Estrategia Metropolitana de Ciberprevención: una propuesta para Nuevo León

Metropolitan Cyber Security Strategy: a proposal for Nuevo León

Fernando Margarito Velazquez Flores* y
Dante Octavio Isau Garza Fabela

Recibido: 23-02-2021
Aceptado: 08-06-2022

Resumen

El uso de las tecnologías de la información y la comunicación constituyen un eje fundamental en la interacción de los seres humanos. Debido a su desarrollo se ha logrado una globalización en los diversos ámbitos como lo es económico, político, social y cultural. Dicho avance ha traído consigo nuevas amenazas en un mundo no físico en el cual un individuo o grupo de individuos pueden llevar a cabo hechos violentos y actividades delictivas. Por ende, el presente documento tiene como objetivo presentar una propuesta de política pública en materia de ciberprevención abordada desde la perspectiva de las instituciones de seguridad.

Cómo citar
Velázquez, F. y Isau Garza Fabela, Dante Octavio. Estrategia Metropolitana de Ciberprevención: una propuesta para Nuevo León. Constructos Criminológicos, 2(3). Recuperado a partir de https://constructoscriminologicos.uanl.mx/index.php/cc/article/view/26

*https://orcid.org/0000-0001-6828-7341
Universidad Autónoma de Nuevo León, México

Palabras clave: *Cibercriminología, ciberdelito, ciberseguridad, policías municipales*.

Abstract

The use of information and communication technologies constitutes a fundamental axis in the interaction between human beings. Due to its development, globalization has been achieved in several fields such as economic, political, social and cultural. This development has brought with it new threats in a non-physical world in which an individual or group of individuals can conduct violent acts and criminal activities. Therefore, this document aims to present a cybercriminological public policy from the perspective of security institutions.

Keywords: *Cybercriminology, cybercrime, cybersecurity, municipal police*.

INTRODUCCIÓN

La Criminología ha sido definida por diversos autores según las perspectivas teóricas y la

época histórica en que fueron enunciadas, siendo entendida como la ciencia empírica e interdisciplinaria encargada del estudio de las conductas antisociales, victimario, víctima, control social (García, 2003), el delito (Garofalo, 1885), la criminalidad (Topinard, 1887), sus causas y medios para combatirla (Saldaña, 1914); teniendo como prioridad la prevención del comportamiento delictivo y la explicación del mismo desde un enfoque holístico (Abrahamsen, 1944). Dentro de los debates en torno a dicha ciencia se encuentra la delimitación de su objeto de estudio ante la diferenciación de campos como la medicina forense, derecho penal, psicología, por mencionar algunos (Rodríguez, 1979).

Para hacer frente a los diversos fenómenos subyacentes de la sociedad, esta ciencia ha tenido que evolucionar, lo cual ha permitido el desarrollo de criminologías especializadas o la denominada criminología contemporánea con el fin de comprender la multidimensionalidad de las realidades (Buil, 2016; Hikal, 2013 y Ordaz y Figueroa; 2017).Dichas especializaciones nacen con el objetivo de poder crear conocimiento innovador en el ámbito científico y nos permite visualizar las áreas en donde el criminólogo puede desempeñarse como lo es la victimología forense, social, ambiental e informática entre otros (Hikal, 2016).

Es en este último ámbito, tal como lo señalan Felson y Clarke (1998) los cambios sociales y tecnológicos producen nuevas oportunidades delictivas, por lo cual la criminología ha reconocido los problemas que se dan en la red, abordándolos desde diversas corrientes teóricas (Rojas, 2018). Es de señalar que el crimen se ha ido modificando y ha dado pie a una nueva criminalidad donde cualquier persona física o jurídica que se relacione en internet puede ser víctima de un delito, o en este caso ciberdelito (Sancho, 2017). Ante ello, emergen debates acerca de si las teorías criminológicas tradicionales son aplicables o si ha de tratarse de una misma delincuencia con un semblante distinto, por ello, la importancia del estudio de dicho fenómeno.

MARCO TEÓRICO

El ciberespacio

Desde el siglo XXI el contexto internacional ha visualizado una hiperglobalización impulsada por el uso de las tecnologías de la información y la comunicación, teniendo como resultado una digitalización, misma que se ha vinculado con transformaciones sociales, políticas y económicas a un ritmo acelerado en sociedades contemporáneas, lo que ha permitido definirlo como la cuarta revolución industrial o Revolución 4.0 y dando pauta a la creación de un nuevo escenario de interacción humana: el ciberespacio (Fernández, 2018).

El ciberespacio surge como un nuevo dominio del entorno operativo y de la oportunidad delictiva, además de las ya tradicionales como lo es tierra, mar, aire y espacio. Sin embargo, el ciberespacio destaca entre los demás, debido a que puede escalonar al medio físico generando un mayor conflicto (Feliu, 2012).

Durante la década de los setenta el uso de ordenadores a nivel mundial hizo que las manifestaciones de la delincuencia informática se vieran vinculadas con el ámbito económico, como lo es fraude, robo de datos, espionaje etc. Para la década de los ochenta, el uso de

ordenadores personales era cada vez mayor, lo cual dio pie al surgimiento de la piratería, dando inicio en software para posteriormente expandirse en la década de los noventa a productos como música y películas. Fue también en la década de los noventa y el crecimiento del uso de internet lo que llevó a la difusión de contenidos ilegales como lo es pornografía infantil, discursos racistas, discursos xenófobos u otros ataques con la finalidad de causar algún daño (Hernández, 2009).

De esta manera, el ciberespacio nace como una dimensión universal, anónima y en constante cambio. Dentro de las características básicas que se pueden encontrar en este escenario están la deslocalización, transnacionalidad, neutralidad y descentralización. La primera de ellas se debe a que no está en un espacio concreto. En una segunda instancia, se refiere a que no posee fronteras reales ya que no pertenece a una nación en particular y permite el acceso desde cualquiera de ellas. La tercera de estas características corresponde a la neutralidad que tiene el usuario para tener acceso en un horario y lugar indeterminado. Por último, en internet no existe una autoridad que rija leyes o normas desde una perspectiva gubernamental para atender el cibercrimen (Miró, 2011).

CIBERCRIMINALIDAD Y CIBERCRIMINOLOGÍA

Al referirnos al cibercrimen o la cibercriminalidad hablamos de una macrocategoría dentro del ciberespacio. Los debates conceptuales y terminológicos han hecho que algunas denominaciones sean sustituidas (Hernández, 2009; Jaishankar, 2007). El ciberdelito derivado del término anglosajón *cybercrime,* mismo que engloba la delincuencia relacionada con el uso de las tecnologías de la información y la comunicación (Miro, 2011), ha sido denominado de diversas maneras de acuerdo con los múltiples contextos en que se desarrolla como computerdelikte, computercrimes, cibercriminalidad, criminalidad informática e informatizada, delitos informáticos, criminalidad mediante computadoras, entre otros (Hernández, 2017).

A continuación, se presentan algunas de las definiciones presentados por autores en cuanto a los términos anteriores:

La Organización de Cooperación y Desarrollo Económico (OCDE) en 1983 define el computer crime como "...cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos" (OECD, 1984).

Lima (1984) refiere el delito por computadora como cualquier acto ilícito penal en el que las computadoras, su técnica y funciones desempeñan un papel ya sea como método, medio o fin.

Beltramone, Herrera y Zabale (1998) consideran el delito informático como toda conducta con características delictivas, sea típica, antijurídica y culpable, que atente contra el soporte lógico de un sistema de procesamiento de información a través del uso de las tecnologías de la información.

En el décimo Congreso de las Naciones Unidas del año 2020 sobre prevención del delito y

tratamiento del delincuente, refiere que se entenderá por delito cibernético todo aquel que puede cometerse por medio, en ó contra un sistema informático (Naciones Unidas 2020).

Para Campoli (2006) los delitos informáticos son aquéllos en los que un sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente por medio de la utilización indebida de medios informáticos.

Por su parte, Téllez Valdez (2008) clasifica los delitos informáticos de dos maneras: atípico y típico. El primero de ellos hace alusión a aquellas actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin; el segundo corresponde a las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin.

El Grupo de Expertos Gubernamentales (GGE) en Ciberseguridad en el contexto de la Seguridad Internacional de Naciones Unidas ha pronunciado la importancia de llevar a cabo acciones desde la perspectiva local de los Estados para hacer frente a las nuevas amenazas y riesgos. Derivado de dichas amenazas y experiencias en casos transnacionales es que se llevó a cabo el Convenio de Budapest en 2001 para los Estados miembros del Consejo de Europa y otros Estados. El objetivo del anterior consistió en ejecutar una política penal destinada a prevenir la criminalidad mediante internet, a través de una legislación apropiada de cada Estado (García y Peña, 2017).

En América Latina el cibercrimen ha sido un escenario de oportunidad debido a que hay un bajo riesgo de ser identificados, procesados y sentenciados en comparación con EEUU y la Unión Europea. Es de señalar que los intentos por atender este tipo de hechos en el contexto latinoamericano en su mayoría son deficientes debido a que no cuentan con los conocimientos, equipo tecnológico e infraestructura suficiente para llevar a cabo este tipo de acciones. Aunque México no se encuentra adscrito a dicho convenio, esto no limita a que se puedan adoptar acciones a fin de fortalecer las leyes de la materia (García y Peña, 2017).

El aumento de delitos y conductas violentas que abundan en el ciberespacio ha obligado a que los profesionales en criminología desarrollen un nuevo campo denominado Cibercriminología (García y Peña, 2017). Partimos desde la identificación de las principales problemáticas presentes que son hacking, infecciones malware, ciberfraudes, ciberacoso sexual, ciberbullying, difusión de mensajes de odio, éstos contemplan finalidades diversas desde los ámbitos económicos, políticos, social, personal, mismas que son problemáticas criminológicas distintas. Además de ello, conforme a cada uno de las problemáticas referidas anteriormente se pueden identificar a diversos grupos en situación de vulnerabilidad (Hernández, 2017). La evolución de la cibercriminología basada en el estudio de los determinantes delictivos y sus características es un fenómeno más complejo, debido a que su dinámica es cambiante ha obligado a los estudiosos de dicho tema a focalizarse en un área específica como lo es cibercrímenes sexuales, fraudes financieros, suplantación de identidad, entre otros conflictos y crímenes nacientes en el ciberespacio (García y Peña, 2017; Hernández, 2017).

CIBERSEGURIDAD, RIESGOS CIBERNÉTICOS Y CIBERATAQUES

El conflicto es un hecho inherente en la historia de la humanidad, cuando el diálogo u otros medios de pacificación no funcionan los seres humanos tienden a recurrir a actos violentos a fin de dañar o neutralizar a una persona, propiedad e institución. Los mencionados sucesos tienden a llevarse a cabo mediante acciones políticas, económicas, psicológicas y cibernéticas, causando una vulneración en la sociedad, territorio e infraestructura crítica (Tzu, 1994).

El inicio del dominio del ciberespacio con la finalidad de salvaguardar la integridad de sus habitantes fue un área abordada por las grandes potencias como lo es Rusia, Estados Unidos y China (Gaitán, 2018). En América Latina el tema de ciberseguridad ha ido apareciendo en la agenda pública (Álvarez, 2019; Pérez, 2019), en 2018 se tiene un registro de ciberataques a bancos mexicanos que generaron pérdidas millonarias, lo cual genera un precedente; sin embargo al ser actos que no han puesto en riesgo a sus habitantes mediante algún tipo de crisis económica, social, política en comparación con otros contextos a nivel mundial, el resultado de dichos actos ha sido atendido mediante acciones preventivas de fortalecimiento de software especializado (Aguilar, 2019).

Los riesgos cibernéticos y los ciberataques surgen como las nuevas contingencias vinculadas a la ciberseguridad, el primero de ellos consiste en afectaciones ante una vulneración en las tecnologías que utilizan; mientras que los ciberataques son un intento no autorizado a fin de obtener el control de un sistema, dispositivo electrónico o red informática con la finalidad de extorsionar, extraer datos, o simplemente sabotear su funcionamiento (McKinsey & Company, 2018). Por ende, la ciberseguridad es el conjunto de acciones tomadas por organizaciones e individuos para establecer las medidas y gestiones necesarias para reducir la probabilidad de sufrir un ciberataque y/o riesgos cibernéticos y que la población se sienta segura en el ciberespacio (Herrera, 2020; McKinsey & Company, 2018; Unión Internacional de Telecomunicaciones, 2008).

La Unión Internacional de Telecomunicaciones informó el aumento del número estimado de usuarios de Internet de 4,100 millones en 2019 a 4,900 millones en 2021, cifra que se aproxima al 63% de la población mundial (Unión Internacional de Telecomunicaciones, 2021). Es de señalar que, durante el 2020, primer año de la pandemia COVID-19, el número de internautas creció un 10.2%, mismo que representó el mayor aumento en una década (Asociación de internet, 2021)

Según el Informe de Riesgos Globales 2020 del Foro Económico Mundial, el riesgo de ciberataques a la infraestructura crítica y el fraude o robo de datos se clasificaron entre los 10 principales riesgos con mayor probabilidad de ocurrir y con mayor impacto (FEM, 2020a). La publicación Perspectiva de Riesgos del COVID-19 identificó los ciberataques como una de las principales preocupaciones a nivel mundial y la tercera mayor preocupación para las empresas debido a la constante digitalización (FEM, 2020b). Dicha intranquilidad se pone de manifiesto debido al aumento de ciberataques hasta en 4000% (Banco de México, 2021).

El Consejo Mexicano de Asuntos Internacionales (Comexi) estimo que 978 millones de personas fueron afectados por el ciberdelito en todo el mundo (McKinsey & Company, 2018). Los ciberataques se focalizan principalmente en el sector privado, donde el 82% consistió en cibercrimen, 13% ciberguerra, 3% hacktivismo, 2% ciberespionaje (Pessiri, 2019 citado en Aguilar, 2019).

El informe del Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe de la Organización de los Estados Americanos (OEA) estima que el 92% de las organizaciones financieras ha llegado a sufrir algún tipo de ciberataque, donde el 37% resultó de manera exitosa (Organización de los Estados Americanos, 2018). Los costos para la economía mundial derivados de los delitos cibernéticos se estima que sobrepasan los 2 billones de dólares anuales (McKinsey & Company, 2018; Towers, 2018).

México se encuentra dentro de los 10 principales países con ataques cibernéticos a nivel mundial, y el primero en la región de América Latina. En 2018 el 80% de las empresas mexicanas fue víctima de un ciberataque al menos en los últimos doce meses, de dicho porcentaje únicamente el 30% de ellos tenía algún tipo de plan, protocolo o procedimiento previsto en caso de llegar a suscitarse dichos hechos (Towers, 2018).

Por su parte, la cifra estimada para México corresponde a más de 33 millones de mexicanos que fueron víctimas del cibercrimen, es decir, 1 de cada 4 habitantes del país (McKinsey y Company, 2018).En general se puede considerar que 8 de cada 10 delitos informáticos que ocurren, no llegan a ser conocidos por el Estado y 1 de cada 100 podría llegar a tener una condena efectiva (Observatorio de Delitos Informáticos de Latinoamérica, 2017).

Desde la perspectiva legal, una de las principales dificultades al hablar sobre delitos informáticos, es su conceptualización, por ende, desde su fundamento al hacer alusión a la delincuencia informática tenemos que hacer mención del denominado derecho informático. En el anterior se estudia el régimen jurídico del software, el derecho de las redes de transmisión de datos, documentos y contratos electrónicos, régimen jurídico de las bases de datos, los delitos informáticos, así como otras conductas nacidas del uso de ordenadores (Hernández, 2009).

Conocer y determinar los diferentes tipos de delitos informáticos existentes permite hacer uso de herramientas efectivas para hacer frente a la seguridad de la información. Con base en lo anterior, la impunidad y propuestas de políticas públicas en la administración de justicia ha sido producto de la falta de entendimiento de los riesgos existentes en el ciberespacio (Acosta, Benavides y García, 2020; Aguilar, 2019).

Ante la falta de una legislación específica en ciberdelitos, esto impide su persecución y sanción, cuya conducta no puede ser adecuada a los códigos estatales existentes. Por ello, los gobiernos deben de comenzar a preocuparse en la inclusión de estos tipos de hechos, así como los retos en la preservación de la evidencia digital (Campoli, 2005).

Contemplar una agenda de ciberseguridad es uno de los principales retos para las naciones de Latinoamérica. Lo anterior se debe a que las principales amenazas para este territorio consisten en ataques dirigidos por malware para robo de información, donde las técnicas utilizadas tienden a ser el spear- pishing (correo electrónico a fin de infectar) y el watering-hole (infecta con malware sitios web de terceros utilizados por los usuarios) (Aguilar, 2019).

A pesar del mejoramiento de las capacidades en materia de ciberseguridad, en América Latina y el Caribe se encuentran en una etapa inicial, es decir, la mayoría de los países de esta región apenas han comenzado a formular e implementar políticas en materia de seguridad cibernética. Lo cual ha llevado a la preocupación constante de las organizaciones mexicanas a destinar recursos a nivel público y privado para contar con personal en materia de seguridad y privacidad de la información (Banco Interamericano de Desarrollo, 2020).

USO DE TIC Y ANTECEDENTES DE POLÍTICAS PÚBLICAS EN EL CONTEXTO MEXICANO

De acuerdo con los datos presentados por Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020, se estima que en México existen 84.1 millones de usuario de internet de seis años o más, lo que representan el 72% de la población a nivel nacional (INEGI, 2020).
La edad de los usuarios de internet se concentra entre los 12 a 34 años de edad. Así mismo, los tres principales medios de conexión para el usuario de internet fueron 96% celular inteligente, 33.7% computadora portátil y 22.2% televisor con acceso a internet. Entre las principales actividades que informaron realizar los usuarios de internet se encuentra el 93.8% para comunicarse, 91% buscar información y 89% acceder a redes sociales (INEGI, 2020).

En relación con la penetración de internet en cuanto a usuarios de acuerdo con las entidades federativas, Nuevo León lidera con el 84.5% cifra por encima de la Nacional que es de 72% (INEGI, 2020). Ante dichas cifras y las características de la región los usuarios se encuentran expuestos constantemente a riesgos cibernéticos o algún ciberataque.

Para el contexto mexicano la ciberseguridad ha sido un tema abordado desde 2002, con la finalidad de atender las problemáticas de delincuencia y organizaciones delictivas se creó la Policía Cibernética, asignada a la Policía Federal Preventiva. En el año 2013 dicho tema se incluyó en los planes y programas de gobierno, como lo es el Plan Nacional de Desarrollo 2013-2018, el Programa de Seguridad Nacional y el Programa de Seguridad Pública, éstos últimos de los periodos 2014-2018.

El Plan Nacional de Desarrollo 2013-2018 dentro de su meta “México en Paz”, en su objetivo 1.2. Garantizar la Seguridad Nacional, Estrategia 1.2.3. Fortalecer la inteligencia del Estado Mexicano para identificar, prevenir y contrarrestar riesgos y amenazas a la Seguridad Nacional, establece en una de sus líneas de acción llevar a cabo estudios, investigaciones e iniciativas de ley con la finalidad de fortalecer la dimensión de las operaciones de seguridad, en este caso las llevadas a cabo en el ciberespacio

y la ciberseguridad.
Con dicho antecedente, el Programa Nacional de Seguridad Pública 2014-2018 explica la importancia que conlleva contar con objetivos estratégicos, coordinación de autoridades y una visión multidimensional en materia de seguridad cibernética y ciberdefensa.

Su estrategia 2.7 consiste en: Detectar y atender oportunamente los delitos cibernéticos.

Líneas de Acción:

- *2.7.1 Fortalecer las capacidades y la infraestructura tecnológica de las instituciones de seguridad pública para prevenir e investigar delitos cibernéticos.*
- *2.7.2 Desarrollar investigación científica para la prevención e investigación de los delitos cibernéticos.*
- *2.7.3 Implementar acciones contra delitos cibernéticos de mayor impacto: pornografía infantil, fraude, extorsión, usurpación de identidad y contra derechos de autor.*
- *2.7.4 Diseñar protocolos de operación para la prevención de delitos cibernéticos en las instancias que administran información considerada reservada o confidencial.*
- *2.7.5 Promover la creación y fortalecimiento de unidades especializadas en la prevención e investigación de delitos que se cometen por internet.*
- *2.7.6 Desarrollar un modelo de policía cibernética para las Entidades Federativas.*
- *2.7.7 Generar indicadores y estadísticas de delitos informáticos para el diseño de estrategias de prevención.*
- *2.7.8 Impulsar acciones para consolidar los esquemas de seguridad cibernética que coadyuven al desarrollo de la economía digital.*
- *2.7.9 Fortalecer la seguridad de la infraestructura tecnológica estratégica del país*

Dentro de dicho plan también se contemplaba detectar y atender de manera oportuna los delitos cibernéticos mediante una estrategia de ciberseguridad llevada a cabo por la Policía Federal, así como la necesidad de desarrollar un modelo de policía cibernética para cada una de las entidades federativas.

En 2017 se crea la Estrategia Nacional de Ciberseguridad (ENCS) siendo el octavo país en América Latina en contar con un documento de esta naturaleza. Si bien, ya se contaba desde años con un Equipo de Respuesta a Incidentes de Seguridad (CSIRT) y un Centro de Respuesta a Incidentes Cibernéticos (CERT) para prevenir y atender las amenazas, dicho documento formó parte del desarrollo de ejes transversales a fin de consolidar y desarrollar capacidades de acción y reacción en relación a la ciberseguridad (Gobierno de México, 2017).

Se llegó a tener un registro de 51,000 denuncias ciudadanas atendidas, más de 200,000 incidentes cibernéticos, la desactivación de 17,000 sitios fraudulentos y se emitieron más de 2,000 alertas de ciberseguridad a instituciones públicas y privadas (Gobierno de México, 2017).

Actualmente el Plan Nacional de Desarrollo 2019- 2024 (Centro Nacional de Control de Energía ,2019) a través de sus políticas en materia de seguridad y desarrollo desprende la Estrategia Digital Nacional 2021-2024, misma

que se divide en dos ejes de acción: I Política Digital y II Política Social. El eje I Política Digital en la Administración Pública Federal plasma en uno de sus objetivos específicos la promoción de una cultura de seguridad de la información que genere certeza y confianza a las personas usuarias de los servicios tecnológicos institucionales y gubernamentales, para ello, dentro de sus líneas de acción se establece la implementación de un Protocolo Homologado para la Gestión de Incidentes Cibernéticos entre las Instituciones; coordinación entre autoridades para prevención y atención de incidencias cibernéticas, así como la promoción de buenas prácticas a través del el Centro Nacional de Respuesta a Incidentes Cibernéticos (Diario Oficial de la Federación de México, 2021).

En el eje II Política Social se encuentra ofrecer internet inalámbrico en todo el país basado en el bienestar social del pueblo mexicano con una visión humanista del uso de estas tecnologías a fin de eliminar las brechas de marginación, pobreza y desigualdad social; acto que de cumplirse traerá consigo retos en cuanto a normativas para la protección de la privacidad de las personas que accedan a internet mediante estas redes públicas (Diario Oficial de la Federación de México, 2021).

El reconocimiento de los delitos mediante el uso de las tecnologías de la información y la comunicación ha hecho que la inteligencia sea la base el desempeño de las fuerzas del orden, por ello, en la Estrategia Digital Nacional 2021-2024 se pretende orientar a la Policía Cibernética con capacitaciones especializadas, así como fortalecer las capacidades tecnológicas que permitan a las instituciones de seguridad de los tres órdenes de gobierno el intercambio seguro de la información en prevención y persecución del delito (Diario Oficial de la Federación de México,2021).

Por su parte, el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos busca fortalecer la Ciberseguridad en las Dependencias Federales, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado del país. Consta de un modelo de operación de cinco pasos los cuales consisten en identificar, proteger, detectar, responder y restaurar los servicios que brinden los múltiples actores involucrados con la menor afectación posible contemplando un plan de resiliencia (Gobierno de México, 2021b).

Es de mencionar que además de la gestión y monitoreo proactivo de los múltiples actores involucrados en una fase de respuesta y recuperación se menciona la necesidad las actividades post-incidentes que incluyen la presentación de denuncias ante el Ministerio Público y la generación de estadísticas oficiales de incidentes en el país en coordinación con el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, y seguimiento de indicadores de Ciberseguridad (Gobierno de México, 2021b).

Expuesto lo anterior, México sigue reiteradamente con los mismos objetivos básicos plasmados en otras estrategias digitales, si bien, se puede identificar una base en aspectos sociales, económicos, culturales, legales y político inclusive catalogados en un futuro como derechos fundamentales, tal es el

caso del acceso a Internet y las TIC, pero no garantizando una ciberseguridad. Por ello, dicha estrategia se puede interpretar como un discurso meramente cualitativo de ideales o acciones a realizar sin un desarrollo y plan de trabajo de cada una de las instituciones a participar, así como su transversalidad con la política de ciberseguridad, las capacidades de resiliencia, especificando las responsabilidades y atribuciones para cada uno de los organismos.

POLICÍA CIBERNÉTICA: EL CASO DE NUEVO LEÓN

Con base en los acuerdos del Consejo Nacional de Seguridad Pública, aprobados en su Cuadragésima Primera Sesión Ordinaria en la Acuerdo 06/XLI/16 celebrada el 20 de diciembre de 2016 se aprueba el Modelo Homologado de Unidades de Policía Cibernética que deberá ser implementado a partir de 2017 (Diario Oficial de la Federación, 2017).

De esta manera se atribuye a los Estados la responsabilidad de activar protocolos para una intervención activa en la prevención y sanción de los delitos de esta índole, así como la generación de grupos de investigación enfocados en el análisis de las causas y consecuencias derivadas de dichos actos (García y Peña, 2017).

El "Modelo Óptimo de la Función Policial. Diagnóstico nacional sobre las policías preventivas de las entidades federativas", elaborado por el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP) con fecha de corte de la información al 31 de diciembre de 2020, revela que, aunque el estándar a nivel nacional es que los 32 estados cuenten con unidades especiales de Policía Cibernética, únicamente 30 entidades cuentan con ella, cifra que representa el 93.7%. Derivado de ello, únicamente 17 entidades (56.6%) de las policías cibernéticas refirió contar con el equipamiento necesario (SESNSP, 2020).

Para el caso de Nuevo León se tiene un registro de 11 integrantes que conforman la policía cibernética (CIPOL), de los cuales únicamente un integrante (9%) recibió una capacitación especializada, acción que se puede vincular con las acciones plasmadas en la Estrategia Digital Nacional 2021-2024 ante la ausencia de personal profesionalizado en dicha área. A pesar de que el promedio nacional de elementos asignados a dichas unidades es de 14, se visualiza un área de oportunidad para el Estado debido al aumento de reportes y delitos sobre dicha índole. Además de esto, en comparación con otros Estados la cantidad de integrantes es menor, ejemplo de ello es la Ciudad de México que cuenta con 58 integrantes seguida por Yucatán con 37 (SESNSP, 2020).

A nivel nacional la Secretaria de Seguridad y Protección Ciudadana, mediante una rueda de prensa, expresó que hay evidencia de población menor de edad que ha sido privada de su libertad. El modus operandi era establecer conexión por medio de videojuegos, irse ganando la confianza de las personas con quienes interactúan, para posteriormente llevar a cabo el secuestro e incorporarlos al crimen organizado para realizar funciones de "halconeo". Procedente a esto se difundió un decálogo de ciberseguridad para protección de

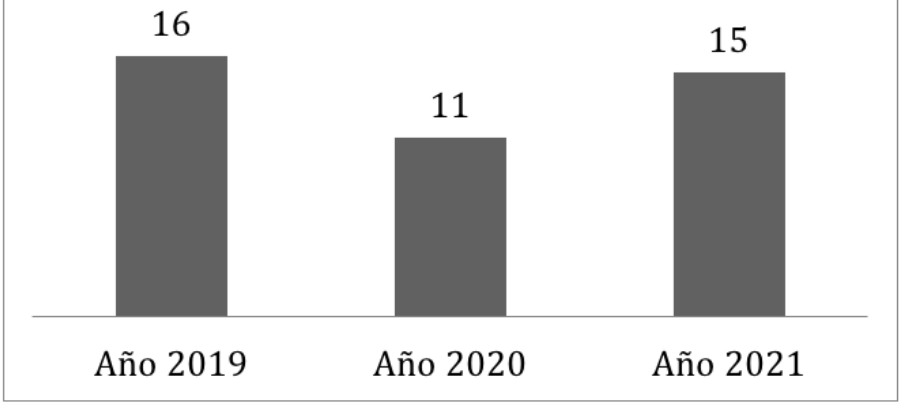
menores en el Boletín 118/2021 (Gobierno de México, 2021).

Dicho lo anterior, Nuevo León no es un espacio ajeno a esto, por lo cual diputados del mencionado Estado han realizado un llamado a las instituciones de seguridad, específicamente a la Secretaría de Seguridad Pública del Estado para que ésta instancia, a través de la policía cibernética vigile, identifique y localice las posibles amenazas que se dan por parte de los grupos criminales en estos sitios, así como llevar a cabo campañas informativas sobre los riesgos y medidas que deben de tomarse al interactuar en entornos virtuales (Recio, 2021).

Existen crecientes retos en materia de ciberseguridad que deben ser atendidos desde las fuerzas policiales (Velázquez, 2020). De acuerdo con el Plan Estratégico para el Estado de Nuevo León 2015-2030, en el eje temático Seguridad y Justicia, se establece que el servicio tradicional de Policía ha sido rebasado. Por lo cual es necesario integrar la inteligencia policial, el análisis delictivo y contar con una estrategia local de ciberseguridad y ciberinteligencia a fin de expandir las capacidades y herramientas en cuanto a prevención de la violencia y la reacción ante el delito (Consejo Nuevo León, 2022).

En Nuevo León, la institución responsable de la persecución y el esclarecimiento de los hechos delictivos es la Fiscalía General de Justicia del Estado (FGJNL), donde los retos para la legislación son aún mayores (Cassou, 2009) debido a que se cuenta con un registro mínimo de carpetas de investigación en relación con hechos cibernéticos.

Grafico 1. Carpetas de investigación de delitos por medios electrónicos 2019-2021 Estado de Nuevo León.
Figure 1. Cyber Crimes case files from 2019-2022 Nuevo León State



Fuente: Elaboración propia con base en datos de la FGJNL.

Entre dichas carpetas de investigación se encuentra el delito por medios electrónicos, sin embargo, en las estadísticas presentadas por la institución antes mencionada no se cuenta con un desglose en relación con otros delitos. Lo cual deja un hueco para la generación de políticas públicas en materia de prevención y atención de Ciberdelitos, identificando dicha área de oportunidad.

El Consejo Nacional de Seguridad Pública, en su Cuadragésima Séptima Sesión Ordinaria, celebrada el 16 de diciembre de 2021 establece en el acuerdo 10/XLVII/21 la necesidad de contar con información actualizada en materia de ciberdelitos, por ende, se propone un Registro Nacional de Incidentes Cibernéticos. Este registro tendrá como fin la prevención y atención a dichos hechos en las 32 entidades federativas de la República Mexicana, a través de las Secretarías de Seguridad Pública Estatales en coordinación con la Unidad de Policía Cibernética y la Fiscalía General (Diario Oficial de la Federación, 2021b).

Ligado a ello, la Clasificación Internacional de Delitos con Fines Estadísticos de la UNODC incluye dentro de sus desagregaciones adicionales o etiquetas la variable de "Acto relacionado con la ciberdelincuencia" con el fin de mejorar la coherencia y comparabilidad internacional, mismo que puede surgir como un instrumento para estandarizar a nivel nacional las estadísticas de delito. Con ello, se abarca la manifestación del delito, ejemplo de ello: fraude a través de Internet, acoso cibernético o violación del derecho de autor mediante la difusión electrónica (UNODC, 2015).

¿EN QUÉ CONSISTE LA ESTRATEGIA DE CIBERPREVENCIÓN PARA NUEVO LEÓN?

Algunas de las áreas de oportunidad que se encuentran presentes ante una explicación de la realidad en que se comportan los ciberdelitos se debe a que son pocas las instituciones que están capacitando en cómo prevenirlos desde los diversos sectores como lo es público y privado; existe una enorme cifra negra de la criminalidad informática; falta de medición de ciberdelitos; estadísticas equivocadas o no oficiales debido a que son empresas privadas las que se están encargando de realizar dichos estudios; y escasos estudios criminológicos que aborden dichos tópicos (Pecoy, 2011).

Debido a estos grandes desafíos, la Facultad de Derecho y Criminología de la Universidad Autónoma de Nuevo León creó el Centro de Investigaciones de Cibercriminalidad, Derecho Digital y Ciberseguridad, el cual busca contribuir a la comprensión y reducción de estos hechos mediante recomendaciones, análisis, implementación y evaluación de las políticas, normas y estándares internacionales de operación para la seguridad de la información y ciberseguridad, así como su contexto jurídico y legal.

Vinculado a ello, surge la iniciativa y necesidad en primera instancia de crear de manera metropolitana y no individual, una policía cibernética municipal que venga a fortalecer a la policía cibernética estatal. La Organización de las Naciones Unidas ha identificado la falta de especialización de las policías en el campo de los ciberdelitos, lo cual obliga a repensar las estrategias de prevención de la violencia y la

delincuencia. Por ello, dentro de las estrategias de fortalecimiento se encuentra la atención a estos en cuanto a prevención y justicia penal (UNODC, 2020).

Dentro de la misma estrategia se considera la especialización de la Policía Cibernética Municipal, dada la incapacidad de ubicar a la cibercriminalidad. La estrategia se denomina "metropolitana", no porque se refiera al territorio o a la jurisdicción, sino a la forma de actuar y de fortalecer las capacidades institucionales dentro del área metropolitana de Monterrey (AMM), independientemente de que el presunto delincuente se encuentre en otro municipio, estado o país. Es decir, una estrategia que involucre a los 13 municipios que la conforman: Apodaca, Cadereyta Jiménez, El Carmen, García, San Pedro Garza García, General Escobedo, Guadalupe, Juárez, Monterrey, Salinas Victoria, San Nicolás de los Garza, Santa Catarina y Santiago.

Dicha propuesta, suscita el modelo Pentahélice que promueve la articulación de la política pública entre los cinco sectores estratégicos: academia, gobierno, industria, sociedad y ambiente en favor de la sociedad (CONACYT, 2019).

La estrategia consiste en lo siguiente:

1. Creación de una Ley de Prevención de Delitos Cibernéticos para Nuevo León.
2. Especialización de la Policía Cibernética Estatal (CIPOL).
3. Creación de las Policías Cibernéticas Municipales (CIPOL Municipal).
4. Fiscalía Especializada en Delitos Cibernéticos.
5. Creación de un Consejo Estatal de Prevención de Delitos Cibernéticos.
6. Creación de un Observatorio del Ciberdelito.

¿Cómo se implementa?

1. Ley: Actualizar en materia legislativa sobre problemáticas emergentes y contingencias en los entonos virtuales en el sector público y privado, ciberdelitos, con el objetivo de brindar seguridad a las personas en el ciberespacio.
2. Especialización CIPOL: El diagnóstico realizado por el SESNSP expone la necesidad de brindar capacitación especializada a los elementos ya existentes para el desempeño óptimo de sus funciones.
3. CIPOL Municipal: Formar un grupo especializado de analistas que contribuyan a la prevención de la violencia y delincuencia en el ciberespacio en cada uno de los municipios del AMM para la implementación de dicha estrategia y los grupos de investigación para el estado de Nuevo León. La Policía Cibernética Municipal llevará a cabo pláticas informativas, patrullaje cibernético, alertas cibernéticas, así como informar, proveer y difundir el perfil y modus operandi de los cibercriminales a la población en general y los riesgos en los cuales se pueden ver implicados ante el uso de Internet, correo electrónico (Gmail, Outlook, yahoo) y redes sociales como Facebook, Instagram, Twitter, Whatsapp, blogs, websites, etc.
4. Fiscalía Especializada: Derivado de las acciones legislativas será necesario contar con un plan de persecución penal que vaya dirigida a este tipo de violencias y delincuencia para la investigación y persecución de delitos. Mismo que tendrá que verse reflejado con indicadores cuantitativos conforme a las carpetas de investigación y la formulación de un semáforo de ciberdelitos (Velázquez, 2021).
5. Consejo: Constituir un grupo de ciudadanos de los diferentes ejes estratégicos como lo es academia, gobierno, empresas y sociedad civil para el seguimiento de acuerdos, monitoreo y evaluación de los resultados de la estrategia.
6. Observatorio: Establecer un instituto de investigación para la generación de informes estadísticos y análisis de políticas públicas en relación con el tema de cibercriminalidad. Así como el monitoreo del semáforo de Ciberdelitos de la FGJNL para la medición de estos hechos.

Para lograr los objetivos anteriormente plasmados se propone un ejercicio corresponsal que involucre al Centro de Investigaciones de Cibercriminalidad, Derecho Digital y Ciberseguridad de la UANL; Fiscalía General de Justicia de Nuevo León; la Unidad de Policía Cibernética de Seguridad Pública del Estado de Nuevo León; el Poder Judicial del Estado de Nuevo León para llevar a cabo la actualización de sus jueces, el Poder Legislativo para la creación de una Ley de Ciberprevención. Además, de vincular dichas instituciones a organizaciones nacionales e internacionales para su fortalecimiento en la materia.

CONCLUSIONES

Derivado de la pandemia COVID-19 y el incremento de la actividad mediante el uso de las tecnologías de la información, se ha dejado en evidencia las vulnerabilidades existentes en el ciberespacio. México se encuentra alejado de la comprensión de las ciberamenazas y ciberataques a nivel global para la vulneración de la seguridad pública y nacional, dicho

enunciado se puede sustentar con el aumento de ciberataques en dicha región. Con una nula visión en sus protocolos desde el enfoque local hasta el internacional (Aguilar, 2019).

El tema de seguridad informática se ha maximizado en el ámbito empresarial mediante el uso de big data, protección de activos, espionaje, etc.; sin embargo, en seguridad pública el proceso ha sido más lento y no se ha visualizado con el mismo impacto, utilizando los medios convencionales de la región como lo es georreferenciación, análisis estadístico, así como el aumento de policías y patrullaje para labores de disuasión. Por resultado, los nuevos retos que presentan los policías son de prevenir los delitos con el uso de inteligencia y el desarrollo tecnológico mediante estrategias en materia de prevención y atención de ciberdelitos (Villalobos, 2020).

En diversos contextos, el interés por el campo de la ciberseguridad ha llevado a crear programas de formación integral a autoridades y organizaciones privadas interesadas en fortalecer sus capacidades institucionales (Álvarez, 2019). Una resiliencia cibernética requiere promover la ciberseguridad con un enfoque integral y políticas transversales (Herczynski, 2020).

Los retos de una estrategia de prevención en materia de ciberdelincuencia y ciberseguridad consta de tomar como base aquellas acciones que han funcionado internacionalmente como lo es el Convencio de Budapest; Declaracion de Doha; así como a acciones planteadas por la Secretaría de la Commonwealth y aquellas en el 12° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (Centro Internacional para la Prevención de la Criminalidad, 2018).

Como resultado de las problemáticas emergentes, uno de los retos consta de armonizar los marcos jurídicos en torno a las definiciones destinadas con la finalidad de proteger a la población contra la ciberdelincuencia, desde los procedimientos nacionales, competencias legales y el cumplimiento de las facultades, atribuciones y obligaciones de ley de las autoridades. Para ello, en el contexto mexicano ya se cuentan con iniciativas de ley en materia de ciberseguridad (López, 2020).

La ley surge como una herramienta que permite responder a los nuevos desafíos de la sociedad. La legislación también debe actualizarse sobre nuevos conceptos, debido a que muchas de ellas se encuentran centradas en objetos físicos y declinan particularidades del uso de las tecnologías de la información y la comunicación. Por ello, han surgido planteamientos sobre las disposiciones generales del derecho penal y la necesidad de atender los requerimientos en cuanto a los delitos informáticos específicos (UNODC, 2013).

De este modo, ante la nueva realidad en que vivimos, es necesario que desde las funciones del Estado se intervenga de una manera efectiva en temas relacionados a la prevención y sanción de los delitos. Para ello, se deben analizar las causas y consecuencias de los mismos. Se hace alusión a dicho tema debido a que la manera en que los individuos interactúan se ha ido modificando con el avance tecnológico (García y Peña, 2017).

La ciberseguridad es clave para la sostenibilidad y el cumplimiento de los Objetivos de Desarrollo Sostenible (ODS), por lo cual para lograr que las ciudades sean más seguras y resilientes; exista paz, justicia e instituciones sólidas y alianzas para lograr los objetivos es necesario considerar a los gobiernos locales y policías municipales dentro de los escenarios para llevar a cabo estrategias de prevención, atención y disuasión de los Ciberdelitos (Naciones Unidas, 2022).

En coordinación con diferentes instancias de seguridad y justicia, se debe elaborar una "Agenda Local de Riesgos de Ciberseguridad para el Estado de Nuevo León". De esta manera se pueden generar avances hacia una cultura de paz, cooperación social, solución participativa y ruptura del paradigma tradicional de los sistemas de justicia y poder dar solución a las problemáticas emergentes (Velázquez y Garza, 2019).

Es de añadir, que así como algunos autores refieren la necesidad de aprovechar el vínculo entre instituciones públicas y privadas para la creación de una Agencia Nacional de Ciberseguridad (Aguilar, 2019). Desde el ámbito local, se visualiza un área de oportunidad similar, por ello, es inevitable pensar en la creación de una unidad estratégica que cuente con personal especializado para el análisis y estudio en materia de ciberdelitos.

Más allá de lo planteado en este texto, se pretende que el tema de la cibercriminalidad llegue a la agenda de los Gobernantes del Estado de Nuevo León. Se busca construir una política para prevenir los incidentes mediante un ejercicio corresponsal y de retroalimentación de la información, utilizando la inteligencia colectiva (Núñez, Trujillo y Hackett, 2020), que involucre a cada uno de los cuatro sectores estratégicos de la sociedad como lo es academia, sector público, sector privado y sociedad civil.

TRABAJOS CITADOS

Abrahamsen, D. (1944). *Crime and the human mind*. Nueva York: Columbia University Press.

Acosta, M., Benavides, M. y García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia,* Vol.25(89),351-368. ISSN: 1315-9984. Disponible en: https://www.redalyc.org/articulo.oa?id=29062641023

Aguilar, J. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *URVIO Revista Latinoamericana de Estudios de Seguridad*, (25), 24-40. https://doi.org/10.17141/urvio.25.2019.4007

Álvarez, D. (2019). La paz y la seguridad internacionales en el ciberespacio. *Revista Chilena de Derecho y Tecnología*. *Vol. 8 núm.* 2.págs. 1-3. Doi. 10.5354/0719-2584.2019.55827

Asociación de internet (2021). 17° Estudio sobre los Hábitos de los Usuarios de Internet en México 2021. Mexico: The Competitive Intelligence Unit. Disponible en: https://irp.cdn-website.com/81280eda/files/uploaded/17%C2%B0%20Estudio%20sobre%20los%20Ha%CC%81bitos%20de%20los%20Usuarios%20de%20Internet%20en%20Me%CC%81xico%202021%20v16%20Publica.pdf

Banco de México (2021). *Reporte de Estabilidad Financiera,* Diciembre 2021. Disponible en: https://www.banxico.org.mx/publicaciones-y-prensa/reportes-sobre-el-sistema-financiero/%7B18265301-01FF-CE2A-F381-19BB9DCB1E4B%7D.pdf

Banco Interamericano de Desarrollo (2020). *Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y*

el Caribe. Reporte Ciberseguridad 2020. Washington DC: OEA

Beltramone, G.; Herrera, R. y Zabale, E. (1998). Nociones básicas sobre los delitos informáticos. Disponible en: http://rodolfoherrera.galeon.com/delitos.pdf.

Buil, D. (2016). ¿Qué es la criminología? una aproximación a su ontología, función y desarrollo. *Derecho y Cambio Social,* 13 (44) pp1-56. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=5456246

Cassou. J. (2009). Delitos informáticos en México. *Revista del instituto de la Judicatura Federal*. Núm. 28

Campoli, G. (2005). Pasos hacia la reforma penal en materia de delitos informáticos en México. AR: *Revista de Derecho Informático*, núm. 079. Disponible en http://www.alfa-redi.org/rdi-artículo.shtml?x=974

Campoli, G. (2006). Los dos delitos más comunes y controversiales cometidos por medios informáticos: clonación de tarjetas de crédito y phishing o transferencias electrónicas ilegítimas. AR: *Revista de Derecho Informático,* núm. 101. Disponible en http://www.alfa-redi.org/rdi-artículo.shtml?x=8083

Centro Internacional para la Prevención de la Criminalidad (2018). 6° Informe internacional sobre la prevención de la criminalidad y la seguridad cotidiana: Prevenir la ciberdelincuencia. Montréal: Centro Internacional para la Prevención de la Criminalidad.

Centro Nacional de Control de Energía (2019). Plan Nacional de Desarrollo 2019-2024. México: Gobierno de México. Disponible en https://www.gob.mx/cenace/acciones-y-programas/plan-nacional-de-desarrollo-2019-2024-195029.

Consejo Nacional de Ciencia y Tecnología (2022). PENTAhélice y la Innovación Abierta. Recuperado de: https://conacyt.mx/conacyt/areas-del-conacyt/desarrollo-tecnologico-e-innovacion/programa-estrategico-nacional-de-tecnologia-e-innovacion-abierta-penta/

Consejo Nuevo León (2022). *Plan Estratégico para el Estado de Nuevo León 2015-2030*. México: Gobierno de Nuevo León. Disponible en: https://planestrategico.conl.mx/

Diario Oficial de la Federación. (2013). *Plan Nacional de Desarrollo 2013-2018*. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5299465&fecha=20/05/2013

Diario Oficial de la Federación (2014). *Programa para la Seguridad Nacional 2014-2018*. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5342824&fecha=30/04/2014

Diario Oficial de la Federación (2014b). *Programa Nacional de Seguridad Pública 2014-2018*. Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5343081&fecha=30/04/2014

Diario Oficial de la Federación (2017). *Acuerdos del Consejo Nacional de Seguridad Pública, aprobados en su Cuadragésima Primera Sesión Ordinaria, celebrada el 20 de diciembre de 2016*. Mexico: Secretaria de Gobernación. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5468583&fecha=04/01/2017#gsc.tab=0

Diario Oficial de la Federación de México (2019). *Plan Nacional de Desarrollo 2019-2024*. México: Secretaría de Gobernación. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5565599&fecha=12/07/2019#gsc.tab=0

Diario Oficial de la Federación de México (2021). E*strategia Digital Nacional 2021-2024*. México: Secretaría de Gobernación. Recuperado de https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gsc.tab=0

Diario Oficial de la Federación de México (2021b). *Acuerdos del Consejo Nacional de Seguridad Pública, aprobados en su Cuadragésima Séptima Sesión Ordinaria, celebrada el 16 de diciembre de 2021*. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5639615&fecha=29/12/2021

Feliú, L. (2012). La ciberseguridad y la ciberdefensa. *El ciberespacio. Nuevo escenario de confrontación., ISBN 978–84-9781-724-0* (2012), 37–69. Disponible en https://dialnet.unirioja.es/institucion/ceseden/listalibrosporeditor?codigo=3361&inicio=101

Felson, M., y Clarke, R. (1998). *Opportunity makes the thief: Practical theory for crime prevention*. *Vol*. 98. Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.

Fernández, J. (2018). *La hiperglobalización y su impacto*. Cuadernos de estrategia, 199, 83-118. https:// dialnet.unirioja.es/servlet/articulo?codigo=6831584

Foro Económico Mundial (2020a). *The Global Risks Report 2020*. Recuperado de: https://www.weforum.org/reports/the-global-risks-report-2020

Foro Económico Mundial (2020b). *COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications*. Recuperado de https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implication

Gaitán, A. (2018). Ciberguerra. *La consolidación de un nuevo poder en las relaciones internacionales contemporáneas*. Colombia: Ediciones USTA.

García, J. y Peña, D. (2017). Cibercriminalidad y postmodernidad: La cibercriminología como respuesta al escenario contemporáneo. *Actualidad Penal,* Número 31, pp. 329-364.

Garcia, P. (2003). *Tratado de criminología* (3 ed.). Valencia: Tirant Lo Blanc.

Garofalo, B. (1885). *Criminologia: Studio sul delitto, sulle sue cause e sui mezzi di repressione*. Turin: Fratelli Bocca.

Gobierno de México (2017). Estrategia Nacional de Ciberseguridad. Disponible en: https://bit.ly/2AEvAtU

Gobierno de México (2021). Presenta SSPC decálogo de ciberseguridad para protección de menores. Disponible en: https://www.gob.mx/sspc/prensa/presenta-sspc-decalogo-de-ciberseguridad-para-proteccion-de-menores?state=published

Gobierno de México (2021b). Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos. México: Secretaria de Seguridad y Protección Ciudadana/ Guardia Nacional. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/676695/Protocolo_Nacional_Homologado_de_Gestion_de_Incidentes_Ciberneticos.pdf

Hernández, L. (2009). El Delito Informático. Eguzkilore. *Cuaderno del Instituto Vasco de Criminología* Núm. 23 Pág. 227-243

Hernández, R. (2017). Prolegómeno de la informática en la actividad del criminólogo y el criminalista. *Visión Criminológica-criminalística*. pp. 18-27. Disponible en https://revista.cleu.edu.mx/new/descargas/1701/articulos/Articulo07_Polegomeno_de_la_inforormacion_en_la_actividad_del_criminologo_y_el_criminalista.pdf

Herrera, P. (2020). El enfoque de género en la Política Nacional de Ciberseguridad de Chile. Revista chilena de derecho y tecnología, 9(1), 5-31. https://dx.doi.org/10.5354/0719-2584.2020.51577

Herczynsk, P. (2020). *La perspectiva integral de la UE para afrontar las amenazas del ciberespacio*. Ciberseguridad riesgos, avances y el camino a seguir en américa latina y el caribe. Banco Interamericano de Desarrollo/ Organización de los Estados Americanos. Disponible en https://publications.iadb.org/es/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Hikal, W. (2013). *La especialización de la criminología: De lo general a lo específico, ¿hacía una neocriminología? teoría de las criminologías específicas"*, en Derecho y Cambio Social, Año 10, Nº. 32, edición online.

Hikal, W. (2016). *"Las criminologías específicas: de lo general a lo especializado"*, en Anuario Internacional de Criminología y Ciencias Forenses, Nº. 1, 2016, pp. 363-366.

Instituto Nacional de Estadística y Geografía (2020). *Encuesta Nacional sobre Disponibilidad y uso de las TIC en Hogares (ENDUTIH)*. México: INEGI.

Jaishankar, K. (2007). Establishing a theory of cyber crimes. International Journal of Cyber Criminology, 1(2), 3. ISSN: 0974 – 2891

Lima, M. (1984). Delitos Electrónicos en Criminalia. México. *Academia Mexicana de Ciencias Penales*. Porrúa. No. 1-6. Año. pp.100.

López, J. (2020). Iniciativa ciudadana de nueva ley, mediante la cual se expida la "Ley de Ciberseguridad del Estado de San Luis y sus Municipios". México: Gaceta Parlamentaria.

Miró, F. (2011). La oportunidad criminal en el ciberespacio. *Revista Electrónica de Ciencia Penal y Criminología*, 1–55.

McKinsey & Company (2018). *Perspectiva de ciberseguridad en México*. México: Consejo Mexicano de Asuntos Internacionales.

Naciones Unidas (2020). Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. Viena, 10 a 17 de abril de 2000.

Núñez, A., Trujillo, G. y Hackett, L. (2020). *Herramientas de inteligencia colectiva*. México: CIDE.

Naciones Unidas Para El Desarrollo (2022). PNUD. Disponible en https://www.undp.org/es/sustainable-development-goals

Observatorio de delitos informáticos de Latinoamérica (2017). Informe 2017. Disponible en https://www.odila.org/pdf/Informe_ODILA_2017.pdf

OECD (1984). Computer related criminality: analysis of legal policy in the OECD Area, ICCP

Oficina de las Naciones Unidas contra la Droga y el Delito (2013). *Comprehensive Study on Cybercrime*. Nueva York: Naciones Unidas.

Oficina de las Naciones Unidas contra la Droga y el Delito (2015). Clasificación internacional de delitos con fines estadísticos. Viena: Oficina de las Naciones Unidas contra la Droga y el Delito.

Oficina de las Naciones Unidas contra la Droga y el Delito (2020). *Visión estratégica de UNODC para América Latina y el Caribe 2022-2025*. Colombia: UNODC.

Ordaz, D. y Figueroa, J. (2017). *Hacia una criminología contemporánea*. VOX JURIS, Lima (Perú) 33 (1): 113-122.

Organización de los Estados Americanos (2018). *"Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe"*. Disponible en https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Pecoy, M. (2011). Delito en el comercio electrónico. *Prisma Jurídico*. 10 (1), 209-224.

Pérez, F. (2019). *Riesgo cibernético y ciberseguridad. Documento de Trabajo* No. 181. Secretaria de Hacienda y Crédito Público/ Comisión Nacional de Seguros y Fianzas. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/478193/181.- Riesgo Cibern tico y Ciberseguridad 2019.pdf

Recio, K. (2021). Diputados piden a Aldo Fasci fortalecer la policía cibernética de Nuevo León. Milenio. Disponible en: https://www.milenio.com/politica/piden-fasci-fortalecer-policia-cibernetica-leon

Rodríguez, L. (1979). *Criminología*. México, D.F.: Editorial Porrúa

Rojas, E. (2018). *"Una criminología para las redes sociales virtuales"*. [Tesis doctoral, Universidad Autónoma de Nuevo León]. http://eprints.uanl.mx/16006/

Saldaña, Q. (1914), *Los orígenes de la criminología*. Madrid: Victoriano Suárez.

Sancho, C. (2017). Ciberseguridad. Presentación del dossier. URVIO, *Revista Latinoamericana de Estudios de Seguridad,* (20),8-15. ISSN: 1390-3691. Disponible en: https://www.redalyc.org/articulo.oa?id=552656641001

Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (2020). *Modelo óptimo de la función policial diagnóstico nacional sobre las policías preventivas de las entidades federativas*. México: Secretaria de Seguridad y Protección Ciudadana.

Téllez, J. (2008): *Derecho Informático*. 4ª ed. México: Mc Graw Hill

Topinard, P. (1887). L'anthropologie criminelle. Revue d'Anthropologie, 2, 658-691.

Towers, W. (2018). Riesgo Cibernético. Disponible en: https://www.willistowerswatson.com/-/media/WTW/Insights/2018/12/riesgo-cibernetico-2018-wtw.pdf

Tzu, S. (1994). *El arte de la guerra*. USA: Barnes y Noble Inc.

Unión Internacional de Telecomunicaciones (2008). Serie X: Redes de datos, comunicaciones de sistemas abiertos y seguridad. Seguridad en el ciberespacio-Ciberseguridad. Aspectos generales de la ciberseguridad. Ginebra: UIT.

Unión Internacional de Telecomunicaciones (2021). Comunicado de prensa. Disponible en: https://www.itu.int/es/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx

Villalobos, H. (2020). El desarrollo tecnológico en materia policial: una receta de éxito para la prevención del delito. *Revista de Relaciones Internacionales, Estrategia y Seguridad,* 15(1),79-97. ISSN: 1909-3063. Disponible en: https://www.redalyc.org/articulo.oa?id=92764558006

Velázquez, F. (2020). *Estrategia Metropolitana de Ciberprevención*. Consulta pública para el Plan Estratégico

de Nuevo León 2030, rubro Seguridad y Justicia. México: Consejo Nuevo León.

Velázquez, F. (2021). Buscan con semáforo alertar sobre ciberdelitos en Nuevo León. Disponible en: https://vidauniversitaria.uanl.mx/campus-uanl/buscan-con-semaforo-alertar-sobre-ciberdelitos-en-nuevo-leon/

Velázquez, F. y Garza, D., (2020). Justicia restaurativa y trabajo social en el sistema de justicia cívica de Nuevo León. *Trabajo Social y Políticas Sociales*, 7(Año 7), 1522–1537. ISSN: 2395-8456. Disponible en: http://www.coloquio.ftsydh.uanl.mx/index.php/ano-7/

—

Fernando Margarito Velazquez Flores
Afiliación: Universidad Autónoma de Nuevo León, México

Licenciado en Derecho por la Facultad de Derecho y Criminología de la Universidad Autónoma de Nuevo León. Cuenta con dos especialidades: 1) Especialidad en Prevención del Delito por la Universidad de Ciencias de la Seguridad de Nuevo León y, 2) Especialidad en Análisis de la Información por la Universidad de Seguridad y Justicia de Tamaulipas (USJT). Maestreando en Derecho Procesal Penal con estudios en Delitos informáticos en la Universidad Autónoma de Nuevo León y en Desarrollo de Políticas de Seguridad y Justicia por la USJT. Cuenta con 10 años de experiencia en seguridad pública. Ha participado en la construcción de Unidades de Análisis e Inteligencia Policial a nivel municipal. Actualmente se desempeña como consultor en materia de seguridad y justicia. Además, es catedrático nivel licenciatura en la Facultad de Criminología de la UANL donde imparte las materias de Ciberseguridad y Seguridad en Tecnologías de la Información; es miembro Fundador y Coordinador del Laboratorio de Ciberprevención y del Observatorio del Ciberdelito dentro del Centro de Investigaciones de Cibercriminalidad, Derecho Digital y Ciberseguridad de la UA

Dante Octavio Isau Garza Fabela
Afiliación: Universidad Autónoma de Nuevo León, México