Gênero & Direito
Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 6 - Nº 03 - Ano 2017 (Spanish Edition)
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

FACTORES QUE CONTRIBUYEN A LA PREVENCIÓN DE LOS DELITOS INFORMÁTICOS EN EL ESTADO DE TABASCO

Alex Javier López González[1]
Laura López Díaz[2]
Rubén Jerónimo Yedra[3]

Resumen: La enorme dependencia de la sociedad respecto a los sistemas informáticos y electrónicos está haciendo que ésta sea más vulnerable a los posibles ataques cibernéticos. Además, Internet es un medio de fácil acceso, donde cualquier persona, puede realizar un ataque que es complicado de asociar, con la cual, la red se está convirtiendo en ese lugar ideal para que los delincuentes y los terroristas lleven a cabo sus acciones y actividades. De ahí, que el ciberdelito, haya pasado a ser de las más importantes amenazas que parecen acechar a la sociedad. Por tal razón, a la lo largo de este artículo se muestran estadísticas de cada uno de los factores que contribuyen a evitar los posibles ataques cibernéticos y las actividades delictivas en el ciberespacio. Asimismo, medidas que se han realizado para evitar que aumenten los delitos informáticos.

Palabras Claves: Delitos informáticos, normas regulatorias, sexting

Abstract: The enormous dependence of the society on the computer and electronic systems is making it more vulnerable to possible cyber-attacks. In addition, the Internet is a way of easy access, where anyone can carry out an attack that is complicated to associate, with which, the network is becoming an ideal place for criminals and terrorists to carry out their actions and activities. Hence, Cybercrime has become one of the most important threats that seem to stalk the society. For this reason, throughout this article we will show statistics of each of the factors that contribute to avoiding possible cyber-attacks and criminal activities in cyberspace. In the same way, we will present some measures that must be

[1] Licenciado en Informática Administrativa. Profesor en el Instituto Universitario Panamericano Campus Villahermosa.
[2] Doctora en Educación. Profesora Investigadora en la División Académica de Informática y Sistemas de la Universidad Juárez Autónoma de Tabasco.
[3] Doctor en Educación. Profesor Investigador en la División Académica de Informática y Sistemas de la Universidad Juárez Autónoma de Tabasco.

taken to prevent the increase of cybercrimes.

Keywords: Cybercrimes, Regulatory Laws, sexting

INTRODUCCIÓN

En la actualidad las Tecnologías de la Información y Comunicación (TIC), en particular el Internet es un gran sistema creado por los seres humanos, que implica la conexión de millones de dispositivos que conforman redes descentralizadas para formar una gran red global.

Los gobiernos en conjunto con millones de usuarios y empresas utilizan esta tecnología para el desarrollo de funciones que se desarrollan a diario. La seguridad en Internet se convierte en un trabajo crítico que causa estragos en la vida cotidiana. Cada día existen miles de ataques que se materializan principalmente por estados, naciones, gobiernos, y ciberdelincuentes. Sin embargo, es común escuchar a cerca de nuevos sucesos delictivos (extorciones, violaciones, robos, pornografía infantil, asesinatos, ciberbullying, sexting etc.), por ello, la investigación digital pasa a formar parte en la aportación de pruebas testificales para esclarecer dichos desacatos, que se cometen con mayor relevancia y naturalidad.

La introducción de las TIC, en muchos aspectos de la vida cotidiana ha dado lugar al desarrollo del moderno concepto de sociedad de la información. Este desarrollo de la sociedad de la información proporciona grandes oportunidades. Un acceso sin obstáculos a la información supone un apoyo a la libertad puesto que el flujo de la información cae fuera del control de las autoridades estatales. Los desarrollos técnicos han mejorado la vida diaria; por ejemplo, los servicios bancarios y de compra en línea, la utilización de los servicios de datos móviles y la telefonía de voz por Internet (VoIP) son sólo ejemplos del avanzado grado de integración de las TIC en nuestras vidas diarias.

Sin embargo, en el uso desmedido y desenfocado de las TIC (computadoras, teléfonos móviles, Tablet y el internet) han propiciado ataques contra la infraestructura de la información y los servicios de Internet pues causan en la actualidad daños a la sociedad de una forma nueva y crítica. Ya que se han llegado a cometer distintos tipos de delitos como, los fraudes en línea, la difusión de pornografía infantil y extorsiones, robos etc. Por mencionar

algunos son ejemplos de delitos relacionados con la informática que se cometen a gran escala todos los días, lo que da paso a lo hoy se conoce cono delitos informáticos y un delito informático, suele entenderse por toda aquélla conducta ilícita susceptible de ser sancionada por el derecho penal, consistente en el uso indebido de cualquier medio informático o como cualquier conducta, no ética o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos (López, 2004).

Para Téllez (2004), Los delitos informáticos son aquéllas actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables, establece como característica de dichos antijurídicos que son conductas delictivas de cuello blanco, porque se requieren conocimientos técnicos; son acciones ocupacionales por realizarse cuando el sujeto activo labora, y son acciones de oportunidad pues se aprovecha la ocasión o el universo de funciones y organizaciones de un sistema tecnológico y económico.

DESARROLLO

Las nuevas tecnologías crean nuevas vulnerabilidades, ya sean en los teléfonos móviles, computadoras, Tablet etc., creando una serie de cambios y adaptaciones en la sociedad las cuales pueden ser buenas o malas, lamentablemente estos cambios sino en su mayoría, si se está reflejando en una buena parte de la sociedad una conducta indebida en cuanto al uso de las TIC, propiciando una serie de delitos en el ámbito informático lo que se conoce actualmente como ciberdelitos o delitos informáticos o también como cibercrimenes pero es conveniente definir antes lo que se entiende por delito informático. Aunque existen diversas definiciones al respecto; Hernández (2009), considera como delito informático: “toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas.

Los delitos informáticos van a la par del desarrollo de las tecnologías de la información, con el desarrollo de la tecnología, la sociedad se ha visto en un

panorama de avance y desarrollo en todas sus áreas; por desgracia, la delincuencia también se ha beneficiado de esto, entre los beneficios que ofrece el uso de redes de comunicación a los delincuentes se encuentran: la capacidad de cometer delitos en y desde cualquier parte del planeta, velocidad, gran cantidad de víctimas potenciales y anonimato, entre otros. (Loredo y Ramírez, 2013). En general y dada las definiciones anteriores se puede decir que la Ciberdelincuencia en sentido preciso (delito informático), comprende cualquier comportamiento ilícito realizado mediante operaciones electrónicas que atentan contra la seguridad de sistemas informáticos y de los datos que éstos procesan.

EL USO INCORRECTO DE LOS DISPOSITIVOS TECNOLÓGICOS

Para cometer un ciberdelito sólo hace falta un equipo básico. Delitos como la difamación o el fraude en línea no necesitan más que una computadora o teléfono celular y el acceso a Internet, y pueden llevarse a cabo desde una casa. Pueden cometerse otros delitos más minuciosos utilizándose en ese caso herramientas informáticas especiales.

Todas las herramientas necesarias para cometer delitos más minuciosos pueden encontrarse en Internet y, generalmente, de forma gratuita. Con ellas, los delincuentes pueden atacar otros sistemas informáticos con tan solo un clic. Los ataques más habituales son ahora menos eficaces, ya que las empresas de programas informáticos de protección analizan las herramientas actualmente disponibles y se preparan para ese tipo de ataque. Los ataques más comunes suelen diseñarse exclusivamente para objetivos específicos. Pueden encontrarse herramientas informáticas para cometer ataques por denegación de servicio (DoS), diseñar virus informáticos, desencriptar información y acceder en forma ilegal a sistemas informáticos.

Con las actuales herramientas informáticas se ha logrado la automatización de muchos ciberdelitos, y los delincuentes pueden llevar a cabo numerosos ataques en muy poco tiempo. Además, las herramientas informáticas simplifican los ataques, de modo que hasta los usuarios menos experimentados pueden cometerlos. Se cuenta también con herramientas para descargar archivos de los sistemas de intercambio de archivos o para colocarlos en ellos. Debido a la gran

disponibilidad de herramientas informáticas especialmente concebidas, el número de posibles delincuentes ha aumentado de forma espectacular, es por ello que están formulando diferentes iniciativas estatales, nacionales e internacionales en materia de legislación para combatir las herramientas informáticas que propician ciberdelitos.

En sentido general, ciberdelincuencia (delitos relacionados con los computadores) comprende cualquier comportamiento ilícito cometido por medio de un sistema informático o una red de computadores, o relacionado con éstos, incluidos delitos tales como la posesión ilícita y la puesta a disposición o distribución de información mediante sistemas informáticos o redes de computadores, así como los secuestros virtuales, extorsiones telefónicas, sexting, ciberbullying, entre otros.

TIPOS DE CIBERDELITOS

La utilización de la tecnología de la información con fines delictivos y la necesaria reacción jurídica son cuestiones que se debaten desde los inicios de esta tecnología. En los últimos años se han adoptado diversas soluciones en los planos nacional, regional y estatal. Una de las razones por las que el tema sigue siendo desafiante es el constante progreso tecnológico, así como la variedad y diversidad de las técnicas que se emplean para cometer los delitos cibernéticos algunos de los delitos cibernéticos o informáticos que son considerados por la a Organización de las Naciones Unidas (ONU), son:

1. Fraudes cometidos mediante manipulación de computadoras:
    - Manipulación de los datos de entrada.
    - Manipulación de programas.
    - Manipulación de datos de salida.
    - Fraude efectuado por manipulación informática.
2. Falsificaciones informáticas
    - Utilizando sistemas informáticos como objetos.
    - Utilizando sistemas informáticos como instrumentos.
3. Daños o modificaciones de programas o datos computarizados.
    - Sabotaje informático.
    - Virus.
    - Gusanos.
    - Bomba lógica o cronológica.

- Acceso no autorizado a sistemas o servicios.
- Piratas informáticos o hackers.
- Reproducción no autorizada de programas informáticos con protección legal.

Además de estos también se consideran los siguientes los cuales son llevados a cabo muy comúnmente en la actualidad.

- Ataques contra sistemas y datos informáticos.
- Usurpación de la identidad.
- Distribución de imágenes de agresiones sexuales contra menores estafas a través de internet.
- Intromisión en servicios financieros en línea.
- Producción de virus.
- Botnets (redes de equipos infectados controlados por usuarios remotos).
- Phishing (adquisición fraudulenta de información personal confidencial).

Sin embargo, no son los únicos, también existen delitos relacionados con el uso de las redes sociales y acceso a todo tipo de información tales como:

- Acceso a material inadecuado (ilícito, violento, pornográfico, etc.)
- Adicción (distracciones para los usuarios).
- Problemas de socialización.
- Robos de identidad acoso (pérdida de intimidad).
- Sexting (manejo de contenido erótico).
- Ciberbullying (acoso entre menores por diversos medios: móvil, internet, videojuegos, etc.).
- Cibergrooming (método utilizado por pederastas para contactar con niños y adolescentes en redes sociales o salas de chat)

TIPOS DE DELINCUENTES INFORMÁTICOS

Así como existen una gran cantidad de delitos relacionados con el uso de sistemas informáticos, también existe una amplia gama de delincuentes. Por un lado, son los expertos en seguridad informática a los que es común referirse con término de “hacker”. Una

definición del término es la que brinda el (Oxford English Dictionary (OED), 2010). Una persona que usa su habilidad con las computadoras para tratar de obtener acceso no autorizado a los archivos informáticos o redes. En primera instancia, esta definición asocia una conducta delictiva a todo hacker; pero en el ámbito informático tales se clasifican en dos tipos:

White hat hacker: se dedican a buscar vulnerabilidades en redes y sistemas sin realizar un uso malicioso de estas y posteriormente reportando los fallos. Las formas en que se monetiza esta actividad son varias: se busca reputación en el sector, sistema de recompensas, trabajando como consultor o responsable de seguridad en una compañía.

Black hat Hacker: individuos con amplios conocimientos informáticos que buscan romper la seguridad de un sistema buscando una ganancia, ya se obtener bases de datos para su posterior venta en el mercado negro, venta de "xploits" (vulnerabilidades de seguridad), robo de identidad, cuentas bancarias, etc. otro tipo de delincuentes que son aquellos que hacen uso del anonimato en internet con el fin de realizar conductas poco éticas: acoso, cyberbullying, estafas, pornografía infantil, turismo sexual, etc.

FACTORES QUE CONTRIBUYEN A LA DISMINUCIÓN DEL CIBERDELITO

La seguridad informática hoy en día debe desempeñar un papel importante en el avance en curso de la tecnología de la información, así como de los servicios de Internet para mejorar la ciberseguridad y proteger las bases de la información, es esencial para lograr la seguridad y el bienestar de cada país. Conseguir un servicio de Internet más seguro (y proteger a los usuarios de Internet) se ha convertido en parte integrante del desarrollo de nuevos servicios, así como de la política gubernamental. La disuasión del ciberdelito es una componente integrante de la ciberseguridad nacional y estatal tomando en cuenta la estrategia de protección de la infraestructura de la información crítica. En particular, ello incluye la adopción de las medidas jurídicas adecuadas contra la utilización fraudulenta de las TIC a efectos delictivos o de otro tipo y contra las actividades destinadas a afectar la integridad de las infraestructuras críticas nacionales y estatales. A nivel nacional,

se trata de una responsabilidad compartida que requiere una acción coordinada para la prevención, preparación, respuesta y recuperación de la normalidad tras los incidentes por parte de las autoridades gubernamentales, del sector privado y de los ciudadanos. A nivel regional e internacional, ello supone la cooperación y coordinación con los socios pertinentes. La formulación e implantación de un marco y estrategias nacionales para la ciberseguridad exige, por tanto, un enfoque amplio y completo.

Como por ejemplo el perfeccionamiento de sistemas de protección técnica o la enseñanza de los usuarios para evitar que se conviertan en víctimas de ciberdelito, pueden ayudar a reducir el riesgo de ciberdelito. El desarrollo y apoyo de las estrategias de ciberseguridad son un elemento vital en la lucha contra el ciberdelito. Los retos de tipo jurídico, técnico e institucional son de carácter mundial y de gran alcance y pueden abordarse únicamente mediante una estrategia coherente que tenga en cuenta el quehacer de los distintos interesados y las iniciativas actuales dentro de un marco de cooperación internacional.

Otro ejemplo para la prevención que se ofrece es la siguiente lista de las principales categorías de riesgo para las cuales la firma antivirus alemana Avira (2012), ofrece protección:

- Adware (muestra contenido publicitario en las actividades del usuario)
- Spyware (recopila datos personales y los envía a un tercero sin consentimiento del usuario)
- Aplicaciones de origen dudoso (programas que pueden poner en riesgo el equipo)
- Software de control backdoor (permiten el acceso remoto al equipo)
- Ficheros con extensión oculta (Malware que se oculta dentro de otro tipo de archivo para evitar ser detectado)
- Programas de marcación telefónica con coste (generan cargos en la factura de manera fraudulenta).
- Suplantación de identidad (phishing).
- Programas que dañan la esfera privada (Software que mermar la seguridad del sistema).
- Programas broma.
- Juegos (distracción en el entorno laboral) Software engañoso

(hacen creer el usuario que esta vulnerable y lo persuaden para comprar soluciones) Utilidades de compresión poco habituales (archivos generados de manera sospechosa).

LEYES - NORMAS REGULATORIAS

En México se han dictado diversas leyes para regular y castigar este tipo de delitos, entre las principales se encuentran: el código penal federal (2013), en su título noveno referente a la revelación de secretos y acceso ilícito a sistemas y equipos de informática:

Artículo 211 Bis. A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Artículo 211 bis 1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa. De igual forma en el Artículo 211 bis 2 a bis 5 se en listan los delitos, y correspondientes condenas, cometidos en equipos informáticos propiedad del estado, materia de seguridad pública e instituciones que integran el sistema financiero.

De igual manera se realizó un convenio sobre la ciberdelincuencia, firmado en Budapest, el 23 de noviembre de 2001, por los estados miembros del consejo de Europa, en cual México participa como observador permanente, se reconoce el problema de la ciberdelincuencia y la necesidad de una cooperativa trasnacional para abordarlo, en el cual se definen diferentes aspectos como: Definición de los delitos informáticos medidas que deben adoptar en sus legislaciones cada uno de los países miembros Jurisdicción sobre la información facilitar información entre los estados de ser necesario en alguna investigación.

Asimismo, en su artículo 9 se hace mención de los delitos relacionados

con la pornografía infantil con el cual se busca clasificar como delito los actos de: producción, oferta, difusión, adquisición y posesión de material pornográfico en el que se involucre un menor en cualquier sistema informático.

Estos son algunos factores que intervienen en la prevención de un ciberdelito sin embargo las cuestiones políticas y gubernamentales fungen como un pilar muy importante en la prevención de estos, utilizando implementar estrategias que se puedan desarrollar en poco tiempo, puesto que las mayorías de las estrategias en materia de ciberseguridad y ciberdelito se concentran en documentaciones muy temporales, que no ofrecen una información demasiado completa. Se dedican por lo general a destacar la importancia del tema, a revalidar la voluntad de actuar y a manifestar decisiones generales sobre lo que convendría hacer para mejorar la ciberseguridad. La mayoría de las estrategias no proponen soluciones concretas. Se considera que una estrategia debe aportar una solución a un determinado obstáculo o complicación para ser resuelto en la medida que sea posible, pero de manera inmediata.

PREVENCIÓN DEL CIBERDELITO EN EL ESTADO DE TABASCO

En el estado Tabasco, de acuerdo a la nota periodística que publico el periódico Excélsior, Ofelia Sánchez Frías, titular de la Unidad de Investigación de Delitos Informáticos de la FGE, indicó que las denuncias por "sexting" son más recurrentes en los últimos años expreso que, “en tres meses han registrado más de 30 casos, se trata de víctimas locales y de agresores tabasqueños, es increíble que en menos de dos horas un pederasta puede hacer que un niño se desnude y le envíe fotos. Llevan 10 casos, algunas direcciones IP son locales, y otras son redes de otros Estados”, refirió la funcionaria.

Por ello, a través de la Secretaría de Educación, la Unidad de Delitos Informáticos de la Fiscalía General del Estado (FGE) y la Secretaría de Salud, Tabasco se prepara para enfrentar las amenazas de delitos informáticos, principalmente contra los que atentan contra los niños y jóvenes.

Por lo cual se arrancará un programa para prevenir y cuidar los contenidos que los niños y jóvenes ven en las redes sociales, y advertir sobre las amenazas que significan los retos como La Ballena Azul, o los riesgos de

ser víctimas de cyberbullying, grooming, sexting y robos de identidad.

Las tres dependencias realizarán talleres y pláticas en las cuatro mil 900 escuelas de nivel básico de los 17 municipios del Estado, expuso el secretario de Educación, Ángel Solís Carballo.

Expresó que dichos talleres, pláticas y capacitaciones serán impartidas por personal de las tres dependencias citadas, (Excélsior, 2017).

Con la información anterior, se puede decir que se están tomando medidas de prevención contra el ciberdelito en el Estado, y de igual forma se están llevando a la práctica con base en una investigación de campo realizada mediante un cuestionario que se aplicó al personal de la Dirección del Centro Estatal de Análisis, al departamento de Evaluación de la Información y la Secretaría de Seguridad Pública. A continuación, se muestra de manera gráfica algunas de las medidas que se toman para prevenir los ataques delictivos de manera digital y algunos otros factores que son muy importantes conocer.

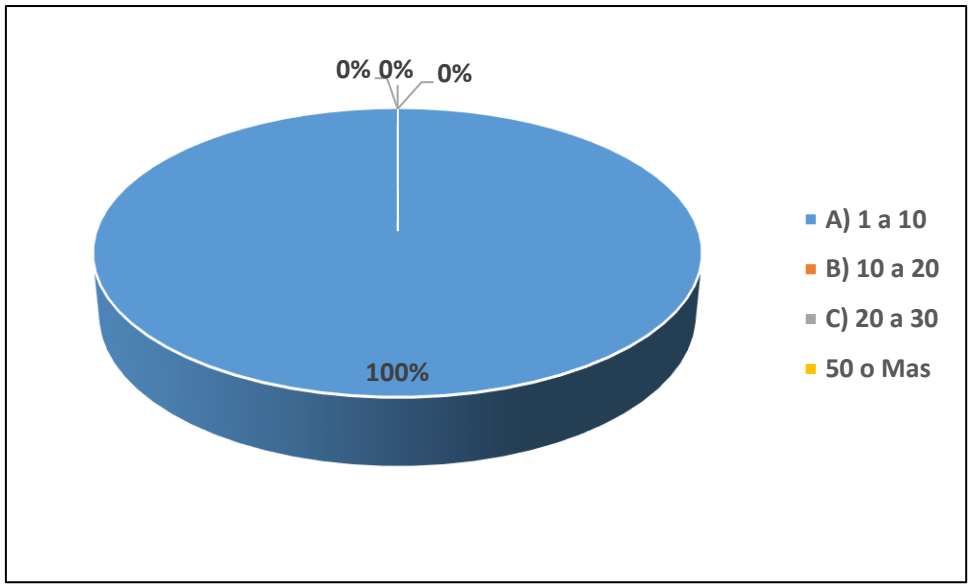

Figura 1.-Reportes de delitos cibernéticos que se reciben a diario.

En la figura 1, se ilustra que al día se denuncian de 1 a 10 delitos cibernéticos, lo que significa que gracias a esas denuncias se pueden prevenir más delitos, siendo de vital importancia que se den a conocer estos delitos para accionar ante ellos y así las autoridades

correspondientes tomen estrategias adecuadas para su solución.

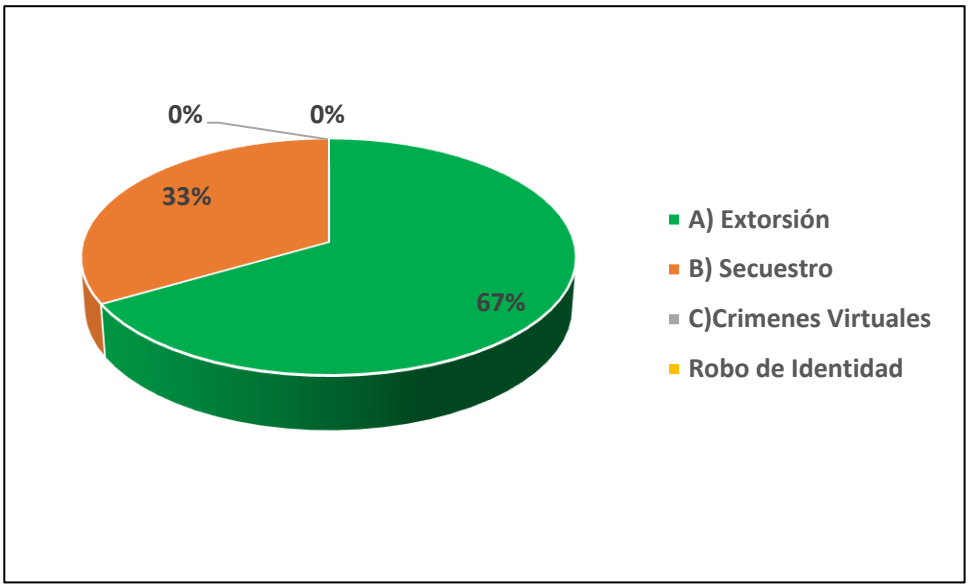

Figura 2.- Tipo de delito cibernético más reportado.

En la figura 2, se muestra que el delito más reportado es la extorsión con un 63% respuestas a favor, considerando que en la actualidad cometer una extorsión es más fácil para cualquier persona, mientras que el 33% de las personas encuestadas respondió que el secuestro.

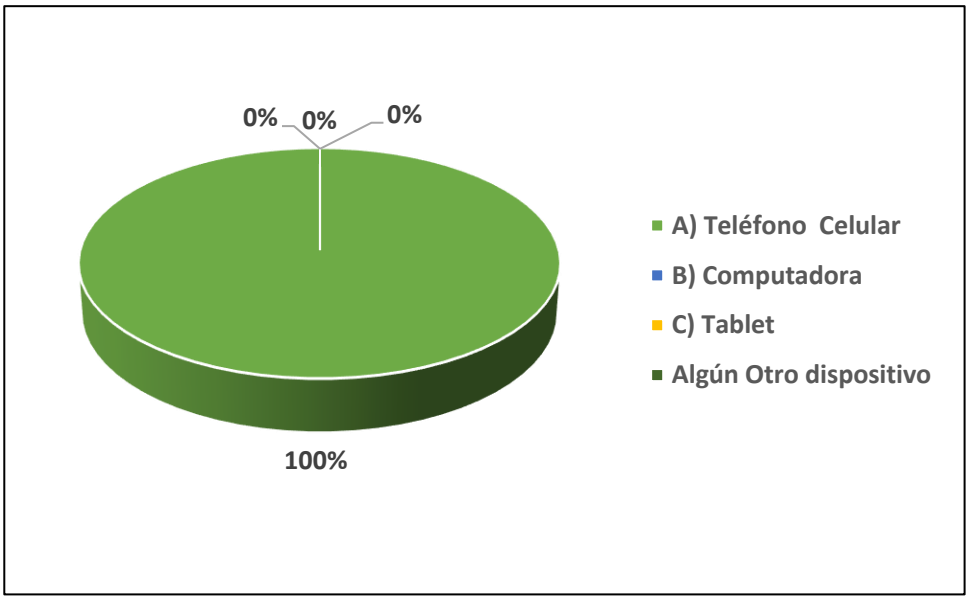

Figura 3.-Dispositivo tecnológico más utilizado para cometer un delito cibernético.

En la figura 3, se aprecia que el dispositivo más utilizado es el teléfono celular con un 100%, al ser uno de los dispositivos móviles de mayor demanda en el mercado, los teléfonos celulares, se vuelven un objetivo claro de las mentes criminales para materializar sus acciones delictivas, a través de una llamada telefónica o mensajes o alguna otra vía.

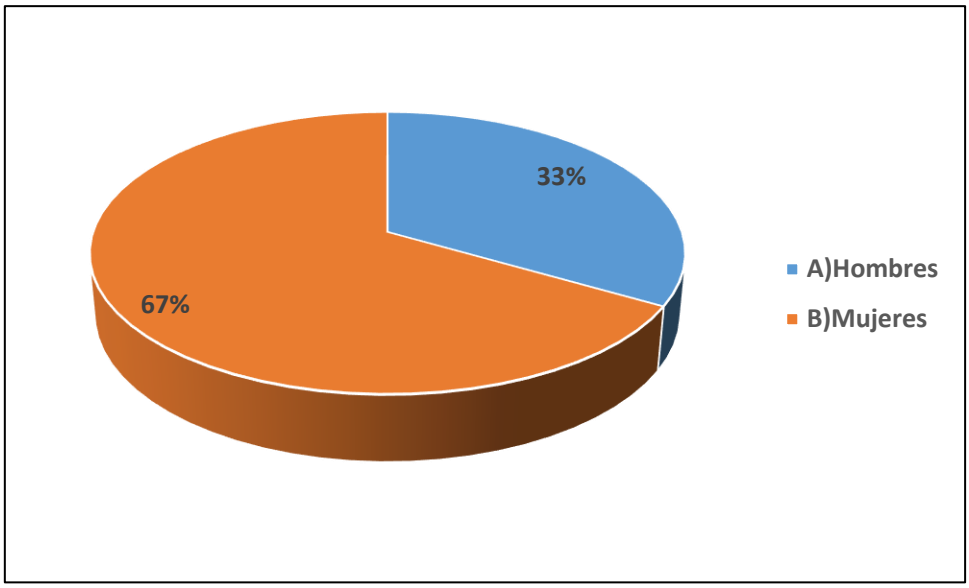

Figura 4.- Reporte de quien realiza más denuncia de delito cibernético.

Todos son expuestos a cualquier delito, sin embargo, en la figura 4 se aprecia que las mujeres son las que realizan el mayor número de denuncias, con un 63 % de los resultados obtenidos, sin dejar a un lado que el 33% de los encuestados dijo que los hombres también emiten su denuncia, es importante recalcar que tanto niños, jóvenes y adultos pueden sufrir cualquier tipo de delito cibernético sin importar el sexo.

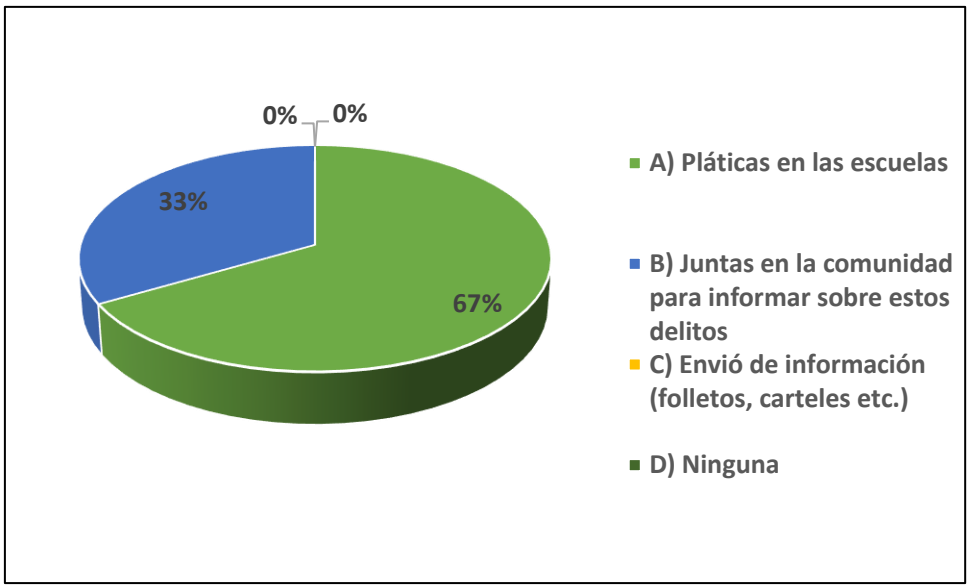

Figura 5.- Medidas para la prevención de un delito cibernético.

Para toda acción una reacción y es que ante los casos denunciados se han tomado medidas preventivas para combatir este tipo de delitos, el 67% de los encuestados respondió que una de las medidas que implementan son las pláticas en las escuelas ya que al parecer los jóvenes son más propensos a caer en ciertos delitos por falta de experiencia y el 33% dijo que de igual forma se implementan juntas comunitarias para prevenir estos ataques cibernéticos.

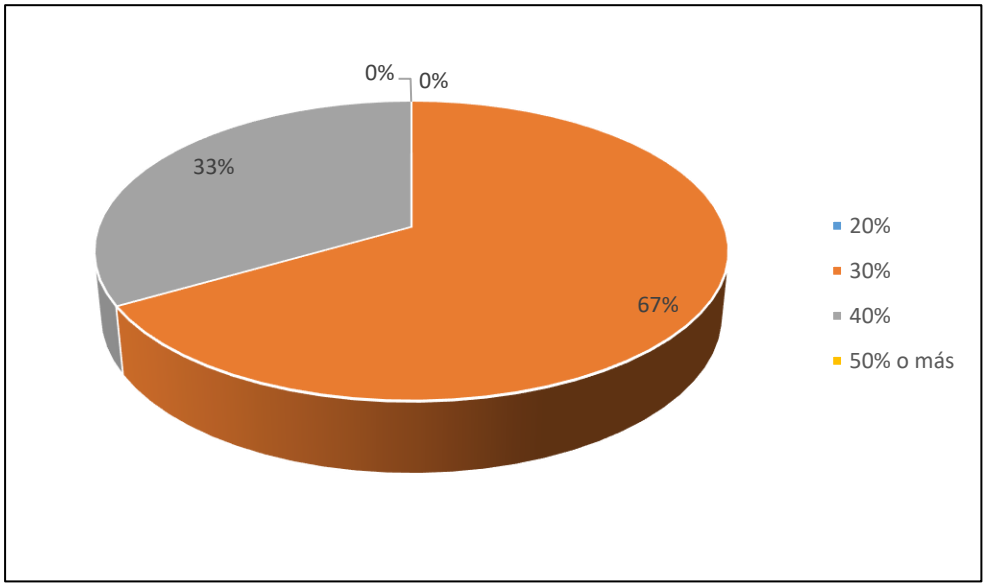

Figura 6.- Disminución de los delitos cibernéticos.

En la figura 6, se muestra que el 67% personas encuestadas dijo que los delitos cibernéticos han disminuido en un 30% y el 33% contesto que en un 40%, ambos porcentajes arrojan respuestas positivas para el estado, sin embargo se esperan que se reduzca en mayor porcentaje.

Con los resultados obtenidos, se puede observar que las medidas de prevención que el gobierno del Estado a través de las organizaciones encargadas está realizando las actividades antes señaladas, con la ayuda de las denuncias que se realizan se han podido resolver casos de ciberdelito lo que ha dado pauta para poder identificar cual es el delito mayor cometido y a través de que medio tecnológico es realizado. Con los resultados obtenidos de la investigación se pudo constatar que el teléfono celular es el instrumento más utilizado para cometer ciertos delitos, con mayor frecuencia a los jóvenes, y sobre todo a las mujeres, por lo que se recurren a las pláticas en las escuelas y juntas comunitarias para abordar el tema de ciberdelito y brindar información sobre cuáles serían las medidas de prevención que cada persona debe tomar en cuenta para evitar ciertos ataques y gracias a estas medidas se ha podido reducir el índice de delitos cibernéticos en un 30% y 40% para lo que va del año, además que en la página oficial de la Fiscalía General del Estado de Tabasco se dan algunas recomendaciones.

Figura 7.- Cibertips Fuente: Unidad de Investigación de Delitos Informáticos, http://www.fiscaliatabasco.gob.mx/Contenido/UnidadDelitosInformaticos

CONCLUSIÓN

Las actividades tecnológicas toman relevancia en nuestras vidas, se está expuesto a nuevos riegos, pero mantener un ambiente de comunicación seguro para todos los usuarios es el principal reto para los gobiernos de los países en vías de desarrollo, tal es el caso de México, el cual, ha dado el primer paso con la implementación de un marco regulatorio que permita frenar el crecimiento exponencial de los delitos informáticos en últimos años, a través de implementación de nuevas estrategias para combatir el ciberdelito o delitos informáticos ya que el Internet se ha convertido en el espacio ideal para la ciberdelincuencia puesto que ofrece fácil acceso que cualquier persona que posea cualquier dispositivo tecnológico y este a su vez accede a un cúmulo de información en muchos casos sin restricción alguna lo que ocasiona los distintos delitos cometidos en materia de tecnología, hay que tener en cuenta que por mucho que se empeñen las agencias o secretarias de seguridad de los Estados, es imposible garantizar la seguridad plena de los sistemas informáticos, sim embargo el tomar iniciativas para combatirlos frena un poco estos tipos de delitos que se han vuelto muy comunes en la actualidad, los cuales más allá de la

acción gubernamental y de las instituciones encargadas de combatirlo, nosotros como personas pensantes y razonables hay que contribuir para no ser víctimas de un delito como la extorsión, Ciberbullying por citar algunos, tomando medidas de seguridad para nuestras páginas sociales, redes y cuentas en internet, además de hacer caso omiso a las llamadas de personas totalmente desconocidos para nosotros y estar atentos a las indicaciones que las autoridades emiten con respecto de que hacer en caso de ser víctima.

BIBLIOGRAFÍA

Avira Operations GmbH & Co. KG. (2012). "Centro de ayuda - Avira Free Antivirus".

Ciberdelito en Tabasco, consultado el 08 de Julio de 2017 en: http://www.excelsior.com.mx/nacional/2017/05/19/1164512

Código Penal Federal (2013). Última reforma publicada DOF 25 enero.

Hernández, L. (2009). "El delito informático". Eguzkilore, Cuaderno del Instituto Vasco de Criminología. nº 23. pp. 227243.

López, E. (2004). Delitos en particular, México, Porrúa, p. 270.

López, M. (2007). Análisis Forense Digital, Universidad Nacional de Educación a Distancia - España.

Loredo, J. y Ramírez, A. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. Facultad de Ciencias Físico Matemáticas Universidad Autónoma de Nuevo León San Nicolás de los Garza, Nuevo León, México.

Téllez, J. (2004). Derecho informático, México, McGraw-Hill, 3ª. ed., p. 163.

Oxford University Press, (2010). "hacker". Oxford Dictionaries, Oxford Dictionaries.

Unidad de investigación de Delitos Informáticos, consultado el 15 de Julio de 2017 en: http://www.fiscaliatabasco.gob.mx/Contenido/UnidadDelitosInformaticos