El cibercrimen en México

C.P. y Mtro. Jacob Narváez Cortés
Presidente de la Comisión de PLD del Colegio de Contadores Públicos de Morelos, A.C.
Director General de Consejería C&J, S.C.

Síntesis

Originado por la pandemia, un número mayor de personas y empresas se conectan por trabajo o negocios a las redes de informática por diversos medios, como computadoras y teléfonos inteligentes, lo que incrementa el universo de posibles víctimas del cibercrimen. La propuesta del presente trabajo es informar y prevenir las formas de ciber ataques que puedan afectar en lo personal o a las empresas y qué medios podemos utilizar para mitigar ser víctimas del delito de crimen cibernético.

La delincuencia es un problema de tipo social que vive nuestro país; la ola delincuencial se ha incrementado progresivamente a partir de las últimas dos décadas. La impunidad y las bajas tasas de encarcelamiento contribuyen a la comisión del delito, por lo que es importante señalar que a la par de los delitos como el secuestro, narcotráfico, tráfico de armas y el homicidio doloso derivados de la famosa guerra contra el narcotráfico, se encuentra el crimen cibernético (cibercrimen).

Con la conexión a las redes cibernéticas, en donde podemos, por Internet, conectarnos en tiempo real a cualquier parte del mundo, existe siempre la posibilidad de que millones de cibernautas sean víctimas potenciales de este delito; es decir, el hecho de que muchos ingresemos a la red y estemos conectados nos pone en un riesgo potencial de ser víctimas de este delito, por ejemplo: fraudes con tarjetas bancarias, clonación de tarjetas, cargos por compras no efectuadas e inclusive robos de identidad, y virus malicioso en nuestra red de equipos de cómputo.

El vertiginoso desarrollo tecnológico y el poder de la informática han demandado de la ciencia del Derecho ponerse alerta en el ámbito de las leyes; por tal motivo, la vicepresidenta de la Mesa Directiva de la Cámara de Diputados, Lic. Lizbeth Eugenia Rosas Montero,

Se debe difundir la importancia de **cuidar los equipos y el cambio de clave**, con el fin de evitar ser un blanco fácil de la delincuencia cibernética

ha manifestado que, en México, en los últimos cuatro años se recibieron 30 mil reportes telefónicos ligados a delitos cibernéticos. De estos, 53% fueron contra dependencias de gobierno, 26% contra el ámbito académico y 21% contra el sector privado y empresarial. Por lo tanto, debido a la complejidad de los delitos en el ámbito jurídico por el uso irracional e indiscriminado de la informática, en México se pueden apreciar, por medio de la siguiente tabla, los delitos más comunes cometidos por el cibercrimen:

Delito	Víctimas afectadas
Suplantación y/o robo de identidad	68%
Fraudes por medios electrónicos	17%
Hackeos	15%

México ocupa el tercer lugar después de China y Sudáfrica en tener la mayor cantidad de víctimas de cibercrimen; por lo anterior, la Cámara de Diputados ha solicitado adherirse al Convenio de Cibercriminalidad de Budapest, ya que la Policía Cibernética de México señala que cada año la economía mundial pierde miles de millones de dólares como resultado de la actividad cibercriminal.

El término cibercrimen se refiere a toda actividad delictiva que implica un ordenador, que se deriva del incremento del acceso a Internet, lo cual ha propiciado nuevos actos de extorsión, vigilancia masiva, robos económicos, filtración de datos, robo de información personal y espionaje. Cada una de las categorías de cibercrimen ha experimentado un crecimiento exponencial, motivados por las ganancias económicas e incluso por el simple ego de ser un *hacker*, para tener la reputación que da la violación de los filtros de seguridad más sofisticados.

Por tal motivo, en México, el panorama se presenta como un campo fértil para el cibercrimen, ya que 90% de las empresas son catalogadas como PyMES, y sus medios de protección cibernética son muy vulnerables y, en algunos casos, carentes de protección contra ciberataques, pues la mayoría utiliza *software* sin licencias autorizadas o gratuitas, lo que coloca a las empresas y entidades gubernamentales en una situación vulnerable a los ataques y, al mismo tiempo, susceptibles a ser víctimas de estos delitos.

Por lo anterior, considero que es conveniente que se conozca y se difunda la importancia de cuidar los equipos y el cambio de clave, con el fin de evitar ser un blanco fácil de la delincuencia cibernética. Se deben citar los ataques a diferentes entidades gubernamentales y particulares, así como el que sufrió recientemente la banca mexicana que dejó sin operar a una de estas instituciones durante varios días, con la pérdida de millones de pesos al haberse vulnerado su sistema de seguridad; asimismo, un organismo gubernamental fue blanco de otro ataque que dejó a los usuarios sin el servicio por varios días, con pérdidas importantes para los usuarios; sin embargo, los particulares cada día son afectados en sus cuentas bancarias o en sus propios equipos de cómputo al verse infectados por algún virus malicioso que le provoca daños importantes.

Las consecuencias del cibercrimen pueden ser devastadoras, por lo que se debe plantear la forma de protegerse de ataques de este tipo. Un primer paso es el uso de antivirus que asegure que los equipos tienen la mejor protección, para evitar que los *hackers* accedan a los datos personales; en el caso de los correos sospechosos, no abrirlos, y que las contraseñas de los correos sean alfanuméricos, diseñadas y ordenadas sin utilizar las mismas a fin de no facilitar la comisión de delitos.