PERIÓDICO	PÁGINA	FECHA	SECCIÓN
Reporte Indigo / Cinco Días	1, 12 - 15	08/11/2022	LEGISLATIVO

UNA AMENAZA REAL

La falta de una ley de ciberseguridad, de acuerdos y colaboración internacional, de inversión y de personal capacitado, ha ocasionado que México sea el país que más ciberataques recibe en Latinoamérica, una situación que se podría agravar si no se garantiza la seguridad de la infraestructura crítica

12

PERIÓDICO	PÁGINA	FECHA	SECCIÓN
Reporte Indigo Cinco Días	1, 12 - 15	08/11/2022	LEGISLATIVO

#Ciberseguridad

UNA AMENAZA REAL

La falta de una ley de ciberseguridad, de acuerdos y colaboración internacional, de inversión y de personal capacitado, ha ocasionado que México sea el país que más ciberataques recibe en Latinoamérica, una situación que se podría agravar si no se garantiza la seguridad de la infraestructura crítica

POR RUBÉN ZERMEÑO
Y JULIO RAMÍREZ
@RubenZermeno
y @julio_ramga

Especialistas en ciberseguridad en América Latina advierten que además de que México es el país más atacado en la región, los esfuerzos de las autoridades federales, legisladores y de la iniciativa privada para mitigar y frenar estas amenazas son mínimos.

La falta de inversión, de políticas públicas, de la firma de tratados internacionales y de personal capacitado, ha ocasionado un caldo de cultivo para que las amenazas digitales crezcan, ya que varias de las herramientas que fueron utilizadas en los ciberataques contra Ucrania durante este año, ya se encuentran en México y podrían caer en manos de los grupos criminales.

Ante este escenario, los especialistas consultados por Reporte Índigo, recomiendan a las autoridades y a la iniciativa privada, invertir más en ciberseguridad, tomarse el problema como una amenaza latente y fomentar desde las escuelas y en las nuevas generaciones la cultura de la ciberseguridad.

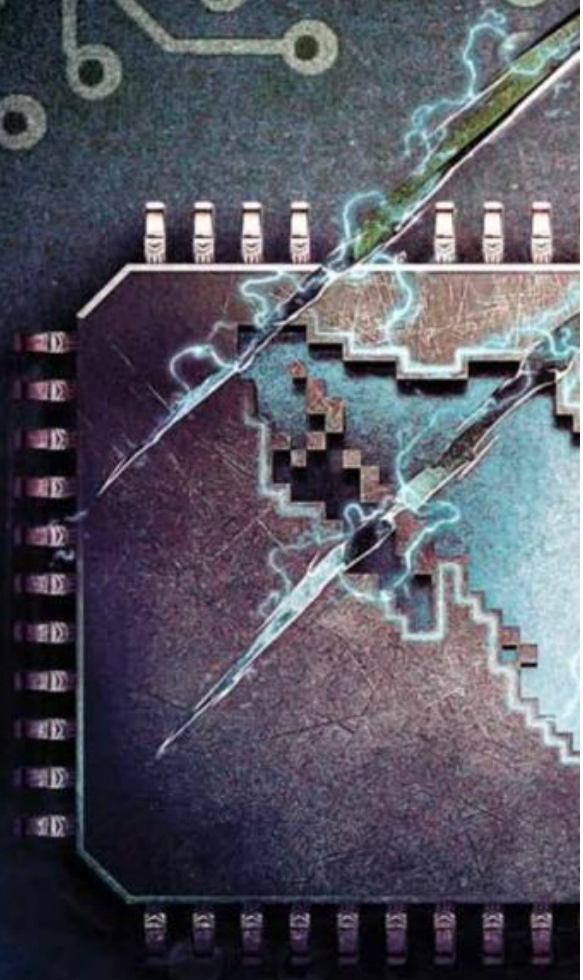
Aunado a esto, urgen a los legisladores federales a expedir cuanto antes la tan necesitada Ley de Ciberseguridad.

Actualmente en el Congreso de la Unión hay seis iniciativas de Ley de Ciberseguridad, sin embargo, ninguna ha sido discutida ni aprobada.

En la Cámara baja se han presentado este año iniciativas al respecto la diputada María Eugenia Hernández (junio) y los diputados Javier Salinas Narváez (octubre) y Javier López Casarín (noviembre).

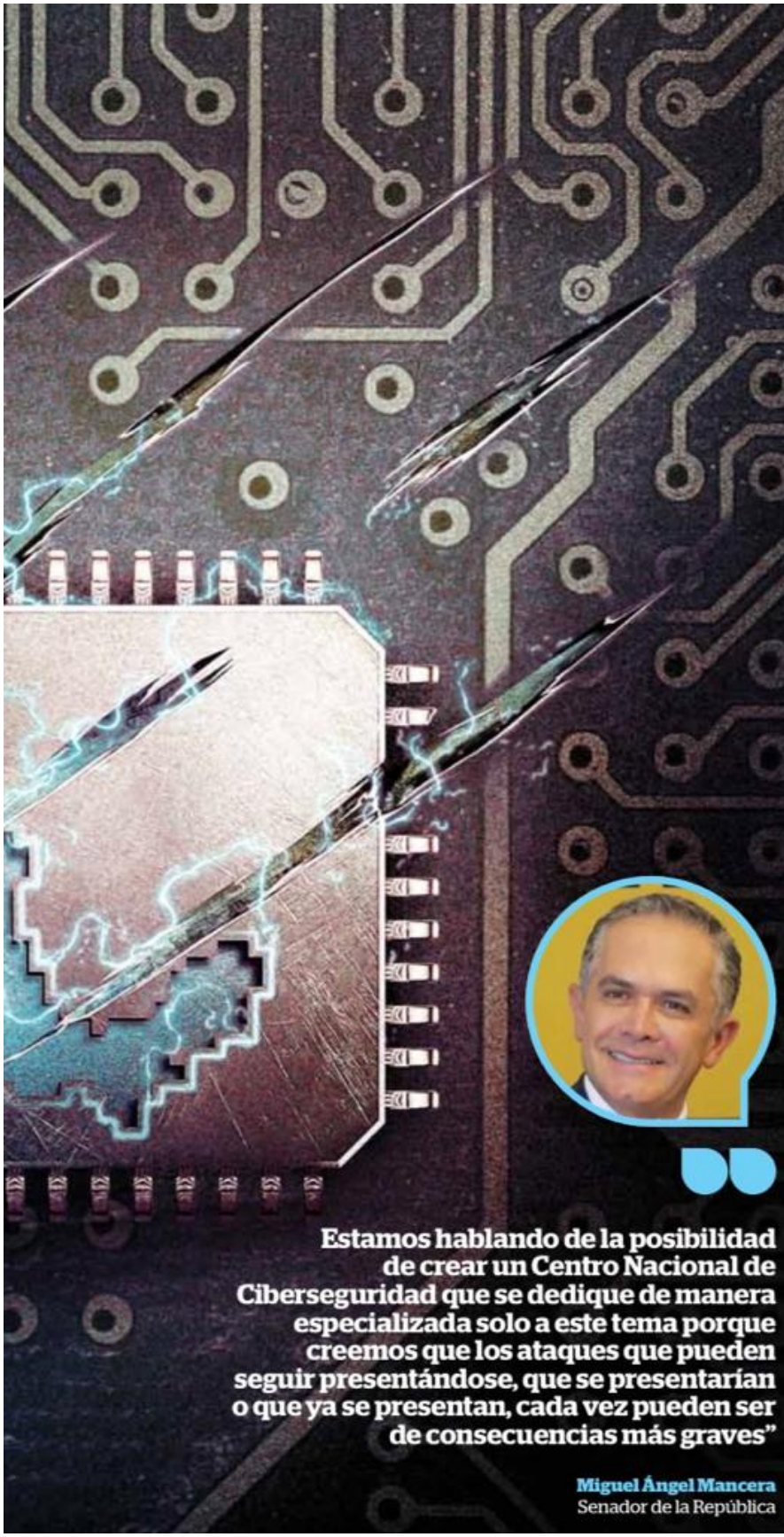
En el Senado de la República lo han hecho las senadoras Alejandra Lagunes Soto (mayo), Jesús Lucía Trasviña Waldernath (mayo) y el perredista Miguel Ángel Mancera (septiembre).

A pesar de que todas estas iniciativas se encuentran congeladas, el exjefe de Gobierno capitalino dice que la Ley de Ciberseguridad se expedirá pronto, estará basada en el artículo sexto de la Constitución y tendrá impacto en varias dependencias



Además del parlamento abierto en el camino a una legislación adecuada, se busca que se hagan definiciones generales, ya que se corre el riesgo de que se requieran actualizaciones al tratarse de una materia que se desarrolla rápidamente

PERIÓDICO	PÁGINA	FECHA	SECCIÓN
Reporte Indigo / Cinco Días	1, 12 - 15	08/11/2022	LEGISLATIVO



y órganos autónomos, pero antes se discutirá en parlamento abierto.

"Es el artículo (sexto) el que se ocupa de todo esto que tiene que ver con la comunicación, con la información, con los servicios de radiodifusión y telecomunicación, el tema de la banda ancha. Entonces, lo hacemos como una ley reglamentaria de este artículo sexto constitucional y de ahí partimos a decir que es de observancia general en todo el territorio para los efectos de su aplicación", expone el senador.

Aunque falta tiempo para su discusión, se trata de un proyecto de ley que tiene que ser amplio e impactar en el sector privado.

"Un enfoque es a la ciberseguridad estatal, pero el enfoque mismo de la ciberseguridad, por ser la ley única, tendrá que ocuparse de todo. Al menos en la concepción que tenemos ahora. No sé si va a ser así, no sé si se va a lograr, pero lo que hoy yo considero y me gustaría escuchar opiniones de ustedes, es que se debe intentar, se debe intentar, debemos intentar hacerlo", dice Mancera.

En su conferencia en la Cumbre de Ciberseguridad 2022 de la empresa Fortinet, el exjefe de Gobierno consideró que la discusión está en un punto de arranque en el Poder Legislativo y que si bien el ataque del Grupo Guacamayas originó que se discuta más rápido, lo ideal es construir una buena Ley de Ciberseguridad.

Mancera habló primero de que se debe constituir una Ley General al respecto, pues se proyecta crear el Centro Nacional de Ciberseguridad como una instancia que apoye a varias dependencias del sector público en este sector.

"Estamos hablando de la posibilidad de crear un Centro Nacional de Ciberseguridad, un centro que se dedique de manera especializada solo a este tema porque creemos que los ataques que pueden seguir presentándose, que se presentarían o que ya se presentan, cada vez pueden ser de consecuencias más graves, más costosas y, por supuesto, más delicadas", expresó.

"Creemos que es importante que se le dé relevancia. Si lo adscribes nada más a un área, vamos a parar exactamente en lo que hoy tenemos", alertó el legislador.

Además del parlamento abierto, en el camino a una legislación adecuada, se busca que se hagan definiciones generales, ya que se corre el riesgo de que se requieran actualizaciones al tratarse de una materia que se desarrolla rápidamente.

En el Congreso de la Unión hay seis iniciativas de Ley de Ciberseguridad, sin embargo, ninguna ha sido discutida ni aprobada a pesar de su importancia

"Vamos a hacer un planteamiento de algunos conceptos que pudieran estar definidos de manera general. Por ejemplo, hay una maestría que se está dando en Nuevo León de ciberseguridad, he visto varios anuncios de diplomados en ciberseguridad y me imagino que debemos tener esas informaciones generales de dónde partir. Esto es lo que quisiéramos aterrizar primero en la ley, en esas partes y en esas definiciones generales".

Explicó que la legislación está en proceso desde 2020 y ahora que se reavivó el tema es indispensable revisar qué se le adhiere al documento.

'Avance lento'

Sobre las iniciativas presentadas y "congeladas" en el Congreso de la Unión, el director general de Fortinent México, Eduardo Zamora, alerta que la Ley de Ciberseguridad avanza lento.

El experto en la materia dice que las propuestas de los legisladores son muy diversas y no se han puesto de acuerdo.

Además expone que en administraciones pasadas se lograron avances en la materia como la Ley de Protección de Datos Personales, pero en el actual sexenio no se ha logrado materializar la tan anhelada ley.

"Actualmente el panorama es distinto debido a que los ataques cibernéticos son cada vez más sofisticados y la legislación que existe no es acorde a los nuevos retos (...) Mientras no se den las condiciones para que en breve se tenga una ley, la vulnerabilidad del Estado continuará latente y se seguirán registrando más incidentes cibernéticos", alerta.

Estamos hablando de la posibilidad de crear un Centro Nacional de Ciberseguridad que se dedique de manera especializada solo a este tema porque creemos que los ataques que pueden seguir presentándose, que se presentarían o que ya se presentan, cada vez pueden ser de consecuencias más graves"

Miguel Ángel Mancera
Senador de la República

ILUSTRACIÓN: JESÚS MARTÍNEZ

PERIÓDICO	PÁGINA	FECHA	SECCIÓN
Reporte Indigo Cinco Días	1, 12 - 15	08/11/2022	LEGISLATIVO

BAJO ATAQUE

Las endebles defensas de México en materia de ciberseguridad lo ha dejado expuesto a múltiples agresiones, las cuales seguirán aumentando hasta que no se tomen medidas legislativas, económicas y culturales para hacer frente al problema

FOTO CUARTOSCURO

De acuerdo con el Informe "Fortiguard Labs Primer Semestre 2022" de la empresa de ciberseguridad Fortinet, en México se detectaron 85 mil millones de intentos de ciberataques de enero a junio de este año.

Las amenazas tuvieron un aumento del 40 por ciento con respecto al mismo periodo del año pasado, cuando se detectaron 60 mil millones.

México es el país más amenazado de la región, ya que en el 62 por ciento de los posibles ataques en América Latina (137 mil millones), el blanco fue nuestro país.

La amenaza más grave fue el ransomware (secuestro de datos). A nivel mundial Fortinet detectó aproximadamente 384 mil intentos de distribución de softwares dañinos, en América Latina fueron 52 mil y en México 18 mil detecciones.

En promedio, 1 de cada 20 intentos de secuestros de datos a nivel mundial ocurre en México.

La lluvia de ataques y amenazas no solamente está dirigida a la iniciativa privada, también a las dependencias del Gobierno.

El 25 de octubre pasado, la Secretaría de Comunicaciones y Transportes se unió a la lista de instituciones del Gobierno que han sufrido la vulneración de sus sistemas, por lo que informó que activó el Protocolo Nacional Homologado de Gestión de incidentes Cibernéticos para intentar mitigar los efectos de la infección en 110 de sus equipos de un virus tipo ransomware.

Entre las secretarías e instituciones violentadas se encuentran la Secretaría de la Defensa Nacional, Petróleos Mexicanos, la Lotería Nacional, el Instituto Mexicano del Seguro Social, Bancomext, el SAT, la Secretaría de Economía y la Comisión Federal de Electricidad.

Sobre esta situación, el director general de Fortinet México, Eduardo Zamora, alerta que los ataques seguirán aumentando, ya que cada vez son más masivos, más sofisticados y los cibercriminales utilizan tecnología propia.

"Nuestro Gobierno no solo está en pañales, está un paso atrás, muy lejos de donde deberíamos de estar. Debemos cuidar la infraestructura crítica (telecomunicaciones y servicios básicos) porque si las instituciones no se preparan, en poco tiempo van a estar en problemas. (...) También se debe de asignar presupuesto con visiones a tres o cinco años porque la ciberseguridad es algo que se debe estar actualizando" opina.

En promedio 1 de cada 20 intentos de secuestros de datos a nivel mundial ocurre en México

"Nuestro Gobierno no solo está en pañales, está un paso atrás, muy lejos de donde deberíamos de estar. Debemos cuidar la infraestructura crítica porque si las instituciones no se preparan, en poco tiempo van a estar en problemas"

Eduardo Zamora
Director general de Fortinet México

Educación y profesionalización

En Latinoamérica hacen falta cubrir 700 mil puestos de expertos en ciberseguridad, afirma Jaime Chanagá, Field Chief Information Security Officer (CISO) para Fortinet Latinoamérica, el Caribe y Canadá.

"A nivel mundial, el Foro Económico Mundial ha determinado que hay una brecha de talento de más de tres millones y medio de profesionales en ciberseguridad que se necesitan. En América Latina tenemos una brecha de talento de 701 mil profesionales que no existen en el mercado.

"Las vacantes están ahí, los sectores de industria necesitan, los gobiernos necesitan especialistas con entrenamiento técnico y profesional, y no existe ese talento en este momento", explica Jaime Chanagá.

Por su parte, Arturo Torres, coordinador de la Maestría de Seguridad de la Información y docente de la Licenciatura de Seguridad y Tecnologías de la Información en la Universidad Autónoma de Nuevo León, dice que se deben mejorar los programas y seguir formando gente profesional.

"Como docente no me gusta decir que no existen profesionales, porque hemos creado a nuevos profesionales que inclusive ya trabajan a nivel internacional, pero el uso constante de la tecnología demanda que las organizaciones requieran más profesionales. No significa que no existan, pero la industria los está demandando, es importante tener un plan de estudios sólido entregado por profesionales", comenta.

PERIÓDICO	PÁGINA	FECHA	SECCIÓN
Reporte Indigo Cinco Días	1, 12 - 15	08/11/2022	LEGISLATIVO

DE UCRANIA A MÉXICO

Los conflictos bélicos aumentan la creación de tecnologías diseñadas para dañar gobiernos, muchas de las cuales no están reguladas y se pueden adquirir por otras organizaciones criminales a través del mercado negro

"El internet y las cibercomunicaciones abren fronteras, pero también les abre las puertas a los grupos delictivos"

Arturo Torres
Estratega de Seguridad de FortiGuard Labs

Arturo Torres es estratega de Seguridad de FortiGuard Labs, el área que se encarga de la investigación y el desarrollo contra amenazas.

Todos los días monitorea la cantidad de ataques con el objetivo de enfrentar a los criminales, analizar las tendencias en sus delitos y así crear estrategias defensivas.

Además, la oficina donde labora colabora con 400 agencias de inteligencia a nivel mundial y forma parte medular del Foro Económico Mundial.

"El internet y las cibercomunicaciones abren fronteras, pero también les abre las puertas a los grupos delictivos.

"Para entender el problema es importante clasificar las amenazas: tenemos a los cibercriminales que buscan remuneración económica a través de actividades delictivas; a los ciberterroristas, cuyo objetivo es afectar a un país con un fin político; y finalmente a los hacktivistas, que buscan probar algún punto por alguna ideología. Los tres los hemos visto y operan en América Latina y en México", explica.

En el caso de los cibercriminales, el especialista señala que varias bandas internacionales residen en México y las han logrado detectar gracias a los modelos que utilizan de ransomware y malware.

En cuanto a los terroristas, revela que han detectado en México amenazas y artefactos que se utilizaron en el conflicto entre Rusia y Ucrania.

"Muchos de estos conflictos geopolíticos que pasan al otro lado del mundo generan artefactos maliciosos con el objetivo de destruir sistemas operativos y afectar estructuras críticas como la luz eléctrica, que sería un duro golpe para la economía.

"Estos artefactos que se salieron de control ya se encuentran en el mercado negro y la darkweb. En nuestro monitoreo detectamos especialmente en México estos artefactos destructivos que se crearon para el conflicto de Ucrania. Los hemos visto, no hemos tenido reportes de que hayan destruido alguna estructura crítica, pero podría haber algún incidente", alerta.

Finalmente, el especialista comenta que el país necesita blindarse, comunicarse y colaborar.

"La motivación de estos grupos va a aumentar, se hablan todos los días y nosotros debemos hacer lo mismo, crear comunidad para protegernos", finaliza.

Varias bandas internacionales de cibercriminales residen en México y las han logrado detectar gracias a los modelos que utilizan de ransomware y malware