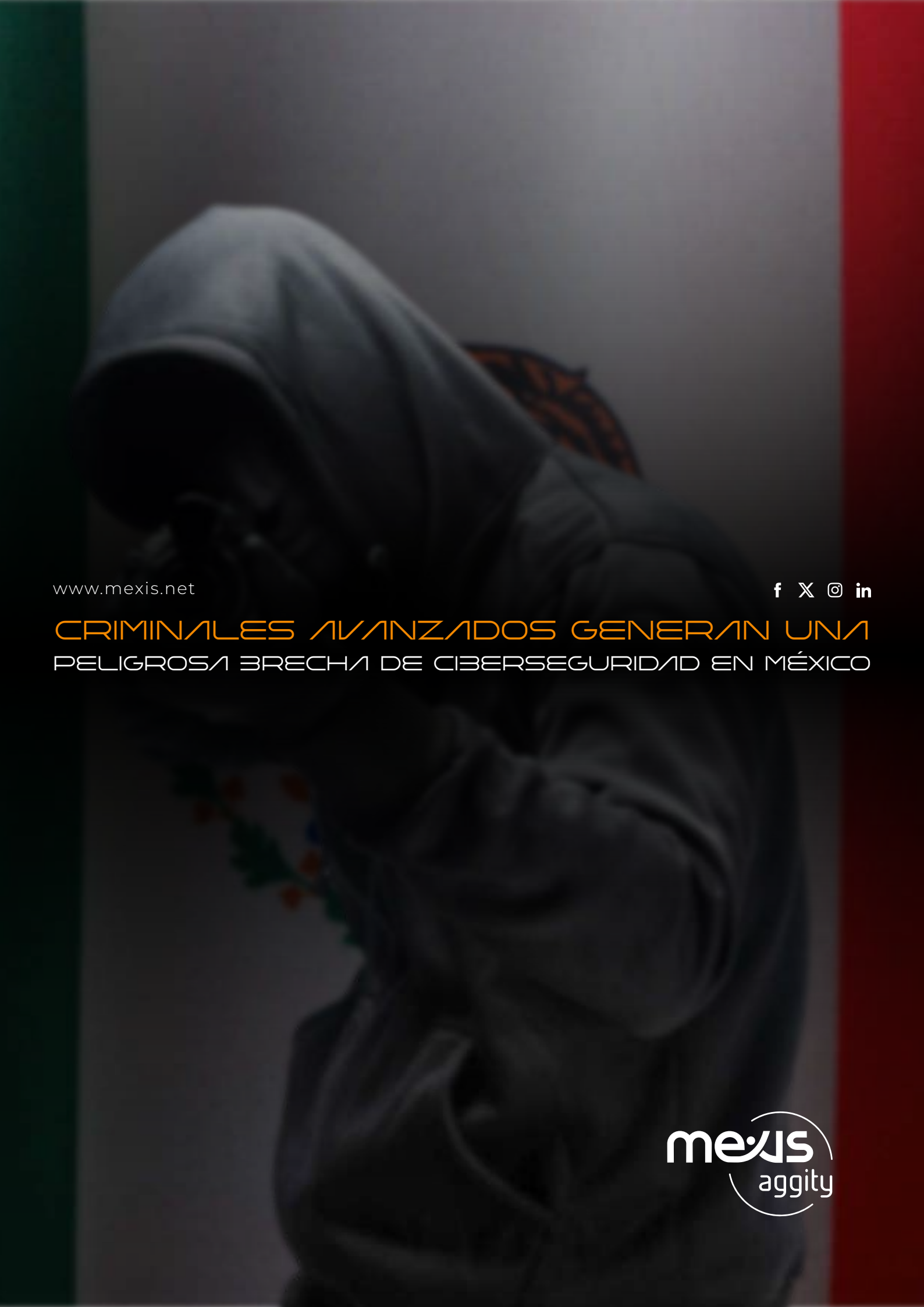
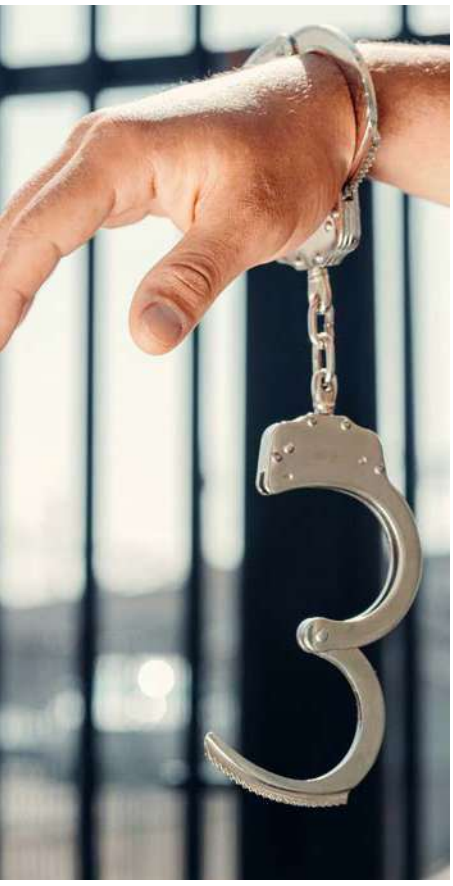


www.mexis.net

CRIMINALES AVANZADOS GENERAN UNA PELIGROSA BRECHA DE CIBERSEGURIDAD EN MÉXICO

mexis aggity



Uno de los retos más complejos que enfrentan las autoridades es lograr que los responsables del cibercrimen comparezcan ante la justicia nacional

Autoridades reactivas y criminales avanzados generan una peligrosa brecha de Ciberseguridad en México.

A menudo se tilda a los ciberatacantes de oportunistas por la manera en que seleccionan a sus víctimas. **Paradójicamente, esta misma calificación puede aplicarse a las autoridades, cuya respuesta ante el cibercrimen ha sido igualmente circunstancial, reactiva y limitada.**

Desde hace años, las acciones gubernamentales en materia de seguridad digital se han centrado casi exclusivamente en sancionar a quienes son sorprendidos en flagrancia cometiendo actividades ilícitas, **dejando de lado la investigación a fondo de las estructuras criminales más complejas y evitando confrontar a los grupos que generan los mayores daños.**

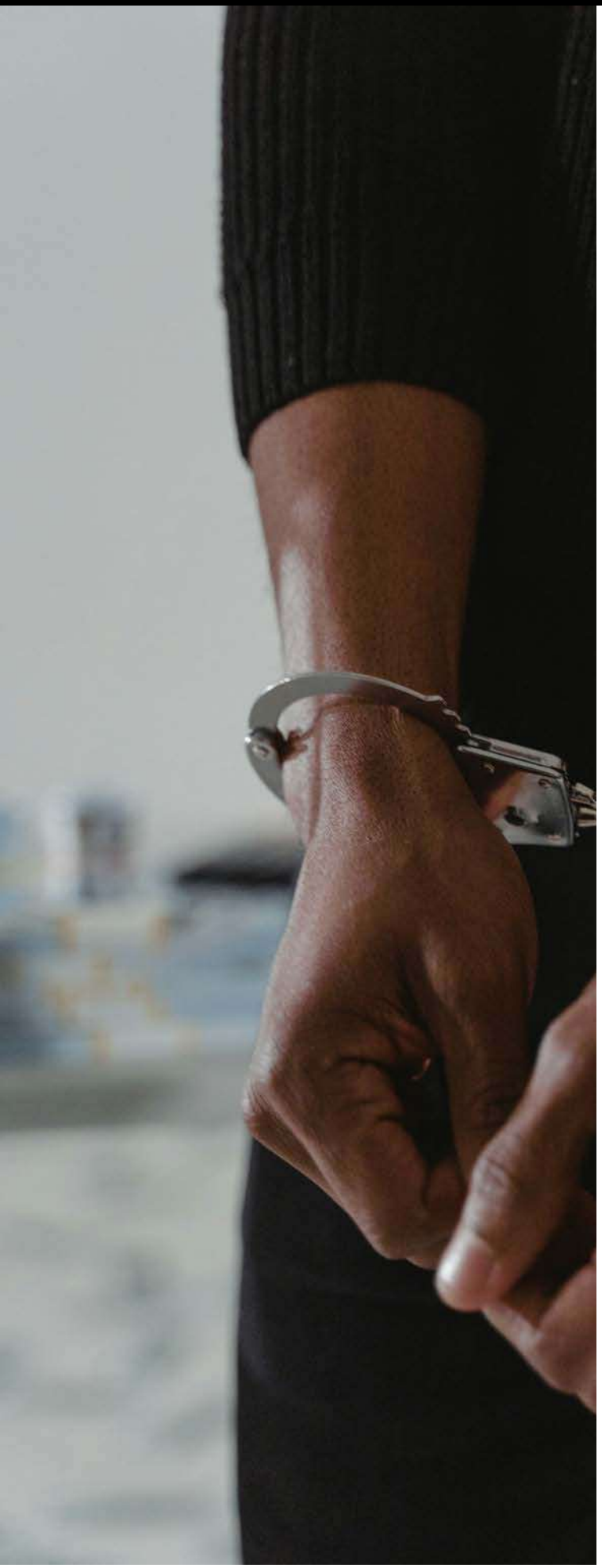
Este enfoque superficial demostró ser claramente inadecuado con la intensificación del cibercrimen durante la pandemia de COVID-19. Ante este panorama, era imperativo que las instituciones mexicanas reorientaran sus esfuerzos, abandonando la visión fragmentada enfocada en actores individuales y priorizando la identificación y desarticulación de figuras clave dentro del ecosistema delictivo, **como los brokers de acceso inicial, quienes facilitan el ingreso a redes comprometidas para múltiples grupos criminales.** Estos intermediarios deberían ser tratados con el mismo rigor que las mafias organizadas y recibir sanciones acordes a su rol central en la cadena delictiva.

En la actualidad, la lucha contra los líderes de bandas cibercriminales exige una estrategia basada en inteligencia estructurada y no en meras declaraciones de buena voluntad. **Sin embargo, la respuesta institucional ha sido débil y fragmentada.**

En los casos en que existen investigaciones, estas no han profundizado lo suficiente ni han partido de la premisa fundamental de que cualquier persona que participe de forma consciente en un grupo delictivo digital ya sea como desarrollador, administrador, afiliado o colaborador debe ser considerada parte de una conspiración criminal, y, en consecuencia, corresponsable de los perjuicios económicos generados, que ascienden a cientos de millones de dólares.

Desde esta perspectiva, **un atacante con apenas una docena de incidentes comprobados podría ser vinculado legalmente a más de 1,400 ciberataques,** simplemente por su rol activo dentro de una organización delictiva estructurada.

En términos generales, **las autoridades mexicanas han mostrado escasa disposición para utilizar, en toda su amplitud, las herramientas legales ya existentes, como las disposiciones contra el crimen organizado, en su combate al cibercrimen.** A día de hoy, el país sigue careciendo de un marco jurídico que permita sancionar penalmente cualquier actividad realizada en el contexto de una organización criminal activa. Esta omisión legal es particularmente preocupante si se considera que **un afiliado que emplea ransomware de una pandilla cibernética y canaliza parte de sus ganancias hacia dicha agrupación** cumple, sin duda, con los criterios de pertenencia a una estructura criminal, y por tanto, debería ser investigado, detenido y procesado.



Es frecuente que quienes participan en este tipo de delitos intenten minimizar su responsabilidad, argumentando que solo tuvieron una participación marginal. Sin embargo, el ransomware se ha consolidado como una amenaza grave, persistente y sumamente destructiva. **Mientras el Estado mexicano no emplee todas las herramientas legales a su alcance, será cada vez más difícil contener esta modalidad delictiva.**

Asimismo, resulta evidente que el Estado mexicano no ha explorado a fondo el uso creativo y expansivo de su marco legal actual para adaptarlo al fenómeno delictivo digital, **lo que ha creado vacíos normativos que terminan beneficiando a los agresores.**

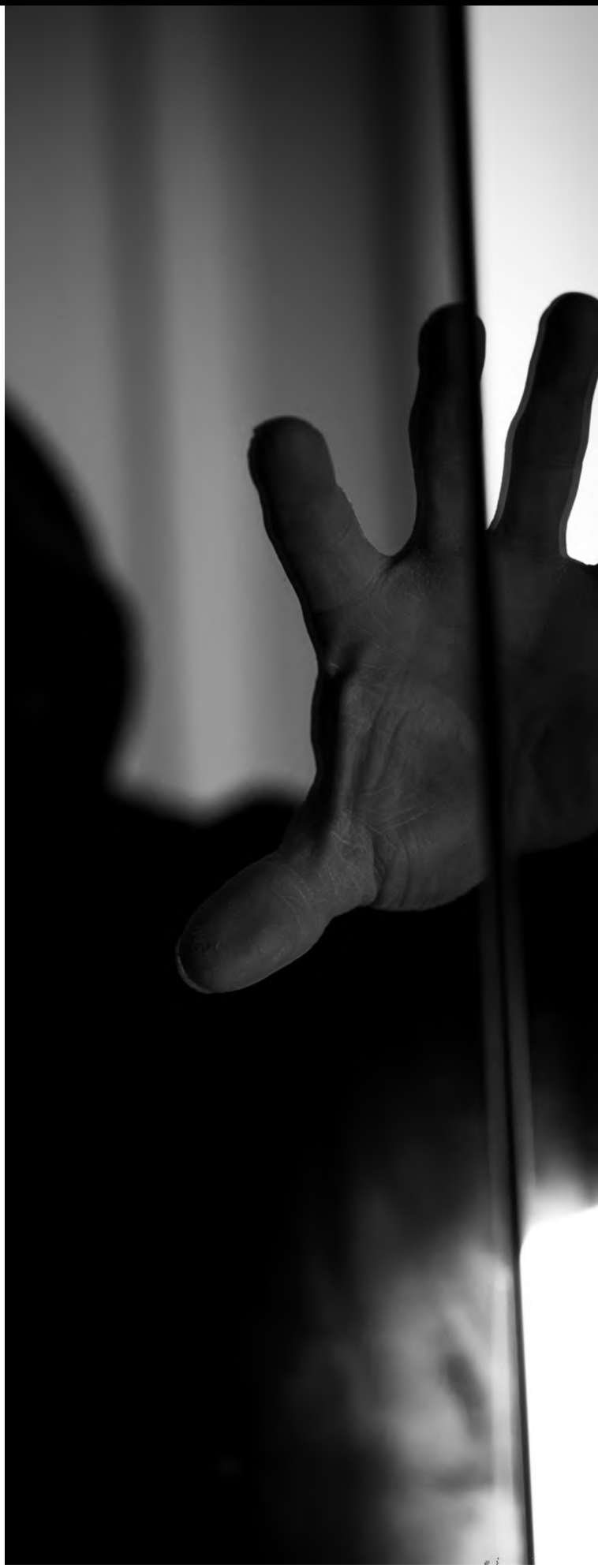
Uno de los retos más complejos que enfrentan las autoridades es lograr que los responsables del cibercrimen comparezcan ante la justicia nacional. **Incluso en los casos en que los delincuentes se encuentran en países aliados, la falta de mecanismos sólidos y protocolos de cooperación internacional obstaculiza seriamente la colaboración jurídica.** Aunado a ello, no basta con reformas legales; se requiere una inversión sustancial en infraestructura logística, talento especializado y capacidades operativas para abordar estos casos con eficacia.

A este panorama se suma un desafío adicional: la marcada disparidad entre las leyes sobre cibercrimen a nivel internacional. En muchos países, para que proceda una extradición, el delito imputado debe estar igualmente tipificado en la legislación del país donde se encuentra el acusado, lo que limita seriamente las posibilidades de procesar judicialmente a los responsables.

Aunque la extradición no siempre sea viable, México sí podría impulsar acciones legales que restrinjan la movilidad internacional de los atacantes, bloqueen sus flujos económicos y debiliten su capacidad operativa y de cooperación con otros actores delictivos. **No obstante, para que esto suceda, es indispensable contar con una legislación de ciberseguridad clara**, robusta y con mecanismos efectivos de colaboración entre el gobierno, el sector privado y actores internacionales. Lamentablemente, esas condiciones aún no están presentes en el país.

México enfrenta desafíos significativos en su lucha contra el cibercrimen, debido tanto a la ausencia de un marco legal integral como a las limitaciones de sus capacidades institucionales. En el primer semestre de 2024, el país fue el objetivo del 55% de los ciberataques reportados en América Latina, con más de 31 mil millones de intentos registrados.

Estas amenazas que incluyen desde ransomware y phishing hasta prácticas de extorsión han golpeado con fuerza a instituciones gubernamentales y sectores estratégicos como el financiero, comercial e industrial, generando pérdidas económicas que superan los 40 millones de dólares. La cercanía económica con Estados Unidos, combinada con una digitalización acelerada que se sustenta en infraestructura tecnológica obsoleta, ha convertido a México en un blanco atractivo para el crimen cibernético.



Aunque se han implementado algunas medidas, como la creación de nuevas dependencias especializadas, **estas acciones resultan insuficientes frente a una amenaza que evoluciona rápidamente. Grupos criminales, entre ellos cárteles como el Cártel Jalisco Nueva Generación (CJNG), han incorporado tecnologías sofisticadas** como deepfakes, criptomonedas y métodos avanzados de anonimato para operar sin ser detectados. Un ejemplo representativo es el caso **Inferno Leaks, ocurrido en febrero de 2025**, cuando un grupo de hackers puso a la venta 701 gigabytes de datos sensibles en la dark web. **Sin un marco normativo sólido que respalde adecuadamente la investigación y el castigo de este tipo de delitos, los esfuerzos continúan siendo ineficaces.**

La Estrategia Nacional de Ciberseguridad de 2017 fue prácticamente ignorada durante el sexenio del expresidente Andrés Manuel López Obrador. Y si bien la actual mandataria, Claudia Sheinbaum, ha anunciado la creación de un centro de ciberseguridad e inteligencia artificial, hasta el momento no ha propuesto una ley concreta en la materia. **Se estima que una legislación en ciberseguridad podría aprobarse en uno o dos años;** sin embargo, mientras tanto, la falta de coordinación institucional y los recursos limitados seguirán entorpeciendo cualquier intento de respuesta efectiva.

Por otro lado, la legislación vigente como **el Código Penal Federal contempla sanciones para delitos como el fraude informático o la alteración de datos, pero sus alcances se limitan al ámbito nacional y no contemplan excepciones para prácticas como el hacking malicioso.** Esta rigidez legal complica aún más la cooperación internacional, ya que la falta de homologación normativa entre países dificulta los procesos de extradición de cibercriminales.

En contraste, en otras regiones del mundo se han logrado avances, aunque modestos, en la contención de ataques y en la reducción de pagos por ransomware. Estos progresos han sido posibles gracias a los esfuerzos coordinados de agencias como Interpol, Europol y el FBI, que han conseguido identificar, arrestar, procesar y visibilizar públicamente a cibercriminales en todos los niveles, además de congelar sus activos financieros y lanzar campañas de desprestigio digital. **Aunque estas medidas no resuelven el problema de fondo, establecen un precedente importante para que las sanciones sean ejemplares y disuasivas.**

México enfrenta un panorama de creciente sofisticación en el ámbito del cibercrimen. No obstante, la ausencia de un marco legal robusto, la insuficiencia de recursos institucionales y la constante evolución tecnológica de los atacantes siguen representando obstáculos críticos para avanzar hacia una protección efectiva del país frente a estas amenazas.

Fuente de información: www.infobae.com
Autor: Víctor Ruiz