

La ciberseguridad en México, ¿una necesidad?

Autor: Patricio Garza | Lunes, 16 de agosto de 2021

En México, como en otros países de América Latina, la adopción del internet sigue creciendo. Actualmente, hay 80.6 millones de usuarios de internet en el país, así como 86.5 millones de usuarios de teléfonos celulares, lo que ha hecho posible la creciente interacción que vemos hoy en día entre individuos, así como entre gobierno y población. Sin embargo, en este contexto, los riesgos y amenazas también han aumentado en número y frecuencia, y han hecho más vulnerables a las personas que llevan a cabo actividades en el ciberespacio. Aun así, no existe una estrategia en el país para atender los retos que representa una mayor dependencia de la tecnología.



Imagen: Pixabay

La pandemia por el COVID-19 trajo consigo cambios radicales en el modo de vida de las personas y en las economías a nivel global. Dentro de ellos, destaca el acelerado aumento en el uso de las tecnologías de la información y la comunicación (TIC) para realizar diversas actividades cotidianas. La tecnología ya no es una opción, sino que se ha convertido

en una necesidad. Herramientas como Zoom, Google, Dropbox, entre otras, están siendo cada vez más utilizadas para llevar a cabo reuniones con amigos o familiares a la distancia y se han convertido en modelos de trabajo para que las organizaciones puedan funcionar evitando la proximidad y la interacción física.

Los riesgos para México

En México, como en otros países de la región, la adopción del internet sigue creciendo. Actualmente, existen 80.6 millones de usuarios de internet y 86.5 millones de usuarios de teléfonos celulares, de acuerdo con datos del Instituto Nacional de Estadística y Geografía (Inegi)¹. Este incremento ha hecho posible la creciente interacción que vemos hoy en día entre individuos, así como entre el gobierno y la población. No obstante, en este contexto, los riesgos y amenazas también han incrementado en número y frecuencia, haciendo más vulnerables a las personas que llevan a cabo actividades en el ciberespacio.

El término “cibercrimen” hace referencia a toda la actividad delictiva que se realiza en línea, a través de una computadora o dispositivo. Estos delitos derivan del incremento del acceso a internet, lo que ha propiciado nuevos actos de extorsión, vigilancia masiva, filtración de datos, espionaje y robos económicos o de información personal.

Casos como la investigación realizada sobre Pegasus han puesto en evidencia cuán vulnerables somos ante este tipo de ataques. Pero, más allá de Pegasus, desde hace algunos años se sabe que nuestro país se encuentra dentro de los primeros lugares a nivel mundial en ciberdelitos: en 2015, México ocupó el tercer lugar, sólo China y Sudáfrica lo superaban.

Ante esto, la Cámara de Diputados exhortó ese año a distintas dependencias de gobierno a informar sobre los resultados en materia de seguridad cibernética y pidió a la Secretaría

de Relaciones Exteriores dar a conocer su posición respecto a la adhesión de México al Convenio de Budapest sobre ciberdelincuencia. Desde entonces, tanto diputados como senadores han señalado en distintas ocasiones la necesidad de suscribir este instrumento internacional, pero la respuesta ha sido que se continúa evaluando la situación².

Dicho convenio es el único tratado internacional que busca hacer frente a delitos informáticos mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones que lo suscriben. Países de América Latina como Chile, Perú, Colombia y Argentina ya forman parte de este convenio, pero México continúa siendo un gran ausente hasta la fecha, ya que únicamente cuenta con estatus de país observador.

De acuerdo con el Módulo sobre Ciberacoso del Inegi, en 2020, 21% de la población mexicana de 12 años y más (16.1 millones de personas) que utilizó internet fue víctima de ciberacoso en algún momento del año. De esta población, únicamente el 9.7%, en el caso de los hombres, y el 11.4%, en el caso de las mujeres, denunciaron el acoso ante el Ministerio Público, la policía o el proveedor del servicio³. También, de acuerdo con el último Sondeo de Seguridad Empresarial, de la American Chamber of Commerce (AmCham) en México, el 80% de las empresas en el país consideró que la seguridad de la información es una prioridad alta. No obstante, el 74% declaró que no recibe o no sabe de ningún apoyo que ofrezca el gobierno en caso de un incidente o ataque relacionado con la ciberseguridad⁴. Estos datos son un reflejo de que no existe vinculación entre sociedad, empresas y gobierno en materia de ciberseguridad.

Las consecuencias del cibercrimen pueden llegar a ser devastadoras. En México, se estima que estos delitos tienen costos de 3 a 5 billones de dólares al año.



Foto: Pixabay

Los aciertos en ciberseguridad

En 2017, el gobierno de Enrique Peña Nieto planteó una propuesta para el desarrollo de una Estrategia Nacional de Ciberseguridad⁵. A pesar de que la propuesta carecía de elementos importantes, como una mayor vinculación entre el gobierno y los distintos sectores de la población, incluyendo a las empresas, fue un primer paso para comenzar a posicionar el tema en la agenda de gobierno. Sin embargo, dicha estrategia no logró convertirse en un documento vinculante y menos en una verdadera política de Estado.

Asimismo, en materia de protección de datos, México cuenta con dos legislaciones separadas: una para el uso de bases de datos públicas y otra para bases de datos privadas. Este marco legal, funciona para regular a particulares y dependencias de gobierno en el uso de los datos personales de sus clientes o beneficiarios. Por un lado, estas leyes no garantizan la seguridad de la información de los datos contenidos en los dispositivos que se utilizan para acceder a internet y realizar actividades. Por otro lado, México no cuenta con una ley dedicada a la ciberseguridad, que abarca más aspectos de todo el ciberespacio y no únicamente los datos contenidos en un dispositivo. Así, las disposiciones existentes en los códigos penales son limitadas y dejan lagunas que dificultan la lucha contra el cibercrimen.

En México existen instituciones encargadas de la seguridad que cuentan con áreas específicas para la atención de los ciberdelitos. Un ejemplo de ello es la Dirección Científica de la Guardia Nacional. También a nivel local, como es el caso del Estado de México, en donde la Secretaría de Seguridad cuenta con una Policía Cibernética encargada de prevenir y atender los delitos cibernéticos. Sin embargo, la falta de un marco legal que sirva para coordinar las actividades de las dependencias y que establezca las bases bajo las cuales se debe actuar en los distintos casos ocasiona que los esfuerzos sean aislados y se diluyan. En 2020, la Cámara de Diputados anunció que ya estaba en discusión una ley para la ciberseguridad, pero hasta la fecha no se ha logrado sacar adelante dicha legislación.

Recomendaciones para México

En reconocimiento a los riesgos del ciberespacio, de acuerdo con la Organización de los Estados Americanos (OEA),

La baja confianza que existe en las autoridades para atender con eficacia el cibercrimen es producto de la falta de una estrategia integral.

a la fecha, 11 países en América Latina han desarrollado una Estrategia Nacional de Ciberseguridad⁶. Argentina, Colombia, Perú y Uruguay, entre otros, han diseñado planes integrales de gobierno en esta materia, como respuesta a los desafíos que plantea regular las actividades digitales sin vulnerar el derecho de las personas a utilizarlas libremente. Estos países han sido acompañados por organizaciones internacionales como la OEA y el Banco Interamericano de Desarrollo (BID) para la creación de sus estrategias, las cuales a su vez se han acompañado de instituciones como la Universidad de Oxford para la correcta implementación de modelos referentes para el desarrollo de una estrategia. En México, es necesario retomar esta discusión e insertarse en el contexto global bajo el cual se están llevando a cabo estas acciones. La inactividad podría traer grandes consecuencias a futuro y nuestro país podría quedarse fuera del proceso.

Asimismo, la adhesión de México a instrumentos internacionales como el Convenio de Budapest sobre ciberdelincuencia es importante para comenzar a tomar mayores acciones en la materia. El intercambio de experiencias a nivel internacional, que forma parte de dicho acuerdo, será una herramienta fundamental para cualquier gobierno que desee fortalecer sus capacidades en ciberseguridad. Por último, es necesario que los legisladores mexicanos den el primer paso con la creación de una ley de ciberseguridad lo suficientemente vinculante para hacer frente a las amenazas.

Referencias:

¹ <https://www.inegi.org.mx/programas/dutih/2019/>

² <http://comunicacion.senado.gob.mx/index.php/informacion/boletines/50022-urgencia-la-sre-concluir-la-adhesion-al-convenio-sobre-ciberdelincuencia.html>; http://sil.gobernacion.gob.mx/Archivos/Documentos/2015/08/asun_3259899_20150814_1439577327.pdf

³ https://www.inegi.org.mx/contenidos/programas/mociba/2020/doc/mociba2020_resultados.pdf

⁴ <https://www.amcham.org.mx/sites/default/files/publications/SondeoSeguridadEmpresarial2018.pdf>

⁵ https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

⁶ <http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp>

Con la colaboración de:

Hans Blomeier, representante de la KAS en México

Laura Philipps, representante adjunta

Patricio Garza, gerente de Proyectos

Jatziry Herrera, gerente de Comunicación

www.kas.de/mexiko

kasmex@kas.de

Síguenos en nuestras redes sociales:

