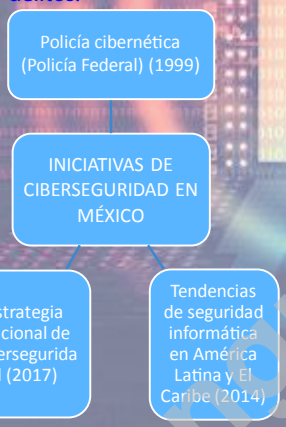
LOS DELITOS INFORMÁTICOS EN MÉXICO Y LA APLICACIÓN DEL DERECHO INFORMÁTICO

Sergio Armando Díaz Sánchez; sdiazs@iingen.unam.mx
Elsa Ximena Herrera García; eherrerag@iingen.uanm.mx
Rosa María Flores Serrano; rfs@pumas.iingen.unam.mx

Introducción y objetivos

En México no existe una legislación penal como tal referente a temas de ciberseguridad, ya que se compone de 32 códigos estatales, un código penal federal, un código penal de justicia militar y diversos tipos de códigos penales esparcidos en leyes especiales federales y estatales, todo ello fundamentado en lo que hoy en día se conoce como Derecho Informático (Conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir, de la informática y de la telemática.) (Blanco, 2016). Con esta falta de comunicación entre instituciones y de la desunificación de los múltiples códigos, los delitos informáticos (Todos aquellos actos dirigidos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos") (Recovery Labs, 2015) no han sido catalogados de manera homogénea, dado que en mayor o menor grado dichos delitos están establecidos de distinta manera en los códigos penales de cada estado.

Dicho lo anterior, se puede asumir que este desorden causa un grave conflicto para poder estandarizar qué actos son causa de una infracción a las leyes mexicanas, así como las penas que deberían ser pagadas para este tipo de actos por parte de los infractores o delincuentes. Sin embargo, pese a que no existen códigos penales claros, sí se están haciendo esfuerzos por regular de manera más efectiva estos delitos.



Metodología

El desarrollo de este trabajo fue mediante la investigación y el análisis de la información recolectada a través de fuentes de información escrita, verbal y digital. Asimismo, se basa en la experiencia y conocimientos previamente adquiridos en cursos, asignaturas de la carrera cursada y un diplomado tomado para poder tener un panorama mucho más amplio de la información que teóricamente deberíamos conocer referente a este tipo de temas.

Resultados y conclusiones

Las Tecnologías de la Información y las comunicaciones demandan del Derecho respuestas innovadoras y generales respecto de los retos que le son intrínsecos. El Derecho, en su papel de administrador de riesgos, se encarga de dotar de seguridad a los diferentes activos de información de una organización, entidad gubernamental, institución, etc.; desde ese punto de vista, se requiere una gestión jurídica permanente de los riesgos, amenazas y vulnerabilidades, como medio para establecer las medidas y controles necesarios que ayuden a mitigar los mismos.

En la sociedad, el Derecho es el agente regulador de la convivencia entre los seres humanos, la Norma Mexicana ISO 27001 (NMX ISO 27001, 2013) (Figura) imparte las reglas y parámetros para que las organizaciones reglamenten y regulen la gestión de sus activos de información de manera segura.

Otro aspecto importante, es que todos los documentos consultados sobre ciberseguridad relacionan el riesgo cibernético en el impacto económico que causan las fallas de seguridad, pero no se hace mención al impacto social que estos pueden tener, por ejemplo: daños a la dignidad humana, a la integridad de las personas, a la credibilidad y reputación de personas físicas y morales (Gobierno de México, 2017).

Por último, habría que analizar qué tantos profesionistas especializados en ciberseguridad se están educando al año en México y el grado de preparación de los mismos. Analizando la curricula de las carreras de Ingeniería en Computación y Licenciatura en Informática de la UNAM y la UNILA respectivamente, se tiene que de estas 2 carreras únicamente se tienen 7 materias dedicadas a este estudio (aproximadamente el 7% del total de materias), lo cual tal vez debería incrementarse para afrontar mejor estos retos.

MEXICO, NUMERALIA EN CIBERSEGURIDAD

2° PAÍS EN ATAQUES CIBERNÉTICOS EN AL

28 PAÍS EN ÍNDICE MUNDIAL DE CIBERSEGURIDAD

$7.6 MIL MILLONES DE PÉRDIDAS

33 MILLONES DE VÍCTIMAS

50 HORAS LIDIANDO CON LAS CONSECUENCIAS

47% MÁS QUE EN AÑOS ANTERIORES

Referencias bibliográficas

Recovery Labs. (2015). Definición de Delito Informático. URL: http://www.delitosinformaticos.info/delitos_informaticos/definicion.html (Obtenido: septiembre de 2018).
ISOTools Excellence México. NMX ISO 27001. (2013). URL: https://www.isotools.com.mx/normas/nmx-iso-27001/ (Obtenido: septiembre de 2018).
Blanco J. (2016). Derecho Informático en México. Enciclopedia Jurídica Online, URL: https://mexico.leyderecho.org/derecho-informatico/ (Obtenido: septiembre de 2018).
OEA (2014). Tendencias de Seguridad Informática en América Latina y el Caribe.
Legislación Informática en México. (2014). URL: https://seguridad.internet2.ulsa.mx(Obtenido: septiembre 2018).
Gobierno de México. (2017). Estrategia Nacional Ciberseguridad. URL: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
Unión Internacional de Telecomunicaciones (UIT) (2017). Global Cybersecurity Index (GCI). URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf