El Estado de la Ciberseguridad en México

Autor: Daniel Villanueva Plasencia
Asociado Senior de Baker Mckenzie Abogados

En un mundo en donde se dice que los datos son el nuevo petróleo, debiera ser lógico que se busque proteger los datos de la misma manera en la que se protege al petróleo. Sin embargo, eso no es necesariamente la realidad, ya que, si bien en México tenemos algunas disposiciones, por aquí y por allá, no hay un marco legal claro ni suficiente para cubrir las necesidades de las personas y empresas en nuestro país. Este debe ser un tema que apremie, ya que según la publicación *Cyberthreat Defense Report 2022*[1], México se encuentra en los primeros lugares de países que reciben más ataques en mundo, lo cual incrementa considerablemente los riesgos de llegar a perder ese preciado petróleo que son los datos de las empresas. Según esta publicación casi la mitad de las empresas consultadas en México admitió haber sido víctima de un ataque de *ransomware* en el último año, y desgraciadamente no parece que estas cifras vayan a disminuir, ya que la creación continua de nuevos datos y dependencia de las empresas en los mismos, hará cada vez más atractivo para los ciber-delincuentes realizar este tipo de ataques. Sin embargo, no se debe confundir la ciberseguridad con la ciberdelincuencia o los ciber-delitos, ya que no son conceptos equiparables.

Desgraciadamente, la realidad nos confirma que, este no es un problema que se pueda solucionar de manera sencilla, aunque en México pareciera que muchas empresas piensan que es así. La ciberseguridad debe ser integral, no puede ser sólo un tema técnico que se pretenda resolver solo con más o mejores *firewalls*. La ciberseguridad debe ser un tema general dentro de las organizaciones y alcanzar más allá de lo técnico, incluyendo también a los demás equipos o áreas en una organización, debe ser parte de la cultura y el modo del trabajo diario. Dentro de las organizaciones, la ciberseguridad debe ser una mentalidad omnipresente, sostenida por un enfoque holístico. Todas las personas dentro de las organizaciones son corresponsables, ya que sin esfuerzos compartidos las superficies de ataque pueden llegar a ser más de las que se puedan resguardar. Los ataques cada vez son más sofisticados, y los daños mayores incluyendo no solo las posibles multas administrativas, sino los riesgos por la posible comisión de delitos por el pago a organizaciones criminales para la continuidad del negocio, y el daño reputacional que esto acarrea.

Ahora bien, para que las personas puedan actuar requieren de marcos de referencia y para eso es indispensable que tanto el poder legislativo, como el judicial, trabajen en conjunto para tener mejores leyes, reglamentos y lineamientos, incluso ratificar tratados internacionales que permitan a México perseguir de mejor manera a los ciber-delincuentes que se encuentran más allá de nuestras fronteras. Respecto de este punto, considero urgente la adhesión de México a instrumentos internacionales como el Convenio de

[1] https://cyber-edge.com/wp-content/uploads/2022/04/CyberEdge-2022-CDR-Report.pdf

Budapest. Al igual que en las organizaciones, desde la administración pública, este tema también debe ser general y holístico, por lo que la ciberseguridad debiera ser parte del concepto de seguridad pública.

La solución a este problema requiere que en una primea instancia las empresas reconozcan y acepten que existe un riesgo y una falta de preparación, para que entonces tomen cartas en el asunto, y posteriormente que exista un marco legal claro y suficiente, así como una autoridad que tenga facultades suficientes para actuar y que esté más cercana a la población. Si bien, en el pasado ya han existido esfuerzos en México para poder avanzar en estos temas, estos han sido opacados por otros asuntos también importantes, por lo que tal problemática se ha dejado de lado. Sin embargo, hay algunas industrias o sectores, que por la sensibilidad de los datos que manejan, sí han tenido un mayor avance, tal es el caso del sector financiero y de salud, en donde por medio de disposiciones técnicas, como Normas Oficiales Mexicanas y disposiciones de carácter general aplicables a las instituciones de crédito, han buscado incrementar la seguridad de la información que manejan. Asimismo, en el último año hemos visto un incremento muy positivo en las iniciativas que se han presentado con respecto a la regulación de ciberseguridad, esperemos que, con toda esa experiencia, podamos construir un mejor marco legal en esa área en México.

Por lo tanto, considero que se debe trabajar para tener una nueva Estrategia Nacional de Ciberseguridad que guie los cambios, así como una Ley Federal de Ciberseguridad, y un conjunto de reformas a otros ordenamientos jurídicos, que permitan organizar los esfuerzos de la sociedad y las autoridades para reducir el número de ciberataques en nuestro país, y a la vez promover que México sea punta de lanza en la región con una ley modelo de ciberseguridad, no solo para recuperarse del rezago que tiene en la materia, sino además para mantener un marco jurídico actualizado aprovechando las mejores prácticas internacionales en ciberseguridad.