Revista de Administración Pública

INAP

La seguridad cibernética en el nuevo entorno operativo

Enrique Francisco Galindo Ceballos*

Presentación

El presente artículo tiene por objetivo establecer una perspectiva de la ciberseguridad desde el punto de vista de los riesgos y afectaciones globales y locales, ocasionadas por los ciberdelitos, así como la perspectiva general de las medidas que ha adoptado nuestro gobierno para contrarrestar sus efectos.

El Gobierno Mexicano, consciente de la situación global y local, ha impulsado estrategias y programas de carácter nacional a fin de realizar acciones específicas para la protección del ciberespacio mexicano. En el artículo también se describe el contexto nacional de la ciberseguridad.

Como definición se entenderá por "ciberdelitos", a las conductas constitutivas de delito relacionadas con afectaciones a la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, a la falsificación y fraude informático, a la producción, transmisión y almacenamiento de contenido por medios electrónicos de pornografía infantil, propiedad intelectual y derechos de autor, así como, al acoso, amenazas y extorsión mediante medios electrónicos, conforme a la generalidad ampliamente aceptada a nivel mundial y establecido en términos del Convenio de Cibercriminalidad de Budapest.

Debido a que las nuevas tecnologías en materia de informática y telecomunicaciones avanzan a pasos agigantados, en diversos países

* Abogado y Maestro en Política Criminal titulado por la Universidad Autónoma de San Luis Potosí. Maestro en Estado de Derecho y Buen Gobierno, y Candidato a Doctor en Gobernanza Global, ambos por la Universidad de Salamanca, España. Ha recibido formación policial en el FBI, las Universidades de Berkeley, de Toledo y Complutense. Ha sido Presidente de la Comunidad de Policías de América (AMERIPOL), organismo del que también fue Secretario Ejecutivo. Fue Comisionado General de la Policía Federal del 2012 al 2016.

del mundo, incluyendo México, la legislación no contempla ciertas conductas constitutivas de delito por vías informáticas, por ello, no pueden considerarse como delito, si no como incidentes o abusos cibernéticos.

En México, la Unidad Cibernética de la Policía Federal surgió como un esfuerzo del Gobierno Federal ante la necesidad de contrarrestar las nuevas modalidades delictivas en el ciberespacio, que se valen del Internet y las nuevas tecnologías para la consumación de delitos. Por ello, para la policía Federal, el ciberespacio, es un nuevo entorno operativo, como lo es el aire, el mar y la tierra. En este tenor, se describen las capacidades de la Policía Federal en materia de ciberseguridad, así como la Estrategia implementada en la materia, la cual tiene como objetivo hacer frente a la ciberdelincuencia, y de impulsar los esfuerzos del Gobierno de la República, para lograr un México en Paz, de conformidad al Plan Nacional de Desarrollo y al Programa Nacional de Seguridad Pública 2013-2018.

Para finalizar el artículo, se hace una introducción al Nuevo Sistema de Justicia Penal Acusatorio, dónde se describe que la envergadura de la reforma constitucional en materia penal representa no sólo un parteaguas en los sistemas de procuración e impartición de justicia, sino un verdadero cambio de paradigma que todos los actores que conforman un Estado democrático de Derecho debemos asumir con responsabilidad y compromiso. En este sentido, debemos de considerar que hemos sido testigos de la conformación de la llamada sociedad de la información y de una evolución tecnológica que avanza a pasos agigantados, la cual ha permitido intensificar el uso de los recursos tecnológicos en nuestras actividades cotidianas, por ello, los delincuentes cibernéticos, encaminan sus actividades delictivas para la obtención de beneficios ilícitos en este nuevo entorno, por lo que, las instituciones de procuración e impartición de justicia deberán enfrentar estos nuevos retos de cara al Nuevo Sistema de Justicia Penal Acusatorio.

Los inicios

Desde la primera revolución industrial y el surgimiento de las máquinas de vapor, a la segunda revolución industrial con el uso de la electricidad y el foco de forma masiva, y una tercera revolución industrial con el nacimiento de la era espacial, las computadoras y el internet, la sociedad global ha sufrido una evolución tecnológica sin precedentes.

Durante las últimas tres décadas del siglo XX, el desarrollo de las Tecnologías de Información y Comunicación (TIC) y el incremento en el uso de Internet, ha estado evolucionando hacia un mundo "híper-conectado", en el que las personas viven conectadas de forma permanentemente a la información a través de diferentes dispositivos como la radio, la televisión, el internet, y el teléfono celular.

Es un hecho que estamos viviendo en la sociedad de la información, cada día más servicios son ofrecidos vía internet, más información es almacenada en la nube y más dispositivos son conectados alrededor del mundo. Las empresas basan cada día más su operación en esta plataforma internacional para mejorar la experiencia de compra, permitiendo a sus clientes acceder desde sus dispositivos móviles a información en tiempo real de sus productos, inventario y costos a la par que observan físicamente los artículos.

El uso de las tecnologías de la información y la incorporación del Internet al mundo real sin duda han sido un factor de desarrollo global, incluso nos están llevando hacia la cuarta revolución industrial mediante la inclusión del concepto del **"Internet de las Cosas"** donde su uso se incorporará a la industria en la producción, distribución y manejo de los productos adaptando servicios a los clientes en cualquier parte del mundo.

De esta forma, han surgido conceptos como **"Ciudad Inteligente"**, que se caracteriza por el uso intensivo de las TIC en la creación así como en el mejoramiento de los sistemas que componen la ciudad para crear, recopilar, procesar y transformar la información que incida en mejores servicios, con ello mejorar la calidad de vida mediante el uso eficiente de sus recursos.

Aspectos relevantes del crecimiento de Internet a nivel global y local

De acuerdo con la Unión Internacional de Telecomunicaciones (UIT), a nivel global hay alrededor de 3 mil 200 millones de cibernautas (44% de la población mundial) con una tasa de crecimiento anual aproximada de 14%[1].

Con base en los Objetivos de Desarrollo del Milenio establecidos por la Organización de las Naciones Unidas a partir del año 2000, la revolución tecnológica de los últimos 15 años ha propiciado un progreso tecnológico, el despliegue de infraestructura y la caída de los precios en los bienes y servicios tecnológicos, lo que ha contribuido al crecimiento en el acceso y conectividad de miles de millones de personas en todo el mundo. A la fecha, existen más de 7 mil millones de abonados a servicios de telefonía móvil en todo el mundo, frente a los menos de mil millones en el año 2000[2].

El escenario en México, de acuerdo con datos de la Asociación Mexicana de Internet (AMIPCI), es notable incremento en la cifra de cibernautas,

[1] Unión Internacional de Telecomunicaciones, ICT Facts & Figures 2015 [en línea], [fecha de consulta: abril 2016]. Disponible en: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

[2] Organización de las Naciones Unidas, Objetivos de Desarrollo del Milenio [en línea], [fecha de consulta: abril 2016]. Disponible en: http://www.undp.org/content/undp/es/home/sdgoverview/mdg_goals/

pasando de 51.2 millones en 2013 a 53.9 en 2014. La AMIPCI identificó que en México se incrementó el comercio electrónico en 2014, llegando a movilizar más de 160 mil millones de pesos, lo que representa un 34% más que en el año anterior[3].

Otro dato relevante de México es la importancia que tienen las micro, pequeñas y medianas empresas (MIPYMES) en el desarrollo económico y social de la nación, ya que datos de Proméxico refieren que existen cerca de 4.2 millones de MIPYMES que generan el 52% del Producto Interno Bruto (PIB) y el 72% de los empleos formales. El 95% de ellas son particularmente pequeñas y medianas e impulsan de manera relevante el crecimiento económico digital del país con el fortalecimiento de sus infraestructuras tecnológicas[4].

Riesgos y afectaciones globales y locales

Con la evolución del Internet y las TIC, también se han generado circunstancias propicias para aquellos que buscan un beneficio personal en detrimento de otros. Las afectaciones derivadas comparten un origen y una serie de características comunes de la actividad delictiva como el bajo grado de riesgo para el delincuente y el alto grado de efectividad y gran impacto, así como la facilidad de ejecución y el anonimato, ya que se puede delinquir prácticamente desde cualquier lugar del planeta donde exista acceso a Internet y afectar a Instituciones o individuos de cualquier parte del mundo. En algunos casos, no es imprescindible grandes conocimientos por parte del delincuente para efectuar algún delito cibernético.

Al respecto, el Foro Económico Mundial considera las fallas de la infraestructura crítica, los ciberataques y el fraude o robo de datos como parte de los principales riesgos globales, incluso entre los primeros diez lugares[5]. Este último ligado al robo de datos personales.

En 2014, los ataques más comunes en el "**Internet de las Cosas"**[6] han sido a los sistemas de terminales de punto de venta (POS por sus siglas en inglés), cajeros automáticos y dispositivos de acceso a Internet en los hogares[7].

[3] Asociación Mexicana de Internet, Estudio Comercio Electrónico en México 2015 [en línea], [fecha de consulta: abril 2016]. Disponible en: https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf

[4] PRODEIIN 2013-2018, Censos Económicos (2009). Micro, pequeña, mediana y gran empresa: estratificación de los establecimientos: Censos Económicos 2009 / INEGI, c2011. 2013 [en línea], [fecha de consulta: abril 2016]. Disponible enhttp://www.institutopyme.org/index.php?option=com_content&view=article&id=134&,

[5] World Economic Forum, Global Risks 2013 [en línea], [fecha de consulta: abril 2016]. Disponible en: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf

[6] Se debe entender por internet de las cosas a la interconexión digital de objetos con Internet para proporcionar información significativa en tiempo real.

[7] Internet SecurityThreat Report, Symantec (2015).

Un estudio realizado por la firma de software Symantec reveló que, a nivel global, la cifra de víctimas es de aproximadamente 12 víctimas por segundo: 1 millón diarias y 378 millones al año. El reporte indica que las pérdidas económicas anuales oscilan entre los 375 y 575 mil millones de dólares[8].

En Latinoamérica, y conforme al estudio realizado por la Organización de Estados Americanos (OEA) en colaboración con la firma de software Trend Micro, se presentó un incremento entre el 8% y el 40% en ataques durante 2012, siendo México el mercado más problemático. Dicho aumento se generó en ciberataques y acciones "hacktivistas", lavado de dinero y ataques a infraestructuras críticas[9].

Quizá ésta sea una de las razones por las que la actividad de programas de cómputo maliciosos (*malware*) también fue una de las principales afecciones, registrándose un incremento del 40% en incidentes cibernéticos en 2012[10]. Se estima que en 2013 la pérdida económica anual en México fue alrededor de los 3 mil millones de dólares según los datos del *Reporte Norton* de 2013[11].

El estudio sobre los hábitos del Internet en México realizado por la AMIPCI (2014) indica que 18.4 millones (36%) de cibernautas son personas menores de edad, un gran número de posibles víctimas de delitos contra menores. El estudio arrojó que el promedio en el tiempo de conexión a Internet de los cibernautas en México es de más de cinco horas al día y que el uso es principalmente para el correo electrónico, redes sociales (9 de cada 10 lo utilizan) y búsqueda de información, en ese orden[12].

De acuerdo a la Encuesta Nacional de Disponibilidad y uso de las TIC en los Hogares, realizada por el Instituto Nacional de Estadística y Geografía en 2015, 55.7 millones de personas son usuarios de una computadora y 62.4 millones utilizan Internet en México. Dicha encuesta indica que el

---

8 Norton by Symantec, Reporte Norton 2013 [en línea], [fecha de consulta: abril 2016]. Disponible en: https://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf

9 Trend Micro, Latin American and Caribbean Cybersecurity Trends and Government Responses [en línea], [fecha de consulta: abril 2016]. Disponible en: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf

10 Trend Micro, Latin American and Caribbean Cybersecurity Trends and Government Responses [en línea], [fecha de consulta: abril 2016]. Disponible en: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf

11 Norton by Symantec, op. cit., [fecha de consulta: abril 2016]. Disponible en: https://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf

12 Asociación Mexicana de Internet, Estudio Comercio Electrónico en México 2015 [en línea], [fecha de consulta: abril 2016]. Disponible en: https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf

9.7% de los usuarios de internet lo utiliza para ordenar o comprar productos en línea y el 9.3% para realizar operaciones bancarias. El 12.8% de los usuarios de internet declaro haber realizado al menos una transacción electrónica (compra o pago por internet) dentro de los 12 meses previos a la entrevista[13].

A partir del contexto anterior, es posible establecer que el diagnóstico presenta tendencias en favor del uso de la tecnología, del acceso a la información y de la reducción de la brecha digital, es también posible notar que los gobiernos mantendrán una política de apoyo al uso de las tecnologías como mecanismo de desarrollo económico, político y social.

Empero, se ha visualizado un crecimiento de la actividad ilícita en el uso de las tecnologías y el Internet así como la constante evolución de éstos últimos, la actividad de la ciberdelincuencia se moverá a la par de dicho desarrollo en gran volumen, por lo que, es imprescindible que las políticas públicas y la legislación nacional consideren a la ciberdelincuencia como un aspecto prioritario nacional.

Así, el término ciberseguridad ha sido objeto de estudio y definición, tal como se expresa en la Recomendación UIT–T X.1205, de la Unión Internacional de Telecomunicaciones[14], quedó establecido como:

> *Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.*
>
> *Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno.*
>
> *La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio, y la confidencialidad.*

[13] Instituto Nacional de Estadística y Geografía, 2015. [fecha de consulta: mayo 2016] http://www.inegi.org.mx/saladeprensa/boletines/2016/especiales/especiales2016_03_01.pdf

[14] Unión Internacional de Telecomunicaciones, UIT 2009, Aspectos Generales de la Ciberseguridad [fecha de consulta: abril 2016]. Disponible en PDF en: https://www.itu.int/rec/T-REC-X.1205-200804-I/es

Ciberseguridad en el contexto nacional

El gobierno mexicano, consciente de la situación global y local, ha impulsado estrategias y programas de carácter nacional a fin de realizar acciones específicas para la protección del ciberespacio mexicano.

En el *Plan Nacional de Desarrollo 2013-2018 (PND)*[15], se establece la Meta Nacional por un México en Paz, que se enfoca en el avance de la democracia, la gobernabilidad y la seguridad de la población. Para alcanzar tales fines, la participación ciudadana se concibe como el eje de la relación entre gobierno y sociedad, ya que permite el desarrollo y fortalecimiento del tejido social que evita el quebrantamiento de la paz, y el mejoramiento de la transparencia y rendición de cuentas, reduciendo la corrupción.

Así mismo, en noviembre de 2013, la Presidencia de la República presentó la *Estrategia Digital Nacional (EDN)* que es el plan de acción que el Gobierno Federal implementará para fomentar la adopción y el desarrollo de las TIC e insertar a México en la Sociedad de la Información y el Conocimiento. Este documento surge en el marco del PND 2013-2018, ya que forma parte de la estrategia transversal "Gobierno Cercano y Moderno". De acuerdo con el índice de digitalización establecido en el Programa para un Gobierno Cercano y Moderno, publicado en el *Diario Oficial de la Federación* el 30 de agosto de 2013, México se encuentra en la última posición en digitalización entre los países de la Organización para la Cooperación y el Desarrollo Económico (OCDE), y la quinta posición en América Latina, con un valor de 37.05 puntos para el año 2011. A partir de tal escenario, se establece el objetivo de la Estrategia Digital Nacional (EDN)[16].

El propósito fundamental de la Estrategia es lograr un México Digital en el que la adopción y uso de las TIC maximicen su impacto económico, social y político en beneficio de la calidad de vida de las personas. La Estrategia surge como respuesta a la necesidad de aprovechar las oportunidades que la adopción y el desarrollo de las TIC crean para potenciar el crecimiento del país.

La EDN considera dentro de su habilitador "Inclusión y habilidades digitales", el que todos los sectores sociales puedan aprovechar y utilizar las TIC de manera cotidiana, señalando dentro de la iniciativa "Habilidades para la Seguridad Digital", el desarrollar proyectos que generen habilidades para la prevención de conductas delictivas contra niñas, niños y adolescentes, como el acoso escolar (incluido el ciberacoso o ciberbullying), el intercambio de mensajes electrónicos con contenido

[15] Plan Nacional de Desarrollo 2013-2018, Presidencia de la República, mayo 2013, [fecha de consulta: abril 2016]. Disponible en: http://pnd.gob.mx

[16] Estrategia Digital Nacional (EDN), Presidencia de la República, mayo 2014, [fecha de consulta: abril 2016]. Disponible en: http://www.gob.mx/mexicodigital

sexual (sexting), pornografía infantil, actos de violencia, y otros abusos, en coordinación con las dependencias e instituciones competentes.

Por otra parte, y por primera ocasión, el *Programa Nacional de Seguridad Pública 2014-2018* (PNSP)[17], estableció en el punto 1.6, un apartado para los Delitos Cibernéticos, señalando que:

> *"…en los últimos años la delincuencia organizada ha hecho uso de estas tecnologías para coordinar y cometer delitos de alto impacto, como pornografía infantil, secuestro, extorsión y trata de personas. De la misma manera, se han utilizado estos medios para realizar fraudes, usurpación de identidad, acceder ilícitamente a sistemas y equipos de informática y cometer delitos contra los derechos de autor.*
>
> *Una de las características del delito informático es que no tiene fronteras, dada la característica inherente de interconexión del Internet, situación que se vuelve aún más compleja dado que los delincuentes cibernéticos comenten actividades que afectan tanto a ciudadanos como a las infraestructuras estratégicas de distintos países."*

Derivado de lo anterior, la atención de los delitos cibernéticos se desarrolló a partir de los delitos de mayor impacto a la población mexicana, estableciéndose como:

> *"Objetivo 2.- Reducir la incidencia de los delitos con mayor impacto en la población."*

Dicho objetivo señala que:

> *"En los últimos años la sociedad mexicana ha sufrido el flagelo de la delincuencia, por lo que una de sus aspiraciones es vivir sin el temor de ser víctima de algún delito..."*

Luego entonces, la Estrategia 2.7, definió como parte de los mecanismos:

> *"Detectar y atender oportunamente los delitos cibernéticos."*

Donde se definieron las siguientes líneas de acción:

> *"2.7.1 Fortalecer las capacidades y la infraestructura tecnológica de las instituciones de seguridad pública para prevenir e investigar delitos cibernéticos.*

[17] Programa Nacional de Seguridad Pública 2014-2018, [fecha de consulta: abril 2016] Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5343081&fecha=30/04/2014

2.7.2 Desarrollar investigación científica para la prevención e investigación de los delitos cibernéticos.

2.7.3 Implementar acciones contra delitos cibernéticos de mayor impacto: pornografía infantil, fraude, extorsión, usurpación de identidad y contra derechos de autor.

2.7.4 Diseñar protocolos de operación para la prevención de delitos cibernéticos en las instancias que administran información considerada reservada o confidencial.

2.7.5 Promover la creación y fortalecimiento de unidades especializadas en la prevención e investigación de delitos que se cometen por internet.

2.7.6 Desarrollar un modelo de policía cibernética para las Entidades Federativas.

2.7.7 Generar indicadores y estadísticas de delitos informáticos para el diseño de estrategias de prevención.

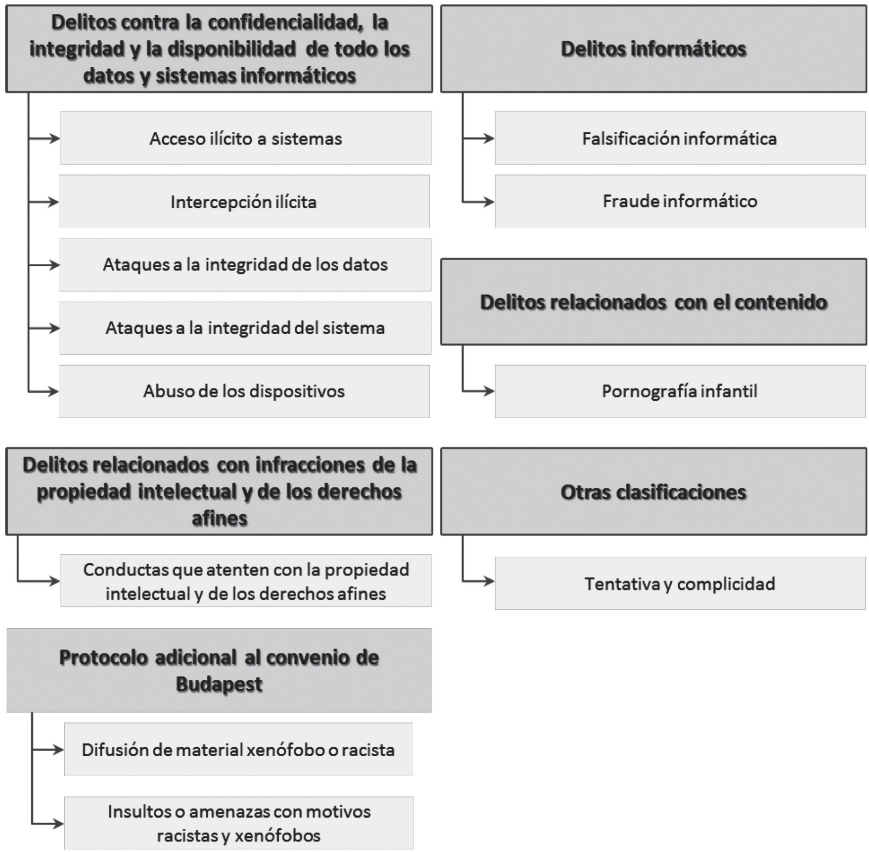
2.7.8 Impulsar acciones para consolidar los esquemas de seguridad cibernética que coadyuven al desarrollo de la economía digital.

2.7.9 Fortalecer la seguridad de la infraestructura tecnológica estratégica del país."

Es importante señalar que las líneas de acción del PNSP 2014-2018 así como la EDN, se encuentran alineadas entre sí al PND 2013-2018; las acciones coordinadas entre las instituciones de los tres niveles de gobierno y del sectores productivos del país son elementos clave para el desarrollo de una Estrategia de alcance nacional, la seguridad es una responsabilidad de todos y la ciberseguridad no es la excepción.

En el terreno de cooperación Internacional, en el año 2001 y ante la necesidad de combatir el crimen cibernético, se firmó en Budapest el Convenio sobre la Ciberdelincuencia, conocido como el Convenio de Budapest; mismo que destaca en su exposición de motivos que la lucha efectiva en contra de la ciberdelincuencia requiere de la cooperación internacional, y como prioridad, la necesidad de la protección de datos personales y del desarrollo de la niñez. México anunció su interés por adherirse a dicho convenio en el año 2014, como parte de las acciones relativas a la reforma constitucional en materia de telecomunicaciones y a la Estrategia Digital Nacional impulsada por la Presidencia de la República. Cabe señalar que la Ciberseguridad es un término acuñado en el contexto del Convenio de Budapest. En dicho convenio se establecen los siguientes delitos[18]:

[18] La Figura 1 fue elaborada por la Policía Federal utilizando la clasificación de los delitos informáticos establecidos en el convenio de Budapest.



Por otra parte, en junio de 2014, en la sede la Conferencias de Ministros de Justicia de los Países de Iberoamérica (COMJIB) en Madrid, el gobierno mexicano firmó su adhesión al "Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia" y a la "Recomendación de COMJIB relativa a la Tipificación y Sanción de la Ciberdelincuencia" como una estrategia para hacer frente a los ciberdelitos con apoyo de la comunidad internacional.

Capacidades de la Policía Federal en materia de ciberseguridad

En México, la Policía Federal, cuenta con una Unidad Cibernética, que se encuentra adscrita a la División Científica y por Reglamento[19] lleva el nombre de Coordinación para la Prevención de Delitos Electrónicos, la cual lleva a cabo acciones de prevención e investigación de conductas ilícitas a través de medios informáticos, monitorea la red pública de

[19] Reglamento de la Ley de la Policía Federal. 27 de mayo del 2010, última modificación 22 de agosto del 2014, [fecha de consulta: abril 2016]. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5143004&fecha=17/05/2010

Internet para identificar conductas constitutivas de delito, efectuando actividades de ciber-investigaciones así como de ciberseguridad en la reducción, mitigación de riesgos de amenazas y ataques cibernéticos, así mismo, efectúa programas de desarrollo científico y tecnológico en materia cibernética.

En temas de Ciberseguridad, la Policía Federal cuenta con el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX), encargado de vigilar la integridad de la infraestructura tecnológica estratégica del país.

El CERT-MX opera áreas especializadas en temas de prevención e investigación de este tipo de ilícitos y es la única autoridad acreditada a nivel federal, para el intercambio de información con policías cibernéticas nacionales y organismos policiales internacionales, con el objetivo de identificar y atender posibles ataques en agravio de infraestructuras informáticas gubernamentales o contra la ciudadanía en general.

La Policía Federal, mantiene un monitoreo permanente de la red pública de Internet, en el cual emplea herramientas especializadas para la detección y respuesta oportuna de ataques en el ciberespacio, que opera las 24 horas del día, siete días de la semana, durante los 365 días del año.

De esta manera, en coordinación con 351 equipos de respuesta a incidentes cibernéticos de 74 países alrededor del mundo, formando parte de la comunidad del *Forum for Incident Response and Security Teams* (FIRST[20]) –foro global donde convergen y colaboran lo equipos de respuesta a incidentes cibernéticos–, se generan y fortalecen líneas de investigación para que en colaboración con las policías cibernéticas de otras naciones, se logre la identificación y ubicación de probables responsables de ataques cibernéticos, sumando esfuerzos con la Procuraduría General de la República.

En materia de prevención, se realiza el intercambio de información, con agencias internacionales, referente a nuevas amenazas cibernéticas descubiertas en servicios, protocolos y fabricantes de *software* y *hardware* lo que permite dar una mejor atención y orientación a la ciudadanía.

De igual forma, se han establecido alianzas estratégicas con empresas privadas internacionales como Microsoft, la Asociación de Bancos de México (ABM) y organizaciones para las tareas de prevención estratégicas como el Desarrollo Integral de la Familia (DIF Nacional).

La ciberseguridad es una responsabilidad compartida, no se puede entender sin una alianza público privada, es por ello que desde la

[20] FIRST [en línea], [fecha de consulta: abril 2016]. Disponible en: https://www.first.org/.

Policía Federal se impulsan acciones conjuntas de concientización en los diferentes sectores productivos a fin de que adopten una cultura de prevención del delito cibernético desde las empresas, el gobierno y la sociedad en su conjunto.

Estrategia de Ciberseguridad de la Policía Federal

A fin de hacer frente a la ciberdelincuencia, y de continuar con los esfuerzos del Gobierno de la República, para lograr un México en Paz, la Policía Federal, a través de la División Científica, alineado al Plan Nacional de Desarrollo 2013-2018 y al Programa Nacional de Seguridad Pública 2014-2018, desarrolló la Estrategia de Ciberseguridad, a fin de hacer frente a la ciberdelincuencia, basada en tres principales ejes:

- Dirigir acciones de prevención y atención de los delitos cibernéticos mediante la difusión masiva de información y orientación a la ciudadanía e instituciones públicas y privadas;
- Detección y atención oportuna de amenazas y ataques cibernéticos a fin de reducir, neutralizar o mitigar las afectaciones a la ciudadanía y los sectores económicos del país, y
- Fortalecer las capacidades técnico-científicas para la investigación de delitos cibernéticos.

Las líneas de acción de la Estrategia de Ciberseguridad de la Policía Federal consideran:

I. Prevención del Ciberdelito

a) *Promover la cultura de prevención en delitos cibernéticos*. Evitar víctimas mediante medios eficientes de difusión de acciones preventivas;
b) *Fortalecer la Atención Ciudadana*. Establecer mecanismos que estén al alcance de la ciudadanía y el fortalecimiento en el seguimiento de la acción policial que genere la credibilidad e incentive la denuncia ciudadana, y
c) *Indicadores y Estadísticas*. Promover el registro de información relacionada con los ciberdelitos a fin de generar datos estadísticos e indicadores de alcance nacional que incidan en el diseño e implementación de políticas públicas en la materia.

II. Modelo Cibernético

a) *Modelo de Policía Cibernética*. Implementar el Modelo en el ámbito estatal a fin de homologar los procedimientos en las entidades federativas que permitan articular esfuerzos y acciones a nivel nacional;

b) *Armonización Legislativa*. Participar de manera activa en la elaboración y revisión de las iniciativas de reformas a la legislación nacional que permitan armonizar la labor policial, ministerial y judicial al entorno local e internacional para la atención de los ciberdelitos, y
c) *Colaboración con Policías Cibernéticas Extranjeras*. Promover el intercambio de información entre instituciones policiales del orbe a fin de colaborar y coordinar operativos regionales.

III. Ciberseguridad

a) *Detección y Atención de Incidentes Cibernéticos*. Fortalecer la atención de incidentes cibernéticos mediante la actualización constante del personal en materia de vulnerabilidades informáticas, tendencias de la ciberseguridad, modalidades delictivas, análisis de código malicioso (malware) y el uso de herramientas especializadas en la detección y mitigación de incidentes;
b) *Protección de Infraestructuras Críticas Informáticas e Industriales*. Coordinar la protección de los activos de información críticos del país mediante el diseño de mecanismos y protocolos de colaboración con los sectores públicos y privados cuyas afectaciones cibernéticas pudieran representar consecuencias económicas, sociales o políticas de gran perjuicio a la nación, y
c) *Investigación Científica y Tecnológica*. Impulsar los avances de la ciencia y la tecnología hacia temas de seguridad pública en coordinación con instituciones académicas y de desarrollo tecnológico con la finalidad de generar productos y servicios orientados a la protección del ciberespacio mexicano con recursos nacionales.

IV. Coordinación e intercambio de información nacional e internacional

a) *Generación de redes internacionales de colaboración*. Establecer vínculos de cooperación y colaboración internacional con instituciones policiales, agencias, equipos de respuesta a incidentes cibernéticos, entre otros, a fin de privilegiar la prevención de los ciberdelitos;
b) *Intercambio de información y operaciones coordinadas*. Fortalecer el intercambio de información de inteligencia policial y la detección de actividad maliciosa en el ciberespacio mexicano con la finalidad de identificar presuntos responsables de los ciberdelitos y su localización a fin de neutralizar sus operaciones y lograr su detención, y
c) *Deep Web y Bit Coin*. Realizar el monitoreo de la red pública de Internet donde los buscadores tradicionales no acceden, a fin de evitar que la ciberdelincuencia opere de manera clandestina

actividades ilícitas como lavado de dinero, venta de armas, narcóticos, programas de cómputo con fines delictivos y otros.

Nuevo Sistema de Justicia Penal Acusatorio

El 18 de junio del 2008 fue publicado en el *Diario Oficial de la Federación* el Decreto por el que se reforman los artículos 16, 17, 18, 19, 20, 21 y 22; las fracciones XXI y XXIII del artículo 73; la fracción VII del artículo 115 y la fracción XIII del apartado B del artículo 123, todos de la *Constitución Política de los Estados Unidos Mexicanos*.

La envergadura de la reforma constitucional en materia penal representa no sólo un parteaguas en los sistemas de procuración e impartición de justicia, sino un verdadero cambio de paradigma que todos los actores que conforman un Estado democrático de Derecho debemos asumir con responsabilidad y compromiso. En consecuencia, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, deberán expedir y poner en vigor las modificaciones u ordenamientos legales que sean necesarios a fin de incorporar el sistema procesal penal acusatorio.

Mediante la reforma constitucional, el procedimiento penal transita del procedimiento semi-inquisitorio al acusatorio y oral, cuyos principios (publicidad, contradicción, concentración, continuidad e inmediación) recoge el artículo 20 constitucional.[21]

Las etapas del sistema penal acusatorio están divididas en:

- Investigación;
- Intermedia, y
- Juicio oral.

La investigación de los hechos que revistan características de un delito podrá iniciarse por denuncia, por querella o por su equivalente cuando la ley lo exija. El Ministerio Público y la Policía están obligados a proceder sin mayores requisitos a la investigación de los hechos de los que tengan noticia.

Dentro de las técnicas de investigación se encuentra la cadena de custodia, como sistema de control y registro que se aplica al indicio, evidencia, objeto, instrumento o producto del hecho delictivo, desde su localización, descubrimiento o aportación, en el lugar de los hechos o del hallazgo, hasta que la autoridad competente ordene su conclusión.[22]

[21] El Nuevo Sistema de Justicia Penal Acusatorio, desde la Perspectiva Constitucional. Primera edición, México, 2011. Consejo de la Judicatura Federal. Poder Judicial de la Federación.

[22] Código Nacional de Procedimientos Penales 2014, Art. 227.

Así mismo, dentro de la etapa del juicio, las partes pueden presentar pruebas periciales, en principio los peritos son personas que cuentan con una experiencia especial en un área de conocimiento, derivada de sus estudios o especialización profesional del desempeño de ciertas artes o del ejercicio de un determinado oficio.[23]

De esta forma, tanto la preservación de los indicios y evidencias de tipo digital y los informes periciales cobran relevancia en el nuevo sistema penal acusatorio, la importancia del trabajo técnico-científico efectuado por áreas especializadas como la Coordinación para la Prevención de Delitos Electrónicos podría ser determinante en la toma de decisiones a cargo de los tribunales en el país.

Por lo anterior, se prevé un incremento en la demanda de investigaciones cibernéticas que realiza la Coordinación para la Prevención de Delitos Electrónicos en atención a las solicitudes de las autoridades competentes para la obtención y/o análisis de evidencia digital como recurso probatorio en el sistema judicial. Asimismo, se debe observar que al hablar de ciberdelitos, el lugar de los hechos en algunas conductas constitutivas de delito puede ser un disco duro, un sistema informático o un servicio en la nube/internet. Lo cual trae consigo la necesidad de profesionalizar a los elementos policiales en los procedimientos, técnicas y herramientas que den certeza al manejo de la evidencia digital a fin de mantener su integridad, confidencialidad y disponibilidad ante las autoridades judiciales.

Es un gran reto y una gran oportunidad para el país la implementación del nuevo sistema penal acusatorio en la época en que vivimos, en donde se reconoce nuevas modalidades de generación de riqueza para los países y sociedades en su conjunto basada en la información digital, y con ello el surgimiento de nuevas modalidades de crimen que afectan el aprovechamiento de los recursos tecnológicos de las sociedades de la información y el conocimiento. Por ello, la Policía Federal, capacita a sus integrantes en el nuevo sistema penal a la par de capacitarlos en los nuevos avances tecnológicos, con la finalidad de entender con claridad la economía del cibercrimen y como poderla prevenir y castigar conforme a las herramientas legales con que cuenta el Estado Mexicano.

Conclusiones

- A fin de contribuir en alcanzar la Meta Nacional “Un México en Paz” y generar las condiciones en el ciberespacio mexicano que ofrezca un entorno seguro a las personas, organizaciones, empresas, gobiernos e instituciones en general, es importante que la labor

[23] Pastrana, Berdejo, 2011. Las etapas del procedimiento penal acusatorio, [fecha de consulta: abril 2016]. Disponible en: http://www.paraosc.segob.gob.mx/work/models/PARAOSC/Resource/125/1/images/4_Etapas_del_Procedimiento_Penal.pdf

de prevención se establezca como parte de la cultura cívica de la población, de manera tal que el Internet como una potencial herramienta de desarrollo económico, político y social sea utilizado de manera responsable. De tal manera, que la responsabilidad no sólo recae en los gobiernos sino también de la sociedad mexicana y los sectores industriales, financieros, económicos y productivos del país, por ello, se estima pertinente el desarrollo de una estrategia nacional que incluya alianzas estratégicas público-privadas, amplia cobertura y colaboración a nivel local, regional e internacional, así como la participación ciudadana como ejes fundamentales de crecimiento y sustentabilidad;

- Dentro de los retos del nuevo entorno operativo, se ampliarán los servicios a través del Internet con el impulso del **"Internet de las Cosas"** y las **"Ciudades Inteligentes"**, lo que implicará nuevas amenazas y ataques en el ciberespacio mexicano, por lo que el fortalecimiento de las capacidades operativas para la prevención e investigación de los ciberdelitos representa un área de oportunidad para los gobiernos quienes deberán establecer sus estrategias a fin de contrarrestar el fenómeno delictivo;
- El Modelo de Policías Cibernéticas para las entidades federativas desarrollado por la División Científica de la Policía Federal representa un esfuerzo en materia de ciberseguridad que ofrece una alternativa a la homologación de procedimientos y el uso de técnicas y herramientas que pretenden sustentar las evidencias necesarias para la prevención e investigación de los ciberdelitos;
- Con la implementación del nuevo sistema penal acusatorio en todo el territorio nacional a partir de junio del 2016, las instituciones policiales, de procuración e impartición de justicia deberán acelerar la curva de aprendizaje sobre las cuestiones técnicas que representa el uso de técnicas y herramientas informáticas a fin de que los procedimientos del proceso penal consigan el objetivo de procurar e impartir justicia de forma pronta y expedita;
- Es importante la revisión y actualización constante del marco jurídico legal de nuestro país, que permita identificar aquellas conductas antisociales que podrían tener vacíos legales en términos de su investigación oportuna y su sanción, en la que el derecho informático constituya una herramienta para el fortalecimiento de la regulación mexicana, y
- Así mismo, es de suma importancia la asistencia legal mutua con otros países del orbe, por lo que se considera revisar la importancia que tiene la adhesión de México al Convenio de Budapest en términos de armonización legislativa a nivel internacional, con la finalidad de allanar el camino a la investigación transfronteriza, la incursión de cibercriminales se ha hecho presente en los últimos años y requiere de una atención integral.

Bibliografía

Asociación Mexicana de Internet, Estudio Comercio Electrónico en México 2015 [en línea], [fecha de consulta: abril 2016]. Disponible en: https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf

Asociación Mexicana de Internet, Estudio Comercio Electrónico en México 2015 [en línea], [fecha de consulta: abril 2016]. Disponible en: https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf

Berdejo, Pastrana 2011. Las etapas del procedimiento penal acusatorio, [fecha de consulta: abril 2016]. Disponible en: http://www.paraosc.segob.gob.mx/work/models/PARAOSC/Resource/125/1/images/4_Etapas_del_Procedimiento_Penal.pdf

Código Nacional de Procedimientos Penales 2014, Art. 227.

El Nuevo Sistema de Justicia Penal Acusatorio, desde la Perspectiva Constitucional. Primera edición, México, 2011. Consejo de la Judicatura Federal. Poder Judicial de la Federación.

Estrategia Digital Nacional (EDN), Presidencia de la República, mayo 2014, [fecha de consulta: abril 2016]. Disponible en: http://www.gob.mx/mexicodigital

FIRST [en línea], [fecha de consulta: abril 2016]. Disponible en: https://www.first.org/.

Instituto Nacional de Estadística y Geografía, INEGI 2015. [Fecha de consulta: mayo 2016] http://www.inegi.org.mx/saladeprensa/boletines/2016/especiales /especiales2016_03_01.pdf

Internet SecurityThreat Report, Symantec (2015).

Norton by Symantec, *op. cit*., [fecha de consulta: abril 2016]. Disponible en: https://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf

Norton by Symantec, Reporte Norton 2013 [en línea], [fecha de consulta: abril 2016]. Disponible en: https://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf

Organización de las Naciones Unidas, Objetivos de Desarrollo del Milenio [en línea], [fecha de consulta: abril 2016]. Disponible en: http://www.undp.org/content/undp/es/home/sdgoverview/mdg_goals/

Plan Nacional de Desarrollo 2013-2018, Presidencia de la República, mayo 2013, [fecha de consulta: abril 2016]. Disponible en: http://pnd.gob.mx

PRODEIIN 2013-2018, Censos Económicos (2009). Micro, pequeña, mediana y gran empresa: estratificación de los establecimientos: Censos Económicos 2009 / INEGI, c2011. 2013 [en línea], [fecha de consulta: abril 2016]. Disponible enhttp://www.institutopyme.org/index.php?option=com_content&view=article&id=134&,

Programa Nacional de Seguridad Pública 2014-2018, [fecha de consulta: abril 2016] Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5343081&fecha=30/04/2014

Refiere al Reglamento de la Ley de la Policía Federal. 27-mayo-2010, última modificación 22-agosto-2014 [fecha de consulta: abril 2016]. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5143004&fecha=17/05/2010

Trend Micro, Latin American and Caribbean Cybersecurity Trends and Government Responses [en línea], [fecha de consulta: abril 2016]. Disponible en: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf

Unión Internacional de Telecomunicaciones, ICT Facts & Figures 2015 [en línea], [fecha de consulta: abril 2016]. Disponible en: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

Unión Internacional de Telecomunicaciones, UIT 2009, Aspectos Generales de la Ciberseguridad [fecha de consulta: abril 2016]. Disponible en PDF en: https://www.itu.int/rec/T-REC-X.1205-200804-I/es

World Economic Forum, Global Risks 2013 [en línea], [fecha de consulta: abril 2016]. Disponible en: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf