COMO CREAR UNA ASOCIACIÓN CIVIL PARA LA PREVENCIÓN DE LA SEGURIDAD TECNOLÓGICA Y CIBERNÉTICA EN EL ESTADO DE PUEBLA

Por

Daniel Vázquez Sentíes

Tesis sometida como requisito parcial para obtener el grado de

maestro en ciencias y tecnologías de seguridad

en el

Instituto Nacional de Astrofísica, Óptica y Electrónica.

Supervisada por:

Dra. Claudia Feregrino Uribe

Instituto Nacional de Astrofísica, Óptica y Electrónica

Dr. Jorge Torres Aguilar

Fiscalía General del Estado de Puebla

Luis Enrique Erro 1
Sta. Ma. Tonantzintla,
72840, Puebla, México.

Puebla de Zaragoza a 26 de julio de 2019

AGRADECIMIENTOS

Al Instituto Nacional de Astrofísica, Óptica y Electrónica, por haberme permitido formar parte de tan distinguida institución y por contribuir a mi desarrollo profesional mediante la maestría en Ciencias y Tecnologías de Seguridad.

A la Dra. Claudia Feregrino Uribe (Instituto Nacional de Astrofísica, Óptica y Electrónica) y al Dr. Jorge Torres Aguilar (Fiscalía General del Estado de Puebla), por tomarse el tiempo de revisar este proyecto de tesis y aportar ideas valiosas en el proceso de elaboración.

Introducción

Sin lugar a dudas, uno de los factores más relevantes en el ámbito público es el de la seguridad, que es un elemento fundamental en la construcción del bien común, ya que a través de ésta es como se tutela y protege la integridad y la vida de las personas, lo cual es claro que no ha sido abordada de la manera más efectiva por parte de las autoridades competentes, concretamente en el eje de la prevención de las conductas delictivas.

Aunado a este hecho, sobreviene un avance exponencial en materia de Tecnologías de la Información y Comunicación (TIC), que si bien es cierto que genera un bienestar social en materia de comunicación, puede trastocarse y convertirse en una gran herramienta delictiva, como lo ha sido en los últimos años a nivel global. A este fenómeno se le ha denominado "ciber delito" o "delito cibernético", es decir, una conducta tipificada como delito, pero con la particularidad de que es cometida por medios tecnológicos, como lo son teléfonos, celulares, computadoras, internet, etc.

La realidad es que ante esto, y al ser la tecnología una materia en constante evolución, ha resultado una labor compleja, tanto para las autoridades como para la ciudadanía, el generar medios y estrategias actualizadas de protección en contra de los hechos de esta naturaleza, ocasionando una alta propensión general a ser víctima y no tener la capacidad y conocimiento necesario para atender la situación.

A partir de lo anterior, es como surge la necesidad ciudadana de asociarse para contrarrestar las conductas criminales que no pueden ser combatidas por el endeble sistema de prevención cibernética actual, por lo que la forma idónea para hacerlo es por medio de una persona jurídica denominada Asociación Civil, que es regulada por el Código Civil, y que tiene por esencia la

persecución de un objeto lícito, posible, que no sea preponderantemente económico, es decir, un fin que contribuya en alguna medida a la sociedad. Que, en atención a la problemática presentada, debe de buscar la prevención de los delitos cibernéticos, por medio de la investigación y difusión de la seguridad cibernética, a través de la generación de cultura cibernética en la población.

Es por esto, que por medio del presente trabajo, de forma ordenada, acorde a una investigación tanto cuantitativa como cualitativa, y conforme a tres capítulos, se demostrará la necesidad de la creación de esta Asociación Civil, además, se fundamentará jurídicamente la misma y se expondrá concretamente en qué consistirá su labor, y cómo a través de ésta, se logrará una verdadera prevención en materia de delitos cibernéticos.

Índice

CAPÍTULO I

ASOCIATIVISMO, SOCIEDADES Y PARTICIPACIÓN CIUDADANA EN MÉXICO

Antes de comenzar a reflexionar acerca del origen, historia, y trascendencia de las sociedades, es fundamental iniciar exponiendo la esencia e importancia de las personas, quienes son aquellos entes que conforman una sociedad, por lo que partiremos de la definición de "persona", para posteriormente poder fundamentar la importancia de ésta y consecuentemente la necesidad de conformar sociedades organizadas que cuenten con fines específicos.

Aristóteles, en su obra "Política", concibe al hombre como un animal racional, es decir, un ser dotado de cuerpo y alma con la particularidad de contar con una característica esencial llamada "raciocinio", del cual emana la capacidad de ser consciente de su existencia, por lo que no sólo busca instintivamente sobrevivir (como cualquier animal), sino racionalmente vivir bien, es decir, hacerse de los medios necesarios para que su vida sea la mejor posible.

Para lograr ese fin, las personas naturalmente dependen y se asocian con otras, sea consciente o inconscientemente desde su concepción hasta su muerte, iniciando con la dependencia del cuerpo de la madre para desarrollarse, hasta su posterior educación, aprendizaje, formación, y realización de actividades para subsistir plenamente; en vista de esta dependencia, las personas se asocian fundamentalmente en pequeños grupos llamados "familias", las cuales, en conjunto con más familias, conformarán una sociedad, que posteriormente y en función del desarrollo de las mismas, se consolidarán en lo que se conoce como un "Estado".

El asociativismo es un fenómeno social bastante antiguo, y se podría decir que inclusive viene aparejado con el hombre mismo, pues aparte de que éste es un ser gregario por naturaleza, ha sido precisamente desde que fundó el Estado y ha vivido en compañía de otros, pero sobre todo,

apoyándose mutuamente con ellos, fue así como sobrevivió y después como evolucionó, fundó ciudades y naciones, alcanzó el auge como ser civilizado, y logró sus mayores avances en todos los aspectos de su vida a través de la ciencia, la tecnología, el arte, y el oficio. Y es así que, finalmente el hombre logró tanto establecer su cultura como poblar y dominar al mundo y sus elementos.

De ese modo, el hombre ha unido fuerzas con otros, por medio de la división del trabajo, y luego, por medio de la especialización del mismo, para alcanzar los mejores resultados en los campos jurídico, político, alimentario, industrial, militar, etc.., pero sobre todo, aprovechando al máximo sus esfuerzos, evitando el derroche innecesario de energías y de recursos. El presente capítulo va a dar cuenta de este importante fenómeno, y de cómo éste deviene en otro, denominado participación ciudadana, que es gente que no ocupa un cargo público, que no es titular de un poder oficial, en tareas que son del Estado y sus poderes, pero en los que coadyuva con el fin de lograr mejores resultados en beneficio de la sociedad.

Asimismo, esta participación también puede conllevar la participación de personas que prestan servicios profesional o laboran en los órganos del Estado, pero que, como ciudadanos, como miembros del cuerpo social más que como titulares de una oficina o poder, hacen un ejercicio de colaboración del tipo ya mencionado con otros ciudadanos, independientemente de que estos tengan un encargo dentro de alguna dependencia, o de que laboren en una empresa, que sean empresarios de cualquier tamaño (es decir, de nivel micro, pequeño, mediano o grande), profesores, estudiantes, amas de casa, jubilados, etc.

Como indican Saavedra, Paúl y Bernal (2012) "la naturaleza de la sociedad asociativista, basada en la igualdad de los individuos y en la ayuda mutua frente a las necesidades comunes, contiene un conjunto de valores que permiten alcanzar niveles considerables de productividad, al

potenciar los recursos humanos, económicos y técnicos a través de la sinergia de grupo" (pp. 189-205). Y esto aplica a todos los grupos sociales y humanos. Ahora bien, por la naturaleza del tema a desarrollarse en la presente investigación, también se identificarán los tipos de sociedades existentes en México.

Por ello, se revisarán las sociedades mercantiles y su clasificación de acuerdo con la ley vigente en la materia, que son en sí organizaciones de carácter lucrativo, es decir, que buscan obtener ganancias económicas a partir de la prestación de servicios o la comercialización de bienes y mercancías en el marco de un mercado con reglas claras, específicas, y bien definidas para tales actividades. Tanto las sociedades como las asociaciones civiles, su fin no es eminentemente lucrativo, debido a que su actividad principal es la ayuda a otras personas, pero sin la forzosa necesidad o requerimiento de un pago por hacerlo.

Lo anterior, fundamentalmente movidos por la filantropía, desarrollan diversas actividades, por ejemplo, ayudar a otras personas, o bien, colaborar con las autoridades, pero en este caso, sin el fin imperioso de recibir recursos económicos, o de que sus miembros reciban algún nombramiento. Las bondades de este tipo de grupos radican en que, aun sin recursos, operan en apoyo al prójimo, y cuando lo reciben, o cuando en su caso se procuran fondos (ése es el término correcto jurídicamente hablando), son capaces de dar resultados dignos de estudio. Procédase al estudio de este tipo de sociedades, a fin de explicar por qué se hubo de elegir una asociación civil y no una sociedad mercantil para la figura que se va a crear.

1.1 Formas de asociarse en México

El derecho mexicano contempla en sus diferentes leyes (Código Civil de cada entidad y Ley General de Sociedades Mercantiles) determinadas formas de asociarse en función de los fines que se persigan, por lo que de manera genérica podrían dividirse en: sociedades mercantiles, sociedades civiles, asociaciones y fundaciones, en razón de esto, es indispensable conocer las características esenciales de cada una de ellas con el objetivo de seleccionar correctamente qué agrupación es más conveniente conformar en función de la actividad a realizar.

Una sociedad mercantil se trata de un contrato que realizan dos o más personas, en el cual éstas estipulan poner algo en común con la mira de repartir entre sí los beneficios que de ello provengan. De acuerdo a Cruz (2017), una sociedad mercantil es “una agrupación de personas que se obligan mutuamente a combinar sus recursos y esfuerzos para la realización de alguna actividad mercantil de forma permanente o temporal, misma que goza con personalidad jurídica de conformidad a la ley del lugar de donde pertenezca" (p. 22).

En un país como México, es posible dedicarse a cualquier actividad económica siempre y cuando ésta sea lícita, y que quien la desarrolle, cubra sus contribuciones fiscales a la autoridad en la medida y posibilidad que tenga y que la ley le imponga, y que nunca podrán ser inusitadas ni excesivas. De ese modo, "el marco jurídico mexicano otorga capacidad a las personas físicas o morales extranjeras para participar en la constitución de una sociedad mexicana o, en su caso, adquirir algún tipo de participación o interés en una sociedad mexicana existente" (Subsecretaría de Competitividad y Normatividad, 2016, p. 1). En tal sentido, y de conformidad con el artículo 1° de la Ley General de Sociedades Mercantiles (2018), se reconocen las siguientes sociedades mercantiles:

- Sociedad en nombre colectivo;
- Sociedad en comandita simple;
- Sociedad de responsabilidad limitada;
- Sociedad anónima;
- Sociedad en comandita por acciones;
- Sociedad cooperativa, y
- Sociedad por acciones simplificada.

La Secretaría de Economía del Gobierno de México, indica que "en la práctica, las sociedades más comúnmente constituidas son las sociedades anónimas y las de responsabilidad limitada en virtud de las ventajas que ofrecen al hacer una clara separación del capital de la sociedad y el patrimonio de los socios" (Subsecretaría de Competitividad y Normatividad, 2016, p. 1).

A continuación, en la tabla 1. se explican las características fundamentales de estas dos sociedades:

Tabla 1. Características fundamentales de las sociedades anónimas y de las sociedades de responsabilidad limitada

	Sociedades anónimas	**Sociedades de responsabilidad limitada**
Número de socios	Mínimo dos socios	Mínimo dos socios, máximo cincuenta socios

Integración del capital social	Acciones. Los socios (accionistas) pueden tener más de una acción	Partes sociales. Los socios solo pueden tener una parte social, independientemente del valor de su aportación a la sociedad
Límite de responsabilidad de los socios	Hasta por el monto de sus acciones	Hasta por el monto de sus partes sociales
Cesión de las partes representativas del capital	Las acciones pueden ser cedidas libremente	Se requiere que los socios que representen la mayoría del capital social aprueben la cesión de las partes sociales .
Límites en la participación de extranjeros	Ninguna, salvo que al momento de constituirla o posteriormente los socios hubieran incluido una cláusula de exclusión de extranjeros, lo que impediría que estos últimos participaran en la sociedad, directa o indirectamente	

Nota: Subsecretaría de Competitividad y Normatividad (2016). Sociedades. México: Secretaría de Economía, pp. 1-2.

Fundar un negocio en México por supuesto que implica una serie de costos, pero no es algo ya tan difícil, complejo, o gravoso como lo fue anteriormente. Los procesos de desregulación han incidido en el aminoramiento y reducción de trámites, requisitos, y hasta gastos, dependiendo del giro, las necesidades, los requerimientos, y el capital de cada persona o grupo de inversionistas. Lo mismo ocurre con la elección del tipo de sociedad a fundar o establecer.

Como indica Mantilla (1965), "el criterio para calificar una sociedad mercantil es estrictamente formal: basta la adopción de alguno de los tipos mencionados en la ley mercantil para que esta sea aplicada a la sociedad, la cual será considerada como comerciante, sujeta a todas las obligaciones de los de esta clase, y con la posibilidad de ser declarada en quiebra en caso de insolvencia. La finalidad social no influye, por tanto, en la calificación de la mercantilidad de la sociedad" (p. 146). De acuerdo con las y los especialistas de CICDE Consultores Fiscales (2019), los requisitos que cualquier sociedad debe reunir son los que se enuncian a continuación:

- Afán de lucro, lo cual significa que la persona moral (la empresa), será constituida para generar beneficios económicos. En caso de que no se busque un beneficio económico, entonces no se trata de una sociedad mercantil.
- Se debe dejar establecida la contribución para solventar las pérdidas, es decir poner en claro cuál es el riesgo inherente al negocio y cómo será sustentado por todos los socios.
- De cuánto será la aportación inicial, es decir, la contribución que harán los socios para arrancar el negocio, puede ser dinero, bienes muebles, inmuebles o incluso trabajo.
- La *affectio societatis*, que es la intención inherente por parte de los socios para lograr el bien común para la sociedad.
- Finalmente, establecer la contribución por todos los socios para solventar las pérdidas, así como aclarar cuál es el riesgo inherente al negocio.

Es relevante mencionar aquí, que en caso de existir alguna irregularidad que provoque una crisis o inclusive la quiebra, se puede responsabilizar a los socios y también a los administradores, y es que la ley prevé todas estas posibilidades. Entonces, estos "responden ilimitadamente de las deudas sociales; por otra parte, en caso de quiebra, las sociedades irregularmente constituidas no

pueden acogerse al beneficio de la suspensión de pagos, y la quiebra en que incurran será calificada, por lo menos, de culpable" (Mantilla, 1965, p. 146).

Hechas estas previsiones, es pertinente conocer la clasificación de personas jurídicas que ofrece el artículo 172 del Código Civil para el Estado Libre y Soberano de Puebla (2018), siendo las siguientes:

"I. El Estado de Puebla y los municipios del mismo Estado;

II. Las asociaciones civiles;

III. Las sociedades civiles;

IV. Las fundaciones;

V. Las demás que reconozca la ley" (p. 140).

1.1.1 Sociedad en nombre colectivo

De conformidad con lo dispuesto en el artículo 25 de la Ley General de Sociedades Mercantiles (2018), la sociedad en nombre colectivo "es aquella que existe bajo una razón social y en la que todos los socios responden, de modo subsidiario, ilimitada y solidariamente, de las obligaciones sociales" (p. 7), donde el término *subsidiario* se refiere al hecho de que en caso de que alguno de los socios no pudiera cumplir con su parte, los demás serían responsables de cubrir ésta en pro de dicho cumplimiento.

A su vez, el adjetivo ilimitado significa como su nombre lo dice, "que no tiene límites en cuanto al tema de responsabilidad, y la solidaridad es una modalidad de obligación que se presenta cuando hay pluralidad de acreedores, de deudores, o de ambos, y cada acreedor puede exigir el todo del objeto y cada deudor debe pagar todo el objeto siempre que, ese objeto sea divisible, física o económicamente" (Gutiérrez, 2003, p. 994). Su estructura jurídica fue originalmente conceptualizada, planeada, y organizada como la forma idónea para cobijar a pequeños grupos de

individuos vinculados entre sí por lazos de confianza recíproca para explotar asociativamente un determinado negocio mercantil, aplicándose principalmente en el prestigio y calidad personal de los socios.

De esta suerte, la sociedad en nombre colectivo enmarca una de las maneras más espontáneas para la organización y desarrollo del trabajo realizado por un conjunto de personas vinculadas asociativamente entre sí con un *propósito comercial*. No obstante, algunos dicen que es un tipo de estructura social al que cada vez se recurre menos, e incluso hay quienes opinan que las sociedades en nombre colectivo han caído totalmente en desuso (Gabuardi, 2016).

Para que ésta llegue a constituirse debe haber *affectio societatis* (requisito mencionado con anterioridad). En la práctica, ese requisito mencionado queda explicitado estatutariamente mediante el uso de una declaración expresa en el que las partes que comparecen ante el Notario Público que formaliza la escritura constitutiva manifiestan que el propósito de su comparecencia ante el fedatario es justamente otorgar un contrato de sociedad.

Por *affectio societatis* debe entenderse la colaboración activa, consciente e igualitaria de todos los contratantes con vistas a la realización del beneficio a dividir. Así considerada, la *affectio societatis* es el elemento subjetivo de la causa, que estimamos esencial, es decir en la realización de un fin común de carácter lucrativo, como dice el CCF de donde se deduce que el motivo del contrato de sociedad no es otro que la participación en los beneficios y en las pérdidas (Rodríguez, 2001).

1.1.2 Sociedad en comandita simple

La sociedad en comandita simple es la que existe bajo una razón social y se compone de uno o varios socios comanditados que responden de manera subsidiaria, ilimitada, y solidariamente, de las obligaciones sociales, y de uno o varios comanditarios que únicamente están obligados al pago

de sus aportaciones (Ley General de Sociedades Mercantiles, 2018). Sus características son las que se enuncian en la lista a continuación:

- Tiene 2 clases de socios: comanditados y comanditarios.
- Su razón social se crea con el nombre de uno o más socios, siempre y cuando sean comanditados, jamás comanditarios.
- No establece un mínimo para su capital social.
- Tiene un número ilimitado de socios.
- La responsabilidad de los socios comanditados es: solidaria, subsidiaria e ilimitada.
- La responsabilidad de los socios comanditarios se lleva solamente hasta el límite de sus aportaciones, salvo -por supuesto- que haya tomado parte en alguna operación o habitualmente hubiese administrado los negocios de la sociedad.
- El administrador será forzosamente un socio comanditado, mientras que el interventor será un socio comanditario.
- No tienen accionistas. Cada socio comanditario tiene un porcentaje de interés específicamente establecido en los ingresos de la entidad.
- Los socios comanditarios no reciben dividendos, pero tienen derecho a su parte de los ingresos.
- El socio gestor es responsable por los activos y pasivos totales de la sociedad.
- Generalmente se utilizan para dos propósitos principales:
    a. Desarrollar proyectos inmobiliarios comerciales.
    b. Ser usadas como una vía de planificación patrimonial (Colegio de Notarios del Distrito Federal, 2016 y Sy Corvo, 2019).

Comandita, en una definición elemental "en grupo", algo que se hace así, de manera colectiva (RAE, 2019). A su vez, comanditar significa "aprontar los fondos necesarios para una empresa comercial o industrial, sin contraer obligación mercantil alguna" (RAE, 2019). La diferencia entre los tipos de socios es que los comanditados son "aquellos que son responsables solidariamente de los resultados de todas las operaciones, por cuanto tienen el manejo o dirección de la compañía o están incluidos en el nombre o razón social" (Ossorio, 2007, p. 177). A su vez, un socio comanditario es el "socio proveedor de capital, sin titularidad en la empresa, para la dirección, administración o gestión, pero con ciertos derechos limitados, que le permiten disfrutar de las ganancias, sin exponerse a la responsabilidad ilimitada de los otros socios (comanditados o colectivos), ya que sólo responden de las pérdidas según la aportación prometida o realizada" (Ossorio, 2007, p. 177).

1.1.3 Sociedad de responsabilidad limitada

La sociedad de responsabilidad limitada es la que se constituye entre socios que solamente están obligados al pago de sus aportaciones, sin que las partes sociales puedan estar representadas por títulos negociables, a la orden o al portador, pues sólo serán cedibles en los casos y con los requisitos que establece la presente Ley (Ley General de Sociedades Mercantiles, 2018). Se trata de una sociedad intermedia que surgió para eliminar las restricciones y exigencias de la sociedad anónima, constituye un tipo social sin alejarse plenamente de los esquemas propios de las sociedades de personas. Sus características son las siguientes:

- El capital social será el que se establezca en el contrato social; se dividirá en partes sociales que podrán ser de valor y categoría desiguales, pero que en todo caso serán de un múltiplo de un peso (artículo 62 de la Ley General de Sociedades Mercantiles, 2018).

- Los socios no responden ante las deudas con su patrimonio personal (Luna, 2018).
- Responsabilidad limitada al capital social y a los bienes de la sociedad.
- Ninguna sociedad de responsabilidad limitada tendrá más de cincuenta socios (artículo 61 de la Ley General de Sociedades Mercantiles, 2018).
- Al constituirse la sociedad, el capital deberá estar íntegramente suscrito y exhibido, por lo menos, el cincuenta por ciento del valor de cada parte social (artículo 64 de la Ley General de Sociedades Mercantiles, 2018).

1.1.4 Sociedad anónima

De acuerdo con el artículo 87 de la Ley General de Sociedades Mercantiles (2018), la sociedad anónima es la que existe bajo una denominación y se compone exclusivamente de socios cuya obligación se limita al pago de sus acciones. Resulta relevante mencionar aquí que en este tipo de organizaciones "interesa el capital que aportan y no las personas [con lo que] las condiciones personales de los socios resultan irrelevantes" (Casado, 2009, pp. 757-758). Tiene por características las que se enuncian a continuación:

- Las acciones en que se divide el capital social de una sociedad anónima estarán representadas por títulos nominativos que servirán para acreditar y transmitir la calidad y los derechos de socio, y se regirán por las disposiciones relativas a valores literales, en lo que sea compatible con su naturaleza y no sea modificado por la presente Ley (artículo 111 de la Ley General de Sociedades Mercantiles, 2018).
- Las acciones serán de igual valor y conferirán iguales derechos. Sin embargo, en el contrato social podrá estipularse que el capital se divida en varias clases de acciones con derechos especiales para cada clase (artículo 112 de la Ley General de Sociedades Mercantiles, 2018).

- Cuando así lo prevenga el contrato social, podrán emitirse en favor de las personas que presten sus servicios a la sociedad, acciones especiales en las que figurarán las normas respecto a la forma, valor, inalienabilidad y demás condiciones particulares que les corresponda (artículo 114 de la Ley General de Sociedades Mercantiles, 2018).
- Se les prohíbe emitir acciones por una suma menor de su valor nominal (artículo 115 de la Ley General de Sociedades Mercantiles, 2018).
- El socio solo aporta el capital y no responde de forma personal las deudas sociales.
- La transferencia de las acciones puede hacerse mediante la venta sin necesidad de disolver la sociedad constituida.
- No contempla un número máximo de socios.
- Opera a través de diversos órganos: el órgano deliberante (la asamblea general), el órgano de administración y el órgano de vigilancia (Dávalos, 2010).
- Es el tipo de sociedad mercantil más común junto con la de responsabilidad limitada.

1.1.5 Sociedad en comandita por acciones

La sociedad en comandita por acciones es la que se compone de uno o varios socios comanditados que responden de manera subsidiaria, ilimitada y solidariamente, de las obligaciones sociales, y de uno o varios comanditarios que únicamente están obligados al pago de sus acciones (artículo 207 de la Ley General de Sociedades Mercantiles, 2018). Sus características son las siguientes:

- La sociedad en comandita por acciones se regirá por las reglas relativas a la sociedad anónima (artículo 208 de la Ley General de Sociedades Mercantiles, 2018).

- El capital social estará dividido en acciones y no podrán cederse sin el consentimiento de la totalidad de los comanditados y el de las dos terceras partes de los comanditarios (artículo 209 de la Ley General de Sociedades Mercantiles, 2018).
- Podrá existir bajo una razón social, que se formará con los nombres de uno o más comanditados seguidos de las palabras y compañía u otros equivalentes, cuando en ellas no figuren los de todos (artículo 210 de la Ley General de Sociedades Mercantiles, 2018).

1.1.6 Sociedad cooperativa

De acuerdo con el artículo 2 de la Ley General de Sociedades Cooperativas (2018), "la sociedad cooperativa es una forma de organización social integrada por personas físicas con base en intereses comunes y en los principios de solidaridad, esfuerzo propio y ayuda mutua, con el propósito de satisfacer necesidades individuales y colectivas, a través de la realización de actividades económicas de producción, distribución y consumo de bienes y servicios" (p. 1). Se observarán los siguientes principios en su funcionamiento, según el artículo 6 de la (LGSM, 2018):

I. "Libertad de asociación y retiro voluntario de los socios;
II. Administración democrática;
III. Limitación de intereses a algunas aportaciones de los socios si así se pactara;
IV. Distribución de los rendimientos en proporción a la participación de los socios;
V. Fomento de la educación cooperativa y de la educación en la economía solidaria;
VI. Participación en la integración cooperativa;
VII. Respeto al derecho individual de los socios de pertenecer a cualquier partido político o asociación religiosa, y
VIII. Promoción de la cultura ecológica" (p. 2).

Tiene las siguientes características:

- Se integrarán con un mínimo de cinco socios (artículo 11 de la Ley General de Sociedades Cooperativas, 2018).
- El régimen de responsabilidad de los socios que se adopte surtirá efectos a partir de la inscripción del acta constitutiva en el Registro Público de Comercio. Entre tanto, todos los socios responderán en forma subsidiaria por las obligaciones sociales que se hubieren generado con anterioridad a dicha inscripción.
- Las personas que realicen actos jurídicos como representantes o mandatarios de una sociedad cooperativa no inscrita en el Registro Público de Comercio, responderán del cumplimiento de las obligaciones sociales frente a terceros, subsidiaria, solidaria e ilimitadamente, sin perjuicio de la responsabilidad penal en que hubieren incurrido (artículo 15 de la Ley General de Sociedades Cooperativas, 2018).
- Para su funcionamiento contarán con los siguientes órganos: La asamblea general, el consejo de administración, el consejo de vigilancia, comisiones, comités y en su caso, un director general y un auditor interno (artículo 34 de la Ley General de Sociedades Cooperativas, 2018).
- Por último, y de acuerdo con el artículo 49 de la Ley General de Sociedades Cooperativas (2018), el capital se integrará con las aportaciones de los socios y con los rendimientos que la Asamblea General acuerde se destinen para incrementarlo.

1.1.7 Sociedad por acciones simplificada

De acuerdo con el artículo 260 de la Ley General de Sociedades Mercantiles (2018), “la sociedad por acciones simplificada es aquella que se constituye con una o más personas físicas que solamente están obligadas al pago de sus aportaciones representadas en acciones. En ningún caso las personas físicas podrán ser simultáneamente accionistas de otro tipo de sociedad mercantil a

que se refieren las fracciones I a VII, del artículo 1o. de esta Ley, si su participación en dichas sociedades mercantiles les permite tener el control de la sociedad o de su administración, en términos del artículo 2, fracción III de la Ley del Mercado de Valores" (p. 44).

El mismo precepto establece que, a diferencia de otras sociedades mercantiles, los ingresos totales anuales de una sociedad por acciones simplificada no podrán rebasar de 5 millones de pesos. En caso de rebasar el monto respectivo, la sociedad por acciones simplificada deberá transformarse en otro régimen societario, por supuesto, entre los contemplados en la Ley General de Sociedades Mercantiles, en los términos en que se establezca en las reglas señaladas en el artículo 263 de la misma.

De acuerdo con lo anterior, el monto establecido en el párrafo (los cinco millones en cuestión) se actualizará anualmente el primero de enero de cada año, considerando el factor de actualización correspondiente al periodo comprendido desde el mes de diciembre del penúltimo año hasta el mes de diciembre inmediato anterior a aquel por el que se efectúa la actualización, misma que se obtendrá de conformidad con el artículo 17-A del Código Fiscal de la Federación. La Secretaría de Economía, agrega, publicará el factor de actualización en el Diario Oficial de la Federación durante el mes de diciembre de cada año.

Por último, el artículo 260 indica que en caso de que los accionistas no lleven a cabo la transformación de la sociedad a que se refiere el párrafo anterior, responderán frente a terceros, subsidiaria, solidaria e ilimitadamente, sin perjuicio de cualquier otra responsabilidad en que hubieren incurrido (Ley General de Sociedades Cooperativas, 2018). Tiene las siguientes características:

- En ningún caso se exigirá el requisito de escritura pública, póliza o cualquier otra formalidad adicional, únicamente que alguno de los accionistas cuente con la autorización para el uso de

denominación emitida por la Secretaría de Economía, que el o los accionistas externen su consentimiento para constituir una sociedad por acciones simplificada bajo los estatutos sociales que la Secretaría de Economía ponga a disposición mediante el sistema electrónico de constitución y que todos los accionistas cuenten con certificado de firma electrónica avanzada vigente reconocido en las reglas generales que emita la Secretaría de Economía (artículo 262 de la Ley General de Sociedades Cooperativas, 2018).

- Su trámite es 100% electrónico.
- La denominación se formará libremente, pero deberá ser distinta de la de cualquier otra sociedad, y siempre deberá estar seguida de las palabras "Sociedad por Acciones Simplificada" o de su abreviatura "S.A.S." (artículo 261 de la Ley General de Sociedades Cooperativas, 2018).

1.1.8 Asociación civil

De acuerdo con el artículo 184 del Código Civil para el Estado Libre y Soberano de Puebla (2018), una "asociación civil se constituye mediante un acto jurídico por el cual se reúnen de manera que no sea enteramente transitoria, dos o más personas, para realizar un fin posible, lícito y común, y que no tenga carácter preponderantemente económico" (p. 142). Esas personas son consideradas socios.

Las características de una asociación civil son las siguientes:

- El poder supremo de las asociaciones reside en la asamblea general (artículo 191 del Código Civil del Estado de Puebla, 2018).
- De acuerdo con lo dispuesto en el artículo 190 del Código en cita, las asociaciones se regirán por su estatuto y por lo que establece el Código Civil del Estado de Puebla, 2018.

- El asociado no votará las decisiones en que se encuentre directamente interesado él, su cónyuge, ascendientes, descendientes o parientes colaterales dentro del segundo grado (artículo 197 del Código Civil del Estado de Puebla, 2018).
- Cada vez que se reúna la asamblea general, deberá incluirse como un punto en el orden del día, el informe que el director o el consejo de directores rendirá sobre el estado que guarde la asociación y la situación económica de la misma (artículo 204 del Código Civil del Estado de Puebla, 2018).
- Los asociados tienen derecho de vigilar que las cuotas se dediquen al fin que se propone la asociación, y con ese objeto pueden examinar los libros de contabilidad y demás papeles de ésta (artículo 208 del Código Civil del Estado de Puebla, 2018).
- La calidad de asociado es intransferible, salvo por causa de muerte (artículo 209 del Código Civil del Estado de Puebla, 2018).

Una asociación civil no es muy diferente respecto de una sociedad mercantil en el sentido de la solemnidad con la que se funda, la seriedad, y claridad con la que debe operar, y la forma en que se organiza y dirige, salvo por su fin inminente y determinantemente no lucrativo. En este sentido, "se dice que la asociación civil es una corporación en virtud de que sus socios se deben regir por sus estatutos que deben estar inscritos en el Registro Público a fin de que surta sus efectos contra terceros, por lo tanto, el contrato que le da origen es formal: debe constar por escrito" (Pérez, 1982, p. 214). Una figura similar es la de las sociedades civiles. Véanse estas.

1.1.9 Sociedad civil

De acuerdo con el artículo 213 del Código Civil del Estado de Puebla (2018), una “sociedad civil se constituye mediante un acto jurídico por el cual se reúnen de manera permanente dos o más personas, para realizar un fin común de carácter preponderantemente económico, lícito, posible

pero que no constituya una especulación mercantil, mediante aportación de sus bienes o industria, o de ambos, para dividir entre sí el dominio de los bienes y las ganancias y pérdidas" (p. 147). Sus características son las siguientes:

- Debe crearse para utilidad común de los socios (artículo 214 del Código Civil del Estado de Puebla, 2018).
- Debe constar en escritura pública y junto con los estatutos, deben ser inscritos en el Registro Público de las sociedades civiles (artículo 217 del Código Civil del Estado de Puebla, 2018).
- A menos que lo establezca la escritura constitutiva, no puede obligarse a los socios a hacer una nueva aportación para aumentar el capital social (artículo 229 del Código Civil del Estado de Puebla, 2018).
- Las obligaciones sociales estarán garantizadas subsidiariamente por la responsabilidad ilimitada y solidaria de los socios que administren (artículo 231 del Código Civil del Estado de Puebla, 2018).
- Los socios gozarán del derecho del tanto (artículo 209 del Código Civil del Estado de Puebla, 2018).

Con fines meramente ilustrativos, derecho del tanto es "la posibilidad jurídica que le da la ley a un copropietario para adquirir, en igualdad de circunstancias, respecto de cualquier tercero, la parte indivisa del bien sobre el que recae la copropiedad, que pretenda vender otro copropietario" (Zamora, 1987, p. 18).

1.1.10 Fundaciones

Proveniente del latín *fundatio-onis*, acción y efecto de fundar; edificar, o instituir, una fundación es un "patrimonio organizado y destinado a un fin altruista lícito que carece de titular y se le concede personalidad jurídica propia con el objeto de que pueda cumplir sus fines" (Pérez, 1982,

p. 262). Se constituye de una finalidad, un patrimonio, y un patronato que la administra. Sus recursos suelen ser altos, precisamente destinados para el cumplimiento de su finalidad u objeto social.

Por supuesto, no se puede negar que las fundaciones son instrumentos institucionales que nuestra sociedad estima convenientes, no sólo y no precisamente por sus ventajas fiscales, sino por su utilidad general, las cuales regularmente se relacionan con actividades filantrópicas y de ayuda a otras personas (ése es, precisamente, uno de los aspectos que las vuelve atractivas y útiles fiscalmente).

Ahora bien, "el concepto de fundación (patrimonio destinado a un fin, al cual la ley atribuye la cualidad de sujeto de derecho) encuentra las propias raíces en el derecho canónico, pero alcanza una completa elaboración sólo en la época moderna, por obra de la especulación jurídica del siglo XIX, particularmente de Heise y Savigny" (Labariega, 2003, pp. 55-56). Lo anterior es una visión histórica sobre su origen.

Como indica Labariega, “fundación” en el sentido técnico y especial de la palabra, consiste en un patrimonio independiente y autónomo (el cual ya fue mencionado unas líneas atrás, constituido en vista de un fin estatutario y que no funciona sino en atención al objeto por realizar, perteneciendo así espiritualmente a una entidad ideal, representativa de la afectación dada a la propiedad. Es pues, la autonomía por excelencia, la independencia constitucional de la propiedad. Esta no pertenece idealmente más que a su destino y no depende de ninguna voluntad individual.

1.1.11 Diferencias entre las asociaciones y las fundaciones

Como se ha podido ver, las asociaciones civiles y las sociedades civiles son muy parecidas, pero tienen una diferencia sustancial: las primeras no tienen como fin el lucro y las segundas sí. Las

fundaciones tampoco son lucrativas, pero sus diferencias podrían ser más notables en otros sentidos que conviene repasar en seguida, antes de exponer por qué no se eligió para su constitución una sociedad mercantil, una sociedad civil, y ni siquiera una fundación:

a. Mientras que las asociaciones y las sociedades evocan un conglomerado de personas, las fundaciones se configuran por un conjunto de bienes.

b. Las primeras cuentan con intereses, fines y medios propios, las segundas los reciben del fundador, por ende, le son ajenos.

c. Por lo que respecta a la voluntad, en la fundación esta proviene del fundador, mientras que en las asociaciones o sociedades deriva de los miembros de la entidad que disponen sobre su constitución, gobierno y fin de la persona moral. De ahí que se hable de una voluntad (colectiva) de la asociación, pero no de una voluntad de la fundación como tal.

   Por ello, se ha afirmado que la asociación es autónoma, puesto que se gobierna a sí misma; mientras que la fundación es heterónoma, ya que es administrada por una voluntad extraña: por la del fundador, patronato (Ley de Instituciones de Asistencia Privada para el Estado Libre y Soberano de Puebla, 2018) o junta directiva, figuras designadas en los estatutos (artículo 36 de la Ley de Instituciones de Asistencia Privada para el Estado libre y soberano de Puebla, 2018).

d. El patrimonio de las asociaciones y de las sociedades se constituye primordialmente por las aportaciones o cuotas de los socios o asociados, en tanto que el patrimonio de la fundación se conforma por los bienes que el fundador destina mediante declaración unilateral de voluntad, a la realización del fin elegido por él.

   Además, en la asociación el patrimonio es un recurso meramente instrumental y no necesariamente constitutivo, puesto que se puede imaginar a una asociación con patrimonio

precario, desproporcionado o incluso sin patrimonio, mientras que en el caso de la fundación esto es simplemente impensable, estaría en contra totalmente de su razón de ser, puesto que es un ingrediente esencial para su constitución y finalidad.

e. Los órganos de las asociaciones y sociedades son dirigentes o dominantes, esto es, gozan de amplia libertad para decidir, mientras que los órganos de la fundación son sirvientes de un fin y han de sujetarse a los límites delineados por el fundador.

f. En las asociaciones y sociedades, el fin señalado para su constitución puede ser eventualmente modificado por los socios, en el caso de la fundación, el fin al ser impuesto por el fundador deviene a ser perenne e inmutable (Labariega,2003).

1.2 ¿Por qué una asociación civil?

De acuerdo con Casado (2009), una asociación civil "no persigue un fin pecuniario y tiene como finalidad principal el bien común" (p. 90).

Por supuesto, la asociación que se propone implementar efectivamente va a perseguir un bien común, el cual es susceptible de materialización en la seguridad para las personas que son usuarias de los diferentes sitios, aplicaciones, y servicios que pueden encontrarse en Internet. Bajo ningún concepto pretende inferirse (o que alguien infiera) que el Sistema Nacional de Seguridad Pública (y las instancias que lo conforman, directa o indirectamente) no dan resultados en su quehacer.

Sin embargo, ningún esfuerzo sobra cuando se trata de prevenir las violencias y la delincuencia, por ende, perseguir y sancionar es responsabilidad, y también, facultad exclusiva del Estado, labor que hace a través de todas las instancias policiales federales y las que corresponde a los órdenes estatales y municipales de gobierno (ministerio público federal, corporaciones policiales federales y la recientemente creada Guardia Nacional). Pero identificarlo, investigarlo,

analizarlo, divulgarlo y prevenirlo, es tarea tanto de los antes mencionados como de todos los miembros del cuerpo social.

Una inquietud latente podría ser la siguiente: que al darse desde la asociación civil esta labor de cooperación, intercambio, y apoyo con la autoridad, así como la de divulgación de los delitos cometidos por medios cibernéticos con y hacia la ciudadanía, se estaría igualmente retroalimentando a la delincuencia, lo mismo la común que la organizada, pero no es así. Se parte de esta premisa: la delincuencia siempre tratará de ir un paso adelante de la ciudadanía, que es su víctima y de la autoridad que es su enemiga natural por cuanto es su perseguidora.

Con todo y eso, tanto la autoridad encargada de la seguridad pública como la ciudadanía deben hacer todo cuanto les sea posible y esté a su alcance para combatir la violencia y la delincuencia. Continuamente, el criminal intenta nuevas formas de delinquir y afectar a la gente, pero entre más informada se encuentre esta última, será menos propensa a dejarse dañar por aquellos que pretenden vivir fácilmente y en la clandestinidad a través de las fechorías.

1.3 Teoría de la participación ciudadana

En el apartado anterior se expusieron algunas de las razones por las que se pretende intervenir en la investigación y prevención de delitos cibernéticos por medio de la sociedad civil organizada a través de una asociación sin fines de lucro, no sólo con la autoridad preventiva en materia de seguridad pública o con la investigadora en materia de persecución del delito, sino incluso con otros tipos de autoridad, como sería el caso del INAOE, que desarrolla e imparte programas de estudios en materia de seguridad, en este caso cibernética, porque al cruzar información con él podrá, lo mismo generar otra nueva, que consolidar la existente. Aquí se hace pertinente, explicar de dónde surge y en qué consiste la participación ciudadana en los asuntos públicos.

El concepto de participación ciudadana, tradicionalmente, en las democracias representativas se asociaba, pero al mismo tiempo, se limitaba a la presencia del individuo que goza de la calidad de ciudadano en el momento de elegir gobernantes, para lo cual acudía a una casilla electoral, emitía un voto por cada cargo a renovarse y fin. De acuerdo con Arbós y Giner (1993), “a través del voto, todos los ciudadanos adultos pueden participar en la designación directa o indirecta de los gobernantes, mediante el ejercicio de un derecho que parece obvio en una democracia contemporánea. Sin embargo, la participación no se agota en las elecciones” (p. 63) y esta aseveración es contundente.

En efecto, hasta aquí se ha visto una democracia meramente instrumental, pero también, utilitaria, es decir, sólo opera para renovar a los titulares de los cargos públicos, pero a los ciudadanos se les utiliza únicamente para eso. Por años, convenientemente funcionó así el régimen, pero poco a poco, la sociedad fue despertando y exigiendo una presencia y una actuación cada vez más patente y activa, con lo cual se fue incrustando en órganos que no podían admitir a políticos de carrera, tales como el hoy llamado Instituto Nacional Electoral o la Comisión Nacional de Derechos Humanos, aunque finalmente también fueron contaminados por intereses partidistas.

De acuerdo con Romero (2010), "la participación de la ciudadanía va de la esfera social en aspectos privados con intereses particulares, a la esfera pública en ámbitos políticos con intereses generales. Lo mismo, podrá ser activa que pasiva, y (...) a esta investigación le interesa la participación política, pero no es la única" (p. 48). El Índice de Participación Ciudadana (IPC), considera que existen al menos tres tipos de participación ciudadana, que son los siguientes:

1. La participación directa;
2. La participación opinativa (sic), y
3. La participación electoral.

La primera se ha dado más en el contexto de lo religioso, en tanto que en la *participación opinativa*, "los sectores sociales más altos participan enviando cartas, contestando encuestas o llamando a medios de comunicación como una forma de expresar sus ideas y convicciones, si bien los sectores más desfavorecidos participan menos" (Romero, 2010, p. 60). La participación electoral, sin embargo, no se ciñe sólo a la asistencia a emitir sufragios en las urnas, sino que, gradualmente, se ha ido avanzando en mecanismos ratificatorios o consultivos, como el referéndum, el plebiscito, la iniciativa popular y otras. Araya (2007), vislumbra los siguientes tipos de participación política:

I. "Participación electoral.
II. Participación política a través de grupos.
III. Participación a través de movimientos colectivos" (pp. 2-3).

Además, distingue los siguientes tipos de participación ciudadana, un poco más activa en el sentido operacional del término:

a. **Participación consultiva y/o asesora:** Se expresa como opinión o manifestación de conocimiento que, en tanto tal, no obliga al sujeto que adopta la decisión.

b. **Participación resolutiva y participación fiscalizadora:** Implican intervención en el curso de la actividad pública (en decisiones) y por lo tanto ambas tienen carácter obligatorio para la administración.

c. **Participación en la ejecución:** Supone que se toma parte directamente en la realización de una actividad en la presentación de un servicio.

La participación ciudadana consta de 4 fases que se enuncian a continuación:

I. **Fase previa o de iniciativa:** se planifica el proceso participativo, se definen objetivos y metodologías de trabajo. Es el momento en el que gremios, instituciones y ciudadanos deben sentirse totalmente incluidos y conscientes de la importancia de los proyectos para el beneficio del municipio o región, para que puedan traducirse en políticas públicas que lleguen a ser finalmente implementadas.

II. **Fase de movilización:** se invita a los ciudadanos y organizaciones a participar del proceso utilizando los canales que se encuentren disponibles para tal fin. Esto se hace con el objetivo de extender la participación a un mayor número de ciudadanos para garantizar que haya pluralismo (gracias a la inclusión de diversas opiniones) y representatividad (en la medida que los participantes, constituyan una muestra significativa de toda la población).

III. **Fase de participación:** se desarrollan las actividades que permitirán que la ciudadanía participe activamente en la planificación, ejecución y control de planes y proyectos. Para esta fase se deben tener en cuenta tres criterios importantes:

- **Información:** los participantes deben conocer la mayor cantidad de datos posibles de forma clara y completa para poderse pronunciar sobre los diferentes temas.
- **Deliberación:** las condiciones deben ser óptimas para que los participantes puedan expresar libremente sus opiniones y puntos de vista.
- **Influencia efectiva:** se debe garantizar que la participación realmente influya en la toma de decisiones, en caso contrario este tipo de procesos pierden credibilidad y desincentivan su continuidad.

IV. **Fase de efectos y resultados:** en esta fase se busca que las decisiones tomadas sean contempladas por los organismos representativos y sean incluidas en la elaboración de políticas

públicas municipales que efectivamente lleguen a ser implementadas (Asociación Conecta Rural, 2019).

Esta asociación propuesta va apenas entrando en la fase previa o de iniciativa, y aún hay mucho camino por recorrer a partir de su creación y escrituración ante un notario público. Sin embargo, la participación comienza desde que surge precisamente la iniciativa y se va configurando hasta que se consolida.

Olvera (2009), refiere que, en el enfoque democrático-participativo, "la participación es vista como el eje de una práctica de la política que permite a los ciudadanos intervenir en los asuntos de interés colectivo a través de la creación de espacios públicos donde no sólo se debaten, sino que se deciden y vigilan, las políticas públicas de los diferentes niveles de gobierno" (p.3).

Sin embargo, como ya ha podido verse con el paso de los años, no se requiere la creación de espacios públicos (entendidos como dependencias o instancias oficiales) como algo forzoso para fomentar la participación ciudadana y ni siquiera para que el público se exprese, pronuncie, o intervenga. Esa participación, a través de asociaciones civiles como la que aquí se plantea, no requiere la creación de esos espacios. Podría, de haberlos, aceptar, y recibir fondos a través de una transferencia que fomente su actividad, pero no persigue un nombramiento oficial, una designación, o un cargo de naturaleza política ni administrativa.

1.4 El Estado como asociado

Es en el rubro de la participación a través de movimientos colectivos y desde una perspectiva consultiva-asesora, donde se inscribe el interés de este sustentante por participar en la actividad no pública, aunque sí en el contexto de labores públicas y sociales, en este caso, relacionadas con la seguridad pública. Por otro lado, crear una asociación civil tampoco lleva oculta a un cargo de

elección popular. No se va a crear una organización parapolítica, sino un colectivo de asociados cuyo fin ha sido claramente expresado. Su socio, no formal, e incluso no material, pero sí de servicio y causa en común.

No se pretende sustituir o suplir de ninguna manera a las instancias federales y locales dedicadas a la investigación, combate, y persecución de los delitos relacionados con medios cibernéticos, sino lo contrario, se pretende coadyuvar con ellas, compartiéndoles la información que, desde los organismos no gubernamentales, o sea las asociaciones civiles, sean capaces de generar. En resumen, no se desestiman los esfuerzos del Estado en las materias que a ambos interesan, conforme a lo que se plantea en esta investigación.

Cuando se habla de tener como socio al Estado, más bien se está hablando de que se le integrará al proyecto mediante la solicitud de donaciones y la búsqueda de convenios con el sector público para desempeñar activamente el objeto social de la asociación, y darle así, cumplimiento. La actividad, se basará en la mutua cooperación y respeto, donde los resultados serán tanto compartidos como recíprocos.

Igualmente, se espera tender un puente para trabajar en coordinación con la iniciativa privada, no sólo desde el enfoque de empresas dedicadas a la seguridad en cualquier línea o rubro (si bien, la ciberseguridad es un aspecto valioso que ya empiezan a brindar distintas compañías), sino a través de la búsqueda de convenios de colaboración con dicho sector, a fin de ofrecer los servicios de conferencias de prevención y trabajar de la mano con instituciones educativas, cuyos pasantes o personas especializadas puedan prestar sus servicios a la asociación y recibir algún beneficio a cambio, como experiencia, liberación de servicio social, promoción de sus habilidades, capacitación, etc.

CAPÍTULO II

MARCO JURÍDICO

Para poder comprender las implicaciones de una conducta humana dentro del ámbito jurídico, es necesario entender los conceptos relativos a los tipos de conductas socialmente negativas que una persona realiza, siendo que, en función de esto, es por lo que podremos hablar de una conducta delictiva y posteriormente de un “delito cibernético”.

2.1 Conducta antisocial y conducta antijurídica

Es importante la distinción entre ambos conceptos, ya que, generalmente para quien no es especialista en cuestiones jurídicas o las que son relativas al derecho, como las ciencias penales y las de seguridad se suelen confundir. A partir de la distinción que en esta sección se haga, se podrá ubicar la diferencia entre una conducta socialmente condenable, llevada al extremo de un delito e incluso de uno menor.

2.1.1 Conducta antisocial

De acuerdo con una definición muy elemental de “sociedad”, esta se entiende como "el conjunto de individuos que comparten una misma cultura y que interactúan entre sí para conformar una comunidad" (Definición, 2019). De lo anterior definición se deriva que lo social tiene este sentido de pertenencia ya que dentro de la comunidad se comparten principios, reglas, y formas de vivir, entre otras cosas, es decir, en cada sociedad existen pautas o modos característicos y propios de ésta, así como una determinada forma de convivencia social.

A partir de ello se entiende que cada sociedad tendrá pautas establecidas que permitan dicha convivencia y que, a priori, han sido establecidas para garantizar el bien común de esa comunidad. Bajo el concepto de bien común podemos encontrar muchas acepciones según el enfoque, ya sea bajo una perspectiva económica, filosófica, social, etc.

Por lo tanto, el bien común sería *"*el conjunto de condiciones que permiten al individuo y sociedad vivir de forma plena. Y el vivir de forma plena, implica estar en armonía con uno y con los demás, sin dañarse o dañar a los demás miembros de la colectividad". Una vez establecido este concepto entenderemos que lo antisocial será precisamente el contrario de lo prosocial, es decir, aquello que perturbe este clima de equilibrio y armonía, todo lo que vaya en contra de los intereses del bien común (Mulero, 2015), o sea, del bien de los miembros de esa sociedad.

Según la Real Academia Española, por antisocial se entiende aquello que es lo opuesto a la sociedad, al orden social. Esto implica, que el comportamiento antisocial será percibido a través de las conductas de un sujeto que son observables, en las que intervienen los movimientos y los pensamientos de esta persona siendo contrarias a las pautas que mantienen el orden social dentro de ese contexto en particular. Sin embargo, cada contexto es distinto y el orden social establecido se fundamenta en principios que no tienen por qué ser los mismos. Esto implica que un mismo comportamiento puede considerarse antisocial en una sociedad, pero no en otra.

Existen otras definiciones realizadas desde otros enfoques como es la realizada por Gallardo, García, Maydeu y Andrés, para estos autores, el comportamiento antisocial es un patrón general de desprecio y violación de los derechos de los demás, que comienza en la infancia o el principio de la adolescencia y continúa en la edad adulta. "El comportamiento antisocial es un fenómeno muy amplio que incluye distintos tipos de acciones, de las cuales destacan diferentes tipos de agresión, robos, engaños, conductas impulsivas, ultrajes y violencia entre sus diferentes manifestaciones. Estos comportamientos se pueden manifestar tanto en el ámbito clínico como normativo" (2009, p. 191).

2.1.2 Conducta antijurídica

Una conducta antisocial es todo aquel comportamiento que va en contra de las normas sociales establecidas. Hay normas de etiqueta, relativas a la adecuada forma de vestir en determinados momentos (por ejemplo, se usa ropa negra durante un velorio, o traje y corbata en determinados contextos de trabajo o convivencia); hay normas de urbanidad, referentes al comportamiento, el desenvolvimiento y el trato social (entre ellas, el saludo); hay normas de protocolo en la mesa, referentes a las buenas maneras y costumbres durante los alimentos en convivencia social (lo cual incluye uso de copas, cuchillería, maridaje entre alimentos y bebidas, fundamentalmente el tipo de vino que corresponde a ciertas comidas, entre otras), y hay muchas más que son de aceptación y observancia general, por lo cual se les considera constituyentes y referentes de un buen trato y convivencia con otras personas.

Comportarse de manera contraria, incluso en franco desafío y desobediencia a esas y otras normas, es considerado antisocial. Por supuesto, no hay que confundir esto con los movimientos contraculturales, sobre los cuales, Moreno (2005) dice lo siguiente: "el término contracultura procede de la traducción literal del inglés counter-culture, y su definición sería cultura en contra [o como dice De Vilena], movimiento cultural enfrentado con el sistema establecido y con los valores sociales dominantes en ese mundo; en una palabra, con la norma entendida como incuestionable o inamovible" (p. 52).

La contracultura, por antonomasia y parafraseando a Ortíz (1996), se asocia a movimientos juveniles, colectivos, que rebasan, rechazan, se marginan, se enfrentan, o trascienden la cultura institucional. Por ello, se confrontan con ella, con la cultura tradicional, dominante, dirigida, heredada, y con cambios para que nada cambie, y que suele ser irracional, generalmente enajenante, deshumanizante, que consolida el *status quo*, y que además de destruir o imposibilitar

la expresión auténtica entre los jóvenes, "acepta la opresión, la represión y la explotación por parte de los que ejercen el poder, naciones, corporaciones, centros financieros o individuos" (p. 129).

Sin embargo, contracultura no quiere decir "antisocial", ya que se trata de movimientos de rebeldía, pero no de agresión, aun cuando las imágenes de estos grupos suelen ser bastante depredadoras o intimidantes, tal es el caso de los punks, los *skinheads* o cabezas rapadas, o los chavos banda en México. En lo antisocial sí se manifiesta ese elemento, por lo cual puede distinguirse esa rebeldía y postura de confrontación con la cultura institucional por actitudes, indumentarias, expresiones artísticas (la mayor de ellas, la música), pero hay un trasfondo ideológico, quizá filosófico en algunas de ellas, y por ende hay normas, códigos y sanciones para sus miembros.

En lo antisocial se puede distinguir una simple conducta de rebeldía, sin mayores fundamentos ideológicos o morales, sino rebeldía así, sin mayor sentido que llevar la contraria a los demás. Incluso, podría hablarse de una rebeldía vandálica (por ejemplo, el grafiteo), pandilleril (que es un fenómeno asociativo, y que, aun terminando en riñas con otras pandillas, no es un crimen), pero que, pese a esto, son muy diferentes de una conducta criminal propiamente dicha. Y es que la antijuridicidad es un elemento del delito cuya presencia es necesaria para que este sea relevante o trascendente en el plano legal. Es por ello que se dice que una acción u omisión típica debe ser antijurídica.

Por ende, se denomina como antijurídica aquella conducta que es ilícita o contraria a (lo dispuesto por el derecho), y esa condición, junto con la tipicidad, permite determinar que se está ante una infracción penal dando paso a una pena o medida de seguridad en consecuencia (Palladino Pellón & Asociados Abogados Penalistas, 2019). Para llegar a la afirmación de que una conducta es antijurídica, se requiere necesariamente un juicio de valor, una estimación entre esa conducta

en su fase material y la escala de valores del Estado (Porte, 1958). “Una conducta es antijurídica cuando, siendo típica, no está protegida por una causa de justificación” (Machicado, 2019).

2.2 Teoría del delito

La palabra delito deriva del verbo latino *delinquere*, que significa abandonar, apartarse del buen camino. La carga jurídico-conceptual, viene estrechamente ligada a la carga histórica. Invariablemente, está ligado a la manera de ser de cada pueblo y a las necesidades de cada época; por lo tanto, los hechos que unas veces han tenido ese carácter, lo han perdido en función de situaciones diversas y, al contrario, acciones no delictuosas, han sido erigidas en delitos. Es así como, termina siendo relacionado con el derecho y con la ley. Véase la tabla 2 para dimensionar el concepto según la perspectiva de diversas corrientes de la ciencia del derecho:

Tabla 2. Concepciones en torno a la noción de lo antijurídico

Escuela	**Delito en la escuela clásica**	**Noción Sociológica**	**Noción jurídica -formal**	**Noción jurídica -sustancial**
Definición	Infracción de la Ley del Estado, promulgada para proteger la seguridad de los ciudadanos resultante de un acto externo del hombre,	Violación de los sentimientos altruistas de probidad y de piedad, en la medida media indispensable para	La suministra la ley positiva mediante la amenaza de una pena para la ejecución o	Como dice Jiménez de Asúa, es un acto típicamente antijurídico culpable, sometido a veces a

	positivo o negativo, moralmente imputable y políticamente dañoso (Carrara, 2007)	la adaptación del individuo a la colectividad. (Garófalo, 2007)	la omisión de ciertos actos. El artículo 11 del Código Penal para el estado de Puebla lo define como el acto o la omisión que sancionan las leyes penales.	condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal.

Nota: Elaboración propia. Información extraída de: Castellanos, F. (2008). Lineamientos elementales de derecho penal. México: Editorial Porrúa; Jiménez de Asúa, L. (1997). Principios de derecho penal. La ley y el delito. Buenos Aires: Abeledo Perrot-Editorial Sudamericana.

2.3 Tipos de delitos

En esencia, hay dos tipos de delitos: culposos y dolosos. En esta sección se verá a ambos, analizando sus características y explorando sus alcances.

2.3.1 Delitos culposos

De acuerdo con Pavón (2012), la culpa es aquel resultado (peligro o daño) típico y antijurídico, no querido ni aceptado, previsto o previsible, derivado de una acción u omisión meramente objetiva

y evitable si se hubieran observado los deberes de cuidado impuestos por el ordenamiento jurídico penal.

Conforme a lo dispuesto en el artículo 14 del Código Penal del Estado de Puebla (2018), la conducta es culposa si se produce el resultado típico, que no se previó siendo previsible, o que se previó confiando en que no se produciría, en virtud de la violación de un deber de cuidado que debía y podía observar según las circunstancias y condiciones personales. De ese modo, son dos las especies principales de la culpa:

I. *Consciente o con representación*. Se produce cuando el sujeto considera como posible la producción del resultado, pero confía en que no se producirá, y sus elementos son:

1. El sujeto considera el resultado, pero no quiere que se realice.
2. El sujeto realiza un acto con falta de cuidado.
3. Se produce un resultado dañoso.
4. El resultado era previsible, pero se confió en que no se produciría.

II. *Inconsciente o sin representación*. Se da cuando el sujeto no previó el resultado por falta de cuidado, teniendo la obligación de preverlo por ser de naturaleza previsible o evitable. Los elementos de esta clase de culpa son los siguientes:

1. El sujeto no considera el resultado material.
2. El sujeto realiza un acto descuidado.
3. Se produce un resultado dañoso.
4. El resultado era previsible.
5. El sujeto no quería, ni se representó el resultado.

De lo anteriormente expuesto se puede deducir que los elementos de la culpa en general son los que a continuación se enuncian:

- *Una conducta voluntaria*. Sólo la acción u omisión voluntaria que ha transgredido el orden jurídico penal puede ser objeto del juicio de culpabilidad.
- *Un resultado típico y antijurídico*. Esto quiere decir que la acción u omisión se adecua perfectamente al hecho comprendido en un tipo penal y en consecuencia resulta contrario a la norma en el juicio objetivo de valoración.
- *Nexo de causalidad entre la conducta y el resultado*. Para atribuir el resultado a un sujeto, debe precisarse la relación causal de aquél con la conducta desplegada.
- *Naturaleza previsible y evitable del evento*. No se puede reprochar el incumplimiento si el evento era imprevisible e inevitable.
- *Ausencia de voluntad del resultado*. Se excluye la posibilidad de la voluntad del sujeto respecto al resultado: en él no existe la intención delictiva para producir el resultado.
- *Violación de los deberes de cuidado*. Que el sujeto haya actuado con imprudencia, negligencia o impericia (Calderón, 2017).

2.3.2 Delitos dolosos

Debe considerarse al dolo como la intención prevista y querida por el agente, dirigida a la obtención de un resultado delictuoso (Roxin, 1977). Consiste en causar intencionalmente el resultado típico, con conocimiento, y conciencia de la antijuridicidad del hecho (Amuchategui, 2012). El Código Penal del Estado de Puebla (2018), indica que la conducta es dolosa si se ejecutó con intención y coincide con los elementos del tipo penal, o si se previó como posible el resultado típico y se quiso o aceptó la realización del hecho descrito por la ley.

2.4 Elementos que configuran los delitos

En la dogmática penal se han presentado diversos posicionamientos sobre la estructura del delito (Franco, 2012). Sin embargo, la estructura que se considera más eficaz para el estudio dogmático de los casos penales deriva de la teoría heptatómica, que considera siete elementos. Se debe precisar que algunos autores distinguen entre elementos esenciales de aquellos, que no lo son, pues no se exigen en todos los delitos.

Tabla 3. Elementos que configuran a los delitos

Aspecto positivo	Aspecto negativo
1. Conducta o hecho.	1. Ausencia de conducta.
2. Tipicidad.	2. Atipicidad.
3. Antijuridicidad.	3. Causas de justificación.
4. Imputabilidad	4. Causas de inimputabilidad.
5. Culpabilidad.	5. Causas de inculpabilidad.
6. Condicionalidad objetiva.	6. Falta de condición objetiva.
7. Punibilidad.	7. Excusas absolutorias.

Nota: Calderón, A. T. (2017). Teoría del delito y juicio oral. México: UNAM-Instituto de Investigaciones Jurídicas.

2.4.1 Elementos propios de los delitos cibernéticos

Como afirman Gutiérrez (1991), "vivimos en plena era de la informática" (p. 37) y Bequiai (1978), las sofisticadas calculadoras electrónicas, funcionales, fiables, y de gran capacidad, han invadido los ámbitos más diversos de las relaciones socioeconómicas, en donde "pocas dimensiones de nuestra vida no se ven afectadas, dirigidas o controladas por el ordenador directa o indirectamente.

Sectores como la banca, los seguros, los transportes, la educación, la bolsa, el tráfico aéreo y terrestre, las administraciones públicas en su conjunto, etc., dependen, en gran medida, de las computadoras. A ellas se les encomienda, ya no sólo el archivo y procesamiento de información sino, incluso, la adopción automática de decisiones".

La revolución informática ha incidido de forma insospechada en el viejo concepto de "la información", revitalizando espectacularmente e incrementando de forma extraordinaria su valor. Agregando que las nuevas técnicas posibilitan una potenciación indefinida de las acumulaciones de datos en poco espacio, de fácil acceso y recuperación, a través de una clave o código único, en cuestión de escasos segundos y de también muy simple interrelación, tratamiento, y transmisión. "Como consecuencia, lo que tradicionalmente hubiera constituido una mera acumulación de datos, hoy, a causa del impacto de la revolución informática, se ha transformado en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico" (Gutiérrez, citado en Arroyo, Tiedemann, 1994, p. 184).

Hablando concretamente de las peculiaridades en cuanto a los delitos cibernéticos tipificados en el estado de Puebla y tomando en cuenta que sólo existen cuatro artículos respecto al tema en el Código Penal de la misma circunscripción, se pueden enunciar, además de los considerados para los delitos en general, las siguientes:

- Se revela, modifica, copia, divulga, destruye o provoca pérdida de información de suma importancia.
- La información debe estar o haber estado contenida en sistemas o equipos de informática.
- Los sistemas o equipos debieron estar protegidos por algún mecanismo de seguridad.
- No importa, más que para la dosificación de la pena, si la persona estaba o no autorizada para acceder al o los sistemas de los que se trate.

- No importa, más que para la dosificación de la pena, si la víctima es el Estado o alguna otra persona física o moral que, en su caso, resguarda un secreto industrial.

2.4.2 Definición de delito cibernético

Los delitos perpetrados mediante las tecnologías de la información y la comunicación (TIC), así como el ciberespacio en donde se cometen, no tienen límites, por lo que resulta difícil la tarea de perseguirlos; sobre todo, si se toma en cuenta que muchos de los ataques tienen la característica adicional de ser anónimos y no dejar huellas. Por ello, la investigación de este tipo de eventos es compleja y no puede ser llevada a cabo por un solo organismo.

Los expertos en seguridad informática no pueden enfrentarse solos a estas amenazas, por lo que es necesario trabajar en sociedad formando equipos multidisciplinarios que incluyas a especialistas de todos los ámbitos posibles, ya que, aun cuando su aportación no sea meramente técnica, su condición de ciudadanos, de colaboradores en una empresa, o en una institución pública o privada, aunada a su capacidad de poder influir socialmente en los demás, resultan ser características deseables para difundir el mensaje que los organismos preocupados por contribuir a mejorar la calidad en la prevención intentan comunicar.

Un delito cibernético se define como “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnere los derechos del titular de un elemento informático, ya sea hardware o software. (Asimismo) el delito informático está vinculado no sólo (con) la realización de una conducta delictiva a través de medios o elementos informáticos, o (con) los comportamientos ilícitos en los que aquellos sean su objeto, sino también (con) la afectación de la

información per se como bien jurídico tutelado, diferente de los intereses jurídicos tradicionales" (Ojeda-Pérez, 2010, p. 49).

2.5 Perpetradores del delito

Por costumbre y de manera genérica se suele enunciar, etiquetar, referir, y vincular a los perpetradores de los delitos con el término "delincuencia" (del latín delinquentia), que al mismo tiempo es la cualidad de delincuente (una persona que comete delitos y, por lo tanto, viola la ley). También se utiliza el término para nombrar a las y los sujetos que delinquen y realizan conductas contrarias al derecho (Sosa, 2015).

Velazco (2006), refiere que "si el delincuente es el 'sujeto que delinque', o lo que es igual, 'sujeto activo o agente del delito', entonces la delincuencia es la 'calidad de delincuente', la 'comisión de un delito' o un 'conjunto de delitos en general, o referidos a un país o época'" (p. 3). Esto es pertinente porque la delincuencia, entendida como los delincuentes, los individuos que la conforman cometen delitos, es decir, infracciones en contra de lo establecido en la ley, pero lo que es delito en estos tiempos, en otros podrían haber sido una conducta de aceptación general.

Por lo tanto, se habla de que son delitos en un momento y en una etapa histórica dada, lo mismo que en un lugar específico. Herrero coincide con esto cuando define a la delincuencia como "el fenómeno social constituido por el conjunto de las infracciones, contra las normas fundamentales de convivencia, producidas en un tiempo y lugar determinados" (1997, p. 225). Además, refiere Velazco, que hay dos tipos de delincuencia:

a. Delincuencia menor, y
b. Delincuencia organizada.

El mismo autor precisa que, por su escala de acción se puede hablar de una delincuencia estratificada: menor, intermedia y mayor, tal como la clasifica Leticia Salomón, del Foro

Ciudadano de Honduras. Velazco, hace la siguiente precisión: "la delincuencia menor o delincuencia común es la más visible y temida, pero constituye apenas la punta del iceberg. Al hablar de delincuencia intermedia y mayor se está hablando, de facto, de delincuencia organizada, y aunque todas ellas requieren de una mayor preparación de las fuerzas de seguridad pública, la organizada requiere, además, recursos tecnológicos e intelectuales muy avanzados" (2006, p. 5).

2.5.1 Delincuencia común o menor

Es llamada así por ser considerada como la más popular, la que se ve habitualmente y que da como resultado que la población, en general, piense en determinadas zonas como "peligrosas" y asocien a la inseguridad con esto, y tradicionalmente no se le asociaba a mayor peligrosidad, si bien esta percepción ha ido cambiando con el tiempo.

Velazco (2006), refiere que la delincuencia menor es cometida por una o dos personas como máximo, donde se tiene por objetivo la comisión de un delito que podría ser desde una falta menor hasta una grave y calificada, pero que no trasciende su escala y proporción, es decir, no son cometidos por bandas, no hay una gran planeación en los hechos delictivos, o no se pretende operar permanentemente a gran escala. Salomón, indica que los delitos más comunes de este tipo de criminalidad son las siguientes:

- Asalto a transeúntes
- Carterismo
- Violación
- Robo de bienes y artículos menores
- Robo a casas habitación
- Robo de vehículos
- Vandalismo

- Grafitis y pinta de muros y monumentos (citado en Velazco, 2006, p. 6)

Agrega Velazco (2006) que éstos y otros delitos pueden ser cometidos en grandes proporciones y por muchos individuos, con lo cual ya se convierte en una delincuencia organizada, tanto de nivel intermedio como mayor, y que cuando se convierten en tales, se ha dado en decir que se convierten en la "industria del robo", "la industria del secuestro", la "industria del robo de vehículos", etc. Las características de la delincuencia menor son las que a continuación se enuncian:

- No cuenta con una organización compleja.
- No existen códigos que deban acatar los delincuentes.
- No existe como tal una estructura de mando y subordinación.
- Su fin no es más que delinquir para obtener dinero, pero no pretende operar permanentemente a gran escala.

Por último, Velazco complementa estas características haciendo las siguientes precisiones y señalamientos acerca de la delincuencia común o menor:

1. El asaltante puede apelar o no a dos recursos para lograr sus objetivos:
    1. Una precisión técnico-manual elevada y precisa para cometer el ilícito con rapidez, astucia y disimulo, y
    2. el uso de la fuerza con apoyo en ventajas físicas, e incluso, en el empleo de armas.

2. Normalmente existen compradores de bienes robados, que son quienes los adquieren de conformidad con tarifas ya existentes en el mercado negro, mismas que son fijadas por la oferta y la demanda, así como por la situación del entorno local, nacional, e internacional.

3. Regularmente, los delincuentes operan con apoyo de una red de corrupción entre autoridades intermedias (jueces calificadores, agentes del ministerio público del fuero común) y corporaciones de seguridad pública desde sus mandos y efectivos elementales hasta -cuando mucho- sus mandos medios (agentes de policía, jefes de sector, etc.).

2.5.2 Delincuencia organizada

La delincuencia organizada es la "estructura criminal creada con la finalidad expresa de obtener y acumular beneficios económicos a través de su implicación continuada en actividades predominantemente ilícitas y que asegure su supervivencia en diligencias, funcionamiento y protección mediante el recurso de la violencia y corrupción o la confusión en empresas legales" (Corte, 2010).

Lozano (2002), considera que el crimen organizado significa un mecanismo de acumulación, robo, y redistribución de capital propio de la economía informal, que también llega a formar parte de la economía formal local, nacional, y global. Para Velazco (2006), el crimen organizado tiene serias implicaciones del orden económico, ya que constituye una importante derrama de recursos, pues todo el capital generado y distribuido se cubre en efectivo.

Así, la que se denomina organizada es "la delincuencia colectiva que instrumentaliza racionalmente la violencia institucional de la vida privada y pública, al servicio de ganancias empresariales con rapidez. Necesariamente vincula jerarquías de la burocracia política y judicial mediante la corrupción y la impunidad" (Lozano, 2002, p. 17). Finalmente, Lozano (2002) señala las siguientes características de este tipo de criminalidad:

I. Opera bajo una disciplina y códigos de comportamiento mafioso;
II. Actúa con la finalidad de obtener en la forma de prácticas sociales recurrentes -enraizadas en la estructura del trabajo, a nivel local, nacional e internacional- ganancias rápidas sin inversión previa

de capital, de origen ilegítimo e ilegal, mediante la apropiación de objetos de uso privado" y de propiedad ajena.

III. En otras ocasiones, recurriendo a las mismas prácticas, se comercializa con bienes, productos, y servicios de origen ilegítimo e ilegal, con poca o ninguna inversión de capital.

IV. La delincuencia organizada actúa de manera impune en la clandestinidad, protegida -y a veces también dirigida y operada- por autoridades corruptas, delincuentes de alto nivel, especialización y jerarquía, y posee capacidad para utilizar la fuerza en aras de lograr sus objetivos.

V. Con respecto a los bienes, productos, y servicios ofertados por la delincuencia organizada, una vez que estos se ponen en circulación, "quedan definidos sus precios por las condiciones del mercado regional o mundial" -denominado, coloquialmente, mercado negro-, "siendo el mercado, escenario de esta criminalidad organizada".

2.5.3 Delincuentes informáticos

Los autores de aquellas acciones que son consideradas ciberdelitos, es decir los sujetos activos, delincuentes informáticos o cibercriminales, son generalmente concebidos como expertos en el manejo de herramientas tecnológicas (comprendidas en todas las áreas de la informática, telemáticas, sistemas, redes, etc.), con un dominio excepcional de estas y con altas aspiraciones de recompensa por sus ataques. De ese modo, "no podemos negar que la especialización informática facilita a los sujetos a incidir criminalmente por medio de las computadoras" (Acurio del Pinol, 2016, p. 18).

En la actualidad, el acceso a los conocimientos que en algún momento pertenecieron a un grupo exclusivo se encuentra disponible prácticamente a cualquier usuario de Internet, de manera que, inclusive un sujeto con mínimos conocimientos en informática, puede ser capaz de seguir las

instrucciones de un tutorial para llevar a cabo un ataque, aun cuando sus intenciones no sean más que corroborar si es posible replicar el ejemplo.

En el caso que sea, la perpetración de un delito, aunque aparentemente no sea de manera intencional, pero habiendo una clara conciencia de lo que se hace y un pleno conocimiento de causa, hace que la persona sea un delincuente. Y así como hay delitos que son típicamente informáticos, los hay que siguen siendo el mismo crimen en su esencia (fraude, estafa, por ejemplo), sólo que ahora se cometen por otros medios, por ejemplo, las tecnologías.

2.6 Catálogo de delitos cibernéticos

Hay delitos que se perpetraron antes de la aparición y el advenimiento de las computadoras, la Internet, las redes, y otros recursos y tecnologías de la comunicación y la información, las conocidas como TICs, y que en la actualidad también se cometen por estos. Su esencia, como tal, no cambia, sino solamente la forma en la que se llevan a cabo, así como los recursos empleados para ello. La costumbre ha hecho que se les denomine delitos informáticos, aunque nada más lo sean por la vía a través de la cual se realizan. Hay otros que son efectiva, plena y únicamente informáticos. Todos ellos se examinarán en esta sección.

2.6.1 Fraude cibernético

De acuerdo con el artículo 402 del Código Penal del Estado de Puebla (2018), comete el delito de fraude el que, engañando a uno, o aprovechándose del error en que éste se halla, se hace ilícitamente de alguna cosa o alcanza un lucro indebido. Siguiendo este postulado, el 30 de diciembre de 2013, se reformó la fracción XIX del artículo 404, que a la letra dice:

> Las mismas sanciones señaladas en el artículo anterior, se impondrán: Al que dolosamente y con el propósito de procurarse un lucro ilícito, para sí o para un tercero, dañe o perjudique

el patrimonio de otro, mediante el uso indebido de mecanismos cibernéticos, que provoque o mantenga un error, sea manipulando datos de entrada a un equipo de informática con el fin de producir o lograr movimientos falsos en transacciones de una persona física o moral, sea presentando como ciertos hechos que no lo son, o deformando o disimulando hechos verdaderos", ampliando de esta forma su definición original y especificando lo que podríamos entender como "fraude cibernético (94-95).

2.6.2 Delitos sexuales

De acuerdo con el artículo 32 de la Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de Estos Delitos (2018), "se impondrá pena de 2 a 7 años de prisión y de 500 a 2 mil días multa al que, en cualquier medio impreso, electrónico o cibernético contrate, de manera directa o indirecta, espacios para la publicación de anuncios que encuadren en los supuestos de publicidad ilícita o engañosa, con el fin de facilitar, promover o procurar que se lleve a cabo cualquiera de las conductas delictivas objeto de la presente Ley" (p. 12).

A su vez, el artículo 33 del mismo ordenamiento en cita, dispone que se aplicará "pena de cinco a quince años de prisión y de un mil a veinte mil días multa a quien dirija, gestione, o edite un medio impreso, electrónico, o cibernético que, incumpliendo lo dispuesto con esta ley, publique contenidos a través de los cuales facilite, promueva, o procure cualquiera de las conductas delictivas objeto de la misma" (p. 12).

2.6.3 Delitos de espionaje contra las instituciones de seguridad pública y procuración de justicia

De acuerdo al artículo 186 octies del Código Penal del Estado de Puebla (2018), a quien con la intención de obstruir el desempeño legítimo de las instituciones de seguridad pública o de encubrir o facilitar un delito, aceche, vigile, o realice actos tendentes a obtener información sobre la ubicación o actividades de los servidores públicos de las instituciones de seguridad pública o procuración de justicia, que realicen operativos, labores de seguridad pública, persecución, sanción de delitos, o de ejecución de penas, se impondrá una pena de dos a seis años de prisión y multa de cincuenta a doscientos días de salario mínimo.

De acuerdo con el mismo precepto, si la conducta prevista en el párrafo anterior se realiza en relación con operativos para combatir delitos de delincuencia organizada, secuestro, robo de vehículos, trata de personas o narcomenudeo, la pena será de cuatro a diez años de prisión, y si la información a que se refiere este artículo es transmitida a un tercero, por cualquier medio, la pena de prisión se aumentará hasta en un tercio de la sanción que corresponda.

Igualmente, si el delito es cometido por servidor público o por quien haya pertenecido a las fuerzas armadas, instituciones de seguridad pública, o de procuración de justicia, las penas señaladas se aumentarán desde un tercio hasta una mitad de la pena que corresponda, y además se impondrá como sanción la destitución del cargo e inhabilitación de cinco a diez años para ocupar otro cargo en el servicio público (pp. 3-4).

2.6.4 Delitos informáticos

El artículo 475 del (CPEP, 2018), establece que “se impondrá prisión de uno a cinco años, multa de cincuenta a quinientos días de salario y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o

técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial" (p. 114).

Conforme al artículo 476 del (CPEP, 2018), "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 de multa, y 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" (p. 114). Igualmente se dispone que:

- Al que sin autorización modifique, destruya, o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a dos años de prisión y de doscientos a seiscientos días multa (artículo 477, p. 114).
- Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya, o provoque pérdida de información que contengan, se le impondrán de dos a cuatro años de prisión y de trescientos a novecientos días multa.
- Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a dos años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.
- A quien, estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de dos a cinco años de prisión y multa de quinientos a mil días de salario mínimo general vigente. Si el responsable es o hubiera sido

servidor público en una institución de seguridad pública, se impondrá, además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública (artículo 478, p. 115).

2.7 Estrategias para garantizar la ciberseguridad

Los usuarios comunes se encuentran vulnerables debido al desconocimiento de temas en materia de ciberseguridad, por lo que es necesario que tanto las autoridades como organismos no gubernamentales se encarguen de proteger a la ciudadanía, desarrollando estrategias de prevención. Como se ha explicado anteriormente, la asociación civil es la figura que cubrirá parte de las necesidades de los ciudadanos. Sin embargo, estos también deberán contribuir, aprovechando los activos ofrecidos, ya sea que se trate de cursos, talleres o manuales, cuyo fin sea fomentar en ellos la cultura de la prevención.

De esta forma, el trabajo será conjunto y permitirá formar a los usuarios, procurando minimizar al máximo posible sus debilidades, para que estas no puedan ser aprovechadas por la ciberdelincuencia. Es decir, el usuario debe estar preparado a nivel intelectual adquiriendo conocimientos básicos en ciberseguridad; a nivel emocional, para conservar la cordura que le permita actuar ante un posible ataque, además ser consciente para evitar hábitos nocivos de navegación, así como tener noción de cómo proceder en caso de verse en la necesidad de denunciar un delito cibernético, sabiendo a dónde acudir y de qué manera puede preservar o tomar registro de las evidencias que coadyuven al proceso de investigación de un hecho delictivo de esta naturaleza.

2.7.1 Estrategias latinoamericanas en ciberseguridad

En los últimos años, se ha identificado que la actividad de los ataques cibernéticos no es exclusiva de las grandes compañías, ni de los países más desarrollados. Durante 2018, la empresa de

seguridad informática Kaspersky registró un alza de 60% en ataques cibernéticos en América Latina, cuya cifra se estimó en más de 746 mil ataques de malware diarios, es decir, un promedio de 9 ataques de malware por segundo (Saldana, 2018).

México ocupó la posición número dos como el país más atacado a nivel de toda América Latina, recibiendo en promedio 1.5 millones de ataques al día, quedando solamente por debajo de Brasil, además de que el 41% de las empresas más atacadas entraron en la categoría de Pymes, ya que son las que menos protección tienen y, por lo tanto, resultan ser más vulnerables (PC World México, 2018).

Debido a este panorama, algunos países de América Latina han estado trabajando para desarrollar medidas para hacer frente a la ciberdelincuencia, ya que "la importancia estratégica de disponer de un ciberespacio seguro conlleva la creación de un sistema de Ciberseguridad Nacional basado en una Estrategia Nacional de Ciberseguridad (ENCS), es decir, un conjunto de órganos, organismos y procedimientos que permitan la dirección, control y gestión de la seguridad en el ciberespacio" (Leiva, 2015, p. 161).

Es así, que hasta 2017, por lo menos 5 países ya habían diseñado su propia estrategia de ciberseguridad, entre ellos: Colombia, Panamá, Paraguay, Chile, y Costa Rica. A continuación, se muestran los objetivos específicos de cada una de ellas (ver tabla 4).

Tabla 4. Estrategias nacionales de ciberseguridad en América Latina (Colombia, Panamá, Paraguay, Chile y Costa Rica)

País	**Nombre de la Estrategia**	**Objetivos**
Colombia	Política Nacional de Seguridad Digital	1. Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos, involucrando a las partes interesadas. 2. Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de la seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital. 3. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos. 4. Fortalecer la defensa y la soberanía nacional en el entorno digital con un enfoque de gestión de riesgos. 5. Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia

		en seguridad digital, a nivel nacional e internacional.
Panamá	Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas	1. Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio. 2. Prevenir y detener las conductas delictivas en el ciberespacio o el uso de éste para cualquier tipo de delitos o actos ilícitos. 3. Fortalecer la seguridad cibernética de las infraestructuras críticas nacionales. 4. Fomentar el desarrollo de un tejido empresarial nacional fuerte en seguridad cibernética, como referencia para la región.

		5. Desarrollar una cultura de seguridad cibernética a través de la formación, innovación y la adopción de estándares. 6. Mejorar la seguridad cibernética y capacidad de respuesta ante incidentes de los organismos públicos.
Paraguay	Plan Nacional de Ciberseguridad	1. Sensibilización y Cultura. 2. Investigación, Desarrollo e Innovación. 3. Protección de Infraestructuras Críticas. 4. Capacidad de Respuesta ante Incidentes Cibernéticos. 5. Capacidad de Investigación y Persecución de la Ciberdelincuencia. 6. Administración Pública. 7. Sistema Nacional de Ciberseguridad.
Costa Rica	Estrategia Nacional de Ciberseguridad	1. Coordinación Nacional. 2. Conciencia pública. 3. Desarrollo de la Capacidad Nacional de Seguridad Cibernética.

		4. Fortalecimiento del marco jurídico en Ciberseguridad y TIC. 5. Protección de Infraestructuras Críticas. 6. Gestión del Riesgo. 7. Cooperación y Compromiso Internacional. 8. Implementación, Seguimiento y Evaluación.
Chile	Política Nacional de Ciberseguridad	1. Desarrollar una infraestructura de las TIC que, bajo una óptica de gestión de riesgos, sea capaz de resistir y recuperarse de incidentes de ciberseguridad. 2. Garantizar los derechos de los ciudadanos en el ciberespacio. 3. Desarrollar una cultura de ciberseguridad en torno a la responsabilidad en el uso de las TIC, a las buenas prácticas y a la educación. 4. Establecer relaciones de cooperación con otros actores en materia de ciberseguridad y participar de forma activa en foros internacionales.

	5. Desarrollar una industria de la ciberseguridad chilena, que sea útil a los objetivos estratégicos del país.

Nota: Hernández, J. C. (2017). Estrategias nacionales de ciberseguridad en América Latina. Recuperado del portal electrónico del Grupo de Estudios en Seguridad Internacional (GESI), Universidad de Granada (España). Disponible en: http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-américa-latina

2.7.2 Estrategia Nacional de Ciberseguridad

En México existe una creciente dependencia de los servicios basados en tecnologías de la información que, como se ha explicado, se encuentra circundada por un aumento en la cantidad de ataques cibernéticos. En la actualidad, los tres principales ciberriesgos que enfrenta el sector público son el posible robo o alteración a la información que resguarda sobre los ciudadanos, las afectaciones a la operación de servicios públicos y operaciones de entidades gubernamentales, y el potencial daño a la confianza en las instituciones (McKinsey & Company, 2018).

Desde 2017, el Gobierno de la República se ha reunido con expertos en ciberseguridad por medio del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA) para discutir los temas concernientes a esta, así como para compartir experiencias y mejores prácticas. Como resultado de estas mesas de trabajo, se lograron identificar 5 temas fundamentales para mejorar las capacidades de seguridad cibernética del país. Los temas, de acuerdo con el documento *Recomendaciones para el Desarrollo de la Estrategia Nacional de Ciberseguridad (2017)*, son los siguientes:

1. Investigación y desarrollo;
2. Cultura, educación y prevención;
3. Cooperación y coordinación;
4. Normas, criterios técnicos y regulación; y
5. Marco legal.

Derivado de la colaboración entre la Organización de los Estados Americanos (OEA) y el gobierno de México (a través de la Secretaría de Relaciones Exteriores y de su Misión Permanente ante la OEA), el 13 de noviembre de 2017 se presentó formalmente la Estrategia Nacional de Ciberseguridad durante la inauguración de la Tercera Semana Nacional de Ciberseguridad en la Ciudad de México.

El objetivo general de la Estrategia Nacional de Ciberseguridad (2017) es identificar y establecer las acciones en materia de ciberseguridad aplicable al ámbito social, económico, y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano. Asimismo, el documento establece que, para contar con recursos para la gestión de riesgos y amenazas en el ciberespacio, el Estado mexicano deberá fomentar el desarrollo de capital humano, mediante:

Tabla 5. Desarrollo de capital humano mexicano (Estrategia Nacional de Ciberseguridad, 2017)

Formación de:	
I.	Especialistas y profesionales de la ciberseguridad.
II.	Líderes profesionales de la ciberseguridad como conductores de estrategias y políticas.
III.	Profesionales de la investigación y desarrollo para la industria y el comercio de la ciberseguridad.

IV.	Profesionales de la investigación y persecución de los delitos que se cometen a través de las TIC, así como de la procuración e impartición de justicia.

Fuente: Estrategia Nacional de Ciberseguridad. (2017). México: Gobierno de México.

2.7.3 Equipos de respuesta a incidentes en ciberseguridad

Ante la existencia de numerosos incidentes en ciberseguridad, aunado a sus respectivas pérdidas, desde hace 30 años se creó en E.U. la figura de *Equipo de Respuesta ante Emergencias Informáticas* (por sus siglas en inglés CERT), que se trata de un "conjunto de personas responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información" (Barrio, 2011 en Real Academia Española, 2019).

De acuerdo con Riquelme (2018), los dos principales equipos con tal denominación son el Instituto de Ingeniería en Software de la Universidad de Carnegie Mellon, en Pennsylvania, Estados Unidos, y el segundo US-CERT, el equipo de respuesta del Departamento de Seguridad Nacional estadounidense. Los equipos de otros países reciben el nombre de *Equipo de Respuesta ante Incidentes de Seguridad Informática* (CSIRT). Sin embargo, al obtener una certificación por parte de la Universidad de Carnegie Mellon pueden incluir en su nombre la sigla CERT. En México actualmente se encuentran en funcionamiento 4 CSIRT certificados, y los principales enfoques de cada uno se ven en la tabla 6.

Tabla 6. CSIRT certificados en funcionamiento en México

Institución	**Denominación**	**Institución certificadora**	**Enfoque**

Universidad Nacional Autónoma de México	CSIRT (CERT) público	Universidad de Carnegie Mellon	Concentrado en responder a incidentes, analizar amenazas, e intercambiar información de ciberseguridad con otros equipos de respuesta, así como en la generación de estadísticas, boletines, cursos y campañas de divulgación.
Consejo Nacional de Ciencia y Tecnología	CSIRT (CERT) público	Universidad de Carnegie Mellon	Desarrollo de proyectos de investigación que inciden de manera directa en el desarrollo de sectores clave del país: Evaluación de las tecnologías en contextos industriales, gubernamentales y/o sociales, análisis de la relación entre el marco constitucional y legal asociado a las TIC y su impacto.
Universidad Autónoma de Chihuahua	CSIRT (CERT) público	Universidad de Carnegie Mellon	Desarrollo e implementación de programas en materia de seguridad informática, como: capacitación, talleres, impartición de cursos y difusión de boletines relacionados con seguridad informática. También pone a la disposición de empresas, instituciones educativas y a la sociedad civil en general herramientas, material de apoyo,

			manuales, software que contribuyan a fortalecer mecanismos de prevención de delitos informáticos.
Policía Federal	CSIRT (CERT) público	Universidad de Carnegie Mellon	Acciones de prevención e investigación de conductas ilícitas a través de medios informáticos, monitorea la red pública de 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. De igual forma, implementa programas de desarrollo científico y tecnológico en materia cibernética, así mismo es la única autoridad acreditada a nivel federal para realizar intercambio de información con policías cibernéticas nacionales y organismos policiales internacionales.

Nota: Elaboración propia a partir de:

- CERT UNAM (Fecha de consulta: 27 de mayo de 2019). Recuperado del portal electrónico de la Universidad Nacional Autónoma de México. Disponible en: https://www.cert.unam.mx/csi
- ¿Qué es INFOTEC? (Fecha de consulta: 28 de mayo de 2019). Recuperado del portal electrónico del Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación. Disponible en: https://www.infotec.mx/es_mx/infotec/que_es_infotec
- ¿Quiénes somos? (Fecha de consulta: 28 de mayo de 2019). Recuperado del portal electrónico del Equipo de Respuesta a Incidentes y Delitos Informáticos de la Universidad Autónoma de Chihuahua. Disponible en: http://csirtchihuahua.uach.mx/quien.html
- Policía Federal (Fecha de consulta: 29 de mayo de 2019). El CERT-MX se encarga de prevenir y mitigar las amenazas de seguridad informática que ponen en riesgo la infraestructura tecnológica y la operatividad del país. Recuperado del portal electrónico de la Policía Federal. Disponible en: https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es

2.7.4 Proyectos y servicios

Los *Equipos de Respuesta ante Emergencias Informáticas* se encargan de atender las necesidades en materia de ciberseguridad, que van desde la generación de estadística, desarrollo de programas de capacitación a manera de cursos y talleres, desarrollo de productos científicos y tecnológicos,

así como la investigación de conductas delictivas e intercambio de información entre organismos internacionales.

Sin embargo, en febrero de 2018, tras la publicación de la Estrategia Nacional de Cibeseguridad, se estableció la *Subcomisión de Ciberseguridad*, durante la *Comisión Intersecretarial de Gobierno Electrónico*, con el objetivo de "salvaguardar los aplicativos e infraestructura y favorecer la cultura tecnológica de la seguridad". Esta Subcomisión desarrolló la *Propuesta de Líneas de Acción del Eje Transversal de Desarrollo de Capacidades*, y se dio a la tarea de identificar los proyectos implementados en materia de ciberseguridad por parte de instituciones educativas en el país, lo cual fue clasificado en cuatro rubros:

I. Desarrollo de capacidades;
II. Cultura de ciberseguridad;
III. Coordinación y colaboración;
IV. Investigación, desarrollo e innovación, estándares, y criterios técnicos.

2.7.4.1 Proyectos destinados al desarrollo de capacidades

Actualmente, se han creado varios tipos de proyectos que desde un enfoque académico tienden al desarrollo de las capacidades de aquellas personas que directa o indirectamente, con grado o sin él, en lo operativo o lo administrativo, y ya sea en el sector público, el privado, el académico o el social, etc., se dedican a la labor de seguridad pública. Muchos de esos programas son, tanto profesionalizantes, como investigativos, y se estructuran en las siguientes modalidades:

I. Diplomados;
II. Licenciaturas;
III. Especialidades, y
IV. Maestrías.

Igualmente, existen programas breves de formación, como cursos y talleres, pero los que tienen mayor relevancia por su duración y amplitud, son estos. Se están empezando a implementar programas de doctorado, pero, al momento, los consolidados son los ya mencionados. En las siguientes secciones se examinarán los casos de las instituciones mexicanas que ofrecen dichos programas.

Diplomados. Las siguientes instituciones ofrecen en México diversos diplomados con alto reconocimiento en las materias que interesan a la presente investigación. Véase la tabla 7.

Tabla 7. Instituciones mexicanas que imparten programas de diplomado en materia de ciberseguridad

Institución	Programa
Universidad Nacional Autónoma de México	Diplomado en Seguridad de la Información
Universidad Autónoma de Yucatán	Diplomado en Seguridad Informática
Universidad Autónoma de Chihuahua	Diplomado Básico de Seguridad Informática
Universidad Autónoma de Nuevo León	Diplomado en Seguridad de la Información
Universidad Autónoma de Yucatán	Diplomado de Seguridad Informática

Nota: Propuesta de líneas de acción del Eje Transversal de Desarrollo de Capacidades (2018). México: Subcomisión de Ciberseguridad-ANUIES.

Especialidades. En la tabla 8, se presentan las instituciones mexicanas que ofrecen algunos programas de especialidad que tienen reconocimiento de validez oficial de estudios en materia de ciberseguridad y las tecnologías que comparten dicho rubro.

Tabla 8. Instituciones mexicanas que imparten programas de especialidad en materia de ciberseguridad

Institución	Programa
Instituto Politécnico Nacional	Especialidad en Seguridad Informática y Tecnología de la Información
Universidad la Salle-Ciudad de México	Especialidad en Ciberseguridad

Nota: Propuesta de líneas de acción del Eje Transversal de Desarrollo de Capacidades (2018). México: Subcomisión de Ciberseguridad-ANUIES.

Licenciaturas. En la tabla 9 se presenta la institución mexicana que ofrece algunos programas de especialidad que tienen reconocimiento de validez oficial de estudios en materia de ciberseguridad.

Tabla 9. Instituciones mexicanas que imparten programas de licenciatura en materia de ciberseguridad

Institución	Programa
Universidad Autónoma de Nuevo León	Licenciatura en Seguridad en Tecnologías de Información

Nota: Propuesta de líneas de acción del Eje Transversal de Desarrollo de Capacidades (2018). México: Subcomisión de Ciberseguridad-ANUIES.

Maestrías. Por último, se presentan las instituciones que dentro del territorio nacional ofrecen programas de maestría en las materias que interesan a la presente investigación.

Tabla 10. Instituciones mexicanas que imparten programas de maestría en materia de ciberseguridad

Institución	Programa
Instituto Politécnico Nacional	Maestría en Ingeniería en Seguridad y Tecnologías de la Información
Universidad la Salle-Ciudad de México	Maestría en Ciberseguridad
Universidad Autónoma de Nuevo León	Maestría en Seguridad de la Información
Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE)	Maestría en Ciencias y Tecnologías de Seguridad
Universidad Tecnológica De México	Maestría en Seguridad de Tecnología de Información

Nota: Propuesta de líneas de acción del Eje Transversal de Desarrollo de Capacidades (2018). México: Subcomisión de Ciberseguridad-ANUIES.

2.7.5 Investigación, desarrollo e innovación

En esta línea, la única institución en todo el país que cuenta con un área dedicada a la investigación en este sector y las líneas tecnológicas y científicas que le son inherentes, es el Instituto Politécnico Nacional, que tiene al Laboratorio de Ciberseguridad (CISEG), el cual está adscrito al Centro de Investigación de Computación (CIC) de dicho Instituto.

Creado en noviembre de 2014, "es el único laboratorio a nivel nacional especializado en estos temas, que aborda diferentes líneas de investigación como criptografía, seguridad en redes, seguridad en host, forense digital, malware, el Internet de las cosas, ciudades inteligentes, esteganografía, sistemas detectores de intrusos, aplicación de los algoritmos evolutivos para la ciberseguridad, biometría, entre otros" (Cacelín, 2017).

Es de suma importancia mencionar que, en el Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE), en la Maestría en Ciencias y Tecnologías de Seguridad, el alumno Essau

García, está realizando otra tesis de investigación similar a la que aquí, una de sus propuestas es implementar una asociación civil, dedicada a brindar seguridad cibernética a la ciudadanía poblana. En este sentido, el trabajo de García (2019, inédito) se ha enfocado a explorar el fenómeno de la inseguridad en el ciberespacio desde el punto de vista, psicológico, social y criminológico, para lo cual se ha basado en los aspectos y repercusiones del tipo emocional ocasionados por la cibercriminalidad.

El punto central del citado trabajo sostiene que la manera en como las personas se conducen a través de la red, influye directamente al incremento del nivel de vulnerabilidad desarrollado por las víctimas potenciales del ciberdelito. Sin dejar de lado la importancia de los sistemas de seguridad basados en tecnología, el autor resalta la necesidad de reflexionar sobre el factor humano, pues considera a esta naturaleza en sí misma como una vulnerabilidad aprovechable por los ciberdelincuentes, quienes a menudo hacen uso de técnicas basadas en ingeniería social, además de que los mismos internautas llevan a cabo conductas de riesgo que los hacen aún más vulnerables, aumentando las probabilidades de éxito de ataques cibernéticos de tipo como pishing, fraude y ciberacoso.

Por lo tanto, el trabajo aporta una perspectiva sobre la ciberseguridad que es complementaria a la investigación tecnológica, ya que indaga cuales son los hábitos en el uso de internet, propios de los usuarios de la ciudad de Puebla, dentro del rango de 18 a 34 años de edad, perfil que de acuerdo con la Asociación de Internet.mx (2019), correspondo acerca del 40% de la población activa de internautas en nuestro país. Así pues, dicha investigación proporciona una base que contribuye a justificar el porqué de la necesidad por crear una asociación civil dedicada a brindar ciberseguridad en la entidad, al demostrar que existe una relación entre los hábitos y

conductas del internauta poblano y su nivel de consciencia sobre las ciberamenazas, lo cual muestra una tendencia que podría amplificar de manera considerable la cibervictimización.

2.7.6 Cultura de ciberseguridad

En la tabla 11, se enlistan las instituciones mexicanas que cuentan con los programas en formación y fomento de la ciberseguridad.

Tabla 11. Instituciones mexicanas que tienen programas formativos en cultura de ciberseguridad

Institución	**Programa**
Universidad Veracruzana	Plan de Sensibilización sobre Seguridad de la Información
Universidad de La Laguna	Concientización en Seguridad Informática
Universidad Autónoma de Yucatán	Cultura de Seguridad Informática
Universidad Autónoma de Yucatán	Capacitación en Seguridad Informática (Inducción)
Centro de Investigaciones Biológicas del Noreste	Plan Institucional para el Fortalecimiento de la Ciberseguridad
Universidad Autónoma Metropolitana	Concientización

Nota: Propuesta de líneas de acción del Eje Transversal de Desarrollo de Capacidades (2018). México: Subcomisión de Ciberseguridad-ANUIES.

2.7.7 Coordinación y colaboración

Hay un rubro más que se debe revisar, que es el relativo a la coordinación y colaboración en materia de proyectos, tanto implementados como en curso en materia de ciberseguridad entre instituciones educativas mexicanas (ver tabla 12).

Tabla 12. Instituciones mexicanas que tienen actividades y proyectos de ciberseguridad implementados y en curso (coordinación y colaboración)

Institución	**Programa**
Instituto Politécnico Nacional	CSIRT-CIC
Universidad Autónoma de Yucatán	Sensores de Seguridad
Benemérita Universidad Autónoma de Puebla	Implementación de TLS en sitios web de la universidad

Nota: Propuesta de líneas de acción del Eje Transversal de Desarrollo de Capacidades (2018). México: Subcomisión de Ciberseguridad-ANUIES.

2.8 Impacto de los delitos cibernéticos en México

En 2018, México se ubicó en el cuarto a nivel regional entre los países del continente americano, con una puntuación de 0.629lugar del Global Cybersecurity Index (GCI), mientras que a nivel mundial se encontró en la posición 63 (International Telecommunication Union, 2018), lo cual representa un avance de 5 posiciones respecto a 2014, cuando se encontraba en el noveno lugar. Esta escala considera cinco indicadores que describen la situación de cada país en cuanto a medidas legales, técnicas, organizacionales, de capacitación, y de cooperación en la materia de este estudio.

De acuerdo con la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés), el país demostró que su principal fortaleza eran las capacidades técnicas y su principal

debilidad las orgánicas (NOTIMEX, 2015). Si se toma como base este panorama, resulta comprensible que las cifras reportadas durante los últimos años respecto al robo de información sensible y pérdidas financieras hayan ido incrementando de manera considerable.

2.8.1 Impacto económico

A pesar de los avances evidenciados en cuanto a capacidad técnica, en 2018 se demostró que el Sistema de Pagos Electrónicos Interbancarios (SPEI) del Banco de México, considerado como uno de los más seguros en el mundo recibió un ataque cuya consecuencia fue la pérdida de 400 millones de pesos (Morales, 2018). Desafortunadamente esto demuestra que "México se ha convertido en un objetivo latente para los ataques cibernéticos, sobre todo, ante brechas de seguridad que cada vez son más visibles" (B&MNEWS, 2019).

Y si la cifra aparenta ser importante, resulta ser casi nada en comparación con los 8 000 millones de dólares que se calcula son perdidos a nivel nacional como consecuencia de ataques cibernéticos en términos generales, lo cual aunado a que solo 6% de las Pymes cuentan con una infraestructura que les permita defenderse de ellos (Aetecno, 2019).

El sector empresarial ha tomado muy en serio el impacto económico de los delitos cibernéticos ocurridos en México, por lo que, de acuerdo con Goodman, se calcula que estas destinan alrededor de 600 millones de dólares para detener el cibercrimen, sin embargo, no debe perderse de vista que "mientras que las ciberamenazas crecen exponencialmente, nuestras defensas no" (Rodríguez, 2018).

Sin embargo, se ha logrado emerger algún beneficio a raíz de la situación de nuestro país, este ha sido que se consiguió tener mayor conciencia respecto a la vulnerabilidad de los sistemas, por lo que organismos como la Secretaría de Hacienda, Comisión Nacional Bancaria y de Valores (CNBV), Procuraduría General de la República (PGR), y 11 asociaciones gremiales del sector, se

han unido para la creación del Grupo de Respuesta a Incidentes (GRI), a fin de atender las necesidades del sistema financiero (La otra opinión, 2018).

2.8.2 Impacto social

Se ha hablado sobre el impacto económico en las instituciones financieras, lo cual ha motivado que se tome en serio a la ciberseguridad, sin embargo, es muy importante ver el otro lado del problema y mencionar cual es la situación de los usuarios que pueden ser afectados directa o indirectamente por la ciberdelincuencia, ya sea mediante técnicas de ingeniería social que se hagan pasar por una institución de confianza para robar datos de tarjetas de crédito, a través de correos electrónicos maliciosos, o por medio de ataques directos a los sitios de banca electrónica.

Durante 2018, en México se identificaron alrededor de 4 millones de personas que fueron víctimas de fraude cibernético (Alcocer, 2019). Por supuesto, el impacto no se limita al factor económico, por lo que también es necesario hacer mención de otros tipos de ataques y de la manera cómo influyen en la vida de los ciudadanos. El daño puede calcularse en términos de intimidad, imagen personal, etc.

En abril de 2018, la red social Facebook informó que alrededor de 87 millones de datos personales de sus usuarios fueron comprometidos, debido a que fueron compartidos con la consultora política Cambridge Analytica. De esta cantidad, se destacó que México fue el quinto país más afectado con un total de 789,800 usuarios afectados (Becerril, 2018).

Sin embargo, a menos de un año del incidente, se presentó una nueva exposición de datos de usuarios, esta vez por la plataforma digital Cultura Colectiva, que almacenó en la nube de Amazon 540 millones de datos de usuarios de Facebook, así como números de identificación, comentarios, reacciones y nombres de cuentas (Lara, 2019).

Cabe resaltar que esta información estuvo disponible en descarga directa, de manera que pudo haber sido obtenida por cualquier persona; es decir, que ahora existe la amenaza potencial de que cualquier usuario malintencionado haga uso de dicha información para desplegar distintas campañas de ataques en contra de los afectados. Otros tipos de incidentes que han ocasionado daños considerables en nuestro país han sido los ataques mediante ransomware, ya que México se ubica en segundo lugar a nivel mundial (Reyes, 2018).

Hasta el momento, el ransomware que mayor impacto ha tenido es el de la variedad Wanna Cry, que en 2017 situó a México en el segundo lugar a nivel Latinoamérica con 23.40% del total de detecciones durante 2017 (Kaspersky, 2018). Este tipo de malware no sólo es capaz de cifrar la información, sino que algunas variantes están diseñadas para destruirla, por lo que el impacto en los usuarios puede llegar a ser mayor.

Otra amenaza igual de importante es el criptojacking, que fue la cuarta amenaza más detectada en México durante 2018, pero que a nivel América Latina "ocupó el segundo lugar de registros con el 17.3 % de infecciones" (García, 2018). Un caso interesante fue el de la Secretaría de Educación Pública (SEP), cuyo sitio fue comprometido y cuando los estudiantes hacían uso de este, "el tiempo que tardaba en cargar la información era utilizado para minar criptomonedas" (García, 2018).

Es conducente que, teniendo conocimiento de los delitos informáticos, la sociedad civil en conjunto pueda contribuir a la prevención y combate en contra de éstos, por medio de estrategias específicas y efectivas que den como consecuencia una menor tasa en su comisión, con el objetivo de preservar de una forma más amplia y constantemente actualizada, los derechos de los individuos.

Ahora bien, ya se conocen los delitos informáticos. Es pertinente proyectar la forma en que desde la sociedad civil organizada se pueda coadyuvar en su combate y, mejor aún, en su prevención, lo cual se hará en el tercero y último capítulo.

CAPÍTULO III

CONFORMACIÓN DEL: INSTITUTO PARA EL DESARROLLO Y DIFUSIÓN DE LA CIBERSEGURIDAD A.C

3.1 Características específicas de la A.C.

En este apartado, se especifican situaciones de la Asociación Civil cruciales para concebir el sentido y objetivo de la misma.

3.1.1 Propuesta de Nombre

"Instituto para el Desarrollo y Difusión de la Ciberseguridad A. C."

3.1.2 Propuesta de objeto social

Asociación civil sin fines de lucro, con actividades preponderantes en la **investigación**, prevención, y difusión del modus operandi de los ciberataques más comunes a usuarios, mediante las siguientes acciones:

1. Prestación de servicios de asesoramiento, consultoría, y enlace con las autoridades responsables a nivel nacional, estatal, y municipal.
2. Crear estrategias de divulgación, tales como:
    - Reuniones.
    - Coloquios.
    - Conferencias.
    - Mesas de trabajo.
    - Campañas de mercadotecnia social.

- Campañas de prevención.
- Cursos.
- Talleres.
- Programas de seguridad para usuarios de elementos tecnológicos.
- Otros que se ciñan a la naturaleza de la asociación.

2. Protección de amenazas graves o pandémicas a los sectores más vulnerables, mediante suministro de información crucial.

3. Realizar investigaciones profundas con análisis de datos y monitorear estadísticas que determinen ciberdelitos constantes, innovadores y obsoletos, para que de esta forma se pueda alertar conscientemente a la población, respecto a ellos.

Para lograr dichos fines, será indispensable apoyarse tanto en instituciones educativas como en los tres niveles de gobierno, que posean conocimiento y experiencia en el ramo, con las que se buscará celebrar convenios de colaboración, de tal forma que, de las primeras, los estudiantes puedan liberar su servicio social, así como sus prácticas en esta y de esta forma retroalimentarse y de las segundas, se pueda conseguir cualquier beneficio que coadyuve a llevar a cabo las actividades anteriormente señaladas.

3.1.3 Propuesta de Misión

Promover la generación de conciencia respecto al uso responsable de la Tecnologías de la Información y la Comunicación (TIC), además de establecer un vínculo entre la sociedad, los organismos y el personal profesional interesado en desarrollar programas de prevención y autoprotección en materia de Ciberseguridad.

3.1.4 Propuesta de Visión

Contribuir a la implantación de una cultura en Ciberseguridad, su desarrollo y difusión, a fin de abarcar una amplia extensión del tejido social, para educar y dotar a los usuarios de las TIC de elementos que les permitan hacer frente a las amenazas del Ciberespacio.

3.1.5 Propuesta de Objetivos

General:

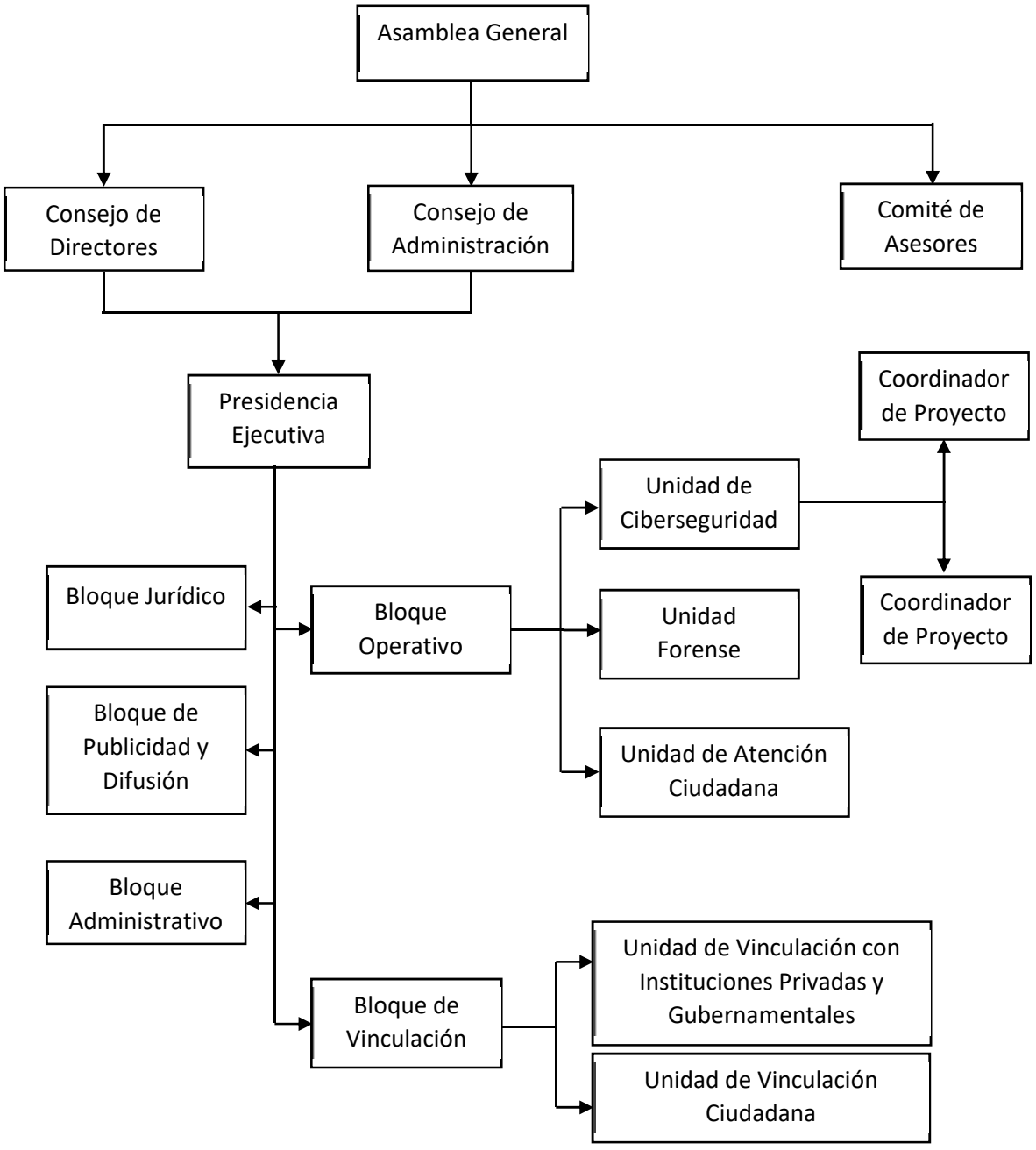
Ser una asociación civil que, respaldada por el derecho, coadyuve en la identificación y análisis de delitos cometidos por medios cibernéticos, en pro de su prevención.

Particulares:

- Brindar instrumentos de carácter didáctico a los ciudadanos con el fin de prepararlos para prevenir ciberataques.
- Promover la protección de los internautas en vinculación con instituciones educativas, del sector público, y la iniciativa privada.
- Brindar atención victimológica a aquellas personas que hayan sufrido algún incidente de Ciberseguridad por medio de las TIC.

3.1.6 Propuesta de organigrama

Figura 1. Organigrama de la Asociación Civil



3.1.7 Descripción de cada bloque

1. Asamblea General. Es el órgano máximo de la Asociación Civil, encargado de la toma de decisiones que persigan el objeto social de la misma y resulten de mayor trascendencia para la propia Asociación Civil.

2. Consejo de Directores. Órgano facultado para ordenar y ejecutar las acciones acordadas en asamblea general con la finalidad de alcanzar los objetivos de la Asociación Civil.

3. Consejo de Administración. Órgano encargado de la supervisión del cumplimiento de la normativa interna, del análisis presupuestario y financiero, así como de la orientación del modelo organizacional de la Asociación Civil que permita el óptimo desarrollo de sus miembros y la propia Asociación.

4. Comité de Asesores. Comité de expertos en el objeto social de la Asociación Civil, integrados para orientar las acciones de los distintos bloques y unidades, con la finalidad de alcanzar objetivos específicos.

5. Presidencia Ejecutiva. Órgano encargado de orientar y supervisar las acciones desarrolladas por los distintos bloques y unidades de la Asociación Civil.

6. Bloque Operativo. Bloque encargado de la atención de los casos y situaciones que requieran la intervención de las unidades especializadas de la Asociación Civil.

6.1 Unidad de Ciberseguridad. Unidad encargada de la investigación y procesamiento de información relacionada con la Ciberseguridad para mantenerla actualizada.

6.1.1 Coordinadores de Proyecto. Responsables del diseño, implementación y evaluación de programas y proyectos específicos para la prevención de delitos cibernéticos.

6.2 Unidad Forense. Unidad de respuesta y atención a incidentes en materia de ciberseguridad, dedicado a recolectar evidencia para el análisis, mitigación de daños, y recuperación de sistemas afectados.

6.3 Unidad de Atención Ciudadana. Unidad encargada de brindar respuesta a las solicitudes de apoyo de la ciudadanía, del seguimiento de los casos y para el asesoramiento legal, tecnológico y psicológico a víctimas de ciberdelitos.

7. Bloque Jurídico. Bloque encargado del control legal de la Asociación Civil, del diseño de contratos y convenios con organismos y entes afines, así como de la implementación de estrategias legales para la asistencia y atención a víctimas de ciberdelitos.

8. Bloque de Vinculación. Bloque encargado de procurar relaciones de colaboración y cooperación con entidades afines, con el objeto de alcanzar los objetivos de la Asociación Civil.

8.1 Unidad de Vinculación con Instituciones Privadas y Gubernamentales. Unidad responsable de establecer relaciones de comunicación y cooperación con instituciones privadas y gubernamentales afines, para la consecución de objetivos comunes.

8.2 Unidad de Vinculación Ciudadana. Unidad responsable de establecer relaciones de comunicación y cooperación con agrupaciones de la sociedad civil afines, para la consecución de objetivos comunes.

9. Bloque de Publicidad y Difusión. Bloque encargado de la comunicación social de la Asociación Civil, su objetivo es difundir información en materia de Ciberseguridad.

10. Bloque Administrativo. Bloque encargado de coordinar los distintos bloques y unidades de la Asociación Civil con el objeto de procurar su operatividad.

3.2 Contenido de capacitación para prueba piloto

Con el objetivo de poner en práctica una de las formas de transmisión de cultura de ciberseguridad en la población con una verdadera aplicación, se llevó a cabo la prueba piloto de una conferencia con el siguiente contenido:

Tema: Curso de introducción a medidas de prevención en ciberseguridad.

Ciberseguridad:

El uso de internet y las tecnologías basadas en este recurso se han generalizado. Prácticamente todos los ciudadanos dependen de algún servicio alojado en la red.

La ciberseguridad es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos (Kaspersky, 2019).

Los usuarios conocen cómo se comportan las aplicaciones y los servicios que utilizan regularmente e intuyen cuando algo va mal. Sin necesidad de ser expertos en seguridad informática, tienen idea del riesgo que representa su comportamiento cuando navegan en internet.

¿Por qué entonces, la cantidad de infecciones por programas maliciosos y el robo de información privada siguen aumentando?

El número de ciberataques aumenta, por lo que se necesita tener una buena gestión de riesgos y no solo preguntarse si uno va a ser atacado, sino cuándo (CSO, 2019).

México es el país con mayor crecimiento en ataques cibernéticos a nivel América Latina (Kaspersky, 2019) y el costo que estos representan asciende a casi 8 mil millones de dólares. Los ataques más comunes tienen que ver con infecciones por Malware y robo de información personal o financiera (tarjetas de crédito) mediante la técnica de "Phishing" (Excelsior, 2019). Entre enero y septiembre de 2018 Profeco recibió alrededor de 1500 quejas por cargos no reconocidos por parte de usuarios de tarjetas de crédito (Blaise, 2019).

Estadísticas y datos duros:

De acuerdo con Google Trends, el interés de los usuarios por la palabra "Ciberseguridad" fue muy elevado el 10 abril de 2019.

El interés de los usuarios por el tema de ciberseguridad, podría estar asociado al tipo de noticias publicadas sobre incidentes relevantes.

Nuevamente el 22 de mayo de 2019 se presentó un índice relativamente elevado de interés por la palabra "Ciberseguridad".

Durante 2018 la Policía Cibernética del Estado atendió 641 denuncias, dentro de las cuales, la ciberextorsión y el ciberfraude fueron los más reportados con una incidencia de 31% y 30% respectivamente.

De acuerdo con INEGI (2019), 10.3 millones de personas experimentaron algún tipo de Ciberacoso durante 2017. Mientras que Puebla se ubicó en el puesto número 7 a nivel nacional, ya que el 19% de su población fue víctima de este delito.

En México, los datos de 789,800 usuarios de Facebook se vieron comprometidos por la operación dirigida por "Cambrigde Analytica" (Becerril, 2018).

Tipos de ciberataques:

- Malware: Abreviatura de "Malicious software", son programas encargados de dañar equipos informáticos y/o extraer información de los usuarios sin su consentimiento.
- Ransomware: "Ransom" significa "Rescate", por lo que es un programa que restringe el acceso a determinados archivos, pidiendo un rescate para liberar esa información
- Troyanos: Programas que al ejecutarlos permiten un acceso remoto al equipo infectado.
- Spyware: Software espía que recopila y transfiere información de un ordenador sin consentimiento de su propietario.
- Pishing: Emails que suplantan identidad de un servicio o compañía, solicitando datos confidenciales del usuario.
- Fraude cibernético: Estafas para realizar transacciones ilícitas en la red.
- Correo basura: O SPAM, son mensajes enviados a varios destinatarios con fines comerciales, invitando al usuario a ingresar a una página o realizar alguna descarga.
- Smishing: Fraude por medio de SMS, con el objetivo de que el usuario ingrese a una página fraudulenta, obteniendo información bancaria.

- Fraude en comercio electrónico: En el servicio de compra venta de productos en línea, la sustracción de datos personales que pueden prestarse al robo de identidad o pagar por tu compra, pero no recibir el artículo a cambio.

Medidas de prevención de ataques cibernéticos:

- Generación de contraseñas robustas

El blog OSI (2018), rescata algunos medios de prevención de ataques cibernéticos, como son: "Evita las contraseñas de menos de 8 caracteres; intercala mayúsculas, minúsculas, números y caracteres especiales; evita las contraseñas fáciles de recordar o de estructura sencilla; no usar conceptos que se relacionen con nosotros; no usar la misma contraseña en varios servicios y cambiarla periódicamente, usar gestores de contraseñas si te cuesta recordar todas".

- Prevención del robo de identidad

El Blog Melimansilla (2017), nos ayuda a contrarrestar el robo de identidad por medio de diferentes consejos, como: "Destruye documentos que ya no utilices; evita compartir tus datos por teléfono o correo electrónico; guarda tus identificaciones y documentos confidenciales; si utilizas redes sociales, fíjate en la información que compartes".

- Protección de datos personales

Según el IFAI (2019), las mejores estrategias utilizar para procurar la protección de datos personales son: "Mantén seguros tus documentos personales en casa y cuando viajes; destruye tus documentos personales cuando hayan dejado de ser necesarios; piensa antes de publicar o compartir información personal; protege tu computadora, smartphone y tablet; ten cuidado cuando

te soliciten información en persona, por internet o teléfono; investiga si recibes tarjetas de crédito, servicios o artículos que no hayas solicitado; mantente alerta ante cualquier transacción bancaria inusual; procura tener siempre a la vista tu tarjeta de crédito o débito".

- Cómo identificar el Phishing

La página Concienciat (2018), nos da consejos para detectar mensajes fraudulentos, como son: "El correo no se está dirigido al usuario por su nombre; la redacción y el lenguaje utilizado son incorrectos; al abrir el enlace solicita ingresar datos personales; el enlace no pertenece al dominio de la compañía solicitante".

- Solicitud de datos bancarios:

Según el blog ADICAE (2014), "Los cibercriminales envían un correo al usuario argumentando que es necesario completar un formulario para actualizar los datos de su tarjeta de crédito, ya que de lo contrario no la podrá usar".

- Medidas para prevenir el Phishing:

La página web El Universo (2018), nos señala diversos consejos para prevenir el pishing, como: "Desconfía de correos con enlaces para introducir tu usuario y contraseña; ante un enlace externo verifica la dirección a la que te ha llevado; hackers pueden utilizar cuentas oficiales para el envío; no envíes tus claves o datos personales por correo; desconfía de correos que tienen faltas de ortografía; nunca respondas a correos que te piden datos confidenciales; si dudas, no hagas clic en el enlace de tu correo, teclea la dirección en tu navegador; ante la mínima duda se prudente y no te arriesgues".

- Medidas para prevenir la infección por Ransomware (Ciberextorsión):

OnBranding (2019) nos señala 8 medidas para prevenir la ciberextorsión o ransomware:

"Mantener copias de seguridad de todos los datos importantes; mantener el sistema operativo actualizado con los últimos parches de seguridad; usar un antivirus con la base de datos de firmas actualizadas; disponer de sistemas antispam a nivel de correo electrónico; no utilizar cuentas con privilegios de administrador; empleo de bloqueadores de Javascript para el navegador; configurar el sistema operativo para que sean visibles las extensiones para tipos de fichero conocidos; y trabajar a través de una máquina virtual evitará en un alto porcentaje la infección anti-debug".

- Medidas para prevenir el Ciberacoso:

Según información de La Vanguardia (2018), las mejores estrategias para prevenir el acoso son: "Mantener los perfiles de las redes sociales en modo privado; utilizar contraseñas con un alto nivel de seguridad; utilizar la función de bloqueo ante usuarios que intenten hostigarle; asegurarse de tener un buen antivirus y cortafuegos; tener precaución al compartir información personal en Internet; no responder a provocaciones de un posible acosador y guardar todo lo que se considere una posible prueba de ciberacoso".

3.2.1 Prueba piloto de la capacitación denominada "Medidas básicas de ciberseguridad"

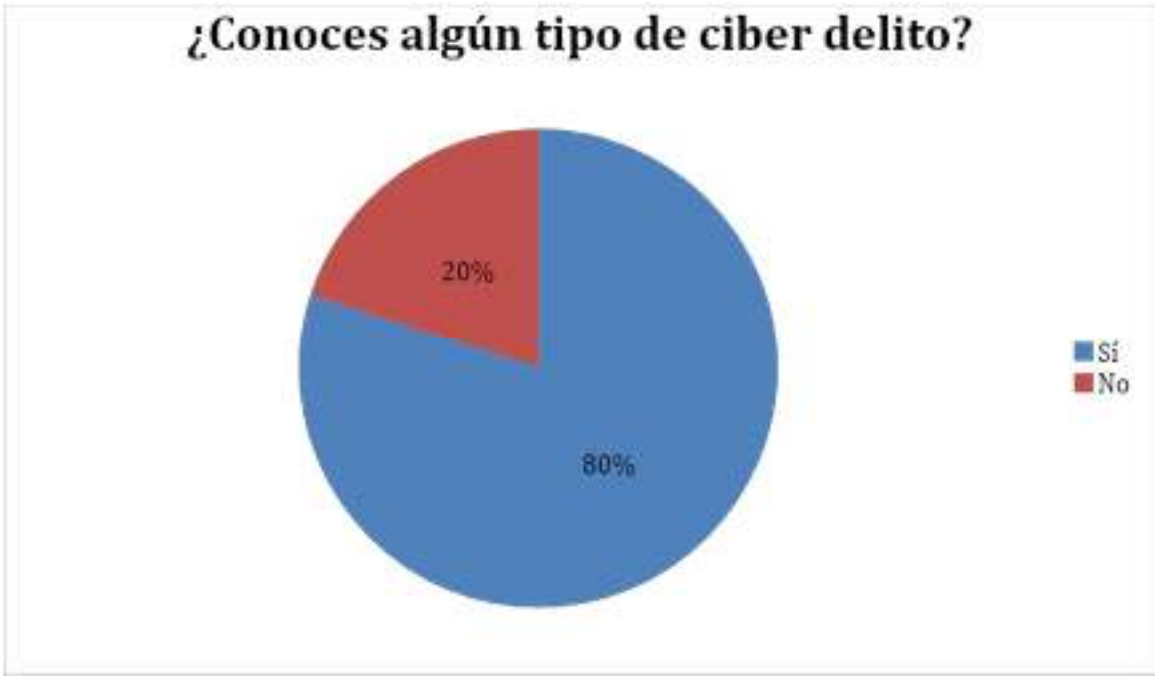
La prueba piloto que aquí nos concierne se llevó a cabo el día 26 de junio de 2019 en las instalaciones de la Benemérita Universidad Autónoma del Estado de Puebla (BUAP), en la cual, el autor del presente trabajo tuvo el honor de ser expositor de la capacitación denominada "Medidas básicas de ciberseguridad".

3.2.2 Encuesta diagnóstico y post conferencia

Dentro de la aplicación de la prueba piloto, y con el fin de recolectar datos acerca de la eficacia del ejercicio de la misma, se realizaron encuestas con preguntas de diagnóstico, para conocer cuál es la información y experiencias con las que la gente cuenta en materia de ciberseguridad. Posteriormente, al finalizar la capacitación, se aplicó una encuesta de salida, en la cual, se realizaron preguntas tendientes a evaluar la efectividad de la prueba piloto acerca de los tipos de ciberataques y procurando la reflexión de los asistentes sobre la ciberseguridad en su vida diaria.

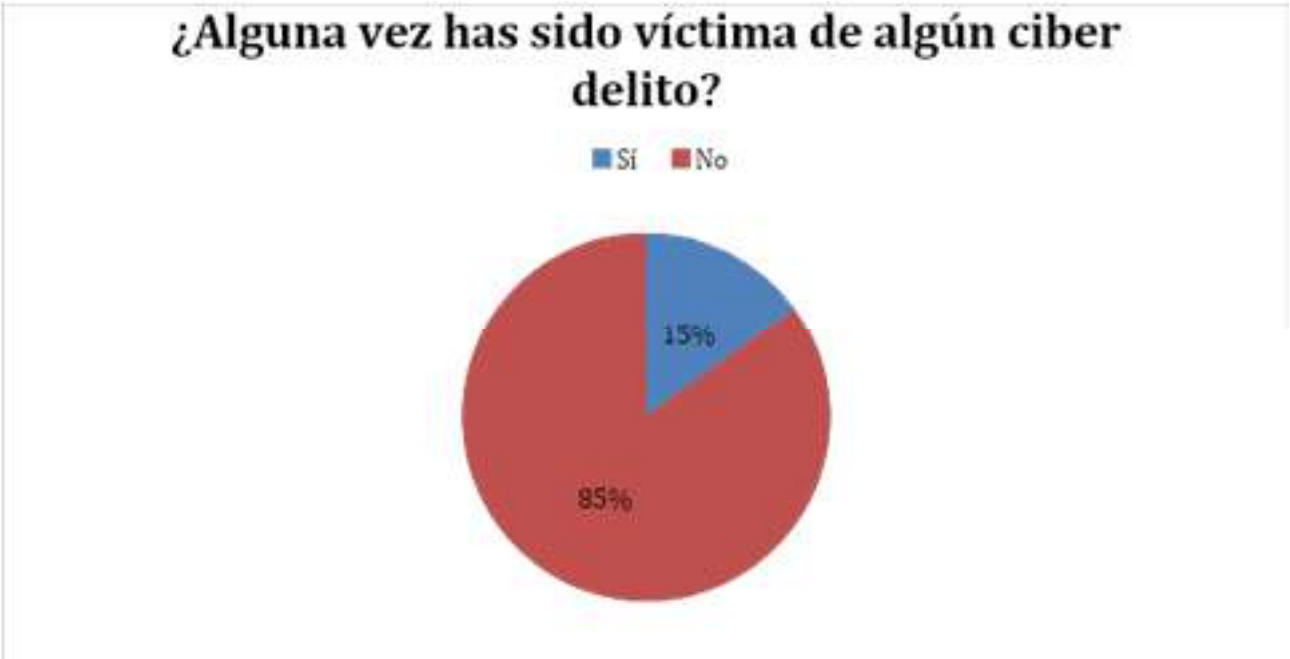
De una muestra de personas, se obtuvieron los siguientes resultados:

Figura 2. Conocimiento de tipificación de ciberdelitos



De la gráfica se desprende que el 80% de los encuestados tiene conocimiento acerca de la existencia de delitos cometidos por medio de Tecnologías de la Información y la Comunicación (TIC).

Figura 3. Cantidad de víctimas de ciberdelitos

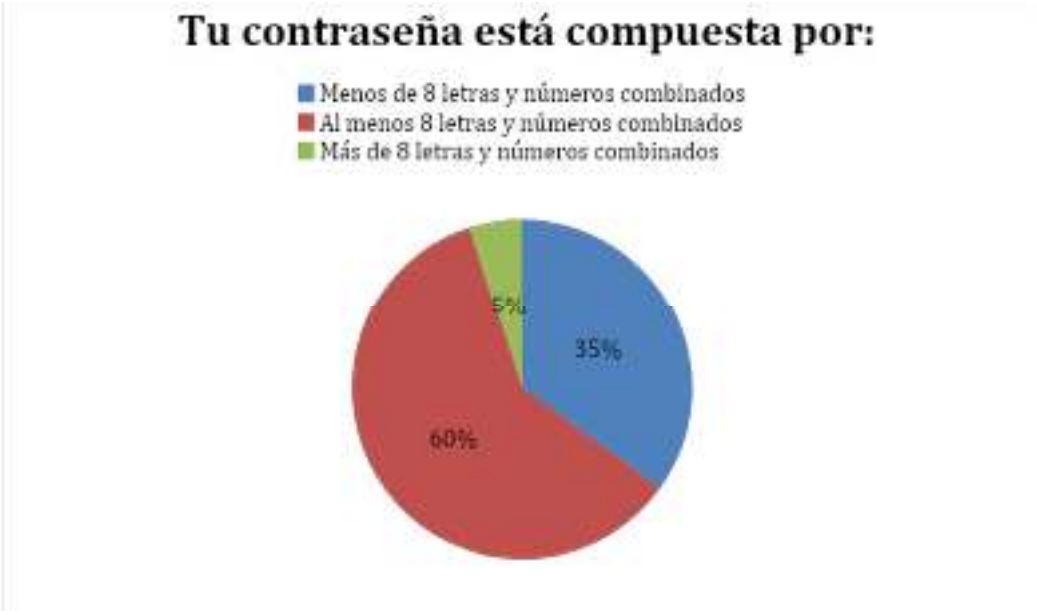


A partir de la Figura 2 y con relación a la Figura 3, se concluye que los encuestados no sólo tienen el conocimiento teórico de la existencia de ciber delitos, sino que incluso han sido víctimas de alguno.

Figura 4. Denuncias presentadas por víctimas de ciberdelitos

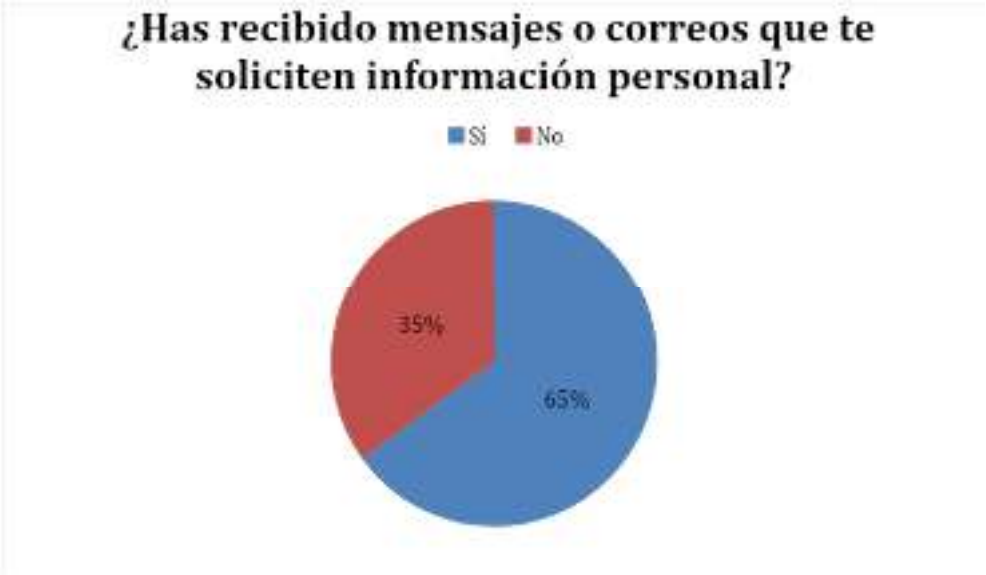
De la cantidad total de personas que han sido víctimas de ciberdelitos, ninguna ha denunciado el hecho.

Figura 5. Estructura alfanumérica de contraseñas



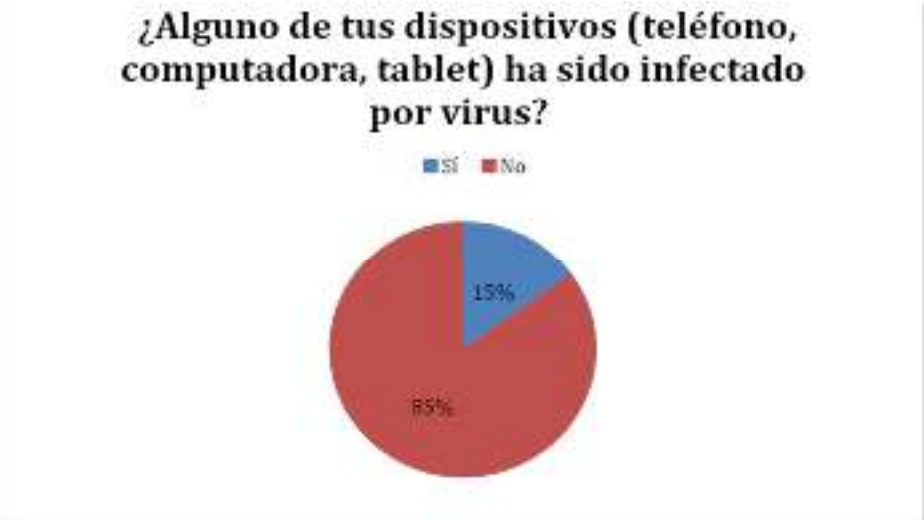
De los resultados contenidos en la Figura 5, se advierte que sólo el 5% de los encuestados ejercita la ciberseguridad en lo concerniente a sus contraseñas.

Figura 6. Mensajes recibidos solicitando información personal



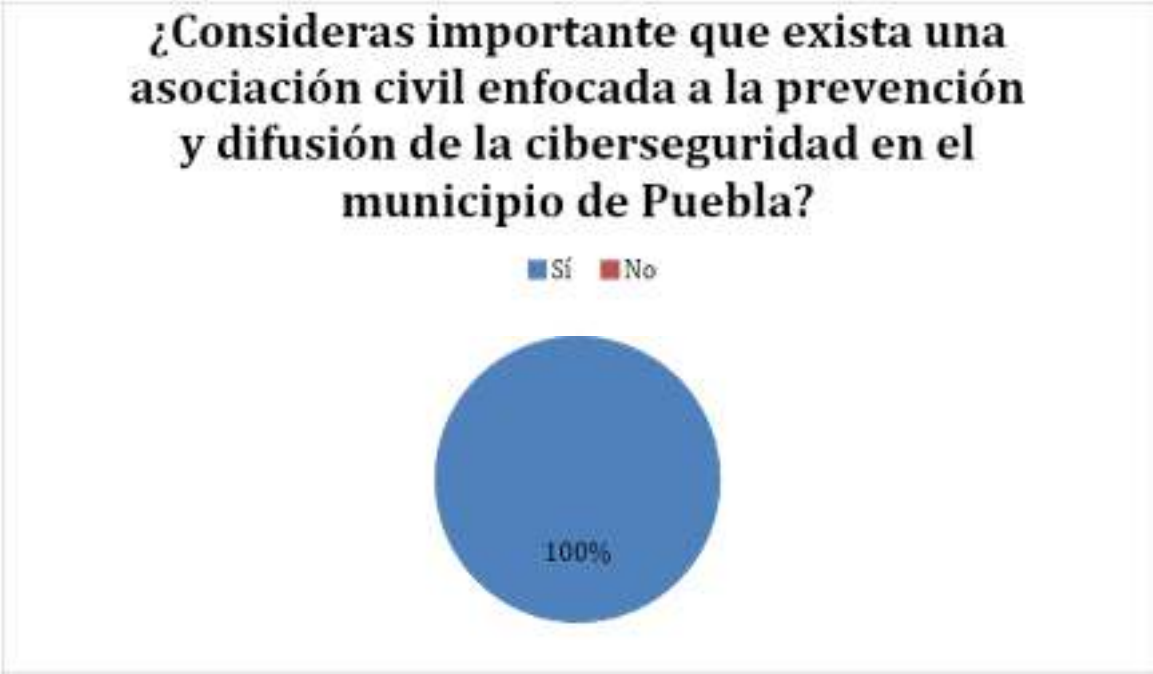
El 65% de los encuestados ha estado expuesto al robo de información personal al recibir algún mensaje o correo electrónico solicitándolo.

Figura 7. Infección de dispositivos electrónicos por virus



Como se observa en la gráfica, los dispositivos electrónicos del 85% de los encuestados ha sido infectado por algún virus.

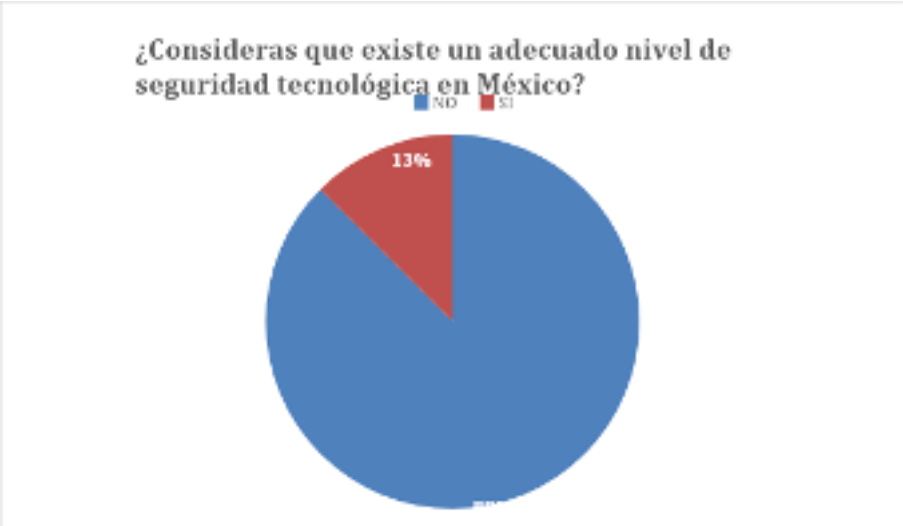
Figura 8. Importancia de existencia de Asociación civil enfocada a la prevención y difusión de la ciberseguridad en el municipio de Puebla



Es de destacar que, a raíz de las experiencias de los asistentes, el conocimiento adquirido y las reflexiones propiciadas, el 100% de los asistentes considera realmente importante la existencia de una Asociación Civil enfocada a la prevención y difusión de la ciberseguridad en el municipio de Puebla.

PREGUNTAS POSTERIORES A LA CONFERENCIA PILOTO

Figura 9. Percepción del nivel de seguridad tecnológica en México



De la Figura 9 se observa que el 87% de los encuestados considera que existe un nivel adecuado de seguridad tecnológica en México, contrastando con el 13% que considera que no es así.

Figura 10. Importancia de una Asociación Civil para la prevención de Ciberdelitos y difusión de temas relacionados con la Ciberseguridad para el Municipio de Puebla

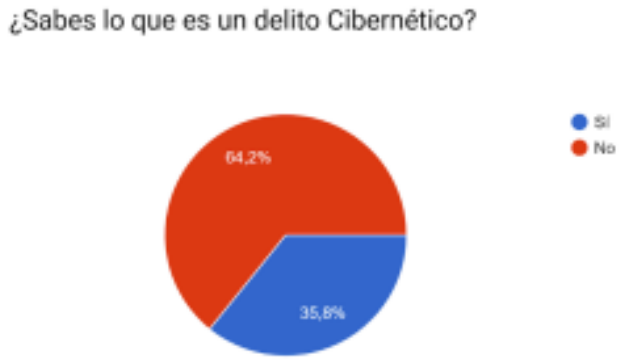
El 100% de los encuestados consideró importante la existencia de una Asociación Civil que difunda información de temas relacionados con la ciberseguridad y que a su vez coadyuve en la prevención de delitos cibernéticos.

Figura 11. Impacto de información en materia de Ciberseguridad

El 75% de los encuestados consideró que posterior al curso impartido incrementaron sus conocimientos en materia de Ciberseguridad, la información compartida puede traducirse en un esquema de prevención de ciberdelitos al contar con los conocimientos técnicos para prevenirlos.

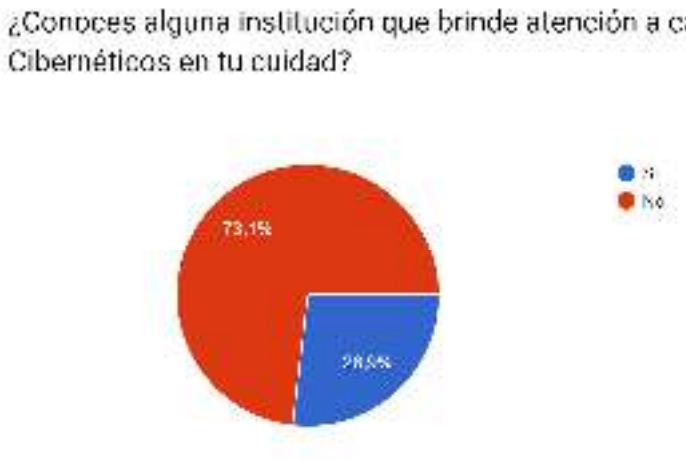
Aunado a las respuestas anteriores, se llevó a cabo una encuesta de manera general a una muestra de 100 personas con características coincidentes en edad, nivel educativo y área de formación profesional, con el objetivo de conocer más a fondo el conocimiento y experiencias de la ciudadanía con relación a los delitos cibernéticos, de la cual se desprenden los siguientes resultados:

Figura 12. Conocimiento de delito cibernético



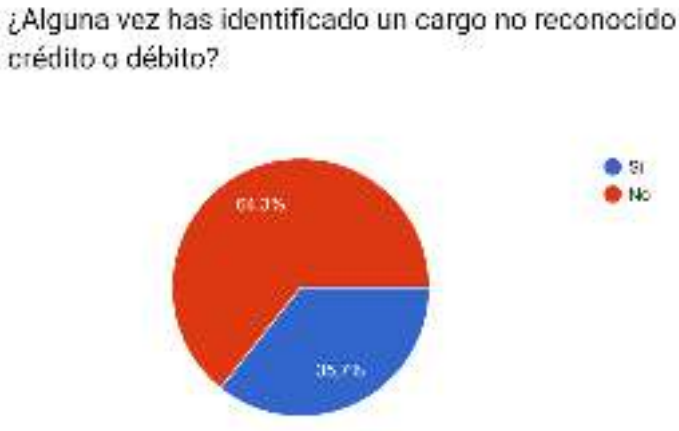
En contraste con los resultados de la Prueba Piloto en la que los encuestados están estudiando alguna carrera profesional con las Tecnologías de la Información, sólo el 35.8% de los encuestados tiene conocimiento del concepto de "delito cibernético", denotando así la falta de cultura cibernética y la necesidad de informar a la ciudadanía acerca de cuestiones básicas sobre seguridad en esta materia.

Figura 13. Instituciones de atención a delitos cibernéticos



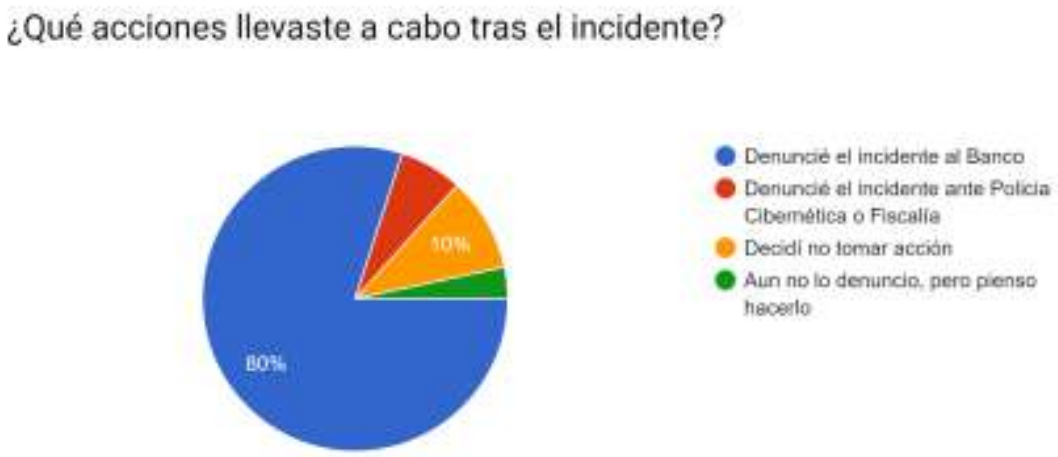
Si bien es cierto que acorde a la gráfica la mayoría de los encuestados (73.1%), no conocen institución alguna que brinde atención a las víctimas de delitos cibernéticos, también lo es que no existen muchas instituciones que lo hagan, dando por consecuencia un desconocimiento en razón de inexistencia.

Figura 14. Cargos no reconocidos en tarjetas de crédito o débito



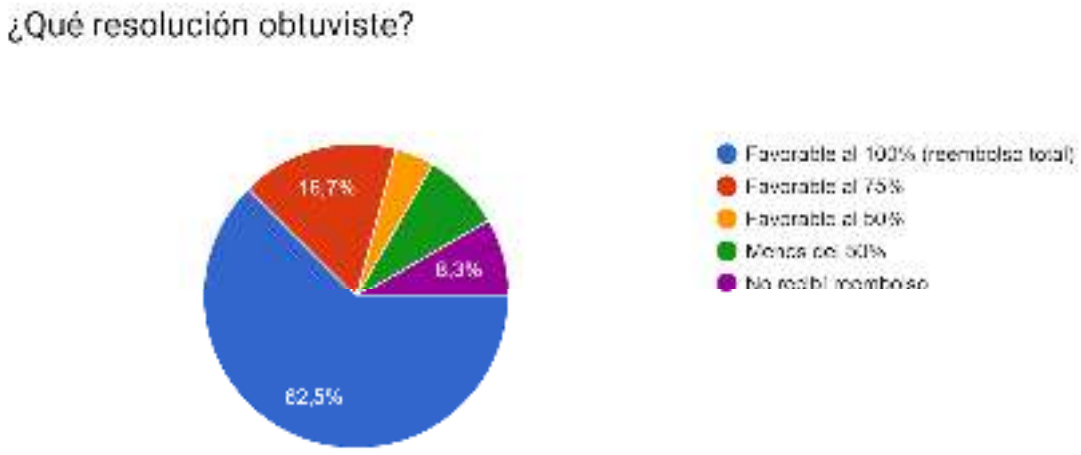
A pesar de no conocer el concepto de delito cibernético por parte de la mayoría de los encuestados, el 64.3% del total ha sufrido alguno.

Figura 15. Acciones tomadas tras incidente delictivo



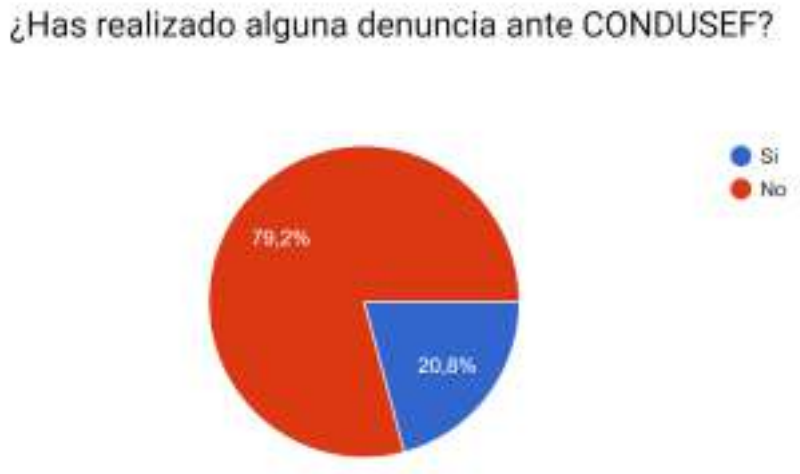
De las personas que han sufrido algún cargo no reconocido en sus tarjetas bancarias, el 80% denunció el incidente con el banco, mientras que el 10% decidió no tomar acción alguna frente al hecho.

Figura 16. Porcentaje favorable respecto a las reclamaciones por cargos no reconocidos



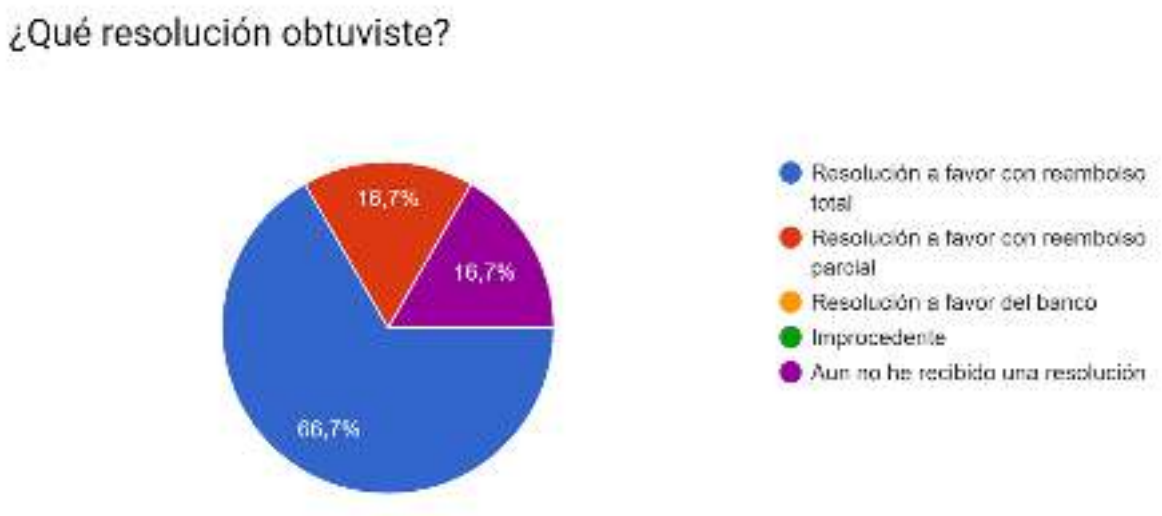
El 62.5 % de los encuestados refirió que han recibido un reembolso total por “cargos no reconocidos” que contrasta con el 8.3 % que refirió que no recibió ningún rembolso.

Figura 17. Porcentaje de denuncias presentadas por usuarios de servicios financieros ante la CONDUSEF



De los encuestados el 79.2 % afirmó haber presentado alguna denuncia ante la Comisión Nacional para las Defensa y Protección de Usuarios de los Servicios Financieros lo que refiere que existe conocimiento de las funciones que ejerce este organismo.

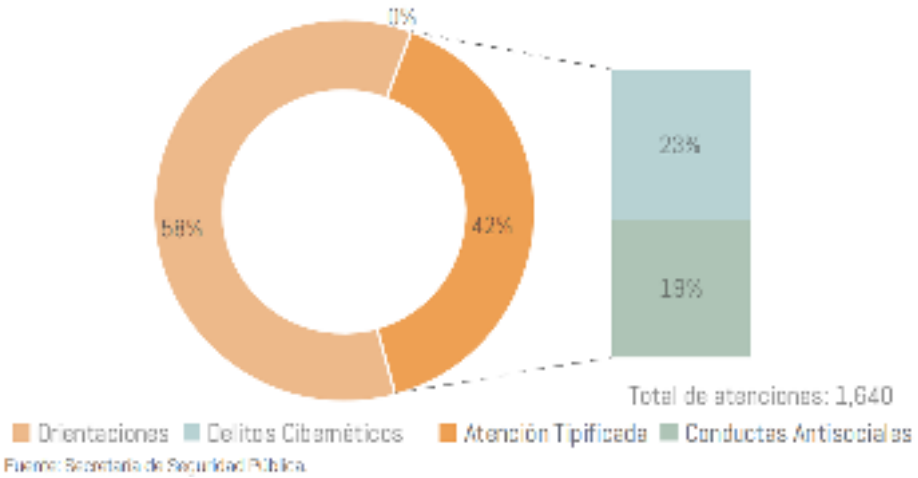
Figura 18. Porcentaje de personas que fueron favorecidas con el resolutivo emitido por la CONDUSEF



Un 66.7% de los encuestados afirmó que el resolutivo emitido por la CONDUSEF resultó favorable al ordenar el reembolso total de las operaciones no reconocidas por los usuarios de servicios financieros, porcentaje que aumenta al sumar el 16.7 % al que el resolutivo los favorecía de forma parcial con el reembolso de las referidas operaciones.

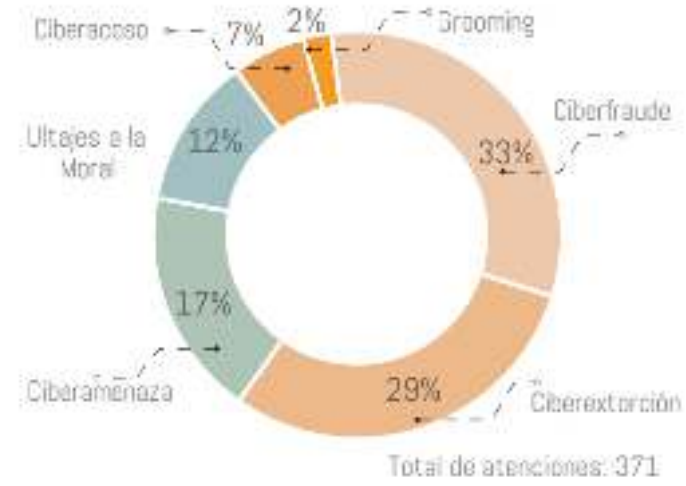
Asimismo en el informe de gestión presentado por el Gobernador del Estado en el Julio de 2019 y que comprende el periodo de Enero a Junio del mismo año, la Secretaría de Seguridad Pública del Estado proporcionó datos estadísticos entre los que destacan 4 aspectos que van desde el diagnóstico hasta las acciones emprendidas en la materia, el primer rubro destaca un incremento del 34% respecto del año 2018 en las atenciones de la Policía Cibernética con respecto a las conductas probablemente constitutivas de delitos, resaltando que en el periodo que comprende de Enero a Junio de 2019, el número de atenciones brindadas por la policía cibernética fue de 1640 casos.

Figura 19. Porcentaje de atención por tipo, 2019



El segundo aspecto del informe de Gestión posiciona como delito de mayor incidencia al ciberfraude con un 33%, seguido de un 29% a la ciberextorsión y en una tercera posición a la ciberamenaza, tal como se muestra en la figura 20.

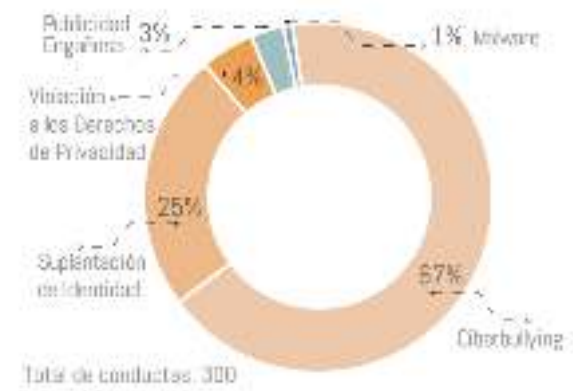
Figura 20. Delitos cibernéticos por tipo, 2019



Fuente: Secretaría de Seguridad Pública.

El tercer aspecto que se aborda en el informe menciona que a través de los medios informáticos se han registrado conductas antisociales que afectan a la ciudadanía, posicionando como primer lugar al *Ciberbullying* con un 67%, seguido de un 25% por la *suplantación de identidad,* estos datos ponen de manifiesto el incremento de conductas que llegan a afectar el tejido social.

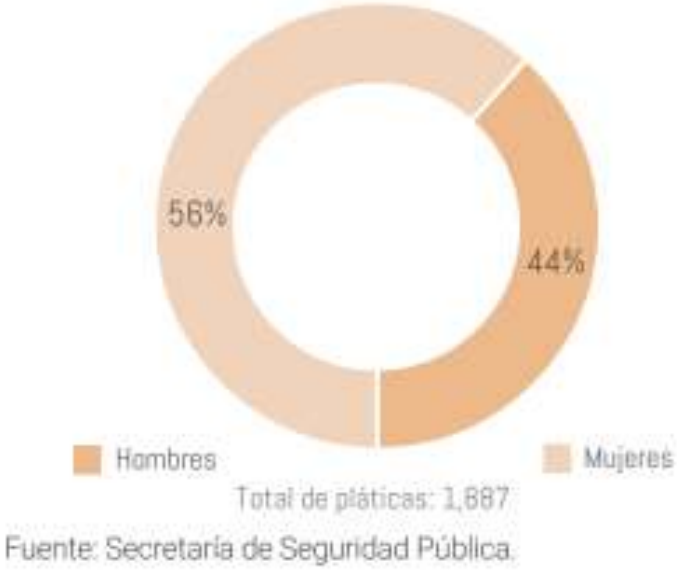
Figura 21. Conductas antisociales por tipo, 2019



Fuente: Secretaría de Seguridad Pública

El cuarto rubro refiere que se implementaron acciones para combatir las conductas delictivas y antisociales detectadas en los medios informáticos, estas acciones consistieron en cinco ciclos de pláticas que se integraron de 45 ponencias, logrando llegar a más de 2000 personas de diferentes medios sociales como padres de familia, estudiantes, docentes y empresarios, sumando un total de 1,887 pláticas.

Figura 22. Personas beneficiadas con las acciones contra los ciberdelitos y conductas antisociales.



Los datos presentados en el informe de Gestión en el presente año (2019), pueden ser comparados con los registrados en 2018 en el que se atendieron 1, 163 casos de denuncias de conductas delictivas por medios cibernéticos y que en 2017 fueron atendidos 803 casos, de lo información analizada es posible observar un incremento en la incidencia de conductas delictivas y antisociales por medios cibernéticos (Informe Estatal de Evaluación, FASP, Estado de Puebla, 2018).

3.3 Acciones concretas de la Asociación

Si bien es cierto que la labor consistente en la persecución del delito le corresponde a la autoridad por medio de un organismo autónomo denominado “Fiscalía”, también lo es que, como ciudadanía, concretamente a través de agrupaciones con determinados fines, podemos contribuir en diferentes

rubros del bien común. De acuerdo al objetivo que nos concierne, planteamos concretamente las acciones siguientes, las cuales han quedado enunciadas en el objeto social:

1.- Investigación, prevención y difusión de modus operandi de ciberataques

Siendo ésta la labor general de la Asociación Civil, y desde la cual emanan todas las demás acciones a realizar.

Si partimos del hecho de que las Tecnologías de la Información y Comunicación (TIC) no son estáticas, sino que están en constante evolución, consecuentemente lo hacen las conductas delictivas realizadas por medio de estos instrumentos, por lo que hace necesaria la labor de investigación constante de las estrategias usadas por los sujetos activos del delito, y de este modo mantener en actualización continua a la Asociación Civil, para que así, pueda ser efectiva frente al panorama social. Esta labor sería realizada por el equipo denominado: Unidad de Ciberseguridad, que ha quedado precisado en el organigrama.

Partiendo de la premisa de que la Asociación está constantemente actualizada respecto a todo lo concerniente a la comisión de "ciberdelitos", es conducente que pueda diseñar estrategias de prevención efectivas aptas para que la ciudadanía pueda aplicarlas de forma sencilla; función que realizarían los Coordinadores de proyecto.

Teniendo ya los elementos necesarios para poder brindar apoyo a la ciudadanía en general, es necesario difundir todo el trabajo realizado para su aplicación a la vida cotidiana de los usuarios de Tecnologías de la Información y Comunicación (TIC). Labor que sería realizada por los siguientes órganos en diferentes medidas:

- Unidad de Atención Ciudadana.
- Bloque de Vinculación.
- Unidad de Vinculación con Instituciones Privadas y Gubernamentales.
- Unidad de Vinculación Ciudadana.
- Bloque de Publicidad y Difusión.

2.- Asesoramiento

Como parte del apoyo directo a la ciudadanía, se tendrá un contacto personal con aquellas personas que tengan un particular interés en el tema, sea con motivo de prevención o en calidad de víctimas de algún "ciberdelito", y de este modo, se le pueda brindar:

a. Asesoría legal, de tal forma que el ciudadano pueda contar con el apoyo jurídico de abogados para que le den seguimiento a su caso o a sus dudas, y acompañarlo durante el procedimiento penal a cargo de la Fiscalía.

b. Asesoría tecnológica a cargo de especialistas en el área, para que, de este modo, en un futuro existan menos probabilidades de que el asesorado pueda ser víctima de esta clase de delitos.

c. Acompañamiento psicológico, ya que es evidente que el daño provocado por un delito no es sólo material, sino también interno para la víctima, por lo que se procurará que exista la menor afectación en este sentido.

De todo esto, la Unidad de Atención Ciudadana estará a cargo.

3.- **Enlace gubernamental y con asociaciones e instituciones educativas**

El alcance y eficiencia del proyecto de la Asociación se dará en gran parte por las formas de llegar a la ciudadanía, y del conocimiento y confianza que ésta tenga del propio proyecto, por lo que está estipulado que existan convenios de colaboración con diferentes organizaciones e instituciones, para que de este modo no se quede en una labor aislada, sino en conjunto; además de tener vínculos y espacios de colaboración con los entes gubernamentales en sus tres órdenes: federal, estatal y municipal, y de este modo, poder realizar un trabajo complementario y que realmente aporte integralmente al fin buscado.

Se propone que, al ser una Asociación Civil, es decir sin fines de lucro, los alumnos de instituciones educativas que decidan formar parte puedan liberar el servicio social y prácticas profesionales que les correspondan, además de un apartado para voluntarios.

De estas cuestiones estarán comisionadas los siguientes órganos:

- Bloque de Vinculación.
- Unidad de Vinculación con Instituciones Privadas y Gubernamentales.
- Unidad de Vinculación Ciudadana.
- Bloque Jurídico.

4.- Estrategias de divulgación

Una de las labores fundamentales de la Asociación es la promoción de estrategias para prevenir los “ciberdelitos”, además de divulgación de información relevante en el tema para que la ciudadanía tenga un conocimiento más amplio y pueda dejar de ser vulnerable frente a estos

posibles ataques; por esto es que constantemente se realizarán labores en materia de propagación, por medio de: Reuniones, coloquios, conferencias, mesas de trabajo, Campañas de mercadotecnia social, campañas de prevención, cursos, talleres, y programas de seguridad para usuarios de elementos tecnológicos. Todo esto en conjunto con los enlaces gubernamentales y con otras organizaciones e instituciones educativas con los que haya generado vínculos de colaboración.

Esto será posible gracias a la función de los siguientes órganos: Bloque de Publicidad y Difusión, Bloque de Vinculación.

5.- Suministro de información crucial

Dentro de este ámbito, es de explorado conocimiento el alcance de publicaciones en sitios web, por lo que, aprovechando el contexto y la capacidad propia de algún elemento publicado en internet, el Bloque de Publicidad y Difusión tendrá, dentro de sus funciones, la de publicar contenido informativo que resulte útil para los usuarios en materia de protección frente a las ciberamenazas.

6.- Monitorear estadísticas ciberdelitos constantes, innovadores y obsoletos (Investigación y análisis de datos)

Para lograr una mejor estrategia de prevención y combate a los ciberdelitos, es fundamental conocer la incidencia de cada uno de éstos, así como los medios de Tecnologías de la Información y Comunicación (TIC) tanto mayor como menormente usados para la comisión de los mismos. A partir de los incidentes delictivos que se presenten, se dará un seguimiento a éstos, recolectando toda la información concerniente a su forma de comisión, para su posterior análisis y monitoreo de conducta.

Por lo que la Unidad de Ciberseguridad y la Unidad Forense tendrán, dentro de sus facultades, la investigación de los mismos.

3.3.2 Resultados esperados

De acuerdo con la formalidad del proyecto y a la metodología llevada en el mismo, es fundamental establecer con claridad aquello que se pretende obtener a partir de las acciones concretas llevadas a cabo, por lo que a continuación se explican los resultados esperados.

-Implantación, desarrollo y difusión de cultura de ciberseguridad.

En razón del escaso conocimiento social acerca de ese tema, además de la constante evolución del mismo, resulta relativamente sencillo la tarea de cometer delitos por medio de Tecnologías de la Información y Comunicación (TIC), por lo que es fundamental, en primer lugar, informar a la ciudadanía acerca de los ciberdelitos y la ciberseguridad, por lo que dentro de los resultados esperados, estará la implantación de una cultura de ciberseguridad, para que de este modo, se tenga una noción y un conocimiento esencial del tema, que progresivamente la asociación irá desarrollando y actualizando por medio de sus diferentes estrategias, y así se conforme una verdadera sociedad consciente.

-Uso responsable de TIC

Como parte de una cultura de ciberseguridad, se pretende como resultado de la labor de la asociación, que los ciudadanos logren usar responsablemente las Tecnologías de la Información y Comunicación (TIC), no sólo en un rubro teórico, sino realmente aplicado a su día a día en un sentido técnico.

-Elementos contra amenazas cibernéticas

No obstante conocer del tema, es indispensable que se cuenten con los elementos necesarios para que las personas no se encuentren en estado de indefensión frente a las amenazas cibernéticas, por lo que, como resultado del trabajo, la ciudadanía contará con los medios necesarios para prevenir los ciberataques que intenten perpetrar contra ellos, además del conocimiento necesario para poder adquirir y utilizar esos elementos.

-Confiabilidad en la Asociación como acompañante

Otro de los resultados esperados, es que la ciudadanía pueda contar con la asociación como un medio efectivo de apoyo frente a la situación sufrida, es decir, será efectiva en la medida en que existan personas a las cuales se les esté acompañando; siendo que, sería la comprobación de que realmente existe confianza por parte de la gente en el apoyo brindado por la asociación.

-Información efectiva y actualizada

Resultado de la constante labor de cada una de las áreas en la recopilación, análisis y procesamiento de información, será proporcionar a la ciudadanía los últimos avances en temas de ciberseguridad, y de este modo, exista una prevención funcional frente a la evolución constante de las estrategias utilizadas por personas que cometen conductas delictivas por medio de Tecnologías de Información y Comunicación (TIC).

-Detrimento en índice delictivo en materia de ciberdelitos

3.4 Generación de recursos para autosustentabilidad

En México, resulta evidente que la mayoría de las Asociaciones Civiles sostienen su actividad a través de tres fuentes de financiamiento principales; la primera: la inversión privada o filantrópica, la segunda: la inversión pública y la tercera: de los ingresos autogenerados por los bienes o servicios ofrecidos por las propias asociaciones, siendo la primera la más importante aunque a su vez la más limitada, por lo que al largo plazo genera insuficiencia y limitaciones en la operación de las Asociaciones Civiles.

Si bien es cierto que el aspecto financiero juega un papel fundamental en la operatividad de toda asociación civil, no lo es todo, también resulta de suma importancia el capital humano que contribuye en su funcionamiento, por lo tanto, los personas que desempeñan alguna labor al interior de una organización de la sociedad civil se convierten en un recurso vital para alcanzar los resultados que persigue la asociación civil.

El presente apartado se plantean las estrategias del tipo financiero y humano que permitirán a la Asociación Civil plena y continua operatividad, a fin de garantizar el objeto principal de su función: prevenir los delitos en materia de Ciberseguridad.

1. **Estrategia de sostenibilidad en su aspecto humano**

Son diversos los factores que permiten el buen funcionamiento de una organización social, entre los que destacan el financiero, el legal y el organizacional, aunque resulta de mayor trascendencia el humano, pues este resulta fundamental para su buen funcionamiento y para la consecución de sus objetivos.

El alcance e impacto de las acciones que emprende la sociedad civil organizada dependerá del nivel de organización que esta tenga, pues serán sus miembros quienes fungirán como ejecutores de las acciones. La forma en que lo hagan determinará los resultados y la mejora en la calidad de vida de la sociedad.

Lo anterior no podrá ser posible si no se cuenta con el capital principal: las personas, por ello la Asociación Civil que plantea esta investigación se sujetará al siguiente esquema de factor humano que permitirá su sostenibilidad.

Además de contar con sus miembros fundadores en los cargos o puestos que se determinen en Asamblea General conforme al organigrama establecido, se plantea un esquema de factor humano que promueva el desarrollo de sus demás miembros, así como la inserción de más personas dedicadas a la materia objeto social de la Asociación Civil: la Ciberseguridad.

Ahora bien, el primer aspecto de sostenibilidad del factor humano consiste en el desarrollo de los miembros, así como de la captación de personas afines al objeto social de la asociación civil desde estudiantes, docentes y expertos en la materia que coadyuven a la operatividad de la asociación.

Tabla 13. Esquema de sostenibilidad de factor humano

TIPO	ESQUEMA	PERIODOS	DURACIÓN
SERVICIO SOCIAL	Investigación	2	
	Programas de capacitación	Enero-junio	6 meses

		Junio-diciembre	
PRÁCTICA PROFESIONAL	Unidades o Bloques	4	
	Investigación	Enero-marzo	3 meses
	Programas de Capacitación	Abril-junio Julio-septiembre Octubre-diciembre	
VOLUNTARIADO	Investigación Programas de Capacitación	Permanente	Indefinido

El esquema de sostenibilidad que se plantea para la asociación permitirá un flujo de capital humano permanente, lo que resultará en el esfuerzo constante para la consecución de los objetivos.

Este esquema consiste en la inserción de personas con interés en el objeto social que persigue la asociación, procurando en su primera fase el vínculo con universidades públicas y privadas para el ingreso de estudiantes de licenciaturas afines y que se encuentren en etapa de realizar servicio social para diseñar, desarrollar e innovar en las estrategias planteadas por la asociación para incidir en la prevención de delitos cibernéticos y aporten a la materia de Ciberseguridad.

La segunda fase consistirá en vincular a los estudiantes de áreas especializadas en materia de ciberseguridad de las universidades públicas y privadas para que a través del desarrollo de su

práctica profesional aporten conocimientos innovadores en materia de Ciberseguridad y permitan alcanzar objetivos específicos.

La tercera etapa contempla un vínculo permanente con personas afines a la materia de Ciberseguridad y que deseen aportar a la consecución de los objetivos de la asociación de forma voluntaria.

2. Estrategia de sostenibilidad en su aspecto económico

La capacidad de acción y de impacto de las organizaciones de la sociedad civil suele ser determinada por su capacidad financiera, lo anterior resulta de gran trascendencia ya que la fuente principal de sus ingresos es representada por los donativos de particulares que suelen ser importantes, pero al largo plazo insuficientes.

Si bien es cierto que las asociaciones civiles no persiguen un ánimo de lucro, los mismos necesitan de recursos económicos para su funcionamiento, por lo que resulta necesario el diseño de un esquema presupuestario que le permita plena y continua operatividad.

El diseño de una estrategia de sostenibilidad económica deberá observar lo dispuesto en la ley vigente, los objetivos que se persiguen y el tiempo en que desean ser alcanzados, esta estrategia consistirá en diversificar los mecanismos para lo obtención de recursos y podrán ser recursos privados, públicos y autogenerados para la obtención de resultados.

Tabla 14. Financiamiento

TIPO DE FINANCIAMIENTO	DESCRIPCIÓN	BENEFICIOS

PRIVADO	Inversión privada.	Comprobantes deducibles de impuestos a inversionistas privados.
PÚBLICO	Convocatorias públicas para financiamiento de proyectos específicos.	Proyectos alineados a objetivos conjuntos.
PROPIO	Servicios de consultoría y capacitación a particulares.	Fomento a la cultura de prevención de delitos en materia de ciberseguridad.

La primera parte consistirá en obtener conforme a las leyes vigentes la denominación de "donataria autorizada" con el objetivo de hacer atractiva la inversión del sector filantrópico (privado), esta denominación permite a la asociación emitir comprobantes fiscales deducibles de impuestos a los inversionistas privados, es de destacar que este tipo de recursos son más flexibles en cuanto su destino y uso a diferencia de los recursos públicos, por lo que los recursos privados sustentaran los gastos operativos, de personal y de administración de la asociación, también podrán impulsar o financiera proyectos específicos.

Ahora bien, la segunda etapa consistirá en alinear los proyectos conforme a lo dispuesto por la norma mexicana vigente, misma que plantea un esquema de fomento a las actividades realizadas por las Organizaciones de la Sociedad Civil, la referida ley fomenta, apoya y promueve a este sector para el cumplimiento de sus objetivos, la Ley Federal de Fomento a las Actividades realizadas por la Organizaciones de la Sociedad Civil (9 de febrero de 2004) dispone en su artículo tercero que las Organizaciones de la Sociedad Civil *"Podrán acogerse y disfrutar de los apoyos y*

estímulos que establece esta ley, todas las agrupaciones u organizaciones mexicanas que, estando legalmente constituidas, realicen alguna o algunas de las actividades a que se refiere el artículo 5 de la presente ley y no persigan fines de lucro ni de proselitismo partidista, político-electoral o religioso, sin menoscabo de las obligaciones señaladas en otras disposiciones legales".

La Ley Federal de Fomento a las Actividades realizadas por la Organizaciones de la Sociedad Civil en coordinación con la ley del Impuesto sobre la renta, plantean un esquema de financiamiento público para proyectos específicos, estos recursos generalmente son auditados para asegurar el cumplimiento de objetivos e impacto de los proyectos implementados, por lo que representan una oportunidad para el impulso de proyectos que cumplan con altos estándares e impacto en la sociedad.

La tercera parte consistirá en la generación de ingresos propios a través de un esquema de servicios de consultoría y capacitación a terceros en temas de ciberseguridad, estos podrán ser ofertados a instituciones educativas, empresas y todo aquel mercado interesado en prevenir los delitos en materia de ciberseguridad.

La unificación y desarrollo en las estrategias de factor humano y financiero darán a la asociación un esquema de sostenibilidad sólido que traducido en términos de operatividad permitirá un eficiente funcionamiento acompañado de un óptimo desempeño para el alcance de objetivos.

3.3 Comparativo con otros organismos

Tabla 15. Otros organismos

Nombre de la Asociación	Descripción	Características	Ubicación y datos
Asociación Mexicana de Ciberseguridad (AMECI)	Organización mexicana encargada de asesorar a las organizaciones en el ámbito de seguridad de la información.	• Dirigida principalmente a empresas. • Servicios que se pueden solicitar: • Análisis de Vulnerabilidades. • Pentesting. • Cumplimiento Seguridad de la Información. • Protección de datos personales. • Soluciones en DRP. • Análisis de riesgos. • Sistema SGSI. • Servicios de consultoría en seguridad de la información.	Web: https://www.ameci.org Dirección: Calle Zacatecas No.24 Col. Roma Norte México, CDMX C.P. 06700

Consejo Mexicano de Asuntos Internacionales (COMEXI)	Asociación Civil sin fines de lucro dedicada al estudio, análisis y diálogo sobre las relaciones internacionales. Su objetivo es generar propuestas que contribuyan a la toma de decisiones y que incidan—de manera estratégica—en la definición e implementación de las políticas públicas que afectan a México.	• No se dedica exclusivamente al tema de la ciberseguridad, aunque sí lo aborda frecuentemente. • En lo relativo a esta tesis, presenta un panorama amplio y general sobre el impacto de la ciberseguridad en importantes campos de nuestra sociedad e intenta crear conciencia de la importancia que tiene entender los riesgos y actuar sobre ellos. • Señala algunas de las llamadas mejores prácticas, que se han desplegado en diversos países en esta materia.	Web: https://www.consejomexicano.org Dirección: Sierra Mojada 620, Oficina 502 Torre Magnum Colonia Lomas de Chapultepec 11000 Ciudad de México Artículo relacionado con el tema: https://consejomexicano.org/multimedia/1528987628-817.pdf

Frente Nacional por la Sororidad	Grupo de 30 organizaciones que se dedican a enfrentar la violencia digital principalmente.	• Promotoras de la Ley Olimpia, convirtiendo a Puebla en el segundo Estado, después de Yucatán en conseguir una reforma que tipifica los delitos de género en la esfera digital. • Para el Frente existen dos modalidades de violencia digital: la primera es la que afecta la sexualidad que puede ser extorsión, trata y difusión de contenido íntimo sin consentimiento y la segunda es la que no está relacionada directamente a un tema sexual, cuando no hay difusión de contenido íntimo sino cuando se utilizan las fotografías de alguien en perfiles falsos para difamar, o el acecho, el ciberacoso y las amenazas,	Web: https://defensorasdigitales.org/quienes-somos/

		entre los que está también la violencia y agresiones digitales que sufren periodistas y activistas. • Se dedican a difundir y a promover la cultura digital con perspectiva de género. • Crearon el violentómetro digital.	
SocialTIC	Es una organización sin fines de lucro dedicada a la investigación, formación, acompañamiento y promoción de la tecnología digital e información para fines sociales.	• Busca empoderar de manera segura a actores de cambio en América Latina reforzando sus acciones de análisis, comunicación social e incidencia a través del uso estratégico de tecnologías digitales y datos.	Web: https://socialtic.org/

Asociación de Auditoría y Control de Sistemas de Información (ISACA)	Es una organización que imparte seminarios, organiza eventos y talleres con temas referentes a Auditoría, Control y Seguridad de Información.	• La asociación se enfoca actualmente en el aseguramiento, gobierno, y seguridad de TI además proporciona certificaciones reconocidas a nivel mundial en materia de aseguramiento/auditoría (CISA), seguridad (CISM), gobierno (CGEIT) y riesgos (CRISC).	Web: http://www.isaca.org/chapters7/Monterrey/Pages/default.aspx
Observatorio de violencia de género en medios de comunicación (OVIGEM)	Derivado de la solicitud de declaratoria de Alerta de Violencia de Género contra las Mujeres (AVGM) para el estado de Puebla en julio de 2016, el grupo especializado para atender la	• Trabaja en la elaboración de análisis, diagnósticos y recomendaciones a los medios de comunicación, desde la perspectiva de género y combate a la violencia contra las mujeres. • Elaboran diagnósticos sobre la condición que guardan los medios de comunicación e	Web: https://www.ovigem.org/ Dirección: Avenida 21 Oriente No. 404. Colonia El Carmen. C.P. 72530 Teléfono: (222) 6 04 63 74

	solicitud, en su 4ª recomendación, propone "la creación de un observatorio de medios de comunicación locales con el fin de eliminar visiones sexistas y estereotipadas, prevenir la violencia de género e impulsar el respeto de los derechos humanos de las mujeres". Inicia sus operaciones en septiembre del 2017, con apoyo del Consejo Ciudadano de	información y plataformas digitales en materia de género y violencia hacia las mujeres. • Promueven cambios en los contenidos a través de la emisión de recomendaciones. • Promueven la aplicación de la normatividad en materia de defensoría de audiencias.	Correo: contacto@ovigem.org

	Seguridad y Justicia del Estado de Puebla (CCSJP).

Nota: Elaboración propia. Información extraída de:

- AMECI (Fecha de consulta: 7 de junio de 2019). Recuperado del portal electrónico de la Asociación Mexicana de Ciberseguridad: https://www.ameci.org/index.php/
- COMEXI (Fecha de consulta: 5 de junio de 2019). Recuperado del portal electrónico del Consejo Mexicano de Asuntos Internacionales: https://www.consejomexicano.org/
- "La violencia digital también puede ser violencia de género". Periodista: Aranzazú Ayala Martínez. Artículo de la Revista Lado B (Fecha de consulta: 4 de junio de 2019). Recuperado del portal electrónico de Lado B: https://ladobe.com.mx/2019/01/la-violencia-digital-tambien-puede-ser-violencia-de-genero/
- ISACA (Fecha de consulta: 10 de julio de 2019). Recuperado del portal electrónico oficial: http://www.isaca.org/chapters7/Monterrey/Pages/default.aspx
- ISACA (Fecha de consulta: 10 de julio de 2019). Recuperado del portal electrónico oficial: http://www.isaca.org/chapters7/Monterrey/Pages/default.aspx
- SOCIALTIC (Fecha de consulta: 10 de julio de 2019). Recuperado del portal electrónico Oficial de SocialTic: https://socialtic.org/

CONCLUSIONES

Acompañado a la constante evolución tecnológica que la humanidad genera a diario, las formas de cometer hechos delictivos también lo hacen, por lo que, tanto las autoridades competentes en materia de prevención del delito, como las persecutoras del mismo, así como la ciudadanía, tienen la responsabilidad de generar estrategias que puedan combatir los delitos cometidos por medio de Tecnologías de la Información y Comunicación (TIC). Sin embargo, acorde a la investigación realizada, no existe en México una adecuada cultura cibernética por ninguno de los entes antes mencionados, por lo que la población en general resulta vulnerada en materia de seguridad.

Consecuencia de lo anterior, es la poca tipificación delictiva que existe respecto de esta clase de conductas antisociales, así como la escasa tecnología utilizada en la investigación y persecución de las conductas ya tipificadas, que en conjunto con la falta de información y de acompañamiento a la ciudadanía, resultan en un endeble sistema que es propenso a ser sujeto de ciber ataques sin repercusiones jurídicas.

Al no existir institución alguna que pueda dar eficazmente solución a estas cuestiones, es necesario que la ciudadanía se organice y constituya un ente civil, que, en conjunto con las autoridades, establezca estrategias que puedan brindarle realmente seguridad a la población respecto al uso de dispositivos electrónicos. Labor que es posible a través de la figura jurídica denominada Asociación Civil, que se configura siendo ésta un ente con un objeto social específico que no busca fines preponderantemente económicos.

En los párrafos anteriores se han abordado diversos aspectos técnicos y legales que sustentan la propuesta de la presente tesis, misma que tiene como finalidad contribuir a prevenir la incidencia de ciber delitos en la población en general, además de fomentar una cultura de la

prevención, también se estará contribuyendo a un estado de seguridad para la ciudadanía al navegar por internet.

Atendiendo a los datos históricos y estadísticos presentados en páginas anteriores resulta clara la necesidad de atender la problemática y emprender acciones tendientes a combatir los ciberdelitos en el municipio de Puebla, dichas acciones encuentran su pilar fundamental en la participación activa de la ciudadanía como agentes transmisores de conocimientos en la materia.

Esta participación de la ciudadanía debe ser encausada para generar los resultados esperados, por lo tanto y derivado del análisis del sistema normativo mexicano vigente, se contempla como figura ideal la creación de una asociación civil como figura legal que permita unir las acciones individuales para contribuir a lograr el objeto social que la misma ha de perseguir.

Una asociación civil como la que se plantea permitirá a sus miembros en primero momento un amplio margen de acción para lograr incidir en la prevención de los ciber delitos, en segundo término, su constitución legal resulta óptima para el ejercicio de diversas funciones que permitan alcanzar objetivos más específicos.

Esta asociación civil pretende implementar acciones tendientes a prevenir la incidencia de los ciberdelitos en el Municipio de Puebla, sus acciones estarán destinadas a capacitar a los diferentes sectores de la sociedad desde la población en general, academia, gobierno y el sector privado.

La asociación civil ofrecerá un esquema organizacional para que los diferentes sectores puedan participar y contribuir desde su área de especialización al fortalecimiento de las acciones con el objetivo de hacerlas más efectivas.

En este esquema de participación se contarán con periodos y figuras específicas para que todo aquel interesado en materia de ciber seguridad pueda aportar sus conocimientos y contribuir a la reducción en la incidencia de ciberdelitos.

Asimismo, se contará con un esquema para que el sector filantrópico (privado) pueda contribuir en el sostenimiento financiero de los proyectos, reconociendo sus contribuciones económicas y beneficiándolos con la deducción de los impuestos correspondientes, lo que generará una atracción importante de capital.

La estructura organizacional y el esquema de participación que la asociación ofrece logrará multiplicar los esfuerzos colectivos en materia de ciber seguridad, encausando iniciativas a favor de una cultura de prevención que contrarreste la incidencia de los ciberdelitos, es dable resaltar que la atención a este fenómeno delictivo se refleja en diversos ámbitos, abarcando operaciones simples como la navegación en páginas de internet dedicadas a la venta de productos o servicios hasta las operaciones bancaria-financieras.

Son diversas las conductas que al día de hoy todavía no son contempladas como delitos, aun cuando estas causan agravios al patrimonio de una gran número de ciudadanos, conductas que van desde el robo de información personal y hasta bancaria, lo aquí referido también es sostenido en el Informe Anual 2017 de la CONDUSEF, el informe resalta las reclamaciones interpuestas por usuarios de servicios financieros quienes sostienen sus reclamaciones por no reconocer las operaciones que se realizan desde sus cuentas de débito o crédito.

Estas conductas, aunque son más perceptibles entre la ciudadanía también impactan al sector gubernamental y privado, aunque las consecuencias en estos sectores conllevan afectaciones

de gran relevancia, principalmente del tipo económico, pues las sumas afectadas resultan ser de gran importancia.

Por lo tanto es de gran relevancia y necesidad la atención de esta problemática de manera urgente, pues la tecnología avanza a pasos agigantados y los conocimientos en la materia aún son escasos, de igual forma derivado del análisis de las encuestas aplicadas como parte de la metodología para sustentar esta propuesta se observó que la población muestra desconoce en alto grado los riesgos a los que están expuestos al navegar por internet, también se observó que aun cuando han sido víctimas de este tipo de delitos no han sabido la forma de proceder.

Atendiendo a lo aportado por esta investigación, resulta de gran trascendencia crear instancias y mecanismos de acción que prevengan este tipo de acciones, al tiempo de contrarrestar la incidencia de este tipo de conductas que sin duda afectan a todos los sectores de la sociedad.

Las acciones implementadas por la asociación generaran resultados desde la ciudadanía aportando conocimientos tendientes a prevenir estas conductas y se potencializaran con la aplicación de programas de capacitación al interior de los sectores de mayor nivel como el gubernamental y el privado, logrando mejorar la estadística en materia de ciberseguridad.

Referencias

Legisgrafía

Cámara de Diputados del H. Congreso de la Unión. (2018). Ley General de Sociedades Mercantiles (2018). Recuperado el 26 de junio de 2019 en: http://www.diputados.gob.mx/LeyesBiblio/pdf/144_140618.pdf

Cámara de Diputados del H. Congreso de la Unión. (2018). Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de Estos Delitos. México: H. Cámara de Diputados. Recuperado el 28 de junio de 2019 en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPSEDMTP_190118.pdf

Cámara de Diputados del H. Congreso de la Unión. (2019). Código Penal del Estado de Puebla (2019). México: Secretaría de Gobernación.

Gobierno del Estado de Puebla. Orden Jurídico Poblano. (2018). Código Civil para el Es Estado Libre y Soberano de Puebla. Puebla: H. Congreso del Estado de Puebla. Recuperado el 26 de junio de 2019 en: file:///C:/Users/Poo/Downloads/Codigo_Civil_para_el_Estado_Libre_y_Soberano_de_Puebla27072018.pdf

H. Cámara de Diputados. (2018). Ley General de Sociedades Cooperativas. México: H. Cámara de Diputados. Recuperado el 27 de junio de 2019 en: http://www.diputados.gob.mx/LeyesBiblio/pdf/143_190118.pdf

H. Congreso del Estado de Puebla. (2018). Ley de Instituciones de Asistencia Privada para el Estado Libre y Soberano de Puebla. Puebla: H. Congreso del Estado de Puebla.

Bibliografía

Acurio del Pino, S. (2016). Delitos informáticos: generalidades. Washington: Organización de Estados Americanos.

Amuchategui, G. (2012). Derecho penal. México. Editorial Oxford.

Araya, E. (2007). Participación ciudadana. Santiago, Chile: Universidad de Chile.

Arbós, X. y Giner, S. (1993). La gobernabilidad. Ciudadanía y democracia en la encrucijada mundial. Madrid: Siglo XXI.

Bequiai, A. (1978). Computer crime. Lexington: Heath Lexington Books.

Calderón, A. T. (2017). Teoría del delito y juicio oral. México: UNAM-Instituto de Investigaciones Jurídicas.

Casado, L. (2009). Diccionario de derecho. Lima: Valetta Ediciones.

Castellanos, F. (2008). Lineamientos elementales de derecho penal. México: Editorial Porrúa.

Colegio de Notarios del Distrito Federal. (2016). Comandita simple. Siglas: S. en C. Recuperado el 26 de junio de 2019 en: http://www.colegiodenotarios.org.mx/documentos/sociedades/s4.pdf

Corte, L. y Giménez-Salinas, A. (2010). Crimen organizado: evolución y claves de la delincuencia organizada. Barcelona: Ariel.

Cruz, F. (2017). Sociedades mercantiles. México: UNAM-División de Universidad Abierta.

Dávalos, M. S. (2010). Manual de introducción al derecho mercantil. Instituto de Investigaciones Jurídicas-UNAM-Nostra Ediciones.

Franco, R. (2012). Delito e injusto. México: Porrúa.

García, E. M. (2019). Obtención de una perspectiva psicosocial en materia de ciberseguridad. (Tesis de maestría inédita). Maestría en Ciencias y Tecnologías de Seguridad. Instituto Nacional de Astrofísica, Óptica y Electrónica. Puebla, México.

Gobierno de México. (2017). Estrategia Nacional de Ciberseguridad. México.

Gutiérrez, E. (2003). Derecho de las obligaciones. México: Porrúa.

Gutiérrez, M. (1994). Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa. En Arroyo, L. y Tiedemann, K. (Eds). Estudios de derecho penal económico, de Estudios de derecho penal económico (pp. 183-208). Cuenca, España: Ediciones de la Universidad de la Universidad de Castilla-La Mancha.

Gutiérrez, M. L. (1991). Fraude informático y estafa: aptitud del tipo de estafa en el derecho. Madrid: Ministerio de Justicia.

Herrero, C. (1997). Criminología (parte general y especial). Madrid: Dykinson.

International Telecommunication Union (ITU). (2018). Global Cybersecurity Index (GCI). Ginebra: ITU Publications.

Jiménez de Asúa, L. (1997). Principios de derecho penal. La ley y el delito. Buenos Aires: Abeledo Perrot-Editorial Sudamericana.

Lozano, C. (2002). El crimen organizado del robo de automotores. México: Ángel Editor.

Mantilla, R. L. (1965). Panorama del derecho mexicano (tomo II). México: UNAM.

McKinsey & Company (2018). Perspectiva de ciberseguridad en México. México: Presidencia de la República-Organización de Estados Americanos.

Olvera, A. J. (2009). La participación ciudadana y sus retos en México. Un breve estudio del desarrollo de la cultura y de las instituciones participativas y diagnóstico de su problemática

actual, con propuestas para hacer funcionales las instancias de participación democrática. México: Secretaría de Gobernación.

Ortíz, J. A. (1996). La contracultura en México. México: Grijalbo.

Ossorio, M. (2007). Diccionario de ciencias jurídicas, políticas y sociales. Guatemala: Datascan.

Pavón, F. (2012). Manual de derecho penal mexicano. México: Editorial Porrúa.

Pérez, A. E. (1982). Asociación. En Diccionario jurídico mexicano (tomo I) (pp. 214-215). México: UNAM.

Pérez, A. E. (1982). Fundaciones. En Diccionario jurídico mexicano (tomo IV). México: UNAM.

Porte, C. (1958). Programa de la parte general del derecho penal. México: Universidad Nacional Autónoma de México-Facultad de Derecho.

Propuesta de líneas de acción del Eje Transversal de Desarrollo de Capacidades. (2018). México: Subcomisión de Ciberseguridad-ANUIES.

Rodríguez, J. (2001). Tratado de sociedades mercantiles. México: Porrúa.

Romero, J. D. (2010). Los consejos de participación ciudadana como instancias evaluadoras de políticas públicas, caso municipio de Puebla (Tesis doctoral en Administración Pública, Instituto de Administración Pública del Estado de Puebla, Puebla).

Roxin, C. (1977). Derecho penal, parte general, tomo I "Fundamentos. La estructura de la teoría del delito". Madrid: Civitas.

Subsecretaría de Competitividad y Normatividad. (2016). Sociedades. México: Secretaría de Economía.

Velazco, E. (2006). La delincuencia en la era de la globalización. Puebla: Cátedra Iberoamericana de Ingeniería Política

Hemerografía

Aristóteles. La política. Madrid: Ediciones nuestra raza. Recuperado el 26 de junio de 2019 en: http://fama2.us.es/fde/ocr/2006/politicaAristoteles.pdf

Gabuardi, C. A. (enero-junio, 2016). La sociedad en nombre colectivo en México. Derecho Privado Cuarta Época, año III, N° 5, 3-52.

Gallardo-Pujol, D., García-Forero, C., Maydeu-Olivares, A. y Andrés-Pueyo, A. (febrero, 2009). Desarrollo del comportamiento antisocial: factores psicobiológicos, ambientales e interacciones genotipo-ambiente. Neurología, 48 (4), 191-198.

Labariega, P. A. (mayo-agosto, 2003). La fundación en derecho privado mexicano. Derecho Privado Nueva Época, Año II, N° 5, 53-107.

Leiva, E. A. (2015). Estrategias nacionales de ciberseguridad: estudio comparativo basado en enfoque Top-Down desde una visión global a una visión local. Revista Latinoamericana de Ingeniería de Software, 3 (4), 161-176.

Moreno, S. (julio-agosto, 2005). Nueva era y contracultura. Casa del Tiempo N° 78-79, 51-62.

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E. y Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11 (28), 41-66.

Saavedra, M. L., Paúl, F. y Bernal, D. (2012). El asociativismo como estrategia para enfrentar a un mercado competitivo: un estudio de caso de las pequeñas empresas farmacéuticas. QUIPUKAMAYOC, 20 (38), 189-205.

Zamora, M. Á. (junio, 1987). El derecho del tanto de los arrendatarios de casa habitación y la intervención notarial. Derecho Notarial Mexicano Año XXXI, N° 96, 15-35.

Webliografía

ADICAE. (2014). Nuevo ataque mediante pishing, esta vez para clientes del Banco Santander y Banco Pastor. Recuperado el 25 de junio de 2019 en: http://blog.adicae.net/consumidores-2014/files/2014/08/Phishing Santandercompleto.jpg

Aetecno. (2019). Costo de los ciberataques supera los US$8.000M en México. Recuperado el 30 de mayo de 2019 en: https://tecno.americaeconomia.com/articulos/costo-de-los-cibera taques-supera-los-us8000m-en-mexico

Alcocer, J. (2019). Delitos cibernéticos dejaron pérdidas por 10 mmdp en 2018. Recuperado el 1 de junio de 2019 en: https://www.publimetro.com.mx/mx/noticias/2019/01/06/delitos-ciberneticos-dej aron-perdidas-10-mmdp-2018.html

Asociación Conecta Rural. (2019). ¿Qué es la participación ciudadana? Recuperado del portal electrónico de la (Colombia). Recuperado el 29 de mayo de 2019 en: https://conectarural.org/sitio/participando/

Asociación de Internet,mx. (2019). 15º Estudio sobre los hábitos de los usuarios de internet en México 2019. Recuperado en: https://www.asociaciondeinternet.mx/es/

B&MNEWS. (2019). Lanza Infosecurity Mexico su Summit 2019 con Garry Kasparov y Marc Goodman como oradores principales. Recuperado el 30 de mayo de 2019 en: https://www.businessandmarketingtodaynews.com/content/lanza-infosecurity-mexico-su-summit-2019-con-garry-kasparov-y-marc-goodman-como-oradores

Barrio, M. (2011). La ciberdelincuencia en el Derecho español. En Revista de las Cortes Generales. 83, 273-305. Recuperado de Real Academia Española. Diccionario del español jurídico el 01 de julio de 2019 en: https://dej.rae.es/lema/cert

Becerril, A. (2018). México, quinto país más afectado por extracción de datos a Facebook por Cambridge Analytica. Recuperado del diario electrónico El Economista el 1 de junio de 2019 en: https://www.eleconomista.com.mx/tecnologia/Mexic o-quinto-pais-mas-afectado-por-extraccion-de-datos-a-Facebook-por-Cambridg e-Analytica-20180404-0088.html

Cacelín, J. (2017). Laboratorio de Ciberseguridad, vigilando el ciberespacio en México. Recuperado el 28 de mayo del 2019 en: http://www.cienciamx.com/index.php/tecnologia/tic/15236-laboratorio-cibers eguridad-vigilando-ciberespacio-mexico

Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación. (2019). ¿Qué es INFOTEC? Recuperado el 28 de mayo de 2019 en: https://www.infotec.mx/es_m x/infotec/que_es_infotec

CERT UNAM (2019). Recuperado el 27 de mayo de 2019 en: https://www.cert.unam.mx/csi

CICDE Consultores Fiscales. (2019). Diferentes tipos de sociedades en México. Recuperado el 20 de marzo de 2019 en: https://cicde.mx/diferentes-tipos-sociedades-mexico/

Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (2018). Fortalecimiento de los mecanismos de Ciberseguridad. Recuperado el 25 de mayo de 2019 en:

https://www.gob.mx/cidge/ articulos/fortalecimiento-de-los-mecanismos-de-ciberseguridad?idiom=es

Comisión Nacional para Prevenir y Erradicar la Violencia Contra las Mujeres. (2018). ¿Has sufrido acoso cibernético? ¡Identifica sus modalidades y protégete! Recuperado el 25 de junio de 2019 en: https://www.gob.mx/conavim/articulos/has-sufrido-acoso-cibernetico-te-decimos-a-donde-acudir

Concienciat. (2018). Información de cómo identificar el pishing. Recuperado el 25 de junio de 2019 en: https://concienciat.gva.es/wp-content/uploads/2018/03/infor_como_identificar_phishing

CONDUSEF. (2018). ¿Ya conoces estos tipos de fraude? Recuperado el 25 de junio de 2019 en: https://phpapps.condusef.gob.mx/fraudes_financieros/imagenes/informate/infografias/tipos_fraudes.pdf

Controversia. (2019). Tipos de ciberataques, más allá del ransomware. Recuperado el 25 de junio de 2019 en: http://www.consultoria-conversia.es/internet/tipos-ciberataques-infografia-ransomware/

Definición. (2019). Social. Recuperado el 3 de mayo de 2019 en: https://definicion.de/social/

Equipo de Respuesta a Incidentes y Delitos Informáticos de la Universidad Autónoma de Chihuahua. (2019). ¿Quiénes somos? Recuperado el 28 de mayo de 2019 en: http://csirtchihuahua .uach.mx/quien.html

Estrategia Nacional de Ciberseguridad. (2017). Recuperado el 23 de mayo de 2019 en: https://mision.sre.gob.mx/oea/index.php/actividades/25-avisos-2017/420-mexic o-mexico-presento-estrategia-nacional-de-ciberseguridad

García, J. C. (2018). Cryptojacking, el secuestro de tus dispositivos para generar criptomonedas... en silencio. Recuperado el 2 de junio de 2019 en: https://www.elfinanciero.com.mx/tech/cryptojacking-el-secuestro-de-tus-dispositivos-para-generar-criptomonedas-en-silencio

García, J. F. (2018). 5 consejos para evitar el pishing. Recuperado el 25 de junio de 2019 en: https://www.eluniverso.com/tendencias/2018/06/13/nota/6809039/5-consejos-evitar-phishing

Gómez, P. (2019). Cada semana 12 poblanos son víctimas de ataques cibernéticos. Recuperado el 25 de junio de 2019 en: https://www.elsoldepuebla.com.mx/policiaca/cada-semana-12-poblanos-son-victimas-deciberdelitos-puebla-3261724.html

Hernández, J. C. (2017). Estrategias nacionales de ciberseguridad en América Latina. Recuperado del portal electrónico del Grupo de Estudios en Seguridad Internacional (GESI), Universidad de Granada (España). Disponible en: http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-américa-latina

IFAI. (2018). Guía para prevenir el robo de identidad. Recuperado el 25 de junio de 2019 en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Prevenir_RI.pdf

Kaspersky Lab. (2018). Kaspersky Lab: Brasil, México y Colombia lideran incidentes de secuestros digitales en América Latina. Recuperado el 2 de junio de 2019 en: https://latam.kaspersky.com/about/press-releases/2017_kaspers ky-lab-incidents-of-digital-kidnappings-in-latin-america

La otra opinión. (2018). Crean "Grupo de Respuesta a Incidentes" contra ciberataques a bancos. Recuperado el 1° de junio de 2019 en: https://www.laotraopinion.com.mx/crean-grupo-de-respuesta-a-incidentes-contra-ciberataques-a-bancos/

Lara, P. (2019). Cultura Colectiva expuso tus datos. Recuperado el 2 de junio de 2019 en: https://www.excelsior.com.mx/hacker/cultu ra-colectiva-expuso-tus-datos/1305715

Luna, N. (2018). ¿Qué es una sociedad de responsabilidad limitada? Recuperado el 23 de marzo de 2019 en: https://www.entrepreneur.com/article/307159

Machicado, J. (2019). Causas de justificación. Recuperado el 6 de marzo de 2019 en: https://jorgemachicado.blogspot.com/2009/03/ causas-de-justificacion.html

Melimansilla. (2017). Robo de identidad. Recuperado el 25 de junio de 2019 en: http://melimansilla2003.blogspot.com/2017/11/robo-de-identidad.html

Morales, C. (2018). Estos dos factores habrían permitido el hackeo del SPEI. Recuperado el 30 de mayo de 2019 en: https://www.forbes. com.mx/estos-dos-factores-habrian-permitido-el-hackeo-del-spei/

Mulero, H. (2015). Comportamiento antisocial. Recuperado el 4 de mayo de 2019 en: http://crimina.es/crimipedia/topic s/310/

NOTIMEX. (2015). México registra rezago en materia de seguridad cibernética. Recuperado el 30 de mayo de 2019 en: http://www.cronica.com.mx/notas/2015/901760.html

Oficina de Seguridad del Internauta. (2018). ¿Sabías que el 95% de las incidencias en ciberseguridad se deben a errores humanos? Recuperado el 25 de junio de 2019 en: https://www.osi.es/es/actualidad/blog/2018/12/05/sabias-que-el-95-de-las-incidencias-en-ciberseguridad-se

OnBranding. (2018). [Imagen]. Recuperada el 25 de junio de 2019 en: https://pbs.twimg.com/media/DH8o-YsXcAAD9wk.jpg

Palladino Pellón & Asociados-Abogados Penalistas. (2019). Antijuricidad y delito. Recuperado el 5 de mayo de 2019 en: https://www.palladinopellonabogados.com/antijuridicidad-y-delito/

PC World México. (2018). México entre los 10 países más ciberatacados. Recuperado el 7 de mayo de 2019 en: http://pcworld.com.mx/mexico-entre-los-10-paises-mas-ciberatacados/

Policía Federal. (2019). El CERT-MX se encarga de prevenir y mitigar las amenazas de seguridad informática que ponen en riesgo la infraestructura tecnológica y la operatividad del país. Recuperado el 29 de mayo de 2019 en: https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-inci dentes-ciberneticos-de-la-policia-federal?idiom=es

Político MX. (2018). Escándalo de Cambridge Analytica reventó también en México. Recuperado el 25 de junio de 2019 en: https://politico.mx/central-electoral/elecciones-

2018/presidencial/esc%C3%A1ndalo-decambridge-analytica-revent%C3%B3-tambi%C3%A9n-en-m%C3%A9xico/

Real Academia Española. (2019). A priori. Recuperado el 3 de mayo de 2019 en: http://lema.rae.es/dp d/srv/search?key=a%20priori

Real Academia Española. (2019). Comandita. Recuperado el 20 de marzo de 2019 en: https://dle.rae.es/?id =9srSKge

Real Academia Española. (2019). Comanditar. Recuperado el 20 de marzo de 2019 en: https://dle.rae.es/?id =9ssb8v3

Real Academia Española. (2019). Gregario. Recuperado el 20 de marzo de 2019 en: https://dle.rae.es/? id=JWNFLFU

Reyes, E. (2018). México es el segundo país más atacado por ransomware. Recuperado el 2 de junio de 2019 en: https://expansion.mx/tecnologia/2018/04/25/mexico-es-el-segundo-pais-mas-at acado-por-ransomware

Riquelme, R. (2018). ¿Qué es un Equipo de Respuesta ante Emergencias Informáticas (CERT)? Recuperado el 25 de mayo de 2019 en: https://www.eleconomista.com.mx/tecnologia/Que-es-un-Equipo-de-Respuesta-ante-Emergencias-Informaticas-CERT-20180122-0009.html

Rodríguez, I. (2018). Ciberataques costaron al país 7 mil millones dólares en 2017. Recuperado el 30 de mayo de 2019 en: https://www.jornada.com.mx/2018/09/27/economia/030n2eco

Saldana, G. (2018). Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina. Recuperado del portal electrónico de Kaspersky. Recuperado el 15 de mayo de

2019 en: https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataques-ciberneticos-en-america-latina/13266/

Sosa, L. (2015). La delincuencia organizada en México. Recuperado el 11 de mayo de 2019 en: https://w ww.gestiopolis.com/la-delincuencia-organizada-en-mexico-ensayo/

Sy Corvo, H. (2019). Sociedad en comandita simple: características, ventajas, desventajas. Recuperado el 19 de marzo de 2019 en: https://www.lifeder.com/sociedad-comandita-simple/

Vanguardia, L., Minuto, A., Contra, L., Vang, B., Fan, M., y Moda, D. (2018). Cómo evitar el ciberacoso en 10 pasos. Recuperado el 25 de junio de 2019 en: https://www.lavanguardia.com/seguros/hogar/20180606/462106086754/como- evitarel-ciberacoso-en-10-pasos.html

Tablas

Figuras

Apéndices

A) CUESTIONARIO SOBRE PREVENCIÓN DE CIBERSEGURIDAD

PARTE 1

Me han informado en qué consiste este cuestionario de tal forma que me queden claros los objetivos del estudio de investigación y que los datos serán usados de forma confidencial:

O No O Sí

Datos personales

1. ¿Qué edad tienes?

2. ¿Cuál es tu género?

3. ¿Cuál es tu grado académico?

4. ¿A qué te dedicas?

A continuación, encontrarás una serie de preguntas que debes leer atentamente, las cuales únicamente son de diagnóstico, por lo que no hay inconveniente si conoces o no la respuesta. Su finalidad es la de contribuir al desarrollo del curso para que los participantes tengan una mejor experiencia.

Recuerda, esto no es un examen, no hay respuestas correctas o incorrectas. Pero es importante que contestes todas las preguntas. Hazlo de la manera más sincera posible.

5. ¿Por qué vía o vías has recibido principalmente información sobre ciberseguridad?

a). Padres, hermanos

0) nunca	1) pocas veces	2) bastante (3 o 4 veces)	3) muchas veces (más de 4)	4) casi siempre

b). Otros familiares

0) nunca	1) pocas veces	2) bastante (3 o 4 veces)	3) muchas veces (más de 4)	4) casi siempre

c). Amigos

0) nunca	1) pocas veces	2) bastante (3 o 4 veces)	3) muchas veces (más de 4)	4) casi siempre

d). Profesores

0) nunca	1) pocas veces	2) bastante (3 o 4 veces)	3) muchas veces (más de 4)	4) casi siempre

e). Medios de comunicación (tv, prensa, radio)

0) nunca	1) pocas veces	2) bastante (3 o 4 veces)	3) muchas veces (más de 4)	4) casi siempre

f). Charlas o cursos sobre el tema

0) nunca	1) pocas veces	2) bastante (3 o 4 veces)	3) muchas veces (más de 4)	4) casi siempre

g. Folletos, libros

0) nunca	1) pocas veces	2) bastante (3 o 4 veces)	3) muchas veces (más de 4)	4) casi siempre

h). Personas expertas con el tema

0) nunca	1) pocas veces	2) bastante (3 o 4 veces)	3) muchas veces (más de 4)	4) casi siempre

6. Me siento suficientemente informado en relación a la ciberseguridad

O No O Sí O Un poco

7. ¿Cuántas horas pasas al día en las redes sociales?

8. ¿A qué edad empezaste a navegar por internet?

9. ¿Sabes qué es la ciberseguridad?

O No

O Sí Explica:

10. ¿Sabes qué es un ciberataque?

O No

O Sí Explica:

11. ¿Sabes qué es el Malware?

O No

O Sí Explica:

12. ¿Sabes cómo funciona el robo de información mediante Phishing?

O No

O Sí Explica:

13. ¿Sabes lo que es Ciberacoso?

O No

O Sí Explica:

14. ¿Sabes lo que es Ransomware?

O No

O Sí Explica:

15. ¿Qué entiendes por "Hacker"?

16. En tu opinión:

O México es un país tecnológicamente seguro

O Ha sido blanco de muchos ataques cibernéticos

17. ¿Te ha llegado a preocupar algún incidente del que te hayas enterado sobre hackers?

O No

O Sí Explica:

18. ¿Recuerdas alguna noticia relevante sobre ataques de hackers en México?

O No

O Sí ¿Cuál?

19. ¿Conoces algún tipo o tipos de ciberdelitos?

O No

O Sí Explica:

20. ¿Has sabido sobre casos de ciberdelitos ocurridos en Puebla?

O No

O Sí Explica:

21. A lo largo de tu vida ¿Has sido víctima de algún ciberdelito?

O No

O Sí Explica:

22. En caso de haber sido víctima, ¿denunciaste?

O No ¿Por qué?

O Sí Explica:

23. ¿Utilizas contraseñas diferentes para cada servicio o aplicación?

O No O Sí

24. Tu contraseña está compuesta por:

O Menos de 8 letras y números combinados

O Al menos 8 letras y números combinados

O Más de 8 letras y números combinados

25. ¿Qué acciones llevas a cabo para evitar que tus datos personales sean robados?

26. ¿Has recibido mensajes o correos que te soliciten información personal?

O No

O Sí Explica:

27. ¿Alguno de tus dispositivos (teléfono, computadora, tablet) ha sido infectado por virus?

O No

O Sí Explica:

28. ¿Has identificado algún cargo no reconocido en tu tarjeta de crédito?

O No

O Sí Explica:

29. Si tuvieras que valorar la sinceridad de tus respuestas al cuestionario, ¿qué puntuación te darías siguiendo la escala de 0 a 10 que figura a continuación?

1 O	2 O	3 O	4 O	5 O	6 O	7 O	8 O	9 O	10 O

Has finalizado el cuestionario

Muchas gracias por tu colaboración

B) CUESTIONARIO SOBRE PREVENCIÓN DE CIBERSEGURIDAD

PARTE II

A continuación, encontrarás una serie de preguntas que debes leer atentamente, las cuales únicamente son de diagnóstico, por lo que no hay inconveniente si conoces o no la respuesta. Su finalidad es la de contribuir al desarrollo del curso para que los participantes tengan una mejor experiencia.

Recuerda, esto no es un examen, no hay respuestas correctas o incorrectas. Pero es importante que contestes todas las preguntas. Hazlo de la manera más sincera posible.

1. Me siento suficientemente informado en relación a la ciberseguridad

O No O Sí O Un poco

2. ¿Qué entiendes por ciberseguridad?

3. ¿Qué entiendes por ciberataque?

4. ¿Qué entiendes por Malware?

5. ¿Cuál es la finalidad de un ataque de Phishing?

6. ¿Cómo evitarías el Ciberacoso?

7. ¿Cómo evitarías el Phishing?

8. ¿Cómo evitarías las infecciones por malware?

9. ¿Consideras que existe un adecuado nivel de seguridad tecnológica en México?

O Sí

O No ¿Por qué?

10. ¿Consideras importante que exista una asociación civil enfocada a la prevención y difusión de la ciberseguridad en el municipio de Puebla?

O No ¿Por qué?

O Sí ¿Por qué?

11. ¿Qué es lo que más te gusto del curso?

12. Si tuvieras que valorar la sinceridad de tus respuestas al cuestionario, ¿qué puntuación te darías siguiendo la escala de 0 a 10 que figura a continuación?

1 O	2 O	3 O	4 O	5 O	6 O	7 O	8 O	9 O	10 O

Has finalizado el cuestionario

Agradecemos nuevamente tu colaboración

C) Fotografía tomada durante el curso piloto.