

II. Servicio de Correlación de Eventos (SIEM) y monitoreo

Se identificó que no se dio la totalidad de los servicios, por lo que se estiman pagos no procedentes por 414.1 miles de pesos por los servicios prestados en 2022 y 295.8 miles de pesos pagados con recursos del ejercicio fiscal de 2023. Al respecto, en el transcurso de la auditoría mediante oficio número DGATIC/414/2023 de fecha 6 de octubre de 2023 se solicitó la intervención de la instancia de control competente.

III. Servicio de Monitoreo

No se mantiene un registro electrónico de control de cambios y configuraciones.

Se concluye que el servicio proporcionado por el proveedor Scitum, S.A. de C.V., no cumplió con su objetivo, ya que durante 2022 existieron deficiencias en la configuración de los servicios de firewall, prevención de intrusos y correlación de eventos y monitoreo, por lo que se estiman pagos no procedentes por 6,780.2 miles de pesos" (ASF, 2023: 15)

La imagen 2 muestra el semáforo de madurez de los controles de ciberseguridad en la Conagua al 2022, es decir el grado de madurez que la Conagua tenía el año previo al ciberataque –y después de siete años de haber sido nombrada instancia de Seguridad Nacional por el Consejo de Seguridad Nacional- para enfrentar ese tipo de eventos.

SEMÁFORO DE MADUREZ DE LOS CONTROLES DE CIBERSEGURIDAD EN LA COMISIÓN NACIONAL DEL AGUA DURANTE 2022

Control	Indicador
CSC Control 1: Inventario y control de los activos organizacionales.	●
CSC Control 2: Inventario y control de activos de *software*	●
CSC Control 3: Protección de datos.	●
CSC Control 4: Configuración segura de activos y *software* organizacionales.	●
CSC Control 5: Administración de cuentas.	●
CSC Control 6: Gestión de control de accesos.	●
CSC Control 7: Gestión continua de vulnerabilidades.	●
CSC Control 8: Gestión de registros de auditoría.	●
CSC Control 9: Protección del correo electrónico y navegador web.	●
CSC Control 10: Defensa contra *malware*.	●
CSC Control 11: Recuperación de datos.	●
CSC Control 12: Gestión de la infraestructura de red.	●
CSC Control 13: Monitoreo y defensa en la red.	●
CSC Control 14: Concientización en seguridad y formación de habilidades.	●
CSC Control 15: Gestión de proveedores de servicios.	●
CSC Control 16: Seguridad en el *software* de aplicación.	●
CSC Control 17: Gestión de respuesta a incidentes.	●
CSC Control 18: Pruebas de penetración.	●

Fuente: Elaborado con base en la información proporcionada por la CONAGUA.

Indicador: ●Cumplimiento aceptable ●Requiere fortalecer el control ●Carencia de control

Imagen 2. Semáforo de controles de ciberseguridad de la Conagua en 2022. Tomado de ASF (2023: 19).

Antes de hablar del ciberataque del 2023 conviene citar lo que la ASF detectó en el rubro de *Orquestación y automatización para Respuesta a Incidentes de Seguridad*:

"No se presentó documentación que acredite que se gestionan los eventos de seguridad y ciberataques con base en las mejores prácticas en la materia propuestas por el proveedor.

[…]

Los procedimientos relacionados con la atención a incidentes de seguridad y el procedimiento de control de cambios y configuraciones no se encuentran alineados con las políticas vigentes de la CONAGUA.

> *La CONAGUA no lleva a cabo las recomendaciones de seguridad que entrega el proveedor en el reporte ejecutivo mensual."* (ASF, 2023: 16)

Las condiciones estaban dadas para lo ocurrido el 13 de abril de 2023, poco importó que algunas áreas de la Conagua fueran instancias de Seguridad Nacional y que, de 2018 hasta el momento del ataque se hubieran erogado más de 3 mil millones de pesos en TIC.

2. El ciberataque de BlackByte

BlackByte es un grupo de hackers *de sombrero negro* cuyas operaciones empezaron a detectarse en septiembre de 2021. Como grupo ofrecían *Ransomware as a Service (RaaS)* y se dedicaban a cifrar los archivos comprometidos en máquinas con Windows incluyendo tanto servidores físicos como virtuales. Sus ataques se basaban en la explotación de los conjuntos de fallas ProxyShell y ProxyLogon en los servidores de Microsoft Exchange. En su momento el grupo utilizó herramientas como AdFind, AnyDesk, NetScan y PowerView para moverse lateralmente (Ruiz, 2023).

Imagen 3. Logo del grupo BlackByte. Tomado del sitio de subasta de información en la darkweb.

Para el año 2022 el grupo vulneró al equipo de futbol de la NFL, los *49ers* de San Francisco. BlackByte abrió nuevos sitios de filtraciones de datos manteniendo una estrategia de publicación y rescate de varios niveles

El mismo año, el Buró Federal de Investigaciones (FBI por sus siglas en inglés) reportó sobre el grupo:

> *"El 13 de febrero de 2022, el FBI reveló que BlackByte había accedido a la red de al menos tres organizaciones pertenecientes a los sectores de infraestructuras críticas de Estados Unidos. Más de 100 ataques detectados, en alrededor de 30 países, han sido el objetivo de los operadores de BlackByte"* (Ruiz, 2023a)

En algún momento, entre finales de 2022 e inicios de 2023, BlackByte desarrolló una nueva versión de su malware: BlackByteNT diseñada para atacar principalmente infraestructura crítica y grandes corporativos. Dicha versión está escrita en C++. La nueva versión también incluyó nuevos controladores para la explotación de la vulnerabilidad *"Bring Your Own Vulnerable Driver"* (BYOVD) con el fin de deshabilitar productos y herramientas de seguridad que puedan interferir con su ejecución. De igual

forma las nuevas capacidades de movimiento y dispersión le permiten llegar hasta computadoras de usuarios finales. La imagen 4 muestra detalles técnicos.

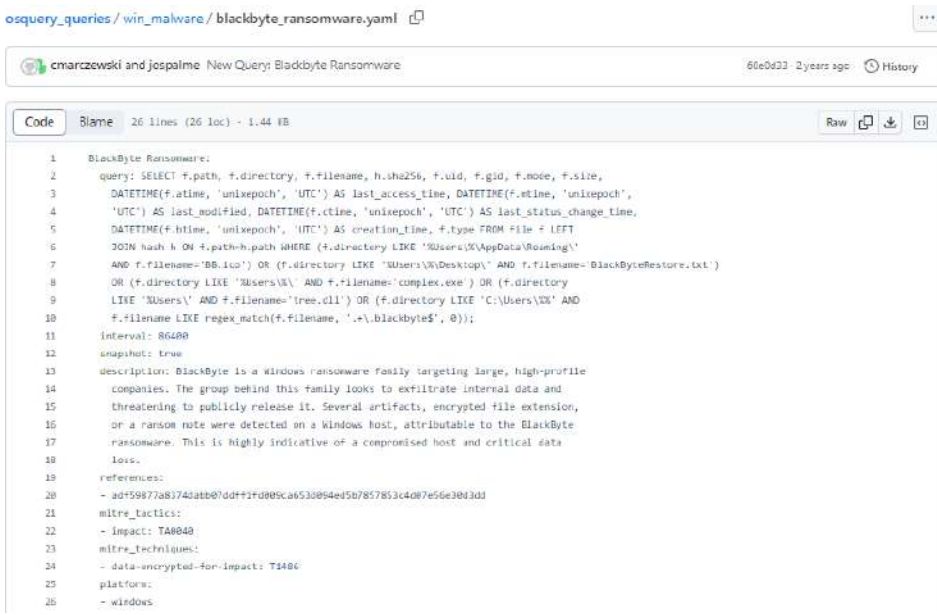


Imagen 4. Detalles técnicos del ransomware BlackByte. Tomado de Github (2023a)

En la madrugada del jueves 13 de abril de 2023 se reportó un ciberataque a los equipos de las oficinas centrales y regionales de la Conagua. A través de un ransomware se cree que se cifraron 15 años de información federal sobre cuencas y agua en México, la totalidad de los más de 12 mil empleados de la Conagua se quedaron sin acceso a los sistemas de cómputo institucionales. Se inhabilitaron todos los servicios administrativos que ofrece la Conagua: permisos, licencias, etc. Derivado del movimiento lateral del malware BlackByteNT hubo afectación directa hacia el Servicio Meteorológico Nacional (SMN), la Secretaría de Medio Ambiente y Recursos Naturales (Semarnat) y el Instituto Mexicano de Tecnología del Agua (IMTA). Hasta la fecha se perdió el control y seguimiento de las concesiones de agua otorgadas a nivel nacional.

En entrevista para medios y bajo condición de anonimato, un funcionario de la Conagua con más de 30 años de antigüedad expresó sobre el ciberataque:

> *"Nunca en la historia reciente había habido tal nivel de caos en los registros hídricos del país y en el funcionamiento de la Comisión; el descontrol es total, nadie puede trabajar en estos momentos sin computadoras y lo peor puede ser lo que nos encontremos cuando se restablezcan los sistemas, ver si no se alteraron o modificaron concesiones."* (Soto, 2023).

Ante tal evento, a lo largo del día del ciberataque la Secretaría de Seguridad y Protección Ciudadana (SSPC) reportó que:

> *"…la Dirección General Científica de la Guardia Nacional logró contener el ciberataque, sin que se registrara una "afectación mayor a los sistemas de información administrativa" […] la Secretaría de Seguridad informó que esta tarde "concluyó la contención" del ataque cibernético a los equipos de cómputo de Conagua. […] se logró contener el ataque y aislar correctamente los equipos de Conagua, aclarando que no se identificó una afectación grave a los sistemas de información administrativa"* (Redacción, 2023).

Distintas versiones del mismo mensaje fueron publicadas en distintos medios de comunicación. Sin embargo, pasados 6 días del ciberataque se publicó en el DOF (Diario Oficial de la Federación) el *Acuerdo por el que se suspenden los términos y plazos de los procedimientos que lleve a cabo la Comisión Nacional del Agua, por existir causas de fuerza mayor originadas por el incidente de seguridad informática ocurrido el 13 de abril de 2023* que en términos generales dicta que los días del 13 al 21 de abril de 2023 se declaran inhábiles para efectos de actos y procedimientos que realiza la Conagua. Posteriormente el acuerdo se prorroga el 27 de abril de 2023 y en el mes de mayo se prorroga por segunda ocasión (Riquelme, 2023).

Para junio de 2023 la ASF reporta en su *Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2022-5-16B00-20-0075-2023* respecto al ciberataque:

> *"El 13 de abril de 2023, la CONAGUA experimentó un ataque de ciberseguridad de tipo ransomware que vulneró sus activos por lo que le requirió a Scitum, S.A. de C.V. la contención de éste; a la fecha de la revisión (junio de 2023), se carece de elementos para asegurar que el ataque haya sido contenido y erradicado. A pesar de que la CONAGUA indicó haber llevado a cabo acciones para deslindar responsabilidades, no se presentó documentación que lo acredite.*
>
> *Se concluye que las deficiencias presentadas durante 2022 continuaron en 2023, por lo que durante el ciberataque en el que un ransomware se propagó en la red de la CONAGUA y comprometió sus activos, éste no fue detectado ni contenido por la solución entregada por el proveedor; no obstante, se efectuaron pagos por 4,843.0 miles de pesos durante el 2023. Al respecto, en el transcurso de la auditoría mediante oficio número DGATIC/414/2023 de fecha 6 de octubre de 2023 se solicitó la intervención de la instancia de control competente."* (ASF, 2023: 16)

Finalmente, tras un monitoreo constante hasta el mes de diciembre de 2023 del sitio de subastas (*auction*) del grupo BlackByte alojado en la darkweb,

al momento de escribir estas líneas no se ha encontrado indicio alguno de la puesta en venta de la información de Conagua (ver imágenes 5 y 6).

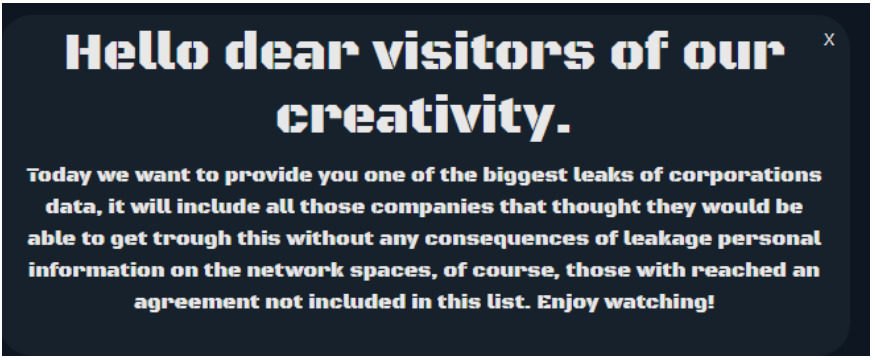


Imagen 5. Mensaje de bienvenida al sitio de subasta de información de BlackByte.

Traducción: Hola querido visitante de nuestra creatividad. Hoy queremos brindarte una de las mayores filtraciones de datos corporativos, incluirá a todas aquellas empresas que pensaron que podrían superar esto sin ninguna consecuencia de fuga de información personal en los espacios de la red, por supuesto, aquellas con las que se alcanzó un acuerdo no están incluidas en la lista. ¡Disfruta! Tomado de la darkweb en diciembre 2023.

Imagen 6. Sitio de subastas de información de compañías atacadas por BlackByte. Tomado de la darkweb.

En la imagen 6 resalta la presencia de Hoteles Xcaret, grupo turístico de importancia en la zona de la Quintana Roo, México, que al no haber llegado a un acuerdo de pago al grupo BlackByte vio expuesta su información en el

ciberespacio[76]. En el caso de Conagua la información no ha sido publicada en dicho sitio. Los especialistas tienen dos hipótesis al respecto: I) Conagua pagó el rescate -sin haberlo hecho público- o bien, II) Aún se encuentran en la fase de negociación con el grupo BlackByte. Independientemente de cual sea la hipótesis más cercana a la verdad, lo cierto es que Conagua se sumó a la nada honrosa lista de instituciones gubernamentales hackeadas durante esta administración: Petróleos Mexicanos en noviembre de 2019; Comisión Nacional de Seguros y Finanzas en noviembre de 2020; Lotería Nacional en mayo de 2021; Secretaría de la Defensa Nacional en septiembre de 2022 e incluso Presidencia de la República en enero de 2024.

Conclusión

La crónica del hackeo a las oficinas de Conagua es cada vez más frecuente en tanto en el 2023 México recibió la mitad de los ciberataques de toda la región de América Latina (Riquelme, 2024). La tragedia de ser una parada obligada en la carrera de los cibercriminales hace que la soberanía del Estado mexicano quede en entredicho.

Las reacciones institucionales de los ataques a los entes de la administración pública bien podrían constituir una obra de cuatro actos:

El primer acto consiste en las advertencias e indicios de fallos que pueden devenir en vulnerabilidades a explotar por hackers. En el caso de Conagua hubo observaciones de la ASF desde varios años previos que ponían de manifiesto la situación de riesgo en que se encontraban los equipos de cómputo e información.

El segundo acto es el ciberataque en sí, se crea caos, nadie sabe qué pasa, no se tiene idea de la magnitud, alcance, origen, responsable y daños provocados en el corto, mediano y largo plazo.

El tercer acto es la negación sistemática de los daños. Aún no se han realizado los respectivos análisis forenses, pero ya hay instituciones -en este caso la SSPC- que salen apresuradamente a mentir a los medios de comunicación diciendo: I) se contuvo el ataque y II) no se registró afectación mayor a los sistemas de información administrativa. Días después del ciberataque se publican en el DOF prórrogas de plazos institucionales de Conagua, meses después los funcionarios de Conagua seguían sin usar sus equipos de cómputo. ¿Por qué si el ciberataque no fue grave? ¿Para qué las prórrogas, si el ataque se contuvo? La negación sistemática es un prólogo de catástrofes mayores.

[76] Más información en la siguiente liga: https://www.reportur.com/estados-unidos/2023/09/19/xcaret-denuncia-ataque-cibernetico-detectado-por-su-equipo-de-ciberseguridad/

Es necesario romper el círculo vicioso de ignorar advertencias-ciberataque-caos-negación del daño. Lo anterior implica no sólo hacer revisiones y auditorías a diestra y siniestra, sino actuar en consecuencia, ejercer los recursos presupuestarios y técnicos necesarios aún si esto va en contra de eslóganes políticos como la llamada *austeridad republicana* o cualquier otro que no reflejan la complejidad y trascendencia de las interferencias en la continuidad de las actividades del Estado mexicano.

"Mientras el gobierno no invierta en ciberseguridad, México será el paraíso para nosotros": Lord Peña[77]

Bibliografía

Auditoría Superior de la Federación -ASF- (2023) Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2022-5-16B00-20-0075-2023. Consultada el 14 de febrero de 2024. Disponible en: https://informe.asf.gob.mx/Documentos/Auditorias/2022_0075_a.pdf

Comisión Nacional del Agua –Conagua- (s/f). ¿Qué es la Conagua? México, Conagua-IFAI. Consultado el 15 de agosto de 2021. Disponible en: http://www.conagua.gob.mx/CONAGUA07/Publicaciones/Folleter%C3%ADa/SGJ-3%202.pdf

Comisión Nacional del Agua –Conagua- (2019a). Estadísticas del Agua en México. Consultado el 7 de febrero de 2024. Disponible en: https://files.conagua.gob.mx/conagua/publicaciones/Publicaciones/EAM_2019.pdf

Constitución Política de los Estados Unidos Mexicanos

Diario Oficial de la Federación –DOF- (2015). Bases de Colaboración que en el marco de la Ley de Seguridad Nacional celebran la Secretaría de Gobernación y la Secretaría de Medio Ambiente y Recursos Naturales, febrero 26, 2015. Consultado el 19 de octubre de 2021. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5383466&fecha=26/02/2015

Diario Oficial de la Federación –DOF- (2017). Lineamientos para el impulso, conformación, organización y funcionamiento de los mecanismos de participación ciudadana en las dependencias y entidades de la Administración Pública Federal, agosto 11, 2017. Consultado el 11 de noviembre de 2021. Disponible en: http://dof.gob.mx/index.php?year=2017&month=08&day=11&edicion=MAT

Durand, A. (2016). Liderazgo, autoridad, trabajo en equipo, la asignación de tareas y su efecto en el Clima Laboral en la Conagua. Tesis de Maestría, UNAM.

[77] Declaraciones del *hacker* autodenominado *Lord Peña* tras el hackeo al Gobierno de la Ciudad de México mediatizado como *Chilango leaks* en abril de 2024. Se estima que la cantidad de información sustraída y puesta a subasta es del orden de 1.4 terabytes (Gómez, 2024).

Github (2023) Ransomware_notes. Consultado el 15 de febrero de 2024. Disponible en:https://github.com/threatlabz/ransomware_notes/blob/main/BlackByte/BBReadme_%5Brand%5D.txt

Github (2023a) osquery_queries/win_malware/blackbyte_ransomware.yaml. Consultado el 15 de febrero de 2024. Disponible en: https://github.com/Cisco-Talos/osquery_queries/blob/master/win_malware/blackbyte_ransomware.yaml

Gómez, I. (2024, 2 de abril) Chilango leaks: hackers de Mexican Mafia 'desnudan' al gobierno de CDMX. Publimetro. Consultado el 2 de abril de 2024. Disponible en: https://www.publimetro.com.mx/noticias/2024/04/02/chilango-leaks-hackers-de-mexican-mafia-desnudan-al-gobierno-de-cdmx/

Instituto Nacional de Administración Pública -INAP- (2015). *Génesis y evolución de la administración pública federal centralizada*. México.

Ley de Aguas Nacionales -LAN- (1992, 1° diciembre). Diario Oficial de la Federación, enero 06, 2020.

Ley de Seguridad Nacional –LSN- (2005, 31 de enero) Diario Oficial de la Federación, mayo 20, 2021.

Ley Federal de Transparencia y Acceso a la Información Pública -LFTAIP- (2016, 09 mayo). Diario Oficial de la Federación, mayo 20, 2021

Reglamento Interior de la Comisión Nacional del Agua –RICNA- (2006, 30 noviembre). Diario Oficial de la Federación, octubre 12, 2012.

Redacción (2023, 13 de abril) Conagua sufre ataque cibernético, SSPC descarta daños. Aristegui Noticias. Consultado el 15 de febrero de 2024. Disponible en: https://aristeguinoticias.com/1304/mexico/conagua-sufre-ataque-cibernetico-sspc-descarta-danos/

Riquelme, R. (2023, 8 de mayo) Semarnat planea prorrogar por segunda ocasión términos y plazos de Conagua por hackeo. El Economista. Consultado el 15 de febrero de 2024. Disponible en: https://www.eleconomista.com.mx/politica/Semarnat-planea-prorrogar-por-segunda-ocasion-terminos-y-plazos-de-Conagua-por-hackeo-20230508-0048.html

Riquelme, R. (2024, 27 de marzo) México recibió la mitad de los ciberataques en América Latina en 2023: Fortinet. El Economista. Consultado el 1 de abril de 2024. Disponible en: https://www.eleconomista.com.mx/tecnologia/Mexico-recibio-la-mitad-de-los-ciberataques-en-America-Latina-en-2023-Fortinet-20240327-0063.html

Ruiz, V. (2023) ¿Qué sabemos de BlackByte y por qué sigue siendo un peligro para las dependencias de gobierno y organizaciones en México? https://www.silikn.com/2023/05/que-sabemos-de-BlackByte-y-por-que.html

Ruiz, V. (2023a) La Secretaría de Medio Ambiente y Recursos Naturales, el Servicio

Meteorológico Nacional y el Instituto Mexicano de Tecnología del Agua en riesgo por el ataque de ransomware contra la Comisión Nacional del Agua. Consultado el 03 de octubre de 2023. Disponible en: https://www.silikn.com/2023/04/la-secretaria-de-medio-ambiente-y.html

Secretaría de Gobernación -SEGOB- (2018). Base de datos de Mecanismos de Participación Ciudadana en la Administración Pública Federal. Consultado el 11

de noviembre de 2021. Disponible en: https://mecanismosdeparticipacion.segob.gob.mx/es/Mecanismos/Consulta

Soto, S. (2023, 08 mayo) El desastre en Conagua: incendios, hackeos y corrupción. El Universal. Consultado el 11 de enero de 2024. Disponible en: https://www.eluniversal.com.mx/opinion/salvador-garcia-soto/el-desastre-en-conagua-incendios-hackeos-y-corrupcion/

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

Transformación de la Gobernanza Pública en la Protección Ciudadana Post COVID-19: Desafíos y Oportunidades para la Seguridad en México

Guadalupe Rivero Rodríguez*

Resumen: Este estudio tiene como propósito analizar y reflexionar sobre las políticas implementadas para mitigar la crisis sanitaria provocada por el virus SARS-CoV-2 y la enfermedad resultante, COVID-19. Con este enfoque, el análisis se centra en la protección y seguridad ciudadana, abordadas desde una perspectiva integral de construcción de paz y gobernanza pública en el contexto post-pandemia. La investigación utiliza una metodología cualitativa que combina el análisis documental y la aplicación de cuestionarios a servidores públicos del sector de seguridad, lo que permite comparar las políticas implementadas entre 2020-2023 y evaluar tanto su efectividad como la percepción ciudadana en términos de seguridad y gobernanza. Los resultados obtenidos evidencian una brecha significativa entre la teoría de las políticas de seguridad ciudadana y su implementación práctica, lo cual afecta de manera negativa la gobernanza pública y debilita la confianza en las instituciones. A raíz de este hallazgo, surge la necesidad de un marco conceptual que facilite el análisis de las interacciones entre el gobierno, la sociedad y los problemas de seguridad, estableciendo una conexión integral entre el sistema político y la administración pública. En este sentido, la administración pública juega un rol esencial, al encargarse de ejecutar decisiones políticas, brindar servicios, coordinar instituciones públicas y aplicar políticas. Estudiosos en el tema como López, Adalberto (2023), destaca la importancia de la confianza social y la legitimidad como pilares para la efectividad de las políticas públicas. Aguilar, Luis (2024) y Martínez-Anzures, Luis M. (2022), subrayan la necesidad de un enfoque interinstitucional y colaborativo que permita implementar

* Doctora en Administración Pública con la investigación: La gobernanza pública en la construcción de paz y la protección ciudadana. México 2012-2021, por el Instituto Nacional de Administración Pública. Maestra en Administración de Organizaciones por la Universidad Nacional Autónoma de México. Investigadora Social, con certificaciones y reconocimientos nacionales e internacionales. Conferencista y asesora en temas de Gobernanza Pública, Paz y Seguridad. Activista y Excandidata a la Titularidad de la Comisión Nacional de Derechos Humanos.

políticas de seguridad inclusivas y efectivas. Por su parte, Muggah, Robert (2021), enfatiza la responsabilidad estatal y la participación ciudadana activa en la construcción de un modelo de seguridad ciudadana. El estudio propone recomendaciones orientadas a fortalecer la capacidad de respuesta de las instituciones gubernamentales en contextos de crisis. Estas medidas se enfocan en mejorar la administración pública y en garantizar una mayor coherencia entre la teoría y la práctica, contribuyendo así a consolidar un marco de gobernanza robusto que fomente la resiliencia social y promueva un entorno de paz y seguridad para la ciudadanía.

Palabras Clave: COVID-19, Gobernanza Pública, Post-Pandemia, Paz, Seguridad Ciudadana.

Abstract: This study aims to analyze and reflect on the policies implemented to mitigate the health crisis caused by the SARS-CoV-2 virus and the resulting disease, COVID-19. With this approach, the analysis focuses on citizen protection and security, addressed from a comprehensive perspective of peacebuilding and public governance in the post-pandemic context. The research uses a qualitative methodology that combines documentary analysis and the application of questionnaires to public servants in the security sector, which allows comparing the policies implemented between 2020-2023 and evaluating both their effectiveness and citizen perception in terms of security and governance. The results obtained show a significant gap between the theory of citizen security policies and their practical implementation, which negatively affects public governance and weakens trust in institutions. As a result of this finding, the need arises for a conceptual framework that facilitates the analysis of the interactions between government, society and security problems, establishing a comprehensive connection between the political system and public administration. In this sense, public administration plays an essential role, being in charge of executing political decisions, providing services, coordinating public institutions and applying policies. Scholars on the subject such as López, Adalberto (2023), highlight the importance of social trust and legitimacy as pillars for the effectiveness of public policies. Aguilar, Luis (2024) and Martínez-Anzures, Luis M. (2022), underline the need for an inter-institutional and collaborative approach that allows the implementation of inclusive and effective security policies. For his part, Muggah, Robert (2021), emphasizes state responsibility and active citizen participation in the construction of a citizen security model. The study proposes recommendations aimed at strengthening the response capacity of government institutions in crisis contexts. These measures focus on improving public administration and ensuring greater coherence between theory and practice, thus contributing to consolidating a robust governance framework that fosters social resilience and promotes an environment of peace and security for citizens.

Keywords: COVID-19, Public Governance, Post-Pandemic, Peace, Citizen Security.

Introducción

La enfermedad COVID-19, causada por el virus SARS-CoV-2,[78] fue notificada por primera vez en Wuhan (República Popular de China), el 31 de diciembre de 2019,[79] y registrada, en los Estados Unidos Mexicanos (México), el 14 de enero de 2020. Las primeras muertes reportadas fueron el 21 de marzo de ese mismo año,[80] a pesar de que la Organización Mundial de la Salud (OMS), la declaró emergencia de salud pública y de preocupación internacional el 30 de enero de 2020.[81] Para el 5 de mayo del año 2023, el doctor Tedros Adhanom Gebreyesus de la OMS, declaró el fin de la pandemia de COVID-19. Posterior a esta notificación, México realizó una evaluación local que permitió demostrar el fin de la misma y el 9 de mayo del año 2023 se publica en el Diario Oficial de la Federación (DOF), el "Decreto por el que se declaraba terminada la acción extraordinaria en materia de salubridad general que tuvo por objeto prevenir, controlar y mitigar la COVID-19", y establece la necesidad de contar con un "Plan de gestión a largo plazo para el control de la COVID-19", aprobado por el Comité Nacional de Vigilancia Epidemiológica (CONAVE), mismo que señala la vigilancia epidemiológica continua bajo la "Estrategia Centinela en Unidades de Salud Monitoras de Enfermedad Respiratoria Viral" (USMER), y con la confirmación de casos mediante la prueba de RT-PCR.[82]

[78] El virus que causa la COVID-19 es el SARS-CoV-22 (severe acute respiratory síndrome. Coronavirus 2, por sus siglas en inglés; en español: coronavirus tipo 2 del síndrome respiratorio agudo grave). Es parte de la familia de coronavirus, que incluyen virus comunes que causan diversas enfermedades, desde resfriados hasta enfermedades más graves (pero menos frecuentes) como el síndrome respiratorio agudo grave (SARS, por sus siglas en inglés) y el síndrome respiratorio de Oriente Medio (MERS, por sus siglas en inglés).

[79] Organización Mundial de la Salud. (2024). Brote de enfermedad por Coronavirus (COVID-19). Recuperado de: https://www.who.int/es/emergencies/diseases/novel-coronavirus-2019

[80] Statista. (2024). Salud e industria farmacéutica. Estado de salud. Número semanal de casos confirmados y muertes causadas por el coronavirus (COVID-19), en México entre enero de 2020 y julio de 2022. Recuperado de: https://es.statista.com/estadisticas/1110089/numero-casos-muertes-covid-19-mexico/

[81] Organización Panamericana de la Salud. (2020). La OMS caracteriza a COVID-19 como una pandemia. Recuperado de: https://www.paho.org/es/noticias/11-3-2020-oms-caracteriza-covid-19-como-pandemia

[82] A partir de la semana 40 de 2023. Secretaría de Salud. Gobierno Federal (2023). Informe integral de COVID-19 en México. Número 4-2023. 30 de diciembre de 2023. Recuperado de: https://epidemiologia.salud.gob.mx/gobmx/salud/documentos/covid19/Info-04-23-Int_COVID-19.pdf

Los reportes oficiales acumulados para el cierre de junio del año 2023 que, México informa corresponden a 7,633,355 casos confirmados[83] y 334,336 defunciones.[84]

Durante la pandemia de COVID-19, era común leer y escuchar afirmaciones como "Crisis sanitaria sin precedentes que ha expuesto las profundas fragilidades de los sistemas de seguridad y protección ciudadana en México." Fuimos testigos de la interrupción de servicios esenciales, como consultas médicas y la cancelación de cirugías previamente programadas, debido a la concentración de recursos en el sector salud y a las restricciones de movilidad impuestas con la consigna de "Quédate en casa." Esta pandemia resaltó la importancia crucial de lograr la eficacia y eficiencia en la capacidad del gobierno para administrar los recursos públicos, tomar decisiones estratégicas, aplicar mecanismos de colaboración y coordinar esfuerzos interinstitucionales.[85] Además, para la post-pandemia, atender la necesidad de fomentar la resiliencia y proteger a la ciudadanía desde un enfoque integral que incluya las dimensiones culturales, económicas, políticas y sociales en la prevención y el combate contra el crimen y la delincuencia organizada (DO), atendiendo las directrices del buen gobierno (BG),[86] sin descuidar la serie de desafíos de diversa naturaleza como la sanitaria, la social, la de vigencia de los derechos humanos (DH), y no menos importante la de seguridad.

La pregunta eje de la investigación: ¿Cómo ha impactado la pandemia de COVID-19 en la gobernanza pública y las políticas de protección ciudadana en México? En función de ello, ¿Qué estrategias son necesarias para fortalecer la construcción de paz y la seguridad en el escenario post-pandemia? El objetivo de la investigación es identificar las estrategias implementadas en términos de seguridad, con un enfoque en la protección y seguridad ciudadana (SC), una perspectiva integral de construcción de paz y la gobernanza pública (GP). Se evalúa la percepción ciudadana respecto a la efectividad del gobierno en la adopción y ejecución de actividades realizadas por la policía y otras fuerzas

[83] Al cierre del mes de junio del año 2023, reporta total de personas confirmadas con COVID-19 de las cuales el 53.66 por ciento son mujeres y 46.34 por ciento son hombres. El 9.57 por ciento son casos hospitalizados y el 90.43 por ciento son casos ambulatorios. Las comorbilidades principales son la hipertensión (11.90 por ciento), seguido de la obesidad (9.59 por ciento), la diabetes (8.74 por ciento), y el tabaquismo (5.41 por ciento). Además, la Secretaría de Salud de Gobierno Federal ha identificado periodos Inter epidémicos, el primero entre la 2ª y 3ª ola, que abarcó de la SE 16 a la 22 del año 2021; el segundo entre la 3ª y 4ª ola de la SE 43 a la 50 del año 2021, el tercero de la SE 10 a la 21 del año 2022, el cuarto de la SE 34 a la 48 del año 2022, el quinto de la SE 5 al corte de información de este informe trimestral. Ídem

[84] Consejo Nacional de Ciencia y Tecnología. (2023). Covid-19 México. Información General Nacional (Confirmados). DGE. Recuperado de: https://datos.covid-19.conacyt.mx/

[85] De entre los mecanismos de coordinación se tiene el acuerdo, convenio, comisión, comité y consulta.

[86] Las directrices del BG sugeridas por las Naciones Unidas son las relativas a: Eliminación del conflicto, garantía de los DH, el Estado de derecho, la transparencia, la rendición de cuentas la seguridad, la justicia, el respeto de la ética y el fomento a la construcción de paz.

de seguridad durante las medidas de contención sanitaria. Se busca determinar si las instituciones contaban con el respaldo legal, la capacitación, la sensibilización, la infraestructura y el equipo necesario para responder adecuadamente a las distintas necesidades durante y después de la crisis sanitaria, caracterizada por cargas desproporcionadas. Adicionalmente, se examina el dilema al que se enfrentaron los servidores públicos de seguridad: cumplir o no con el aislamiento social, conforme a sus atribuciones, con el fin de contribuir a la cohesión social.

Uno de los problemas en temas de (in)seguridad, se origina en la creación de la policía moderna con la falta de independencia respecto de la influencia política, el uso indebido de la capacidad coercitiva y el desafío de mantener el respeto, la aprobación y la cooperación del público con la tolerancia cero, la vigilancia de ventanas rotas y la policía militarizada.[87] A pesar de que la Secretaría de Seguridad y Protección Ciudadana (SSPC), tiene a su cargo el ejercicio de las atribuciones en materia de SP y SN, controlar las políticas de seguridad, criminalidad, drogas, prevención del delito y construcción de paz; establecer los mecanismos de coordinación interinstitucional y de planeación para cumplir el mandato del artículo 21 Constitucional, plantear el "Programa Rector de Profesionalización en materia de SP", proponer al titular SESNSP y de la Conferencia Nacional del Sistema Penitenciario, presidir la Conferencia Nacional de Secretarios de Seguridad Pública (CNSSP), entre otras, la seguridad sigue siendo uno de sus grandes retos a resolver en el país por el diseño institucional en materia de SP, SN y SI que se tiene en el Estado, al ser incompatible desde el enfoque de conceptos entre ambas y la SC, lo que propicia una serie de retos en términos de los procesos y las funciones de la estructura orgánica básica, la capacidad de organización interior de las instituciones públicas, los mecanismos de coordinación interinstitucional, la cooperación y las estrategias preventivas a fin de evitar la realización de faltas administrativas y la comisión de delitos, así como el salvaguardar la integridad de las personas y de su patrimonio -como lo establece el ordenamiento jurídico-, el garantizar, mantener y restablecer la paz social.

Desarrollo

Sin que sea la pretensión exponer un análisis en extenso de las diversas teorías y enfoques a los conceptos que se abordan durante el trayecto de la

[87] Blair, Weinstein, Christia, Arias, Badran, Cheema, Farooqui, Fetzer, Grossman, Haim, Hameed, Hanson, Hasanain, Kronick, Morse, Muggah, Nadeem, Tsai, Nanes, Slough, Ravanilla, Shapiro, Silva, Souza y Wilke. (2021). La policía comunitaria no fomenta la confianza de los ciudadanos en la policía ni reduce la delincuencia en el Sur Global. Blair et al., Science 374, 1098 (2021) 26 November 2021. Recuperado de: https://www.science.org/doi/epdf/10.1126/science.abd3446

investigación, es indiscutible tener presente en términos de gobernanza lo que Aguilar, Luis (2024), sostiene como acción estructurada por las instituciones -acorde con los valores, principios y normas del Estado, determinando su legitimidad social-, y por el conocimiento -modelos causales accionables de las ciencias, las tecnologías y las buenas prácticas de gerencia-, lo que determina su efectividad social,[88] y por otra parte, Martínez-Anzures, Luis M. (2022), que la atribuye a las "Instituciones como unificadoras de la sociedad", además, de lo que refiere Ongaro, Edoardo (2020), como término que se usa para indicar los procesos más amplios de conducir a la sociedad mediante las instituciones públicas y de involucrar a los actores no gubernamentales en las políticas públicas. Finalmente, la definición que realiza Pérez, Rigoberto (2019), como "Buena Gobernanza", al asunto prioritario no sólo para el Estado sino para las instituciones internacionales de desarrollo como el Banco Mundial (BM) y el Fondo Monetario Internacional (FMI).[89]

Por lo que argumento que la gobernanza es un modelo de gestión del Estado con enfoque participativo en el que se convierte en un eslabón fundamental para el diseño, elaboración, implementación y evaluación de las políticas públicas con lo cual permite trascender el paradigma del gobierno unilateral, y con ello se establece una dinámica colaborativa de involucramiento en las decisiones que se tomen como ejercicio de la democracia al amparo del marco jurídico que tiene como fin primordial la protección de la integridad humana y el resguardo de los bienes de la nación, la garantía de la transparencia y la eficiente aplicación de los procesos administrativos, con el abordaje integral de las causas estructurales que generen el desorden social.

Al ser las instituciones las promotoras de la colaboración y la participación ciudadana, pueden desempeñar un papel fundamental en el contexto social, caracterizado por valores, normas y relaciones sociales, que moldean la identidad, la percepción y la actitud de las personas, por ello, señalo el planteamiento que Molenveld, Verhoest, Voets y Steen (2020), refieren en términos de la colaboración como una agenda de investigación en desarrollo, que incluye diversos mecanismos de coordinación para gestionar la administración pública (AP), de manera intersectorial en distintos ámbitos gubernamentales. No sólo se busca entregar servicios a un público específico,

---

[88] Aguilar, Villanueva. Luis F. (2024). La nueva gobernanza pública: un panorama conceptual The new public governance: a conceptual panorama. Perfiles Latinoamericanos, 32(63) | 2024 | e-ISSN: 2309-4982 DOI: dx.doi.org/10.18504/pl3263-001-202. Recuperado de: https://perfilesla.flacso.edu.mx/index.php/perfilesla/article/view/1826/1365

[89] Pérez Rigoberto. (2019). *Administración pública y gobernanza en México. Análisis del cambio institucional en la agenda de BG*. México. Books-©ECORFN. Recuperado de: https://www.ecorfn.org/libros/Administraci%C3%B3n%20p%C3%BAblica%20y%20gobernanza%20en%20M%C3%A9xico.pdf

sino también atender de forma articulada necesidades sociales o prevenir problemas complejos y diversos, considerando las causas en sus orígenes.[90]

Para el caso de la cohesión social, Urteaga, Eguzki (2005), señala lo que Putman, Robert, argumentó como la consecuencia de pertenencia a un grupo, en términos de reciprocidad, solidaridad y confianza entre los mismos integrantes, pasando por las características institucionales e incluso culturales de una sociedad.[91]

El planteamiento de comprender cómo se contribuye al debate sobre la seguridad en el contexto de la pandemia y post-pandemia, más la crisis sanitaria generada por el COVID-19, en la desestabilización del sistema de salud, la gestión de la seguridad en el país y la capacidad del Estado para atender la problemática de la DO y la violencia estructural, son analizadas en términos de los homicidios y el enfoque de la SC. A este respecto, el Banco Interamericano de Desarrollo (BID), refiere en términos de SC a la capacidad de los Estados en asociación con el sector privado, los particulares, la academia y asociaciones comunitarias, vecinales y ciudadanas, para proveer y coproducir un marco de protección de la vida y el patrimonio de los individuos, que permita a los ciudadanos convivir pacíficamente, sin miedo, en aras de alcanzar una mejor calidad de vida.[92] Es la situación de tranquilidad pública y de libre ejercicio de los derechos individuales, cuya protección efectiva se encomienda a las fuerzas de orden público.[93] Para la Organización de los Estados Americanos (OEA), la SC aborda los problemas de criminalidad y violencia desde una perspectiva de los DH, la construcción de mayores niveles de ciudadanía democrática, la seguridad de las personas y grupos sociales como objetivo central de las políticas, esencial en la consecución del bien común en

[90] Herrera-Kit, Patricia; Balanzó Guzmán, Alejandro; Parra Moreno, Juliana; Rivera Chávez, Marcela. (2021). Mecanismos de colaboración interinstitucional: prácticas típicas. Innovar, vol. 31, núm. 79, 2021, Enero-Marzo, pp. 145-159 Facultad de Ciencias Económicas. Universidad Nacional de Colombia. DOI: https://doi.org/10.15446/innovar.v31n79.91888

[91] Urteaga, Eguzki. (2013). La teoría del capital social de Robert Putnam: Originalidad y carencias. Reflexión Política, vol. 15, núm. 29, junio, 2013, pp. 44-60. Universidad Autónoma de Bucaramanga, Colombia. Recuperado de: https://www.redalyc.org/articulo.oa?id=11028415005

[92] Comisión Interamericana de Derechos Humanos. (2009) Informe sobre Seguridad Ciudadana y Derechos Humanos Recuperada de: https://www.oas.org/es/cidh/docs/pdfs/seguridad%20ciudadana%202009%20esp.pdf

[93] Definición de la Real Academia Española (RAE). Recuperado de: https://dle.rae.es/seguridad La palabra "Seguridad", proviene "Del latín (Del lat. securĭtas, -ātis). Cualidad de seguro. Certeza -conocimiento seguro y claro de algo-.
Acotar que el término de "Seguridad Interior"; "Seguridad Nacional", "Seguridad Pública", la palabra no está en el diccionario de la RAE.

una sociedad democrática, una condición donde las personas viven libres de la violencia practicada por actores estatales o no estatales.[94]

El Programa de Naciones Unidas para el Desarrollo (PNUD), considera a la SC como un bien público que implica la salvaguarda eficaz de los DH -vida, integridad personal, inviolabilidad del domicilio y libertad de movimiento- es el proceso de establecer, fortalecer y proteger el orden civil democrático, eliminando las amenazas de violencia en la población y permitiendo una coexistencia segura y pacífica. Es el conjunto de intervenciones públicas llevadas a cabo por diferentes actores estatales y sociales, cuya finalidad es abordar y resolver riesgos y conflictos concretos y visibles, así como hechos violentos o delictivos que lesionen los derechos y libertades de las personas, mediante la prevención y el control de los mismos.[95]

Muggah, Robert (2021), señala que es más fácil describir lo que es la SC que conceptualizarla como tal, prioriza la responsabilidad estatal y la ciudadanía proactiva, enfatiza los enfoques preventivos, la reducción de riesgos y la mejora de los factores de protección en las áreas afectadas por el delito. Promueve modelos orientados a la comunidad, la participación ciudadana y las intervenciones basadas en datos. En términos funcionales, consiste en una amplia gama de prevención primaria y secundaria de la violencia, vigilancia comunitaria y de proximidad, rehabilitación de jóvenes en riesgo y mecanismos de justicia innovadores.[96] Por lo que podemos afirmar que la SC es un concepto multifacético, que implica la construcción de comunidades seguras, la promoción de los DH y la participación activa de la ciudadanía, es un proceso complejo que requiere un enfoque integral y multidimensional, involucrando a diversos actores y considerando las particularidades de cada contexto. Ver Tabla 1.

[94] Organización de los Estados Americanos. Comisión Interamericana de derechos humanos (2009). Informe sobre seguridad ciudadana y derechos humanos. Recuperado de: https://www.oas.org/es/cidh/docs/pdfs/seguridad%20ciudadana%202009%20esp.pdf

[95] Por ello, retoma una especial significación el reconocimiento al Principio "pro persona", entendido como la forma más amplia y favorable que las autoridades deben observar para promover, respetar, proteger y garantizarlos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad, requiere obligadamente el ser observado junto con las directrices del BG como principios para alcanzar las expectativas. Programa Nacional para la Prevención Social de la Violencia y la Delincuencia 2014-2018. Publicado en el Diario Oficial de la Federación (DOF). 30-04-2014.

[96] Dos Ramos y Muggah Robert. (2014). Foreword for "Making Brazilian Cities Safer: A Citizen Security Dialogues Special Edition". Stability: International Journal of Security & Development, 3(1): 17, pp. 1-4, DOI: http://dx.doi.org/10.5334/sta.dn Recuperado de: https://storage.googleapis.com/jnl-up-j-sijsd-files/journals/1/articles/242/submission/proof/242-1-1008-1-10-20140513.pdf

Tabla 1. ***Principales características y enfoque conceptual de la SC***

Autor /Institución	Características Principales	Enfoque
BID .	Coproducción de seguridad, participación ciudadana, enfoque multisectorial, protección integral (vida, patrimonio), mejora de la calidad de vida	Participativo y comunitario
OEA	DH, construcción de ciudadanía democrática, seguridad de personas y grupos sociales, prevención de la violencia	DH y construcción de ciudadanía
PNUD	Bien público, salvaguarda de derechos humanos, orden civil democrático, prevención y control de la violencia	DH y prevención
Muggah, Robert	Responsabilidad estatal y ciudadanía proactiva, enfoques preventivos, reducción de riesgos, participación ciudadana, intervenciones basadas en datos	Prevención y participación ciudadana
RAE	Tranquilidad pública, ejercicio de derechos individuales, protección estatal.	Legal y estatal

Fuente de la tabla: Elaboración propia con base en la información analizada.

Como se puede observar, la diversidad de perspectivas que presentan estas conceptualizaciones sobre la SC nos brinda una visión rica y compleja, la importancia de garantizar la seguridad, algunas enfatizan la participación ciudadana y la coproducción de seguridad (BID, Muggah), mientras que otras se centran en el papel del Estado (RAE, OEA), la mejora de la calidad de vida (BID), hasta un enfoque más limitado centrado en la protección de los derechos individuales (RAE). Existe un consenso en la importancia del Estado, pero el BID y Muggah destacan también el papel de otros actores como la sociedad civil y el sector privado. Además, hacen referencia a diversas herramientas para garantizar la seguridad ciudadana, como la prevención, la participación ciudadana, la justicia, y el fortalecimiento institucional.

Para el caso de la Seguridad Nacional (SN), se ha definido como la capacidad del Estado de mantener su independencia, su integridad y su funcionalidad contra fuerzas hostiles que le creen amenazas.[97] Piñeiro, José (2011), refiere que es una situación donde la mayoría de los sectores y clases sociales de la nación tienen garantizadas sus necesidades culturales y materiales vitales a través de las decisiones del gobierno nacional en turno y de las acciones conjuntas de las instituciones del Estado, o sea, una situación de relativa seguridad frente a amenazas o retos internos o externos (reales o potenciales)

[97] Coloquio Internacional: Seguridad en las fronteras de México, 2002. Centro de Documentación, información y análisis. Dirección de servicios de investigación y análisis. Subdirección de política exterior. Recuperado de: https://www.diputados.gob.mx/sedia/sia/spe/SPE-ISS-01-07.pdf

que atenten contra la reproducción de la nación y del Estado.[98] Buzan, Barry (1991), refiere, son las medidas que un Estado toma para asegurar su supervivencia en un sistema internacional anárquico. Bull, Hedley (1977), es la condición en la que un Estado se siente seguro frente a amenazas externas. Wolfers, Arnold (1962), es la capacidad de un Estado para salvaguardar sus valores y protegerlos contra amenazas externas. Morgenthau, Hans (1948), la señala como la promoción y protección de los intereses nacionales vitales de un Estado, la supervivencia, integridad territorial y bienestar económico. Von Clausewitz, Carl (1651), es la capacidad de un Estado para hacer frente a la guerra y preservar su integridad territorial y política. Hobbes, Thomas (1651), la define como la protección de la vida y los bienes de los ciudadanos frente a la amenaza de la violencia interna o externa. Ver Tabla 2.

Tabla 2. ***Principales características y enfoque conceptual de la SN***

Autor /Institución	Características Principales	Enfoque
Coloquio Internacional	Capacidad del Estado para enfrentar amenazas externas	Independencia, integridad, funcionalidad
Piñeiro, José	Garantía de necesidades culturales y materiales, protección frente a amenazas internas y externas	Bienestar social, reproducción del Estado-Nación
Buzan, Barry	Supervivencia del Estado en un sistema anárquico	Medidas de seguridad en el contexto internacional
Bull, Hedley	Seguridad del Estado frente a amenazas externas	Sentimiento de seguridad, protección estatal
Wolfers, Arnold	Salvaguarda de valores nacionales	Protección de valores ante amenazas externas
Morgenthau, Hans	Promoción y protección de intereses nacionales vitales	Supervivencia, integridad territorial, bienestar económico
Von Clausewitz	Capacidad para hacer frente a la guerra	Integridad territorial y política
Hobbes, Thomas	Protección de la vida y los bienes de los ciudadanos	Seguridad frente a la violencia interna y externa

Fuente de la tabla: Elaboración propia con base en la información analizada.

Las conceptualizaciones presentadas coinciden en la importancia de proteger al Estado de amenazas externas e internas. Además, la mayoría

[98] Piñeiro, José Luis. (2001). La seguridad nacional de México a inicios de siglo: Reflexiones y propuestas. Recuperado de: https://ru.micisan.unam.mx/bitstream/handle/123456789/20870/L0056_0085.pdf?sequence=1

enfatiza la necesidad de garantizar la seguridad de los ciudadanos. Varían en cuanto al énfasis que ponen en diferentes aspectos de la seguridad nacional, como la seguridad militar, la seguridad económica, la seguridad humana. También difieren en cuanto al nivel de abstracción y la complejidad de sus conceptos. Por lo que se puede interpretar que, la SN, son las acciones, toma de decisiones y la capacidad que el Estado realiza para preservar los intereses nacionales ante las amenazas de grupos criminales transnacionales, presiones políticas, militares, financieras, culturales, sociales y de guerra a fin de mantener su soberanía.

Para el caso de la Seguridad Interior (SI),[99] al igual que la SN no existe una definición universalmente aceptada, empero se tienen propuestas como la Bigio, Didier (2020), que la enuncia como la lucha contra el terrorismo, las drogas, la delincuencia organizada, la delincuencia transfronteriza, la inmigración ilegal, así como el control de los flujos transnacionales de personas (migrantes, solicitantes de asilo, circulación transfronteriza), o incluso el control de cualquier ciudadano que, en principio, no se asemeja a la imagen social de la identidad nacional, las relaciones con las fuerzas armadas, la gestión pública y privada de la seguridad desde un ángulo coercitivo e incluso hasta el intercambio de la base de datos.[100] Wacquant, Loïc (2009), la señala como el control social. Fassin, Didier (2009), la establece como parte de la historia del castigo. Bauman, Zyfmunt (2000), la relaciona con la incertidumbre y la inseguridad de la sociedad, incluso, aunque no tan reciente, pero por la definición de las amenazas internas como la delincuencia, la violencia y la corrupción, la de Gustavo Sainz (1984) que, la señala como la condición en la que los ciudadanos se sienten seguros frente a estas. Ver Tabla 3.

Tabla 3. ***Principales características y enfoque conceptual de la SI***

Autor	Características Principales	Enfoque
Bigio, Didier	Lucha contra amenazas transnacionales y control social	Terrorismo, drogas, delincuencia organizada, control de fronteras, vigilancia
Wacquant, Loïc	Control social	Nuevas formas de control social

[99] SI, su respaldo jurídico es el artículo 129 Constitucional "En tiempo de paz, ninguna autoridad militar puede ejercer más funciones que las que tenga previstas en esta Constitución y las leyes que de ella emanen".

[100] Bigo Didier. (2020). ¿La mundialización de la (in)seguridad? Reflexiones sobre el campo de profesionales de la gestión de las incertidumbres y analítica de la transnacionalización de los procesos de (in)securización. Delito y Sociedad. Revista de ciencias Sociales 49(1) e0002, pp. 5–50. DOI: https://doi.org/10.14409/dys.2020.49.e0002. Recuperado de: https://www.academia.edu/95280573/_La_mundializaci%C3%B3n_de_la_in_seguridad_Reflexiones_sobre_el_campo_de_profesionales_de_la_gesti%C3%B3n_de_las_incertidumbres_y_anal%C3%ADtica_de_la_transnacionalizaci%C3%B3n_de_los_procesos_de_in_securizaci%C3%B3n

Fassin, Didier	Historia del castigo	Evolución de las prácticas punitivas
Bauman, Zygmunt	Incertidumbre y riesgo en la sociedad	Efectos de la modernidad líquida
Gustavo Sainz	SC	Amenazas internas como la delincuencia y la corrupción

Fuente de la tabla: Elaboración propia con base en la información analizada.

Lo que refleja la importancia de proteger a los ciudadanos y garantizar la seguridad, reconocen la influencia de factores globales y sociales en la SI, varían en cuanto al énfasis como la amenaza, el control, la protección, la percepción de seguridad y las causas de la inseguridad, el nivel de abstracción y la complejidad. Con base en ello la SI, es la suma de esfuerzos y mecanismos para proteger a la sociedad contra una amplia gama de amenazas internas como la violencia, el desorden social, el crimen, la delincuencia organizada, la corrupción, el terrorismo, la inmigración ilegal, el flujo de efectivo ilegal a fin de contar con una convivencia pacífica en un contexto moderno y globalizado.

La seguridad pública (SP), es un estado dinámico y multifacético que implica la creación de condiciones sociales, políticas y económicas que permitan a los individuos y comunidades vivir libres de miedo y violencia, garantizando la protección de sus derechos humanos y libertades fundamentales. Se construye a través de la participación de los ciudadanos, las instituciones estatales y la sociedad civil, y se manifiesta en la prevención del delito, la aplicación de la justicia, la promoción de la convivencia pacífica y el bienestar social, todo ello en un contexto globalizado y en constante evolución. Jiménez, Rene (2005), la define como un conjunto de políticas y acciones coherentes y articuladas que tienden a garantizar la paz pública a través de la prevención y represión de los delitos y de las faltas contra el orden público, mediante un sistema de control penal y de policía administrativa. Este tipo de definición se engarza con la necesidad de conocer, profundizar y medir la inseguridad. [101] La Constitución Política de los Estados Unidos Mexicanos (CPEUM), y la Ley General del Sistema Nacional de Seguridad Pública (LGSNSP), señala que la SP es una función concurrente a cargo de los tres niveles de gobierno, que tienen como fin salvaguardar la integridad y derechos de las personas, preservar las libertades, el orden y la paz públicos, la prevención de los delitos, la sanción de las infracciones administrativas, la investigación y la persecución de los delitos y la reinserción social del sentenciado.

Marco Jurídico y Políticas

[101] García Ramírez, Islas de González Mariscal, Vargas Casillas. Coordinadores. (2005). Temas de derecho penal, seguridad pública y criminalística. Recuperado de: https://biblio.juridicas.unam.mx/bjv/detalle-libro/1724-temas-de-derecho-penal-seguridad-publica-y-criminalistica

Para contribuir a la construcción de un marco jurídico de seguridad más robusto, es necesario el reconocer que el Derecho a la SC, SI, SN o SP, no son establecidas como tal en los Estándares Interamericanos del Marco Normativo y Obligaciones Generales de los Estados en Materia de Derechos Económicos, Sociales, Culturales y Ambientales en el Sistema Interamericano (DESCA),[102] a pesar de que desde el "Pacto de San José", se establece la obligación de los Estados Parte de adoptar medidas para lograr establecer una serie de derechos, ninguno de los tipos de seguridad -previamente enunciados es establecido como obligación para ser atendida entre las necesidades básicas del desarrollo humano.

La Carta de la Organización de los Estados Americanos contiene disposiciones referentes al desarrollo integral y bienestar de las personas,[103] por su parte, la propia Comisión Interamericana de Derechos Humanos (CIDH), ha enfatizado una relación directa entre el ambiente físico en el que viven las personas y los derechos a la vida, a la seguridad y a la integridad física, así como el derecho a vivir en seguridad adecuada, paz y dignidad, reconociendo el carácter indivisible, interdependiente, interrelacionado y universal de los DH vinculados también a los servicios públicos como parte de las funciones de los Estados, sin importar que la provisión de estos servicios se presten por agentes privados.

El 20 de abril de 2020, la CIDH lanzó el pronunciamiento CP081/2020, a los Estados miembros para adoptar políticas de sensibilización dirigidas a la fuerzas del orden público y a las autoridades judiciales en materia de identidad y expresión de género a fin de garantizar los derechos de las personas en respuesta a la pandemia del COVID-19 y solicitar que se garantice la "seguridad humana integral", en concordancia con el art. 45 de la Carta de la OEA refiere que, "(…), el hombre sólo puede alcanzar la plena realización de sus aspiraciones dentro de un orden social justo, acompañado de desarrollo económico y verdadera paz".

Durante la pandemia y posterior a la misma se realizaron una serie de reformas a los artículos constitucionales como respuesta a los desafíos surgidos de esa experiencia. De entre estos, destaca el "Derecho a la Protección de la

---

[102] García M. Soledad (2021). Compendio sobre Derechos Económicos Sociales Culturales y Ambientales. Estándares Interamericanos. Relatoría Especial sobre Derechos Económicos Sociales Culturales y Ambientales REDESCA. Comisión Interamericana de Derechos Humanos. Noruega.

[103] La Corte ha reconocido *inter alia*, que la salud es un derecho humano -art. 26 de la Convención Americana-, fundamental e indispensable para el ejercicio adecuado de los demás. Precedente que permite fortalecer el argumento de que este derecho se ve particularmente afectado en el contexto en que concurre ante la inseguridad y la violencia, teniendo como resultado índices de reproducción de las condiciones de pobreza, exclusión social y desigualdades entre otros, aumentando el surgimiento de tensiones sociales, violencia, inseguridad y delincuencia.

Salud (Art. 4)", ya que reconoce el derecho a la salud como prioridad y señala la necesidad de un sistema de salud para el bienestar a fin de garantizar servicios gratuitos y accesibles, especialmente para quienes carecen de seguridad social, propicia el fomento a la inclusión y la cobertura en salud, ocasionada por la vulnerabilidad expuesta por la crisis sanitaria. La "Política de Bienestar y Apoyo Social" (Art. 4 y Transitorios), se observa en la ampliación de los derechos sociales como las pensiones y apoyos para discapacitados permanentes o personas en condiciones de pobreza. Con esta reforma se intenta mitigar el impacto económico de la pandemia, orientado a reducir desigualdades y mejorar el acceso a servicios esenciales. El "Fortalecimiento del Derecho a la Identidad" (Art. 4), reconoce la inclusión de comunidades vulnerables e indígenas, el respeto a la diversidad cultural y lingüística y refuerzan los derechos de las comunidades indígenas y afromexicanas en la toma de decisiones, subrayando la importancia de inclusión en tiempos de crisis, ver Tabla 4.

Tabla 4. ***Artículos Constitucionales Reformados 2020-2023 (Periodo Post-Pandemia)***

	Año			
	2020	**2021**	**2022**	**2023**
Artículo	4, 28, 73, 115, 122	30, 43, 73, 74, 94, 97, 99, 100, 105, 107, 108, 111	Artículo Transitorio Quinto	38, 55, 91, 102, 116

Fuente: Elaboración propia con base en el análisis realizado. Recuperado de: Últimas Reformas DOF 30-09-2024 https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Con base en el análisis a las reformas constitucionales revisadas, ninguna enuncia la relación directa con situaciones pandémicas, se centran en aspectos relacionados con la estructura del Estado, los derechos fundamentales, la organización de los poderes públicos y las políticas en diversas áreas, como seguridad, salud, justicia y desarrollo urbano. Sí bien es cierto que la mayoría de las reformas presentadas tienen un impacto directo o indirecto en materia de SC y SP, algunas de las más relevantes son aquellas que establece la participación de la Guardia Nacional (GN), (Art. 21[104] y Transitorios), con su intervención en apoyo de la SP, especialmente en las

[104] El artículo 21 Constitucional sea claro en términos de SN, SP, SC, SI, el fortalecimiento de la policía -Federal, Estatal y Municipal-, enunciar la asignación presupuestal en términos de capacitación, especialización, certificación, incluso señalar las disciplinas como análisis y razonamiento de datos, coordinación interinstitucional y cooperación, criminología, criminalística, Derechos Humanos (DH), ética, Estado de derecho, escenarios disruptivos, fuerza policial no bélica, prevención, provención, igualdad de género, investigación científica delictiva, procesos administrativos, psicología, sociología, más allá que un listado de obligaciones y sí una obligatoriedad para el diseño institucional de seguridad.

tareas de coordinación para la implementación de programas de emergencia en zonas vulnerables o en situaciones de riesgo sanitario, otorgándoles mayores facultades y su coordinación con las fuerzas armadas mexicanas (FAM).

Se cuenta con Fondo para el Fortalecimiento de las Instituciones de Seguridad Pública (FOFISP), el cual es un fondo considerado en el Presupuesto de Egresos de la Federación (PEF), 2023, a través del cual la Federación transfiere recursos al Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), para beneficiar a las entidades federativas en el fortalecimiento de las Instituciones de SP estatales y municipales.[105] Se establece el aumento en mecanismos de coordinación entre los niveles de gobierno al subrayar la necesidad de una mayor coordinación en seguridad para atender situaciones de emergencia y crisis sanitarias, además, de asegurar los recursos y el monitoreo continuo para adaptarse a situaciones como la pandemia. Además, se establecen límites y condiciones para la participación de las fuerzas armadas en tareas de seguridad pública, buscando garantizar el respeto a los derechos humanos. Por la importancia que tiene el Art. 1° Constitucional y a pesar de que la última reforma fue del 10 de junio del año 2011, es de vital trascendencia ya que señala a las autoridades en el ámbito de sus competencias, como obligación el promover, respetar, proteger y garantizar los principios de universalidad, interdependencia, indivisibilidad y progresividad, no sólo en términos de educación, cultura, salud o vivienda, sino, además, de seguridad. Además del artículo 134 Constitucional y las normas de carácter secundario que establecen los principios de actuación que deben regir en el servicio público.[106]

Con respecto a la Ley de la Guardia Nacional sus últimas reformas publicadas corresponden al 09 de septiembre del año 2022, por lo que el artículo 9, fracción XVIII sigue señalando que, la actuación de la investigación a los delitos por parte de los "elementos" de la GN,[107] son de carácter complementario y de auxilio al Ministerio Público (MP), en la prevención y el combate del delito, incluyendo aquellos investigados hasta el año 2018 por la Agencia Federal de Investigación (AFI), y que derivado de la reforma del mismo año en materia de justicia penal se asignan las atribuciones a la Fiscalía General de la República (FGR) a través de la Policía Federal Ministerial (PFM),

[105] DOF, 31-03-2023

[106] Ley Federal de Procedimiento Administrativo -establece las obligaciones de la APF-, la Ley Federal de Presupuesto y Responsabilidad Hacendaria y la Ley Federal de Austeridad Republicana, en la que se señalan los principios de utilización de los recursos públicos con eficiencia, eficacia, transparencia, economía y honradez. Incluso la organización de las estructuras con racionalidad, austeridad y no duplicidad de funciones, mejora y modernización de la gestión pública.

[107] La GN en la Ley establece que es una fuerza policial de SP de carácter civil, militar y policial, sin embargo, el personal que la integra es de origen militar y su adiestramiento, disciplina y formación, con una profesionalización, valores y filosofía de carácter castrense.

-encargada de la investigación policial de delitos federales, el Centro Nacional de Inteligencia (CNI), creado en el año 2014 (inteligencia policial y la investigación de delitos federales que requieren un enfoque especializado)-. La Secretaría de la Defensa Nacional (SEDENA), la cual conserva su papel en la investigación de delitos federales que involucran a las fuerzas armadas y la Secretaría de Marina (SEMAR), que mantiene su función en la investigación de delitos federales que se cometen en el mar o en contra de instalaciones marítimas.

El Instituto Nacional de Estadística y Geografía (INEGI), modificó la etapa de captación de la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE), 2020.[108] Para el caso de las Estadísticas de Defunciones Registradas (EDR), del año 2020 al 2023,[109] ver Tabla 5.

Tabla 5. ***Total, de homicidios y tasa por cada 100,000 habitantes del 2020-2023***

	2020	2021	2022	2023
Enero a junio [110]				
Total de homicidios por cada 100,000 habitantes	17,123	16,972	15,561	15,082
Tasa de homicidios por cada 100,000 habitantes	13	13	12	12
Anual [111]				

[108]La encuesta se realizó del mes de julio a septiembre y no en marzo y abril, por esta circunstancia, los resultados relacionados con las experiencias de la población, relativos a delitos, se informa "pueden presentar algún grado de subestimación, tanto en víctimas como en incidencia delictiva, relacionada con los actos delictivos experimentados durante 2019". INEGI. (2020). Perspectiva en cifras COVID-19. Recuperado de: https://www.inegi.org.mx/investigacion/covid/

[109] Para el EDR, los datos provienen de los registros administrativos de defunciones accidentales y violentas que generan las EF y que se recopilan mensualmente de las fuentes informantes de las Oficialías del Registro Civil, los Servicios Médicos Forenses y las Agencias del Ministerio Público.

[110] INEGI. Homicidios en México. Enero a junio 2020. Recuperado de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/EstSociodemo/DefcioneshomicidioEn-Jun2020.pdf; Homicidio en México. Enero a junio de 2021. Recuperado de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/do/do2021.pdf Homicidios en México. Enero a junio 2022. Recuperado de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/do/do2021.pdf; Homicidios en México. Enero a diciembre de 2023. Recuperado de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2024/DH/DH2023_Ene-dic.pdf

[111] INEGI. Homicidios en México. Enero a Diciembre 2020. Recuperado de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/EstSociodemo/Defcioneshomicidio2020.pdf; Homicidios en México. Enero a Diciembre de 2021. Recuperado de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/DH/DH2021.pdf; Homicidios de México. Enero a Diciembre de 2022. Recuperado de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/DH/DH2022.pdf.

Total de homicidios por cada 100,000 habitantes	36,579	35,625	32,223	31,062
Tasa de homicidios por cada 100,000 habitantes	29	28	25	24

Fuente de la tabla: Elaboración propia con base en la información analizada.

Los homicidios en México se caracterizan por el uso de armas de fuego en aproximadamente el 70% de los casos, así como por una alta tasa de victimización en hombres jóvenes de entre 20 y 39 años. [112] La disminución observada en los últimos años a nivel nacional no corresponde con las tendencias a nivel subnacional. En el primer caso, la tendencia positiva contribuye a mejorar la percepción de seguridad ciudadana; sin embargo, también plantea interrogantes sobre sus causas, ya sea en relación con los avances en las estrategias de seguridad o con cambios en las dinámicas de la violencia.

La cifra de homicidios fue de 25,967 en 2012, de 36,685 en 2018 y de 31,062 en 2023. A partir de esta información, se observa que la cifra más alta corresponde a 2018, mientras que la de 2023, aunque más baja, sigue siendo superior a la de 2012. Esto sugiere que, aunque ha habido cierta mejora en la seguridad, la situación continúa siendo grave y no ha regresado a los niveles de 2012 (sin que esto signifique que sea la óptima). Con base en la información, no existe una correlación directa y lineal entre los casos de COVID-19 y la tasa de homicidios en las entidades federativas analizadas. Ante esta situación y considerando que las variables son complejas e influenciadas por una serie de factores, se aplicarán cuestionarios a servidores públicos en seguridad pública para profundizar en el análisis cualitativo y contextual, y conocer de cerca su percepción sobre las políticas implementadas durante y después de la pandemia. El análisis de los homicidios, junto con la consideración del contexto de la pandemia de COVID-19, permite comprender mejor este fenómeno y orientar futuras acciones, ver Tabla 6.

Tabla 6. ***Entidades Federativas con mayor presencia de casos de COVID-19 Homicidios por cada 100,000 habitantes***

Año	EF	CACC	EFMH	EF	CACC	EFMH	EF	CACC	EFMH
2023	Guanajuato	373,665	3,746	México	760,698	2,842	Baja California	180,069	2,642
2022	Guanajuato	373,660	4,329	México	130,502	3,257	Baja California	180,112	2,925
2021	Guanajuato	373,650	4,333	Baja California	180,093	3,248	México	130,500	3,119
2020	Guanajuato	373,637	5,370	Chihuahua	174,826	3,468	México	130,493	3,089

Homicidios de México. Enero a Diciembre de 2023. Recuperado de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2024/DH/DH2023_Ene-dic.pdf

[112] Seguridad Ciudadana. Recuperado de: https://seguridadviacivil.ibero.mx/2024/03/04/cinco-miradas-a-la-violencia-homicida-en-mexico/#:~:text=En%20Guanajuato%2C%20se%20cuadruplicaron%20los,para%20despu%C3%A9s%20volver%20a%20subir.

CACC. Casos acumulados confirmados de COVID-19
EFMH. Entidades Federativas con mayor número de homicidios
Fuente: Elaboración propia con base en el análisis Recuperado de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2024/DH/DH2023_Ene-dic.pdf;
https://datos.covid-19.conacyt.mx/#DOView

Si bien el resultado de la correlación puede plantear algunas dudas, cabe añadir que durante la pandemia se observó que las situaciones de violencia estuvieron marcadas por la naturaleza del aislamiento, lo que da como resultado, en primer lugar, un encarecimiento del costo de la vida para las familias, en particular el gasto en cuidados y alimentación, que implicó además un desvío de los alimentos saludables hacia los ultraprocesados, pero además se observó en la dinámica de las relaciones familiares un acentuamiento de la violencia contra las mujeres, de manera peculiar entre las que se encuentran en condición de separadas, viudas y divorciadas, en los ámbitos familiar y también comunitario. [113]

La Ley General de Salud (LGS), se reformó para impulsar intervenciones psicosociales individuales y comunitarias en materia de Salud Mental y Adicciones en estricto apego a los Derechos Humanos a fin de fortalecer estrategias de educación y comunicación para los programas de detectar, atender y prevenir el suicidio, y capacitar al personal de salud en estas materias.[114]

En términos del sector sanitario, se crea la Comisión Nacional de Salud Mental y Adicciones como un órgano administrativo desconcentrado de la Secretaría de Salud,[115]se actualiza el Compendio Nacional de Insumos para la Salud,[116] se actualiza el Libro de Nutriología del Compendio Nacional de

113 Encuesta Nacional de Salud y Nutrición 2021, y Encuesta Nacional sobre la Dinámica de las Relaciones en los Hogares ENDIREH 2021, ambos levantamientos considerados de escala nacional, posterior al censo de Población y Vivienda 2020.

[114] DOF, 16-05-2022

[115] DOF, 29-05-2023

[116] Las especialidades que están experimentando un aumento en las patologías relacionadas con los efectos post-COVID han sido etiquetadas como *'Long COVID'*, y presentan complicaciones en las áreas de Hematología, Enfermedades Infecciosas y Parasitarias, Gastroenterología, Cardiología, Reumatología y Traumatología, Neurología, Oncología, Dermatología, Endocrinología y Metabolismo. Para abordar estas complicaciones, se han considerado diversos medicamentos en el compendio de salud, tales como Isatuximab, Carboximaltosa Férrica, Ceftazidima-Avibactam, Diosmina-Hesperidina, Upadacitinib, Fampridina, Darolutamida, Risankizumab, Fibrinógeno Humano, Labetalol, Perindopril-Amlodipino-Indapamida, Perindopril-Amlodipino, Semaglutida, Dapagliflozina y Ponatinib. DOF, 30-04-2019 y 30-01-2023

Insumos para la Salud,[117] y el Libro de Auxiliares de Diagnóstico del Compendio Nacional de Insumos para la Salud, [118] se firma el Convenio de Colaboración en materia de transferencia de recursos presupuestarios federales con el carácter de subsidios para el desarrollo de acciones correspondientes al Programa Atención a la Salud y Medicamentos Gratuitos para la Población sin Seguridad Social Laboral para el ejercicio fiscal 2020, que celebran el Instituto de Salud para el Bienestar y el Instituto Mexicano del Seguro Social,[119] se publica el Acuerdo General 18/2020 del Pleno del Consejo de la Judicatura Federal, que reforma el similar 13/2020 relativo al esquema de trabajo y medidas de contingencia en los órganos jurisdiccionales por el fenómeno de salud pública derivado del virus COVID-19, [120]

Del análisis realizado a las políticas y estrategias enunciadas en el "Plan de gestión a largo plazo para el control de la COVID-19", del 8 de junio del año 2023, se destaca que no está alineado al "Plan estratégico de respuesta para la enfermedad por coronavirus 2019 (COVID-19), pautas para la planificación operativa de la preparación y la respuesta de los países", del 12 de febrero del año 2020 de la OMS, y el "Informe integral de COVID-19 en México", del 30 de diciembre del año 2023 no da respuesta a las pautas sugeridas por la organización mundial, así como tampoco señala estrategias en términos de coordinación para la SC.

Material y métodos

Se estableció en varios sentidos: I) La indagación de la literatura orientada a la teorización en torno a: COVID-19, GP, Marco Jurídico, SC, SI, SN y SP. II) Se filtraron todos los hallazgos por años y solo se enuncian en la investigación aquellos que correspondían al año de la publicación del 2020 en adelante, sin omitir para estudio, consulta y reflexión los teóricos clásicos y toda información referente a los enfoques sin importar su año, señalad en el apartado de fuentes bibliográficas. III) Se realizó la recopilación de la información y el análisis de esta a fin de estudiar y lograr de dar respuesta a la pregunta eje de la investigación. El tipo de investigación es empírica. El estudio es una investigación mixta de carácter cuantitativa y cualitativa. Se analizan los datos proporcionados por la encuesta ENVIPE del INEGI y los resultados de la encuesta "Desafíos y oportunidades para la seguridad en México post

[117] Para pacientes con enfermedades pulmonares, insuficiencia renal en diálisis, desnutrición (enfermedades correlacionadas significativas con COVID-19, tanto en términos de riesgo de infección como de gravedad de la enfermedad). DOF, 24-09-2021
[118] DOF, 18-01-2021
[119] DOF, 26-09-2020
[120] DOF, 16-07-2020

COVID-19", mismo que se aplicó en la plataforma virtual Google a servidores públicos de SP, ver Figura 1.[121]

Figura 1. ***Portada del cuestionario virtual "Desafíos y oportunidades para la seguridad en México post COVID-19"***

Fuente: Elaboración propia

Resultados

[121] El periodo de aplicación fue del 1ro. al 27 de octubre de 2024. Las interrogantes fueron abiertas, entre ellas: Email, EF, Año de nacimiento, Profesión, Organización en la que labora o laboró del año 2019 al 2024, Años de experiencia en Seguridad. ¿De qué manera cree que la pandemia de COVID-19 ha afectado las dinámicas de gobernanza en la protección ciudadana en su entidad o jurisdicción?, ¿Qué cambios específicos observó en las políticas públicas de protección ciudadana durante y después de la pandemia?, ¿Cómo se gestionaron las prioridades de seguridad durante la pandemia, y cuál fue su rol en este proceso?, Desde su perspectiva, ¿Cuáles fueron los principales desafíos en la implementación de políticas de seguridad pública durante la pandemia?, ¿Qué medidas se adoptaron para garantizar la protección ciudadana durante el confinamiento y las fases más críticas de la pandemia?, ¿Considera que los protocolos de seguridad cambiaron a largo plazo debido a la pandemia? Si es así, ¿cómo?, ¿Cuáles han sido los principales retos en la recuperación y reestructuración de las políticas de seguridad pública tras la pandemia?, ¿Cómo se han transformado las relaciones de colaboración interinstitucional (federal, estatal y municipal) en la gobernanza pública post-pandemia?, ¿Qué papel ha jugado la tecnología en la implementación de políticas de seguridad durante y después de la pandemia?, Desde su experiencia, ¿qué estrategias considera necesarias para fortalecer la construcción de paz y la seguridad pública en el contexto post-pandemia?, ¿Qué acciones considera prioritarias para mejorar la colaboración entre instituciones de seguridad y la ciudadanía para la construcción de paz?, ¿Existen nuevos enfoques o políticas que se deberían implementar para hacer frente a los desafíos de seguridad post-pandemia?, En su opinión, ¿cuáles son las lecciones más importantes que ha dejado la pandemia en términos de seguridad pública y protección ciudadana?, ¿Qué recomendaciones haría para que las políticas de seguridad sean más resilientes frente a futuras crisis globales?

A pesar de las diversas reformas al marco jurídico en materia de seguridad, la conceptualización de la SC y la construcción de paz no han sido consideradas, pese al pronunciamiento de las Naciones Unidas a los países miembros. Incluso el Índice de Estado de Derecho en México 2020-2021 señala que México tiene un Estado de Derecho débil. [122]

La conceptualización de la SN, SI, SP y SC en el sistema jurídico mexicano no está claramente definida, atendida ni expresada, lo cual genera descoordinación, ineficiencia y desinformación, afectando negativamente la capacidad de gobernanza eficaz en la AP.

Con respecto al análisis a las respuestas recibidas de la encuesta aplicada "Desafíos y Oportunidades para la Seguridad en México, Post COVID-19", el año de nacimiento de las personas participantes oscila entre el año 1947 y 1996. Las EF en las que laboran los servidores públicos que contestaron son Ciudad de México, Chiapas Michoacán de Ocampo, México, Morelos, Oaxaca, Puebla, Tlaxcala, Veracruz de Ignacio de la llave. Las instituciones públicas que representan son la Secretaría de Marina (SEMAR), el Centro Médico Naval (CEMENAV), la Secretaría de Seguridad y Protección Ciudadana (SSPC), la GN o Secretaría de SP (estatal), cuentan con un promedio de 11.40 años de experiencia y representan una amplia diversidad profesional, entre abogados, especialistas en sistemas informáticos, aviación, enfermería, policía, militar, administración y politólogos.

Del análisis de las respuestas proporcionadas se puede concluir que los participantes, en general, plantean la importancia de la prevención y la preparación para eventos pandémicos. Se destaca la necesidad de estar preparados para futuras crisis, elaborar planes de emergencia detallados y la realización de simulacros, se enfatiza la importancia de contar con sistemas de salud robustos y bien equipados, además, de permanente educación de la población sobre temas de salud y seguridad, crucial para fomentar los comportamientos preventivos. La necesidad de colaboración y coordinación entre diferentes niveles de gobierno, instituciones y sectores de la sociedad con comunicación clara y transparente, fundamental para generar confianza y facilitar la coordinación. Se reconoce que la seguridad es un problema complejo que requiere un enfoque integral que aborde las causas subyacentes, el uso de herramientas digitales y la tecnología en la gestión de crisis, como la vigilancia epidemiológica y la importancia de proteger los sistemas digitales ante posibles ciberataques. Se reconoce que las pandemias y la inseguridad afectan de manera desproporcionada a los grupos más vulnerables. Se destaca la necesidad de garantizar el acceso equitativo a servicios de salud y otros servicios esenciales para garantizar la salud mental, el bienestar integral especialmente en tiempos de crisis. En resumen, se plantea la necesidad de un cambio de paradigma en la

. [122] La puntuación de México es de 0.5. La puntuación de 1.0 refleja un Estado de Derecho robusto

forma en que abordamos la seguridad. De reactivo a proactivo, de lo individual a lo colectivo, la seguridad es un asunto que nos concierne a todos y requiere de un esfuerzo colectivo, además, las políticas de seguridad deben tener una visión a largo plazo y abordar las causas profundas de los problemas.[123]

Conclusiones

La pandemia ha exacerbado las desigualdades existentes y ha revelado debilidades en la capacidad del Estado mexicano para garantizar la seguridad y el bienestar de sus ciudadanos, lo que generó un vacío de poder que ha sido aprovechado por el crimen organizado, intensificando la violencia y la inseguridad.

Las respuestas emitidas en el cuestionario reflejan una creciente conciencia sobre la importancia de la seguridad y la necesidad de construir sociedades más resilientes, reformas y políticas en torno al enfoque de salud integral en la seguridad fueron para el fortalecimiento de la GN, la implementación de programas de prevención, el uso de tecnología, la protección de grupos vulnerables y la colaboración interinstitucional.

Las propuestas en términos de transformación de la GP en Protección y SC Post COVID-19 son:

I. Atención sanitaria comunitaria para la SC en colaboración con la Policía, la GN y las autoridades locales.
II. Brigadas que realicen tareas de monitoreo de salud en la comunidad, brindar primeros auxilios, y detectar posibles situaciones de riesgo que puedan escalar en problemas de SC.
III. Capacitación, certificación y adiestramiento a los servidores públicos "elementos" de la SP y SC.
IV. Estandarización de protocolos de seguridad en los tres niveles de gobierno en las instituciones de SC.
V. Fortalecimiento de la Seguridad con Enfoque Intercultural y Derechos Humanos.
VI. Políticas públicas diferenciadas.
VII. Programa de Comisiones Ciudadanas de Supervisión Evaluación y Retroalimentación de las políticas de seguridad, integrado por la ciudadanía en la toma de decisiones y en el monitoreo de la implementación de estas políticas.
VIII. Programa de Reinserción Económica y Social para Comunidades Afectadas con acceso a créditos para el emprendimiento.

[123] Encuesta "Desafíos y Oportunidades para la Seguridad en México, Post COVID-19" https://docs.google.com/forms/d/1WOTCyOQJ2Xre6fNKDYONaCJsNpiaSIQthmDag6V8OQw/edit?ts=67146b7f#responses

IX. Programa de Servicio Psicosocial Gratuito incluida la asesoría legal, programas de soporte para jóvenes y familias, y talleres de manejo de estrés y trauma, reduciendo así el riesgo de desintegración social y problemas de seguridad.

X. Programas de prevención de crisis que articule la participación de servicios de salud, seguridad y asistencia social, en comunidades sin importar la concentración poblacional ni el alto o muy alto rezago.

XI. Red de GP que integre las políticas de seguridad y salud pública, coordinada por la SSPC, para responder a crisis emergentes -Red Nacional de Coordinación Interinstitucional para la Respuesta a Crisis Sanitarias, además de la Red de Comunicación y Respuesta que permita la colaboración rápida y fluida entre el Ministerio Público, Guardia Nacional, corporaciones locales de seguridad y el sistema de salud-.

XII. Seguridad en Protocolos de Emergencia Sanitaria.

XIII. Sistema de Monitoreo de Seguridad y Salud Pública.

XIV. Transparencia y la rendición de cuentas en el uso de los Fondos de Seguridad.

XV. Uso de los Mecanismos de Coordinación Multinivel y Transparencia.

El estudio no solo invita a reflexionar sobre las deficiencias actuales en la implementación de políticas, sino que también propone líneas de acción concretas para mejorar la formación y comprensión de los servidores públicos. De esta forma, se busca contribuir a la construcción de un marco de seguridad más robusto, que no solo combata la criminalidad, sino que también promueva la paz y la cohesión social en un escenario post-pandemia.

Referencias bibliográficas

Altavilla, Cristian. (2015). *El neo institucionalismo: su aporte a las ciencias sociales y al estudio interdisciplinario del derecho público.* Revista de la facultad, Vol. VI N° 2 Nueva Serie II (2015) 147-168. Recuperado de: file:///C:/Users/DELL/Downloads/23721-Texto%20del%20art%C3%ADculo-68363-1-10-20190315.pdf

Ackerman-Rose, Palifka-Susan, Bonnie J. (2019). Corrupción y gobierno. Causas, consecuencias y reformas. Madrid. Marcial Pons. Segunda edición. Traducción: Francisca Pou Giménez. Recuperado de: CorrupCión y gobierno

Amnistía Internacional. (2022). Américas: Intentos de militarización de la seguridad pública en la región son una amenaza para los derechos humanos. Recuperado de: https://www.amnesty.org/es/latest/news/2022/11/americas-intentos-de-militarizacion-de-la-seguridad-publica-en-la-region-son-una-amenaza-para-los-derechos-humanos/

Auditoria Superior de la Federación. (2016). Informe del estudio general sobre la situación que guarda la gobernanza en el sector público federal. México. Núm. 1640. Cámara de Diputados.

Bigo Didier. (2020). ¿La mundialización de la (in)seguridad? Reflexiones sobre el campo de profesionales de la gestión de las incertidumbres y analítica de la transnacionalización de los procesos de (in)securización. Delito y Sociedad. Revista de ciencias Sociales 49(1) e0002, pp. 5–50. DOI:https://doi.org/10.14409/dys.2020.49.e0002. Recuperado de: https://www.academia.edu/95280573/_La_mundializaci%C3%B3n_de_la_in_seguridad_Reflexiones_sobre_el_campo_de_profesionales_de_la_gesti%C3%B3n_de_las_incertidumbres_y_anal%C3%ADtica_de_la_transnacionalizaci%C3%B3n_de_los_procesos_de_in_securizaci%C3%B3n

Bobbio, Norberto. (2005). Teoría general de la política. Edición de Michelangelo Bovero. Traducción de Antonio de Caboy y Gerardo Pisarello. Sere Derecho. Colección Estructuras y Procesos. Ed. Trotta. Madrid.

CEPAL. *Acerca de la Gestión Pública*. Recuperado de: Acerca de Gestión pública | Comisión Económica para América Latina y el Caribe

Chica Vélez, Sergio Alberto y Salazar Ortiz, Cristian Andrés. (2016). Nueva y pos nueva gestión pública ¿Continuidad o ruptura de las doctrinas de reforma a partir de 1990? Administración & Desarrollo. 2016:46 (1):100-125. Recuperado de: https://dialnet.unirioja.es/descarga/articulo/6403495.pdf

Chica Vélez, Sergio Alberto. Salazar Cristian Andrés. (2016). *Nueva y pos-nueva gestión pública. ¿Continuidad o ruptura de las doctrinas de reforma a partir de 1990?* Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6403495

Comisión Interamericana de Derechos Humanos. (2009) Informe sobre Seguridad Ciudadana y Derechos Humanos Recuperada de: https://www.oas.org/es/cidh/docs/pdfs/seguridad%20ciudadana%202009%20esp.pdf

Deiss, Joseph (2011). Presidente del sexagésimo quinto período de sesiones de la Asamblea General de las Naciones Unidas. Gobernanza, Seminario regional: Las Naciones Unidas en la gobernanza global. Comisión económica para América Latina y el Caribe. Recuperado de: https://www.cepal.org/es/comunicados/instan-fortalecer-rol-la-onu-la-gobernanza-global

Espinosa, Luciano. (2011). Spinoza. Biblioteca de Grandes Pensadores. Gredos. Madrid Recuperado de: https://ia802604.us.archive.org/19/items/nietzsche-i-completo_202304/Spinoza-_Biblioteca-Grandes-Pensadores_-Baruch-Spinoza.pdf

Estudios de la OCDE sobre Gobernanza Pública. (__) España, de la reforma administrativa a la mejora continua. Resumen ejecutivo. España. Recuperado de: https://www.oecd.org/gov/PGR%20SPain%20Resumen%20Ejecutivo.pdf

Franco Coppola. Declaración del Nuncio apostólico del Papa Francisco en México 15 de septiembre de 2016. México, cuenta con el Programa Nacional de Combate a la Corrupción y a la Impunidad y de Mejora de la Gestión Pública (PNCCIMGP) 2019-2024. DOF, 30-08-2019.

Fruhling, Hugo. (2018). Diferencia entre gobernanza y gobernabilidad. Recuperado de: https://www.youtube.com/watch?v=A4GvyXBCjKA

García Villarreal, Jacobo Pastor. (2010). Prácticas y Políticas Exitosas para Promover la Mejora Regulatoria y el Emprendimiento a Nivel Subnacional. Documentos de Trabajo de la OCDE sobre Gobernanza Pública, 2010/18, Publicación de la

OCDE. Recuperado de: Documentos de Trabajo de la OCDE sobre Gobernanza Pública No. 18 Prácticas y Políticas Exitosas para Promover la Mejora Regulatoria

Gaceta Parlamentario (2024). Iniciativa con proyecto de decreto, por el que se reforman y adicionan diversos artículos de la Constitución Política de los Estados Unidos Mexicanos, en materia de Guardia Nacional", Gaceta Parlamentaria, año XXVII, núm. 6457, 5 de febrero de 2024, disponible en: https://bit.ly/PlanC_GN

González Martín, Miguel. (2007) ¿Ser como Dinamarca? Una revisión de los debates sobre gobernanza y ayuda al desarrollo. Cuadernos de trabajo. Instituto de Estudios sobre el Desarrollo y la Cooperación Internacional (HEGOA). Revista de Fomento Social, No. 241. Volumen, 1, 2006, pp 25-55 ETEA. España. Ed. Lankopi.

Hobbes, Thomas. (). Leviatán. Freeditorial. Recuperado de: https://freeditorial.com/es/books/leviatan/related-books

Humanitarias y de salud, la igualdad de género, la gobernanza, la producción de alimentos y mucho más. Recuperado de: https://www.onu.org.mx/la-onu/

Human Rights Watch. (2022). México: la militarización de la seguridad pública amenaza los derechos humanos. Recuperado de: https://www.hrw.org/es/news/2022/08/26/mexico-la-militarizacion-de-la-seguridad-publica-amenaza-los-derechos-humanos

Instituto Nacional de Estadística y Geografía. (2020). Censo de Población y Vivienda 2020. Recuperada de: https://www.inegi.org.mx/programas/ccpv/2020/ y, https://www.conapo.gob.mx/

López Ayllón, Sergio. Orozco Henríquez, José de Jesús. Salazar Ugarte, Pedro Valadés, Diego. Coordinadores. (2024). Análisis técnico de las 20 iniciativas de reformas constitucionales y legales presentadas por el presidente de la República. Recuperado de: https://biblio.juridicas.unam.mx/bjv/detalle-libro/7483-analisis-tecnico-de-las-20-iniciativas-de-reformas-constitucionales-y-legales-presentadas-por-el-presidente-de-la-republica-febrero-5-2024

López Robles, Adalberto. (2023). El declive de la confianza institucional en México: ¿Desempeño político o cultura?. Revista mexicana de opinión pública versión On-line ISSN 2448-4911versión impresa ISSN 1870-7300. Rev. mex. opinión pública no.34 Ciudad de México ene./jun. 2023 Epub 05-Feb-2024. https://doi.org/10.22201/fcpys.24484911e.2023.34.84413. http://orcid.org/0000-0002-7286-265X

Martha L. Bayón Sosa (2018). *El neo institucionalismo y el Banco Mundial: gobernabilidad y gobernanza*. Economía y Desarrollo. vol.160 no.2 La Habana jul.-dic. 2018. Departamento de Desarrollo Económico, facultad de Economía, Universidad de La Habana, Cuba. Recuperado de: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0252-85842018000200003

Olea Peñaloza, Jorge. (2020). Governance as a contradiction: reflections on the territory in the configuration of environmental governance. Investigaciones Geográficas, 60, 4-17. https://doi.org/10.5354/0719-5370.2020.57251

ONU. Agenda para el Desarrollo Sostenible 2030. Recuperado de: Transforming our world: the 2030 Agenda for Sustainable Development | Department of Economic and Social Affuerzas armadasirs

ONU. Gobernanza efectiva y Democracia. (2023). Recuperado de: https://www.undp.org/es/mexico/nuestro-enfoque/gobernanza-efectiva-y-democracia

Pazinato, Eduardo. (2018). *Líderes para la gestión en seguridad ciudadana y justicia*. 2. Gobernanza y gestión. Centro de seguridad ciudadana. facultad de Derecho de San María, Brasil. Banco Interamericano de Desarrollo. Consorcio académico de la Universidad de Chile. John Jay College of Criminal Justice y facultad de Direito de Santa María.

Pérez Rigoberto. (2019). *Administración pública y gobernanza en México. Análisis del cambio institucional en la agenda de BG*. México. Books-©ECORFN. Recuperado de:https://www.ecorfn.org/libros/Administraci%C3%B3n%20p%C3%BAblica%20y%20gobernanza%20en%20M%C3%A9xico.pdf

Programa de las Naciones Unidas. (2013). Sinopsis: Seguridad Ciudadana. Prevención de Crisis y Recuperado de: https://www.undp.org/sites/g/files/zskgke326/files/publications/08022013_citizen_security_issue_brief%20(spanish).pdf

Rivero-Rodríguez, María Guadalupe de Jesús. (2024). La gobernanza pública en la construcción de paz y la protección ciudadana, 2012-2021. México. INAP.

Rodríguez, Bucio. Luis. (2016). Retos enfrentados por las fuerzas armadas mexicanas durante su participación en la estrategia de combate al narcotráfico del Presidente Felipe Calderón Hinojosa. Revista Internacional de Ciencias Sociales y Humanidades, SOCIOTAM, vol. XXVI, núm. 2, julio-diciembre, 2016, pp. 205-227. Universidad Autónoma de Tamaulipas. Ciudad Victoria, México

Sorj, Bernardo. (2005). Seguridad, seguridad humana y América Latina. Sur, Rev. int. direitos human. 2 (3) • Dic 2005 • https://doi.org/10.1590/S1806-64452005000200004. Recuperado de: https://www.scielo.br/j/sur/a/5RncFCTbxqzmKW85zzsQbgM/?lang=es

Vargas Villamizar, Carlos Enrique (2022). Seguridad multidimensional: entre la ambigüedad conceptual y la necesidad pragmática. rev.relac.int.estrateg.segur. vol.17 no.2 Bogotá July/Dec. 2022 Epub Dec 31, 2022. https://doi.org/10.18359/ries.6140 Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-30632022000200103

Villavicencio Morales, Andrea. (2015). *Tesis La Carta Democrática Interamericana: los supuestos que afectan la institucionalidad democrática y sus mecanismos de defensa*. Pontificia Universidad Católica del Perú. Facultad de Derecho. Asesor. Dr. Walter Albán Peralta. Recuperado de: los supuestos que afectan la institucionalidad democrática y sus mecanismos de defensa.

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

La Inteligencia para la Seguridad Nacional como Elemento de Tutela de los Derechos Humanos

Alejandro Toledo Utrera*

Resumen: Se hace un breve recorrido por las diversas etapas de los derechos humanos y cómo estos van transformando el entorno hasta llegar a cruzarse con los anhelos que busca la seguridad nacional de proteger al país mediante el logro de los objetivos nacionales, y todos aquellos derechos que tutela el Estado para el mantenimiento de la gobernanza y la paz, y cómo los productos de la inteligencia logran intersecarse para salvaguardar el más alto de los derechos como es hablar de la vida, la libertad, seguridad de los datos, la privacidad, el medio ambiente, entre tantos otros que permiten la seguridad física de las personas y proteger dignidad humana.

Palabras Clave: Derechos Humanos, Inteligencia, Parámetro de Regularidad Constitucional, Seguridad Nacional.

Abstract: A brief tour is made of the various stages of human rights and how they transform the environment until they come to intersect with the desires that national security seeks to protect the country, and all those rights that the State protects for the maintenance of governance and peace, and how the products of intelligence manage to intersect to safeguard the highest of rights such as life, liberty, data security, privacy, the environment among many others that allow human dignity.

Keywords: Human Rights, Intelligence, Constitutional Regularity Parameter, National Security.

Introducción

* Economista, Maestro y Doctor en Administración Pública con Mención Honorifica, cuenta con el Postdoctorado Iberoamericano en Nuevos Retos de Gobernanza Pública por la Universidad de Salamanca, *Senior Executive National and International Security, Harvard University, Executive Certificate in Public Policy, Harvard Kennedy School, The Threat of Nuclear Terrorism Stanford University, Espionage, Intelligence and National Security University of Oxford,* es Especialista en Inteligencia y Seguridad Nacional por el INAP, A.C. Ha sido Catedrático de la Facultad de Derecho de la UNAM, es director de Tesis Doctoral en el INAP, A.C. Miembro Asociado del INAP, A.C. Asociado del Centro Olof Palme México y Miembro del *Harvard Club of México*.

En los albores de que las civilizaciones empezaron a dominar el entorno, se organizaron para la caza, recolección, así como la defensa de sus territorios y sobre todo la integridad física ante riesgos y amenazas que, conforme evolucionaban se enfrentaron al conflicto, no obstante, mediante la observación, sin saberlo empezaron a imaginar el desarrollo y bienestar utilizando la herramienta de la Inteligencia para la supervivencia del ser humano en la tierra.

Hemos escuchado hasta la saciedad que la Inteligencia es la segunda profesión más antigua del mundo. La información resulta ser un insumo vital para la toma de decisiones, sin embargo, la asimetría de ésta y su fuerte vinculación al fenómeno de la intención de hacer daño, genera vulnerabilidades debido amenazas y riesgos que enfrenta la humanidad en el siglo XXI. El objetivo es plantear la relación entre la Inteligencia en seguridad nacional y la protección de los derechos humanos.

Al analizar en forma hermenéutica el grabado del libro el *Leviatan* de Thomas Hobbes, es muy interesante observar que el Estado tiene la espada en señal de que cuenta con el monopolio de la fuerza pública y el poder judicial, lo mismo sucede en nuestros tiempos donde el Estado ejerce la recolección de piezas de inteligencia para la toma de decisiones que permiten generar la gobernabilidad, la seguridad física de las personas como objetivos nacionales definiendo la importancia de la seguridad nacional en un mundo contemporáneo.

En el contexto actual, la geopolítica mueve diversas variables en lo social, político y económico evidenciando un área de oportunidad, asegurar los derechos humanos de las personas dentro de la una visión de la inteligencia para la seguridad nacional, basados en la recolección, análisis, diseminación y explotación de la información, buscando con un análisis de pensamiento futuro que la información como producto de inteligencia sea con grado de certeza.

Por lo que, para analizar un tema trascendente dentro de la seguridad nacional que permita tutelar los derechos humanos en el mundo contemporáneo, resulta preciso formularnos la siguiente Pregunta de Investigación:

¿Cómo puede la Inteligencia para la seguridad nacional contribuir a la tutela de los derechos humanos?

Desde una visión holística la Inteligencia para la seguridad nacional, no sólo debe enfocarse en proteger al Estado, sino también en amparar los derechos humanos, mismos que como características, son universales, indivisibles, progresivos, inalienables, interdependientes; por lo que la preocupación es alta al asegurar cada derecho de las personas y, parafraseando a Woody Allen sobre la importancia del futuro, ya que es donde transcurrirá el resto de nuestras

vidas, las personas debemos tener todos los derechos humanos garantizados, bajo el principio de progresividad.

Antecedentes

Para dar respuesta, realizaremos un breve recorrido a los pasajes históricos que ponen en contexto la necesidad de que los derechos humanos sean salvaguardados en todo momento y todo lugar para preservar la dignidad humana.

La Paz de Westfalia (Alemania), termina con una guerra de 30 años, siendo el parteaguas para el orden entre las naciones y es donde la seguridad nacional es entendida como aquella que su principal objetivo de velar por los intereses nacionales, la firma de dicha paz se integró de dos Tratados el *Münster* y el *Onsnanbrük* referidos a la paz; la gran aportación es que se pone en el escenario el concepto de la soberanía reconocida internacionalmente, y con ello, nace a la vida la formalidad de Estado moderno soberano, así como una vía diplomática formal redefiniendo el mapa europeo.

En lo sucesivo, será un instrumento de construcción de orden y de paz entre naciones dando fin a la etapa feudal, y de tal suerte el contar con los servicios de inteligencia permite mantener la integridad de los territorios de cada nación; de hecho Armand Jean du Plessis mejor conocido como el Cardenal Richelieu generaba puentes de plata con su trabajo como Secretario de Estado con piezas de inteligencia para el mantenimiento de paz, lo cual guarda vigencia en el Estado contemporáneo donde la inteligencia para la seguridad nacional y la diplomacia en el entorno geopolítico lo hacen una herramienta imprescindible, como en su momento el Doctor Henry Kissinger logra acabar con la guerra de Vietnam y el acercamiento de Estados unidos con China buscando un balance de paz bajo una visión realista.

El Estado tiene la prioridad de mantener la integridad del territorio, defender la soberanía y que se mantenga intacto el orden constitucional a efecto de que la división de poderes del Estado permita la gobernabilidad y que los riesgos y amenazas sean mitigados, casi utilizando la estrategia del Arte de la Guerra de Sun Tzu, al operacionalizar todas las inteligencias que generen estabilidad en el Estado.

Bajo esta premisa, resulta muy importante para Hobbes utilizar todas las herramientas disponibles, a fin de crear una cultura de inteligencia para la seguridad nacional bajo su pensamiento de miedo y seguridad, que permita la prevención y la anticipación de riesgos, teniendo como objetivo único de presente y futuro, asegurar la permanencia del Estado con todas las características administrativas y con su arquitectura jurídica. En este punto, John Locke comenta que ningún gobierno absoluto es legítimo, pero las coincidencias del pensamiento político entre Thomas Hobbes y John Locke, en que la libertad individual es un derecho de los habitantes y que el Estado

tiene que asegurar la integridad física de los ciudadanos y el territorio, mediante la inteligencia y la seguridad nacional en su aspecto de seguridad colectiva.

> "…con más frecuencia se piensa en la seguridad colectiva como un concepto regional y global representado por instituciones internacionales como la Sociedad de las Naciones y las Naciones Unidas. A menudo, estos acuerdos se sustentan en conceptos de derecho internacional y de ayuda y gobernanza internacionales. Su característica distintiva es su carácter híbrido entre la acción colectiva a nivel internacional y la aceptación de que los Estados-nación son los responsables últimos de su propia seguridad".[124]

Con la revolución francesa surgen esos valores nacionales, que buscan visibilizar los derechos de las personas, enmarcados bajo el lema revolucionario: *Liberté, Égalité, Fraternité*, y derivan en la Declaración de los Derechos del Hombre y del Ciudadano, promulgada en 1789, donde se instituyeron los principios fundamentales como la igualdad ante las leyes, la expresión como una libertad adquirida, tener la certeza del derecho a la propiedad privada y a profesar cualquier religión, llevando las expresiones pensamientos y derechos plasmados en dicha declaración como insumo base para la arquitectura jurídica de las constituciones democráticas y sobre todo, de los tratados internacionales relacionados con derechos humanos.

> "La Declaración de los Derechos del Hombre y del Ciudadano, promulgada en 1789, estableció principios fundamentales como la igualdad ante la ley, la libertad de expresión y de religión, y el derecho a la propiedad. Este documento sirvió de base para el desarrollo posterior de las constituciones democráticas y los tratados internacionales de derechos humanos"[125]

Con ello se inicia una etapa donde el Estado va a salvaguardar o tutelar los hoy conocidos como derechos humanos que se fortalecen bajo el Parámetro de Regularidad Constitucional.

Inteligencia en el contexto de la seguridad nacional

El Ex Director Nacional de Inteligencia de los Estados Unidos James Clapper nos describe cómo los tomadores de decisiones requieren información con grado de certeza para mitigar las amenazas y riesgos conceptualizando a la

---

[124] *Holmes, K. R. (2015). "What is National Security?" The Heritage Foundation. Obtenido de https://www.heritage.org/military-strength-essays/2015-essays/what-national-security,: Index of U.S. Military Strength. U.S.A.: The Heritage Foundation, 17-26, disponible en: https://www.heritage.org/sites/default/files/201910/2015_IndexOfUSMilitaryStrength_What%20Is%20National%20Security*

[125] Alponte J.M. (2017) Lecturas filosóficas (la lucha por los derechos humanos y el Estado de derecho), Instituto Nacional de Administración Pública, A.C. México. P. 95

inteligencia como: "El objetivo de la inteligencia es reducir la incertidumbre para los tomadores de decisiones, ya sea que estén en la Casa Blanca o en una trinchera"[126] por lo que, es más vigente que nunca utilizar el ciclo de inteligencia para generar productos para la toma de decisiones en búsqueda de la seguridad nacional y tutelar el derecho a la vida de los ciudadanos.

Una de las herramientas más poderosas para seguir alimentado todas la decisiones estratégicas, tácticas y operativas como lo pone de manifiesto el Centro Nacional de Inteligencia del Gobierno de México es el Ciclo de Inteligencia, definido como el "Proceso que orienta las acciones de recolección y procesamiento de información con el propósito de integrarlas en productos de inteligencia para los procesos de toma de decisiones."[127]

> "Entre la defensa de la seguridad nacional y el respeto a los derechos humanos existe una relación estrecha, pero no necesariamente positiva. Es frecuente que se violen los derechos de los ciudadanos invocando la seguridad de la nación."[128]

Dentro de las aportaciones de Sergio Aguayo, nos expone que por las razones de Estado se ejercían acciones que violentaban y el derecho de las personas más allá de la legitimidad que impera en pro de la seguridad nacional, pero, si bien es cierto, existían una fase nebulosa de las actuaciones que se ejercía a través de la Dirección Federal de Seguridad y que poco se sabe porque carecía de una rendición de cuentas, pero al llegar a los años 90´s se inician una serie de agrupaciones de la sociedad mejor conocidas como las Organizaciones No Gubernamentales (ONG), que sin lugar a dudas llegan a refrescar el ambiente no sólo en la participación sino que es esas voces piden un gobierno más eficiente y sobre todo transparente.

Aunque si bien, la transformación del Centro de Investigación y Seguridad Nacional órgano desconcentrado de la Secretaría de Gobernación pasa a la Secretaría de Seguridad y Protección Ciudadana mediante la creación del Centro Nacional de Inteligencia a partir del 1 de diciembre de 2018, con el propósito de que la inteligencia no tenga tintes políticos o afines a un gobierno, sino que sirva para generar productos que beneficien a la comunidad.

---

[126] ATHENALAB. (2 de Septiembre de 2020). JAMES R. CLAPPER, ex director de Inteligencia de EE.UU.: "Hoy estamos más seguros que antes del 11-S, pero no necesariamente asegurados". Recuperado el 16 de octubre de 2024, de https://athenalab.org/james-r-clapper-ex-director-de-inteligencia-de-ee-uu-hoy-estamos-mas-seguros-que-antes-del-11-s-pero-no-necesariamente-asegurados-2/: https://athenalab.org/

[127] CNI (18 de febrero de 2020). *¿Qué es la Inteligencia?* Obtenido de https://www.gob.mx/cni/documentos/que-es-la-inteligencia?idiom=es.: Gobierno de México. Fecha de Consulta 15 de octubre de 2024.

[128] Aguayo S. (1997): Seguridad nacional y derechos humanos en México. In: Revista Mexicana de Ciencias Políticas y Sociales, XLI (170), 1997

Pero siempre, los servicios de inteligencia del gobierno estuvieron en duda por su constante violación a los derechos humanos y al cambio del régimen con la llegada del Presidente Vicente Fox, se trató de fortalecer mediante una arquitectura normativa las operaciones y el papel de la inteligencia para la seguridad nacional, sin que aún se pudiera hablar de una cultura de inteligencia que permeara en las instituciones que generan productos de inteligencia, no sólo la esfera pública sino también que el sector privado y académico realizara esfuerzos para crearla.

Un hecho que inicia a generar una cultura de inteligencia ha sido puesto al servicio de la sociedad; encontramos el primer y gran esfuerzo por parte del Instituto Nacional de Administración Pública, posteriormente del Instituto Tecnológico Autónomo de México y la Universidad de las Américas, todas estas instituciones académicas han sido faro en este proceso de generar conocimiento en el área de inteligencia y seguridad nacional, con lo cual, actualmente existe una oferta que permite acceder a este conocimiento de grado científico sin formar parte de las fuerzas armadas o los servicios de inteligencia, que genera comunidad y contribuye al derecho humano a la educación, el cual para el caso de México está plasmado en el artículo 3° de la Constitución Política de los Estados Unidos Mexicanos.

Cuando se creó la Ley de Seguridad Nacional, se tenía como fin último conceptualizar a la seguridad nacional como un bien invaluable de nuestra sociedad entendiendo por ella la condición permanente de paz, libertad y justicia social que, dentro la arquitectura normativa jurídica, procuran pueblo y gobierno *Lato Sensu*, así como la consecución de los objetivos nacionales.

Dentro de la Ley de Seguridad Nacional se toca lo relativo a las garantías individuales y derechos humanos, lo cual pone en relieve que la coordinación debe privilegiar el respeto y tutela de los derechos humanos antes denominadas garantías individuales, lo cual es señalado en el párrafo tercero del artículo 25 de la citada ley.

> (…)
> "En materia de procuración de justicia, el Centro será auxiliar del Ministerio Público de la Federación y prestará cooperación, apoyo técnico y tecnológico, intercambio de información sobre delincuencia organizada y las demás acciones que se acuerden en el Consejo, observando en todo momento respeto a las formalidades legales, las garantías individuales y los derechos humanos."[129]

Es de alta relevancia que la generación de productos de inteligencia, siempre se tutele el respeto el principio de legalidad, lo cual permite que la dignidad de las personas no sea vulnerada y con ello en comunidad mantener el orden y la paz.

[129] Ley de Seguridad Nacional (2005) Diario Oficial de la Federación Tomo DCXVI, N° 21

> "Artículo 31.- Al ejercer atribuciones propias de la producción de inteligencia, las instancias gozarán de autonomía técnica y podrán hacer uso de cualquier método de recolección de información, sin afectar en ningún caso las garantías individuales ni los derechos humanos."[130]

Aunque de manera general, la Ley de Seguridad Nacional encuadra algunos supuestos descritos en párrafos anteriores sobre la tutela de los derechos humanos, será uno de los grandes retos, es realizar una reforma constitucional que vaya acorde con el derecho contemporáneo, y para ello, es imperante para el país, una reforma en esta materia de gran calado en materia de derechos humanos.

La Convención Americana sobre Derechos Humanos o Pacto de San José fue firmada en 1969, cuando se desarrolló la Conferencia Especializada sobre Derechos Humanos, cuyo propósito es la protección de los derechos humanos en América, México al ratificarlo en 1988 acepta su jurisdicción y sus efectos vinculantes, obligándose a garantizar y respetar los derechos delineados en la Convención.

Las sentencias de la Corte Interamericana de los Derechos Humanos han atendido casos en los que los Estados han ejercido indebidamente la seguridad nacional por encima de los derechos humanos, generando violaciones graves a la vida, privacidad, la libertad de expresión, el debido proceso, el medio ambiente y otros derechos esenciales que se encuentran delineados en la Convención Americana sobre Derechos Humanos.

En el caso de México al suscribir el Pacto de San José, y la Convención de Belém do Pará relativo a la desaparición forzada, se generó un cambio de estructura jurídica de nuestra Carta Magna que creó la gran reforma de los derechos humanos de 2011, que deviene del caso líder conocido por la sentencia contra el Estado Mexicano por la desaparición forzada de Rosendo Radilla Pacheco, en el año de 1974, donde fue retenido en un retén militar en el Estado de Guerrero y esa fue la última vez que se le vio con vida.

La Corte Interamericana de los Derechos Humanos, sentenció al Estado mexicano con la Sentencia Radilla Pacheco *Vs* México, para que reformara disposiciones internas y se modificara el Código de Justicia Militar en su artículo 57 fracción II, donde se destaca que un militar al agraviar a un persona civil tendrá que someterse a la jurisdicción civil, con ello salvaguardando el derecho humano al acceso a la justicia como lo señala el artículo 8 "Garantías Judiciales" de la Convención Americana de los Derechos Humanos; por ello, la Corte dejó plasmado en la sentencia en el punto 2.2. Actuaciones de la jurisdicción militar en su inciso a) Jurisdicción competente, que:

---

[130] Ibidem P. 5

> "En consecuencia, tomando en cuenta la jurisprudencia constante de este Tribunal, debe concluirse que, si los actos delictivos cometidos por una persona que ostente la calidad de militar en activo no afectan los bienes jurídicos de la esfera castrense, dicha persona debe ser siempre juzgada por tribunales ordinarios. En este sentido, frente a situaciones que vulneren derechos humanos de civiles bajo ninguna circunstancia puede operar la jurisdicción militar."[131]

En el Caso Miembros de la Corporación Colectiva de Abogados "José Alvear Restrepo" *Vs* Colombia, la Corte Interamericana de los Derechos Humanos en su sentencia del 18 de octubre de 2023, condenó al Estado Colombiano por realizar vigilancia ilegal y persecución por varios años, por el Departamento Administrativo de Seguridad (DAS) realizando labores de inteligencia como la recolección de datos, intervenciones telefónicas fotografías y obtención de datos personales que pusieron es una situación de vulnerabilidad al Colectivo de Abogados "José Alvear Restrepo" (CAJAR) por parte de los organismos de inteligencia del Estado.

Lo cual, en razón de las declaraciones y publicaciones de los funcionarios del gobierno de Colombia sobre el CAJAR y su vinculación a las guerrillas, llevó a la estigmatización y a sufrir amenazas y daños en su labor en defensa de los derechos humanos, toda vez, la inteligencia que se realizaba violentó diversos derechos humanos como el derecho a la vida, la integridad personal, la vida privada, libertad de pensamiento y de expresión, libertad de asociación, a la honra, derecho a conocer la verdad, entre otros.

Lo anterior resulta de suma importancia visibilizarlo para que no vuelva a suceder, lo imperante es analizar cómo el Estado propiamente dicho, salvaguarde esos derechos humanos, que son universales y que buscan en forma atemporal que sean tutelados para que se mantenga la paz y la gobernabilidad democrática de un país.

Otro caso, que revela la importancia de que los servicios de inteligencia realicen sus labores bajo el marco normativo sobre derechos humanos, dentro de la resolución de fecha el 16 de noviembre 2023 la Corte Interamericana de Derechos Humanos, sentenció a Brasil en el Caso Tavares Pereira y otros vs. Brasil, por la responsabilidad del Estado en la muerte de trabajadores rurales en 1997, por realizar una manifestación en *Fazenda São Marcos* del Paraná, donde se reclamaban derechos laborales y tierras para trabajarlas, siendo altamente reprimidos por la policía y en el mismo suceso la muerte de Antônio Tavares Pereira.

---

131 CIDH (2009) Ficha Caso Radilla Pacheco, https://www.corteidh.or.cr/tablas/fichas/radillapacheco.pdf, Fecha de consulta 17 de octubre de 2024.

> "95. Dicho esto, los derechos de reunión y circulación no son derechos absolutos y pueden estar sujetos a restricciones. El artículo 15 de la Convención señala que el derecho de reunión sólo puede estar sujeto a las restricciones previstas por la ley, que sean necesarias en una sociedad democrática, en interés de la ***seguridad nacional***, de la ***seguridad*** o del orden públicos, o para proteger la salud o la moral públicas o los derechos o libertades de los demás. La restricción del ejercicio del derecho de reunión basado en amenazas a la "***seguridad*** pública" sólo debe invocarse cuando la reunión cree un peligro significativo e inmediato para la vida o la integridad física de las personas o un riesgo de daños graves a sus bienes. 132. La imposición de restricciones a las reuniones pacíficas tampoco debe basarse en nociones vagas sobre necesidades de "orden público". En cuanto a la "***seguridad nacional***", sólo puede ser invocada para justificar limitaciones necesarias para proteger la existencia de la nación, su integridad territorial o su independencia política contra la fuerza o la amenaza de la fuerza"[132]

Resulta relevante este caso, para los temas de inteligencia y seguridad nacional, porque la Corte Interamericana de los Derechos Humanos en su sentencia señala que se debe equilibrar la protección y seguridad interna con las garantías de los derechos fundamentales, como lo es el derecho a la vida, la integridad personal y la libertad de expresión y la condena; reside que el uso excesivo de la fuerza ni la violación no se justifican por ningún medio, evidenciando que la seguridad nacional no puede prevalecer sobre la obligación del Estado de proteger los derechos humanos de sus ciudadanos.

Desafíos contemporáneos

La inteligencia para la seguridad nacional permite al Estado tener una caja de herramientas, para generar conocimiento para la toma de decisiones que sea útil para mitigar las amenazas o riesgos a los derechos humanos y a la dignidad de las personas.

Es imposible que en la autarquía los Estados puedan resolver los riesgos y amenazas como lo son: el cambio climático, el cibercrimen, el terrorismo, el lavado de dinero, la desinformación, migraciones masivas, las epidemias, etc., aspectos que afectan el crecimiento, desarrollo económico, la gobernabilidad y sobre todo la integridad física de las personas. Dentro del marco jurídico de la Convención Americana de los Derechos Humanos,

[132] Corte IDH. Caso Tavares Pereira y otros Vs. Brasil. (2023) Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 16 de noviembre de 2023. Serie C No. 507., Párrafo 95

podemos señalar que la inteligencia para la seguridad nacional busca el bienestar y mantenimiento de la paz en cualquier territorio o país y llegan a incorporarse al catálogo los Derechos Económicos, Sociales, Culturales y Ambientales mejor conocidos como DESCA.

La Doctora María Cristina Rosas, ha estudiado que, para generar un análisis de inteligencia para el desarrollo, se necesita abordar fuentes como el Foro Económico Mundial, donde podemos extraer temas con altas probabilidades del riesgo que el mundo contemporáneo puede enfrentar y para nuestro análisis poder incorporar a los DESCA en la modelación de la arquitectura de la Agenda Nacional de Riesgos.

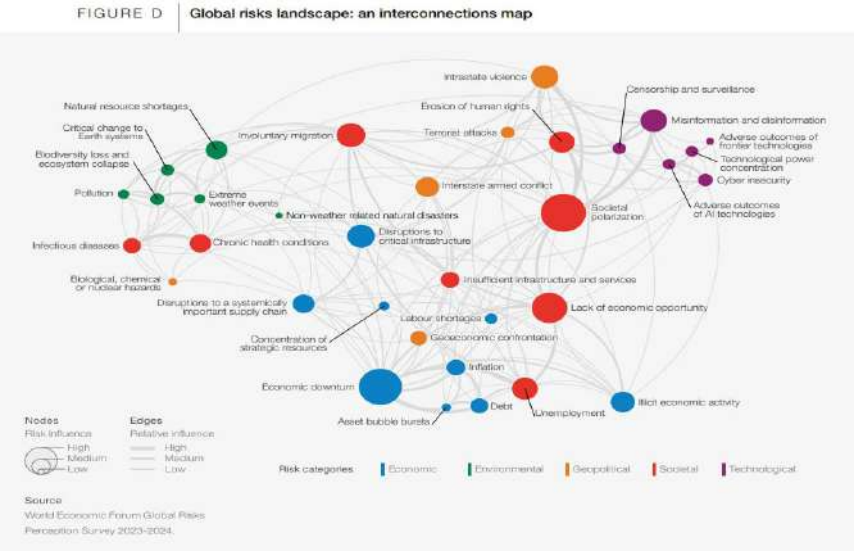
> "La información es poder y este se ha dispersado a una multitud de actores, mismos que desean contar con parámetros que les permitan operar en condiciones ventajosas en la promoción de sus intereses instrumentales particulares."[133]

El contar con piezas de información, nos permite anticiparnos a las crisis y mediante la Agenda Nacional de Riesgos, podemos generar acciones de futuros posibles para atender los temas que tengan impacto en la erosión de los derechos humanos, y para ello, en el gráfico 1 observaremos cómo están parametrizadas las principales amenazas, y sobre todo las acciones de política pública que tiene que tomar y que tutelen cada derecho que adquirimos por el simple hecho de haber nacido.

Por ello, la relevancia de la inteligencia para la seguridad nacional, nos permite visualizar las variables que pueden estar en riesgo o amenaza; al generar productos, como el conocimiento que nos permitan tomar acciones para anticiparnos a las crisis y tutelar el derecho a la vida, la integridad de las personas, la libertad de expresión, prohibición de la esclavitud, las garantías judiciales, protección de la honra y de la dignidad, libertad de conciencia y religión entre otros tantos derechos como los Derechos Políticos y Sociales, así como los DESCA y pensar que podríamos emplear la Inteligencia Artificial como una herramienta que tutele los derechos humanos *verbi gratia* en el derecho a la vida, privacidad y seguridad digital incorporando la inteligencia a un mundo contemporáneo.

Gráfico 1

[133] Rosas, M. C. (2021). *Inteligencia para la seguirdad: mitos y realidades. la experiencia de México*. México: OLOF PALME A.C., Universidad Nacional Autónoma de México, Primera Edición, México.



Fuente: FORUM, W. E. (2024). *The Global Risks. "Global risks landscape: an interconnections map". Obtenido en https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf*

En la arquitectura jurídica mexicana, debemos de tener presente el artículo 1° de la Constitución Política de los Estados Unidos Mexicanos (*Ceteribus Paribus*), que establece el Principio Pro Persona, el cual siempre busca salvaguardar el catálogo de los derechos humanos y evita que la seguridad nacional se vea inmersa en las categorías sospechosas, de las que se citan en su párrafo cuarto, al amparar la tutela de los derechos humanos, ya sea por la supremacía constitucional o a través de alguna jurisprudencia de la Corte Interamericana de los Derechos Humanos respecto a algún tratado del que México sea parte y el que más beneficie a los ciudadanos para acogerse a éste, activando el Parámetro de Regularidad Constitucional.

Ante la evidencia de los riesgos globales y contemporáneos, es inevitable detenernos a reflexionar la manera en que estamos gestionando nuestro presente y cómo debemos visualizar el mundo en constante cambio, debiendo prospectar dentro del espacio cognitivo los temas que significan posibles daños a los derechos humanos y en los que podríamos estructurar una Agenda Nacional de Riesgos.

El cambio climático, ha generado desequilibrios ambientales a nivel global derivado de los gases de efecto invernadero con la probabilidad del 50% que incremente 1.5° centígrados de acuerdo con datos de la Organización de las Naciones unidas (ONU), lo cual, provocará flujos migratorios masivos pasando por México hacia el hemisferio norte y las emisiones de carbono deben de llegar al momento *NetZero*, por lo que de conformidad con el Acuerdo

de París las emisiones para 2030 se tienen que reducir al 45% y llegar a la nulidad para el 2050, tutelando el derecho humano a un medio ambiente sano. Una variable importante es la ciberseguridad, la cual ha llevado a las instituciones públicas, empresas y ciudadanos a la alerta máxima, ya que han sido vulnerados con mayor frecuencia y sofisticadas acciones de ingeniería social como el *phishing*; por otro lado, los ataques a nivel global con *malware* y *ransomware* han incrementado un 350% y un 430% respectivamente, de acuerdo con datos 2020 del Foro Económico Mundial.

En términos geopolíticos, las tensiones y el bajo mantenimiento de la paz ponen en la agenda de la seguridad nacional el tema de las Amenazas Persistentes Avanzadas (APT), los ataques en el ciberespacio son más frecuentes y más sofisticados, haciendo urgente legislar sobre una Ley General de Ciberseguridad enfocada en las sanciones penales por delitos cibernéticos y el fortalecimiento a la cooperación en piezas de inteligencia para combatir dichos ataques en México, con lo cual se protegen el derecho humano a la seguridad y privacidad digital.

Los temas económicos que han transformado las transacciones y el uso de cripto activos, han permitido que sea una herramienta para mover recursos del crimen organizado, principalmente como medio para el lavado de dinero, compra de drogas y financiamiento al terrorismo, por lo que resulta importante que se trabaje desde *blockchain* sobre la base *peer-to-peer,* sin pasar por alguna institución bancaria, por lo que sea a través de transacciones encriptadas que puedan generar una trazabilidad en el horizonte del intercambio de dinero digital en forma criptográfica.

Como herramienta delictiva, debe ser controlada con normativa internacional para combatir las finanzas criminales a nivel internacional como se ha propuesto en la 6ª Conferencia Global sobre Criptomonedas y Finanzas Criminales de 2022, coorganizada por el *Basel Institute* y EUROPOL.

Las desigualdades económicas, deben visibilizar inversiones urgentes al centro-sur del país; detonante del desarrollo y crecimiento económico que, dibuje nuevos rostros sociales que permitan mitigar la inflación, migraciones masivas, continuar la vigilancia marítima, la inteligencia epidemiológica, *Public Compliance* y la seguridad energética nacional; por lo cual en los DESCA se debe tutelar el derecho al trabajo y a las condiciones dignas de un mercado laboral y el acceso al mismo, articulando acciones de política pública para asegurar inversión extranjera directa, -en lo que va de enero a junio de 2024 se han registrado 59,449 millones de dólares- y con ello impulsar a la microempresa -para junio de 2024 la Secretaría de economía señala que existen 4.7 millones- y tener presente el *nearshoring* como motor detonante de la economía mexicana.

Conclusiones

Para dar respuesta a nuestra pregunta de investigación, debemos señalar que los servicios de inteligencia deben potenciar sus capacidades tecnológicas para generar conocimiento a través del ciclo de inteligencia utilizando herramientas de Inteligencia Artificial, que no sólo vayan más allá del carácter de fuentes humanas, sino que se modelen futuros posibles bajo una estructura que emplee el método científico y la innovación, por lo que la inteligencia puede llegar a generar información con grado de certeza que salvaguarde y no violente los derechos humanos como la vida, integridad personal, la honra, la privacidad, seguridad digital y dignidad, DESCA, entre tantos otros y garantizando el *imperium* del Estado.

Las asimetrías sociales están presentes e incrementarán las fracturas en el tejido social, lo cual expone un álgebra muy compleja de resolver mediante acuerdos político-económicos, y se resolverán por la vía del conflicto en términos internos en una zona gris, amplificando la relación de fuerzas derivadas de la polarización, por lo que, se deben proteger los derechos humanos bajo el Parámetro de Regularidad Constitucional y la cooperación flexible en la óptica de una Cultura de Inteligencia como instrumento de Paz y Seguridad Global.

Referencias Bibliográficas

Aguayo S. (1997): Seguridad nacional y derechos humanos en México. Revista Mexicana de Ciencias Políticas y Sociales, XLI (170), 1997

ALPONTE J.M. (2017) Lecturas filosóficas (la lucha por los derechos humanos y el Estado de derecho), Instituto Nacional de Administración Pública, A.C. México. P. 95

ATHENALAB. (13 de septiembre de 2021) *JAMES R. CLAPPER, ex director de Inteligencia de EE.UU.: "Hoy estamos más seguros que antes del 11-S, pero no necesariamente asegurados"*. Recuperado el 16 de octubre de 2024, de CIDH (2009) Ficha Caso Radilla Pacheco https://www.corteidh.or.cr/tablas/fichas/radillapacheco.pdf, Fecha de consulta 17 de octubre de 2024.

CNDH (2018) Aspectos básicos de derechos humanos, México.

CNI (18 de febrero de 2020). *¿Qué es la Inteligencia?* Obtenido de https://www.gob.mx/cni/documentos/que-es-la-inteligencia?idiom=es.: Gobierno de México. Fecha de Consulta 15 de octubre de 2024.

FORUM, W. E. (2024). *The Global Risks. "Global risks landscape: an interconnections map". Obtenido en: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf*

HOLMES, K. R. (2015). "What is National Security?" The Heritage Foundation. Obtenido de https://www.heritage.org/military-strength-essays/2015-

essays/what-national- security,: Index of U.S. Military Strength. U.S.A.: The Heritage Foundation, 17- 26.
CONGRESO DE LA UNIÓN (2005) Ley de Seguridad Nacional, Diario Oficial de la Federación Tomo DCXVI, N° 21
ROSAS, M. C. (2021). *Inteligencia para la seguirdad: mitos y realidades. la experiencia de México.* México: OLOF PALME A.C., Universidad Nacional Autónoma de México. Primera Edición, México.