CIBERSEGURIDAD

Roberto Velázquez Cabrera

Tlapitzalli[1]
22 de diciembre de 2017

La seguridad en Internet es un tema importante actual y futuro. Se han publicado hasta notas de prensa sobre los ataques a la ciberseguridad, como los siguientes y muchos otros.

Los 10 delitos digitales que marcarán la ciberseguridad en 2017:

http://www.expansion.com/economia-digital/innovacion/2017/01/25/588732fce2704e616b8b45bf.html

Los diez mayores ataques informáticos de 2016:

https://www.economiadigital.es/tecnologia-y-tendencias/los-diez-mayores-ataques-informaticos-de-2016_188964_102.html

En este último se incluye la publicación de información de 93 millones de mexicanos.

La banca es la más afectada:

Ataques cibernéticos cuestan 1.8 mdd a la banca:

https://www.forbes.com.mx/ataques-ciberneticos-cuestan-1-8-mdd-a-la-banca/

Por desgracia, no existen estrategias, políticas, programas, sistemas o normas universales aceptadas por todos los países para mejorar la seguridad en Internet y en otros sistemas de telecomunicaciones. Es necesario acordar sistemas en todos los países, porque la red de Internet opera en todo el mundo.

[1] Esta nota fue solicitada por Edmundo Berumen Osuda, de Berumen y asociados y Baktum (http://www.berumen.com.mx/) (http://www.baktun.net/)

Varios organismos internacionales relacionados con las telecomunicaciones han promovido reuniones y emitido recomendaciones sobre ciberseguridad. Uno de ellos es la Unión Internacional de Telecomunicaciones (UIT):

http://www.itu.int/net/itunews/issues/2011/05/38-es.aspx

Ha trabajado con la Oficina de las Naciones Unidas contra la Drogas y el Delito (ONUDD), la Alianza Internacional Multilateral contra las Amenazas de Ciberamenazas (Impact) y empresas privadas especializadas como Symantec (Norton)

Por desgracia, ni siquiera en los países más avanzados en sistemas y equipos de computación y telecomunicaciones han establecido sistemas efectivos y obligatorios de ciberseguridad.

Por ejemplo, en los EUA la *National Telecommunication and Information Administration* (NTIA) es la que ha promovido consultas para tomar medidas correctivas al mayor nivel administrativo federal. Su último *Request for comments* (RFC) es reciente (septiembre 18 de 2017) y ya publicaron un informe de los comentarios recibidos, pero dicen que hasta el 11 de mayo de 2018 estiman tener el reporte final para el Presidente:

https://www.ntia.doc.gov/files/ntia/publications/rfc_comment_summary_20170918.pdf

Algo muy interesante de las últimas consultas RFC, es que publicaron los comentarios sobre *Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats* de los 47 interesados, que incluyen a la mayoría de las principales empresas y organismos que tienen que ver con los sistemas correctivos que puedan establecerse. Se incluyen algunos comentarios técnicos relevantes:

https://www.ntia.doc.gov/federal-register-notice/2017/comments-promoting-stakeholder-action-against-botnets-and-other

Otras agencias federales también participan en *cybersecurity*, como la *Federal Communication Commission* (FCC), que regula a las empresas comerciales de comunicaciones, ha publicado documentos para reducir el riesgo de *cybersecurity*, como el último de junio de 2017, que incluye obligaciones para los *Internet Service Providers* (ISPs), que son otros de los que podrían establecer medidas correctivas operativas en los servicios de Internet:

https://apps.fcc.gov/edocs_public/attachmatch/DOC-343096A1.pdf

La *National Security Agency* (NSA) se ocupa de la seguridad nacional y tiene programas para vigilar a todo el mundo:

https://www.nsa.gov/what-we-do/cybersecurity/

Home Land Security promueve la seguridad pública:

https://www.dhs.gov/stopthinkconnect

En materia de normas, el *National Institute of Estándar and Technology* (NIST) también ha participado en el tema con *National Cybersecurity Framework*:

https://www.nist.gov/programs-projects/cybersecurity-framework

https://www.nist.gov/document-4408

Tiene una página sobre los comentarios recibidos, pero no funciona:

http://csrc.nist.gov/cyberframework/preliminary_framework_comments.html

Tienen muchas páginas con documentos sobre *cybersecurity*; https://csrc.nist.gov/Search?search-keywords=cybersecurity

En México, una Estrategia nacional de ciberseguridad, se formula y publica a un año de que termine el sexenio:

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

Se acaba de celebrar la Tercera Semana Nacional de Ciberseguridad de la División Científica de la Policía Federal:

https://www.gob.mx/ciberseguridad

No publicaron el programa de conferencias:

https://www.gob.mx/cms/uploads/attachment/file/272805/3ra_OK.pdf

No se encontraron los videos de las conferencias presentadas.

Publicaron videos de ponencias presentadas sobre Ciberseguridad del Sistema Financiero. Los comentarios fueron muy generales, sin didcusiones detalladas y no presentaron soluciones efectivas consensadas, aunque mostraron deseos de colaboración. Mencionaron muchos problemas y limitantes, como el de cómo prever los ataques futuros y la falta de talentos que estiman de 2 a 5 millones para dentro de 20 años.

Incluyeron un nuevo Documento de trabajo hacia una estrategia nacional de seguridad:

https://www.gob.mx/gobmx/documentos/documento-de-trabajo-hacia-una-estrategia-nacional-de-ciberseguridad

En el Desarrollo de capacidades incluyen formar funcionarios expertos en ciberseguridad.

En nuestro país, la ley que regula las telecomunicaciones es la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR):

http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_311017.pdf

En su texto, la palabra "seguridad" aparece 37 veces, pero el organismo que la regula, el Instituto Federal de Telecomunicaciones (IFT), no ha publicado normas o protocolos sobre la seguridad de Internet o la ciberseguridad:

http://www.ift.org.mx/

Desde que se emitió la primera Ley de telecomunicaciones, se comentaron sus fallas principales, en un estudio comparativo con la emitida en los EUA[2]. Una de ellas es que cubre principalmente lo comercial, similar a lo que ocurre con la FCC de los EUA. No cubre otros temas nacionales importantes, como lo hace la NTIA de los EUA. Uno de esos temas es todo lo que refiere a los sistemas gubernamentales como la defensa, la educación y otros sectores, y la protección de los usuarios, como la calidad de servicios y la seguridad.

La calidad de los servicios de telecomunicaciones se comenta en una nota anterior[3].

Si el IFT no atiende la seguridad, lo tiene que hacer otra dependencia o entidad, como la Secretaria de Gobernación, con su Policía Federal, que cubren más los contenidos de los sistemas y la redes de las comunicaciones y telecomunicaciones.

Por ejemplo, la Secretaria de Gobernación ya emitió un: "ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias (MAAGTICS).": http://www.normateca.gob.mx/Archivos/66_D_4228_19-02-2016.pdf

Es notable que en la Tercera Semana Nacional de Ciberseguridad no incluyeran a un conferencista del IFT.

---

[2] Velázquez Cabrera, Roberto. La Regulación de las Comunicaciones en México. Analizada como un Sistema de Producción Sectorial, comparada con la de los EUA. Enero de 1997. Estudio realizado para el Instituto Mexicano de las Comunicaciones (IMC).

[3] Velázquez Cabrera, Roberto. ¿Telecomunicaciones de calidad? 2016. http://www.tlapitzalli.com/nuevos/pdf/Telecomunicaciones_de_calidad.pdf

Esa es una falla importante, porque las empresas que proporcionan los servicios de Internet, son unos de los que pueden establecer medidas de seguridad en sus redes que operan.

Las obligaciones de los servicios comerciales de entre los usuarios y los operadores se establecen, en los mejores casos, en el contrato de servicios, pero algunos ya ni los hacen. Las obligaciones de los operadores ante la autoridad gubernamental se establecen en un oficio de concesión, pero no han incluido normas sobre seguridad.

Otros que pueden ayudar son los que ofrecen los sistemas y equipos especializados, para operar las redes y para su protección. Todos son del extranjero, ya que en nuestro país no se producen o generan. Muchas fallas son de terceros o de proveedores.

Algunos equipos y programas comerciales ya incluyen sistemas para atacar a los usuarios.

Usualmente, no se prueban bien los sistemas y equipos antes de ponerlos aperar en la realidad y en muchas ocasiones las fallas se corrigen con parches, después de que ocurren los daños.

Mientras los proveedores de servicios y equipos de computación y telecomunicaciones no estén obligados a incluir la protección sobre la seguridad, no lo van a hacer, menos, si hacen negocio con los productos que venden para ello. Por ejemplo, los virus no se van a eliminar, mientras sea negocio vender programas antivirus.

En el sitio web de la Asociación de Internet MX, no se muestran estudios sobre ciberseguridad, aunque muestran algunas encuestas relacionadas con datos personales entre usuarios y empresas:

https://www.asociaciondeinternet.mx/es/component/remository/Proteccion-de-Datos-Personales/Estudio-de-Proteccion-de-Datos-Personales-entre-Usuarios-y-Empresas/lang,es-es/?Itemid=

Cualquier sistema se ciberseguridad que se establezca debe basarse en una norma legislativa nacional, que no existe actualizada. Para operar el sistema que se establezca, se requiere de personal bien capacitado, que tampoco existe. Desde hace tiempo se recomendó incluir esos temas normativos en las instituciones educativas que ofrecen cursos de posgrado, como el Centro de Investigación en Computación (CIC) del IPN, pero no fue atendida: http://www.cic.ipn.mx/

Ahora, solo incluyen un curso de maestría sobre introducción a la seguridad informática:

http://148.204.64.153/academica/MCC/37-SIP30_Introduccion_a_la_seguridad_informatica_MCCok.pdf

Las escuelas de telecomunicaciones del IPN tampoco cubren los temas normativos y de seguridad en las redes, ya que cubren solo lo técnico:

http://www.sepi.esimez.ipn.mx/telecom/nucleobasico.html

Lo mismo ocurre en otras instituciones educativas importantes como la UNAM:

http://posgrado.telecomunicaciones.unam.mx/maestria-plan.php

Lo primero que hay que hacer en cualquier proyecto nacional nuevo es preparar a los maestros, que no existen localmente, para preparar a los profesionales que lo desarrollen y operen. No se conocen estimaciones abiertas de demanda ni de personal técnico.

Si las instituciones educativas no preparan el personal necesario, los centros de ciberseguridad o los proveedores de equipos y sistemas, son los que podrían ayudar.

El CISEN ya tiene una Escuela de Inteligencia para la Seguridad Nacional del Centro de Investigación y Seguridad Nacional (ESISEN), pero sus cursos no nos abiertos al público en general, ya que son para las entidades relacionadas con la seguridad nacional: http://www.cisen.gob.mx/Esisen.html

¿Cómo pueden aspirar a defender la seguridad nacional?, cuando ya entregaron todo el patrimonio nacional de valor remanente: bancos; energéticos; telecomunicaciones; ferrocarriles; plantas generadoras de energía; minas; ductos; costas; parte del golfo; muchas otras empresas y hasta basureros y el agua de varias ciudades.

Hasta permitieron que agencias del gobierno de los EUA operen en México Centros de Espionaje:

http://www.proceso.com.mx/98712/el-gran-centro-de-espionaje-de-washington

Antes de tener una reglamentación detallada sobre seguridad en telecomunicaciones, ya se están creando centros de ciberseguridad en México, como uno de Microsoft para la Ciudad de México, sin que se sepa bien lo que hacen:

https://www.xataka.com.mx/eventos-de-tecnologia/microsoft-inaugura-centro-de-ciberseguridad-en-la-cdmx

Dicen es para "detectar y solucionar problemas de seguridad digital en México", para "combatir el cibercrimen y desmantelar las redes de botnet que afectan a los clientes de Microsoft en el país" y para “prevenir y combatir los delitos a través de Internet.”

No se sabe lo que han hecho esos centros para contrarrestar ni los *bots* que operan desde el gobierno contra periodistas, intelectuales que exponen la corrupción y luchadores de derechos humanos, como Pegasus de NSO Group de Israel:

https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/

Otro centro de ciberseguridad es de Telmex:

http://blog.telmex.com/2014/09/30/telmex-inaugura-el-primer-centro-de-ciberseguridad-de-mexico-y-latinoamerica/

Dicen que:

"Dentro del Centro de Ciberseguridad, nuestros expertos realizarán un monitoreo de los distintos componentes tecnológicos que estarán habilitados en las redes de nuestros clientes; se emprenderán procesos de investigación y análisis de información para el envío de alertas ante posibles ciberamenazas que servirán como apoyo en la toma de decisiones. Adicional a esto, el equipo coordinará esfuerzos con diversos grupos involucrados en caso de contingencias y la creación de un análisis avanzado que identifique y entienda los rastros y comportamientos de malware. El portafolio de este nuevo centro brindará a los clientes servicios como: Diagnóstico y Protección contra Amenazas Avanzadas; Servicios Forenses Avanzados; Gestión Continua de Ciberriesgos basada en Inteligencia y Ciberinteligencia a través de Internet."

No han informado abiertamente de lo que han hecho de utilidad. Ni siquiera ayudan cuando de presentan fallas en sus servicios de Internet o en su calidad, que es la amenaza más frecuente de Telmex y otros operadores, contra sus clientes. El IFT ni siquiera ha publicado un protocolo para medir la calidad de los servicios de Internet.

Hasta empresas ofrecen servicios de seguridad informática, mientras existan las amenazas. Una dice:

"…donde un equipo especializado y altamente calificado, trabaja las 24 horas al día, los 365 días del año para identificar y responder, mediante soluciones emergentes, ante amenazas y actividad maliciosa contra las organizaciones y así minimizar los impactos financieros y reputacionales derivados de ciberataques."

http://cert.iqsec.com.mx/

En el anexo se comenta la Ley de Seguridad Interior, principalmente sobre la ciberseguridad de esta nota.

ANEXO. Comentarios sobre Ley de Seguridad Interior (LSI)

En el Sistema de Información Legislativa (SIL) de la Secretaria de Gobernación (SEGOB) se encontró un documento de seguimiento[4] y un resumen[5] con un pdf de la LSI[6]. La LSI aprobada fue turnada al Ejecutivo (14-DIC-2017), sin haber atendido las observaciones de emitidas por especialistas de organizaciones nacionales e internacionales.

Tampoco se han conocido discusiones públicas detalladas sobre la LSI y la ciberseguridad.

El texto del articulado de la LSI no incluye las palabras de "ciberseguridad", "Internet", "telecomunicaciones", ni de su seguridad. En el inciso h) del Contexto de la Exposición de motivos sólo se incluyen:

"***** Los ataques a la seguridad cibernética" entre las "...nuevas amenazas y preocupaciones…".

Las "comunicaciones" se incluyen una vez en ese mismo Contexto.

Sin embargo, la "información" aparece 7 veces en el texto (marcada con **negritas**), principalmente en relación a la investigación e inteligencia de la Seguridad Interior y al Sistema de Seguridad Nacional, con facultades muy amplias:

En el inciso h) de la Exposición de Motivos, se dice:

"Ahora bien, en atención a que la Seguridad Interior se enmarca en el ámbito de la Seguridad Nacional, es pertinente hacer uso de los esquemas institucionales que la legislación en la materia ha diseñado, tanto para la toma de decisiones en los niveles estratégico, táctico y operativo, así como para la ejecución de las acciones que se requieran. De ahí que, como se prevé en la presente iniciativa debe apoyarse en el Consejo de Seguridad Nacional para determinar la intervención de la Federación en temas de Seguridad Interior, así como en el Secretario de Gobernación, en su carácter de Secretario Ejecutivo del Consejo, para coordinar el análisis estratégico de los fenómenos que se presenten, sustentado en el sistema de investigación e **información** que se prevé en el artículo 27, fracción XXVI de la Ley Orgánica de la Administración Pública Federal."

Esa fracción de la LOAPF, del Artículo 27.- A la Secretaría de Gobernación corresponde el despacho de los siguientes asuntos, dice:

---

4 http://sil.gobernacion.gob.mx/Librerias/pp_ReporteSeguimiento.php?SID=70b750870322916bbbf9d28a64042cc5&Seguimiento=3636409&Asunto=3441153

55 http://sil.gobernacion.gob.mx/Librerias/pp_ContenidoAsuntos.php?SID=70b750870322916bbbf9d28a64042cc5&Clave=3441153

6 http://sil.gobernacion.gob.mx/Archivos/Documentos/2016/11/asun_3441153_20161104_1478014676.pdf

“XXVI. Establecer y operar un sistema de investigación e **información**, que contribuya a preservar la integridad, estabilidad y permanencia del Estado mexicano así como contribuir en lo que corresponda al Ejecutivo de la Unión, a dar sustento a la unidad nacional, a preservar la cohesión social y a fortalecer las instituciones de gobierno;”

En el punto V del Art. De definiciones sobre las Fuerzas Armadas:

“V. Inteligencia para la Seguridad Interior: El conocimiento obtenido a partir de la recolección, procesamiento, diseminación y explotación de **información** para la toma de decisiones en materia de Seguridad Interior;

En el Art, 6 de III. Uso legítimo de la fuerza:

“Artículo 6.- La **información** que se genere con motivo de la aplicación de la presente Ley, será considerada de Seguridad Nacional, en los términos de la ley de la materia y clasificada de conformidad con ésta y las disposiciones aplicables en materia de transparencia y acceso a la **información**.”

En el punto VI del Art. 12:

“VI. La demás **información** que se considere relevante para justificar la procedencia de la Declaratoria de Protección a la Seguridad Interior y para la toma de decisiones correspondientes.”

En el Art. 28 del Capítulo 4:

“Artículo 28.- Las Fuerzas Federales y las Fuerzas Armadas desarrollarán actividades de inteligencia en materia de Seguridad Interior en los ámbitos de sus respectivas competencias, considerando los aspectos estratégico y operacional, la cual tendrá como propósito brindar apoyo en la toma de decisiones en materia de Seguridad Interior.

Al realizar tareas de inteligencia, las autoridades facultadas por esta Ley podrán hacer uso de cualquier método de recolección de **información**.”

Y en el Art. 29:

“Artículo 29.- En materia de Seguridad Interior, las autoridades federales y los órganos autónomos deberán proporcionar la **información** que les requieran las autoridades que intervengan en los términos de la presente Ley.”

No se mencionan los documentos oficiales publicados con anterioridad sobre ciberseguridad nacional, ni cómo van a relacionarlos con la LSI.

La LSI otorga facultades muy amplias para obtener y usar información, pero clasificada y no bien detallada. No incluye ni las definiciones sobre esos temas básicos y sistemas, que ya han venido operando, sin conocer la reglamentación legal detallada nacional, como ya se ha comentado. Eso significa, entre otras cosas, que puede existir mucha discrecionalidad y opacidad publica sobre su aplicación en la realidad.

Esas limitantes o faltantes legislativos nacionales, también ocurren en países de mayor desarrollo industrial, ya que algunos están en proceso de estudio y consulta y son muy

diversos, aunque los más poderosos ya vigilan lo que se transmite en todo tipo de redes de comunicaciones y telecomunicaciones digitales y analógicas.

La ciberseguridad nacional o interior no ha sido muy comentada con detalle en los medios masivos de comunicacion, ya que se han centrado más en los temas militares y policiacos de la LSI, que desde hace una más de década no han funcionado para proteger al pueblo, ni a la población más afectada.

La vigilancia e investigación de la seguridad nacional tampoco ha servido ni siquiera para prevenir las acciones y operación financiera de los grandes delincuentes ni para evitar la disminución de la soberanía e independencia nacionales, los abusos y la corrupción de los funcionarios que también han entregado el patrimonio nacional, desviado o robado recursos públicos, para beneficio personal, de sus partidos políticos, socios, amigos o familiares.

El 21 de diciembre de 2017, en el DOF se expidió el decreto de la LSI[7], que fue aprobada por el Ejecutivo:

La LSI expedida también incluye 7 veces a la “información”, pero algunos textos fueron modificados, sin alterar mucho el texto anterior.

Tampoco ha sido analizada y discutida con detalle y profundidad en los medios de comunicación ni abiertamente en la academia.

Se ha informado que la LSI va a ser revisada por la Suprema Corte de la Nación, por la gran cantidad de objeciones públicas presentadas por especialistas nacionales e internacionales interesados. Mientras no se pronuncie sobre su constitucionalidad, no se van a aplicar las facultades de los nuevos ordenamientos sobre Seguridad Interior, aunque van a seguir operando como ha venido ocurriendo.

[7] http://www.diariooficial.gob.mx/nota_detalle.php?codigo=5508716&fecha=21/12/2017