CIBERSEGURIDAD, RETOS Y PROSPECTIVA

Oliver González Barrales

1. RESUMEN

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, y de manera general, las medidas a adoptar para contrarrestar sus efectos.

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 medio 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.

PALABRAS CLAVE: ciberseguridad, ciberdelito, ciberdelincuencia, delitos electrónicos, ciberdelincuente.

2. INTRODUCCIÓN

Con el nacimiento de la era espacial, las computadoras y el internet, la sociedad global ha sufrido una evolución tecnológica sin precedentes, llamada hoy en día la tercera revolución industrial. 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 transitando hacia la sociedad de la información, cada día más servicios son ofrecidos vía internet, más información es almacenada en la nube y un mayor número de dispositivos son conectados alrededor del mundo. Las empresas dependen cada vez más de 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 y el mejoramiento de los sistemas que componen la ciudad para crear, recopilar, procesar y transformar la información que incida en mejores servicios y calidad de vida mediante el uso eficiente de sus recursos.

Empero, la innovación tecnológica ha ido acompañada de un aumento en la delincuencia informática, en donde el alcance de los ataques cibernéticos y el daño económico combinado de la ciberdelincuencia ha llegado a un nivel tal que en algunos países la ciberdelincuencia puede haber superado a la delincuencia tradicional. Se ha identificado un aumento en la agresividad de los delitos informáticos[12].

En los últimos años ha tomado auge el término "Crime as a Service" que sustenta que el cibercrimen proporciona herramientas y servicios a través de todo el espectro de la delincuencia en Internet, a los atacantes cibernéticos de bajo perfil hasta terroristas cibernéticos.

3. LA TRICOTOMÍA DEL CIBERDELITO

A la par de la evolución del Internet se han ido generando las circunstancias propicias para aquellos que buscan un beneficio personal a costa de ciberusuarios, las afectaciones derivadas comparten un origen y una serie de características comunes de la actividad delictiva, tal es el caso del bajo grado de riesgo para el delincuente y el alto grado de efectividad e 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[13]. Este último ligado al robo de datos personales.

[12] Internet Organised Crime Threat Assessment, EUROPOL, 2016

[13] 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

La teoría denominada la tricotomía del ciberdelito[14] describe la relación estrecha entre el volumen de atacantes, la ganancia por ataque y el volumen de víctimas. Estas tres estrechamente relacionadas con las medidas a tomar para prevenir o investigar, según sea el caso, las afectaciones por ciberdelitos.

Existe un gran volumen de atacantes que no necesariamente tienen grandes habilidades, un nivel alto de confianza o técnicas de ataque innovadoras, sin embargo, por la falta de concientización en ciberseguridad y protección de un alto volumen de víctimas, pueden generar un alto porcentaje de efectividad con ganancias mínimas por ataque. Esto se traduce en un alto volumen de ganancias obtenidas por la afectación a un alto volumen de víctimas que se puede prevenir en gran medida con una estrategia de concientización en materia de ciberseguridad.

Por otro lado nos encontramos con atacantes más sofisticados, estos cuentan con grandes capacidades y técnicas de intrusión innovadoras, sus ganancias por ataque son altas y regularmente sus ataques están dirigidos a víctimas con un alto perfil económico que a su vez tienen un nivel de concientización, protección y seguridad elevado, por ende, las ganancias son bastas aunque en un bajo volumen de víctimas. Esto se traduce en un alto volumen de ganancias obtenidas en un bajo volumen de víctimas que en muchos casos se tiene que llegar a una investigación cibernética para identificar a los atacantes.

En 2014, los ataques más comunes en el Internet de las Cosas 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[15].

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[16].

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[17].

Quizá esta sea una de las razones por las que la actividad de programas de cómputo maliciosos (malware) también fue una de las principales afecciones,

---

[14] Internet Organised Crime Threat Assessment, EUROPOL, 2016

[15] Internet SecurityThreat Report, Symantec (2015)

[16] 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

[17] 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.

registrándose un incremento del 40% en incidentes cibernéticos en 2012[18]. 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[19].

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[20].

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 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[21].

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[22], quedó establecido como:

---

[18] 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.

[19] 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

[20] 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

[21] 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

[22] 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

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.

4. RETOS EN MATERIA DE CIBERSEGURIDAD

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%[23].

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[24].

El escenario en México, de acuerdo con datos de la Asociación Mexicana del Internet (AMIPCI), es notable incremento en la cifra de cibernautas, 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[25].

---

[23] 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.

[24] 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/

[25] 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

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 Promexico 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[26].

Por otro lado, los delincuentes cibernéticos han evolucionado desde el nacimiento de las Tecnologías de la Información y Comunicación, en la década de 1970, se inició con la experimentación e investigación de las nuevas tecnologías, durante la década de 1980 nace el termino hacer motivados por la curiosidad, en su mayoría experimentación de carácter benigno. Llegando la década del 2000, los script kiddies intentan causar daños y hacerse famosos pero aún sin objetivos claros, evolucionando en 2005 en cibercriminales con objetivos específicos y motivos comerciales, utilizando nuevas técnicas como el phishing, malware y redes de botnets. En la década de 2010 los ciberatacantes son ya profesionales con equipos sofisticados, nacen los grupos hacktivistas con motivos políticos y estratégicos. En los últimos años, se han generado estructuras de ciberdelincuencia organizada para realizar ataques y proveer servicios mediante la utilización de métodos y herramientas sofisticadas.

Derivado de los datos anteriores, se establecen como retos en materia de ciberseguridad las iniciativas que impulsen las capacidades en la investigación, la formación y desarrollo de capacidades en ciberseguridad, la prevención como mecanismo de combate al cibercrimen, la cooperación nacional e internacional, y la armonización legislativa en la materia.[27]:

A. Investigación

Incrementar las capacidades de investigación de los delitos cibernéticos con el objetivo de llegar a los ciberdelincuentes, lo anterior aunado a la cooperación en materia cibernética, hará cada vez más efectiva nuestras capacidades de identificación de los responsables.

- Las entidades que aplican la ley deben tener las herramientas, técnicas y conocimientos para combatir el uso delictivo del cifrado y el anonimato en internet. Se debe seguir centrándose en la atribución y el desarrollo de la inteligencia con el fin de identificar, localizar y procesar a individuos criminales clave para lograr un mayor impacto permanente en la comunidad criminal.

[26] 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 en http://www.institutopyme.org/index.php?option=com_content&view=article&id=134&,

[27] Internet Organised Crime Threat Assessment, EUROPOL, 2016

- Es esencial asignar recursos suficientes para investigar el malware y otros servicios que permiten generar ataques cibernéticos.

- Se debe contribuir y participar en actividades operativas y de prevención relacionados a los ataques cibernéticos. Esto dará lugar a un impacto mayor y más extenso en la lucha contra la criminalidad.

- El intercambio de inteligencia es esencial, esto ayudará a evitar la duplicación de esfuerzos, facilitar el intercambio de tácticas y herramientas, y aumentar la comprensión de las amenazas cibernéticas.

- Debe haber un esfuerzo continuo de todos para dar prioridad a las víctimas en las investigaciones.

B. Formación y desarrollo de capacidades

Especializar a los profesionales en materia de ciberseguridad, incluyendo el uso de monedas electrónicas y darknets para ampliar la cobertura de investigación de los delitos cibernéticos.

- Garantizar que se cuente con la capacitación y los recursos necesarios para el manejo de la evidencia digital en sitio utilizando técnicas como análisis forense de datos.

- Invertir en la formación especializada adecuada requerida para investigar con eficacia los ataques cibernéticos altamente técnicos.

- Dada la naturaleza cambiante de la ciberdelincuencia y el ritmo al que evoluciona la tecnología, existe una necesidad de un enfoque más adaptable y ágil a la investigación y el desarrollo, con miras a la obtención de resultados relevantes de una manera más oportuna.

- A medida que el uso criminal de monedas virtuales continúa ganando impulso, es cada vez más importante garantizar que los delitos informáticos y los investigadores financieros tienen una formación adecuada en la localización, la incautación e investigación de monedas virtuales.

- Un esfuerzo coordinado debe ser tomado por la policía para colaborar con los países donde se compren bienes y servicios con tarjetas de crédito comprometidas.

- La capacitación en Darknets debe ser un tema es un tema transversal para el apoyo de especialistas en múltiples tipos de delitos.

- No es factible o práctico que todos los delitos sean tratados por las unidades de delitos informáticos cuando el delito predicado está relacionado con drogas, armas de fuego o alguna otra mercancía ilícita. Es esencial, por tanto, que el entrenamiento apropiado y soporte de la herramienta se extienda a las personas que trabajan en estas áreas para proporcionarles los conocimientos y la experiencia necesaria.

C. Prevención

Se deben desplegar campañas de sensibilización y concientización en materia de ciberseguridad, invertir en prevención se vuelve un tema de eficiencia sobre la inversión en investigación, después de ocurrido el delito cibernético.

- La inversión de recursos en actividades de prevención puede ser más eficiente que la investigación de los incidentes individuales. Además de la sensibilización y consejos de prevención del delito, las campañas deben aconsejar al público sobre cómo reportar los crímenes cibernéticos.

- Las campañas de prevención no deben centrarse únicamente en la prevención de los ciudadanos y las empresas que puedan llegar a ser víctimas de los delitos informáticos, sino también en la prevención de las consecuencias legales a delincuentes cibernéticos potenciales que se involucren en dicha actividad.

- Las campañas de prevención deben coordinarse con otras organizaciones nacionales e internacionales.

- Se debe fomentar el uso de software de seguridad y la denuncia de los ataques cibernéticos.

- Se debe mantener un enfoque en el desarrollo y la distribución de campañas de prevención y sensibilización. Estas campañas deben actualizarse para abarcar las tendencias actuales.

D. Cooperación

Se debe mantener una cooperación nacional e internacional en materia de ciberseguridad, tanto en el sector público, privado y académico para sumar esfuerzos en la lucha contra el cibercrimen.

- Se deben forjar y mantener la colaboración en materia de ciberseguridad con el mundo académico, el sector privado y el gobierno.

- Se requiere un esfuerzo adicional, a través del intercambio de información más centrado en cumplimiento de la ley, para vincular los casos de fraude de tarjetas. Esto facilitaría la identificación de los grupos del crimen organizado involucrados en el fraude de tarjetas de crédito.

- Se deben llevar a cabo operaciones a gran escala en materia de prevención e investigación del ciberdelito.

- Debe existir una colaboración activa con el Centro Especializado en Respuesta Tecnológica (CERT-MX), para dar seguimiento a las investigaciones criminales derivadas de incidentes cibernéticos.

- Se deben establecer relaciones de trabajo con otras naciones para operar bajo jurisdicciones extranjeras.

- A medida que el uso criminal de monedas virtuales continúa ganando impulso, es cada vez más importante construir y mantener relaciones con la comunidad de moneda virtual, en particular los centros de cambio de moneda virtual.

E. Legislación

Se deben impulsar proyectos de armonización legislativa en materia de delitos electrónicos..

- Se requiere un enfoque armonizado para las investigaciones encubiertas en otras naciones. al respecto, la adhesión al convenio de Budapest (convenio sobre criminalidad) puede ser una opción para la armonización legislativa.

- Se deben sumar esfuerzos para asegurar que las infraestructuras críticas de TICs se encuentren protegidas por la legislación nacional aplicable.

- La armonización legislativa debe tipificar ciertas conductas para no permitir los refugios donde los delincuentes cibernéticos pueden evitar la investigación en su contra y el procesamiento judicial.

- Se debe permitir el intercambio de información y un enfoque coordinado para dar respuesta eficaz a los ataques cibernéticos

graves. En este término, la asistencia legal mutua cobra suma importancia.

5. DECALOGO DE CIBERSEGURIDAD

Para incrementar nuestro nivel de seguridad de la información, a continuación se emiten una serie de recomendaciones generales.

1. Mantener actualizados los sistemas y aplicaciones de cómputo.

2. Utiliza contraseñas robustas con al menos 10 caracteres alfanuméricos y símbolos.

3. Utiliza doble factor de autenticación para servicios en línea, como las de correo electrónico y bancos.

4. Realiza respaldos de manera periódica y guárdalos en discos externos.

5. No abras documentos adjuntos y enlaces que vienen en correos de origen desconocido.

6. No realices depósitos antes de verificar que la operación sea legítima.

7. Desconfía de correos y páginas con ofertas atractivas de artículos y servicios.

8. Comprueba el nivel confiabilidad de los sitios web y la seguridad de su conexión (“https:// ”).

9. Configura los parámetros de seguridad y privacidad en cuentas de correo electrónico y redes sociales.

10. Concientiza entre familiares, amigos y compañeros de trabajo la importancia de la seguridad de la información.

6. CONCLUSIONES

- 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, 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.

- Existe un gran volumen de atacantes que no necesariamente tienen grandes habilidades, un nivel alto de confianza o técnicas de ataque innovadoras, sin embargo, por la falta de concientización en ciberseguridad y protección de un alto volumen de víctimas, pueden generar un alto porcentaje de efectividad con ganancias mínimas por ataque. Esto se traduce en un alto volumen de ganancias obtenidas por la afectación a un alto volumen de víctimas que se puede prevenir en gran medida con una estrategia de concientización en materia de ciberseguridad.

- Los atacantes más sofisticados cuentan con grandes capacidades y técnicas de intrusión innovadoras, sus ganancias por ataque son altas y regularmente sus ataques están dirigidos a víctimas con un alto perfil económico que a su vez tienen un nivel de concientización, protección y seguridad elevado, por ende, las ganancias son bastas aunque en un bajo volumen de víctimas. Esto se traduce en un alto volumen de ganancias obtenidas en un bajo volumen de víctimas que en muchos casos se tiene que llegar a una investigación cibernética para identificar a los atacantes.

- Se establecen como retos en materia de ciberseguridad las iniciativas que impulsen las capacidades en la investigación, la formación y desarrollo de capacidades en ciberseguridad, la prevención como mecanismo de combate al cibercrimen, la cooperación nacional e internacional, y la armonización legislativa en la materia.

- 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.

7. FUENTES DE CONSULTA

- [1] Internet Organised Crime Threat Assessment, EUROPOL, 2016
- [1] 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
- [1] Internet SecurityThreat Report, Symantec (2015)
- [1] 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

- [1] 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.
- [1] 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
- [1] 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
- [1] 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
- [1] 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
- [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.
- [1] 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/
- [1]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&,