UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

DIVISIÓN DE ESTUDIOS DE POSGRADO DE LA FACULTAD DE DERECHO.

DIMENSIONES DE LA CIBERCRIMINALIDAD EN AMÉRICA LATINA

UNA PROPUESTA PARA SU ESTUDIO

T E S I S

QUE PARA OBTENER EL TITULO DE ESPECIALISTA
EN DERECHO INTERNACIONAL PÚBLICO

P R E S E N T A:

LIC. BELINDA SHALOOM PENIEL VILLANUEVA CABELLO

ASESORA: DRA. NATIVIDAD MARTÍNEZ AGUILAR.

.

CIUDAD UNIVERSITARIA 2017.

AGRADECIMIENTOS

A mi Dios el Señor Jesucristo…
Por darme vida, salud y fortaleza para ser capaz
de hacer realidad cualquier aspiración
que tenga en la vida.

A mis padres René y Belinda…
Por su buena crianza, enseñazas y amor incondicional.

A mis profesores del Posgrado de la Facultad de Derecho….
En especial a la Dra. Natividad Martínez Aguilar
por su compromiso y apoyo incondicional
durante la elaboración de esta tesis.

Al Dr. Alfredo Chirino Sánchez…
por su calidad humana, orientación y contribución
a este trabajo de investigación
durante mi estancia en la Universidad de Costa Rica.

Al Centro de Investigaciones sobre América Latina y el Caribe, UNAM…
Por reconocer mi trayectoria académica y profesional,
y otorgarme una beca bajo el Programa
Red de Macrouniversidades de América Latina y el Caribe,
a fin de fortalecer esta Tesis.

DEDICATORIAS

A mi Nación, Latinoamérica y el resto del mundo…
Porque las buenas acciones, traen buenos cambios.

A mi Universidad Nacional Autónoma de México…
Por formar verdaderos profesionistas,
con autonomía y calidad humana.

A la Universidad de Costa Rica…
Por su hermosa hospitalidad y todo lo aprendido.

A ti lector…
Por tu tiempo invaluable y lo positivo
que pueda dejarte esta lectura.

ÍNDICE

CAPÍTULO III.

MARCO JURÍDICO DE LA CIBERSEGURIDAD Y ACCIONES EMPRENDIDAS.

CAPÍTULO IV

ESTRATEGIA INTEGRAL DE CIBERSEGUIDAD PARA AMÉRICA LATINA Y EL CARIBE.

"Las infraestructuras críticas son aquellas sobre las que se erigen servicios esenciales para los ciudadanos. Somos profundamente dependientes de ellas y vulnerables a sus riesgos".

-Fernando José Sánchez.

“Las contraseñas son como la ropa interior: no dejes que otros las vean, cámbialas con frecuencia y no las compartas con desconocidos”.

- Chris Pirillo.

"La libertad y la seguridad son dos caras de una misma moneda, no existe seguridad sin libertad, ni libertad sin seguridad. De cómo se articulen depende el éxito".

-Anónimo.

“CIBERESPACIO: Libertad + seguridad + tecnología + derecho. La solución no está en limitar ninguno, sino en potenciar todos y lograr su equilibrio”.

-Anónimo.

INTRODUCCIÓN

El presente trabajo de investigación nace con la inquietud de analizar uno de los problemas más relevantes de la criminalidad actual “la ciberdelincuencia”, basándome en mi experiencia profesional y académica, al haber egresado de la Facultad de Derecho de la Universidad Nacional Autónoma de México, me di a la tarea de realizar los estudios de la Especialidad en Derecho Internacional Público, así como asistir a múltiples cursos, congresos, seminarios y conferencias sobre temas de: prevención del delito, seguridad pública, seguridad nacional, inteligencia, contrainteligencia, cibercriminalidad, criminología, lavado de dinero, justicia penal internacional, entre otros.

En forma complementaria realicé una estancia en la Universidad de Costa Rica, Costa Rica, mediante el programa Red de Macrouniversidades de América Latina y el Caribe, con el objetivo de fortalecer esta Tesis y tuve la oportunidad de asistir a diferentes instancias, como: la Comisión Interamericana de Derechos Humanos, el Órgano de Investigación Judicial, la Oficina Central Nacional de la *International Criminal Police Organization* (INTERPOL) San José, Costa Rica, entre otras.

En el ámbito profesional trabajé en la Subsecretaría de Participación Ciudadana y Prevención del Delito de la Secretaría de Seguridad Pública de la Ciudad de México, en INTERPOL México, perteneciente a la Agencia de Investigación Criminal de la Procuraduría General de la República, y en el sector financiero en el Banco HSBC, en el área de Prevención de Lavado de Dinero.

A partir de esta trayectoria, obtuve una visión poliédrica sobre los problemas relacionados con la seguridad a nivel global, identificando la importancia y actualidad del tema denominado ciberdelincuencia, al detectar la evolución de los delitos tradicionales como el fraude, el robo, el sabotaje y espionaje, entre otros.

A medida que los delincuentes aprendieron a utilizar las nuevas Tecnologías de la Información y Comunicación en la comisión de los delitos, como son los teléfonos celulares, las computadoras, el internet, redes sociales y todos los mecanismos tecnológicos que hoy en día les permiten llevar a cabo un sinfín de delitos en cuestión de segundos y desde cualquier parte del mundo.

Lo cual me llevó a plantear la siguiente hipótesis: la necesidad de crear una estrategia integral en América Latina y el Caribe en materia se ciberseguridad, basada en la armonización legislativa, mediante la adhesión de todos los países de dicha región al Convenio sobre la Ciberdelincuencia del Consejo de Europa, con la finalidad de fortalecer la cooperación internacional entre las autoridades responsables de investigar los delitos cibernéticos.

Para la comprobación de la hipótesis mencionada se utilizó el método deductivo, mediante el desarrollando esta Tesis en cuatro capítulos, a partir de la investigación documental y de campo, ya que se recolectó información de diversas fuentes públicas, pero también de cursos y conferencias relacionadas con el tema, teniendo un acercamiento directo con las autoridades de las instancias encargadas en la investigación de los delitos informáticos en México y Costa Rica.

En el primer capítulo de esta Tesis se delimitan una serie de conceptos vinculados con el tema de la cibercriminalidad, para generar en el lector un panorama claro del contenido los temas que se abordarán.

El segundo capítulo versa sobre el último estudio que presentó el Banco Interamericano de Desarrollo y la Organización de los Estados Americanos, sobre la situación en la que se encuentran los países de América Latina y el Caribe en materia de ciberseguridad, bajo un enfoque pluridimensional, al considerar 5 dimensiones de análisis: 1) Política; 2) Sociedad; 3) Educación; 4) Legislación; y 5) Tecnología, en cada país de la región.

El objetivo del tercer capítulo de esta tesis es dar a conocer la realidad legislativa actual en materia de ciberseguridad a nivel mundial, así como, la importancia

que tiene el Convenio sobre la Ciberdelincuencia del Consejo de Europa a nivel global, al ser el primer tratado internacional que buscó dar solución a la problemática de la comisión de los delitos informáticos, mediante la armonización normativa entre los países firmantes y fortalecer la cooperación internacional, sobre todo por la naturaleza de los delitos cibernéticos, en los que su investigación requiere de un intercambio de información y cooperación entre las autoridades de los Estados involucrados en el hecho delictivo del que se trate.

Asimismo, se desglosa la labor realizada hoy en día por los distintos organismos internacionales en materia de ciberseguridad, destacando entre ellos la Unión Internacional de Telecomunicaciones (UIT), la Organización de las Naciones Unidas ONU), la Organización Internacional de Policía Criminal (INTERPOL), la Organización de los Estados Americanos (OEA), entre otros.

También, se analiza la situación legislativa que se vive en México en materia de ciberseguridad, identificando algunos delitos cibernéticos que actualmente se encuentran regulados, aunque no de manera general ni armonizada.

Finalmente, el capítulo cuarto busca brindar una alternativa integral para la estrategia de ciberseguridad para los países de América Latina y el Caribe que incluya una armonización legislativa, cooperación internacional en las investigaciones de los delitos cibernéticos que incluya la labor de ciberinteligencia, y el estudio de estos delitos desde la óptica de la victimología.

CAPÍTULO I
CONCEPTOS GENERALES RELACIONADOS A LA CIBERCRIMINALIDAD

1.1 DERECHO INFORMÁTICO

Según la doctrina el término Derecho Informático (*Rechtsinformatik*) fue acuñado por el Dr. Wilhelm Steinmüller, un académico de la Universidad de Ratisbona de Alemania, en el año 1970. No obstante, no es la única forma en la que se conoce sobre la regulación jurídica de la informática y las nuevas tecnologías de la información, a lo largo del mundo, también se le conoce como Derecho Telemático, Derecho de las Nuevas Tecnologías, Derecho de la Sociedad de la Información, Iuscibernética, Derecho Tecnológico, Derecho del Ciberespacio o Derecho de Internet, entre otros.

Hoy en día, el concepto de Derecho de las Tecnologías de la Información y Comunicación ha tomado fuerza en América Latina, llegando incluso a privilegiarse sobre el uso de Derecho Informático.

Cabe señalar que el Derecho Informático es un punto de inflexión del Derecho, todas las áreas del Derecho se han visto alteradas por la aparición de tecnología y la sociedad de información, los cuales fungen como antecedentes necesarios del Derecho Informático, con el objeto de regular jurídicamente la creación, implementación, desarrollo y problemáticas relacionadas con la tecnología y las telecomunicaciones.

Actualmente, al Derecho Informático no se le ha reconocido su plena autonomía como disciplina, por ser un híbrido que puede ser abordado por otras ramas del Derecho, principalmente el Derecho Penal, Derecho Civil y el Derecho Comercial. Siendo la más contemplada por los juristas y expertos en el tema, la del Derecho Penal, la cual desde esa óptica se estaría afrontando a un reto en cuanto a la sanción y clasificación de los delitos. No obstante, el Derecho aún no prevé

muchos actos o ataques informáticos ilegales como delitos, ni la punibilidad correspondiente a los mismos.

Por lo expuesto, se puede conceptualizar al Derecho Informático como un conjunto de principios y normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma; o bien, como una rama del Derecho especializada en el tema de la informática, sus usos, aplicaciones e implicaciones legales.

1.2 DELITOS CIBERNÉTICOS

Los delitos cibernéticos o delitos informáticos, están considerados hoy en día dentro de la criminalidad transnacional, por su evidente comisión en cualquier lugar y tiempo, a medida que el Internet y la tecnología se vuelven cada vez más accesibles a las personas y se toman pocas o nulas medidas de seguridad, los delincuentes toman mayor ventaja de esto para perfeccionar y actualizar sus técnicas delictivas.

Existe un sin fin de conceptos a nivel mundial sobre el vocablo ciberdelito, cibercrimen o delito informático, de los cuales podemos destacar los siguientes:

Julio Téllez Valdés, define a los delitos informáticos como "…actitudes ilícitas en que se tienen a las computadoras como instrumento o fin" (concepto atípico) o las "conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin…" (concepto típico)".[1]

Luis Miguel Bramont- Arias Torres, indica "… en realidad no existe un bien jurídico protegido en el delito informático, porque en verdad no hay como tal un delito informático. Jurídicos que ya gozan una específica protección por el Derecho Penal". [2]

[1] Tellez Valdez, Julio, Derecho Informático, Universidad Nacional Autónoma de México, 1991, pág. 82.
[2] Bramont- Arias Torres, Luis Alberto, El Delito Informático en el Código Penal Peruano, Fondo Editorial de la Pontificia Universidad Católica del Perú, Lima, 1997, pág. 58.

Julio Núñez Ponce, señala que: “En plano de la dogmática jurídico-penal, la criminalidad informática puede suponer una nueva versión de delitos tradicionales”.[3]

María de la Luz Lima, define el delito electrónico “en un sentido amplio como cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin”.[4]

De las definiciones citadas, se puede precisar que en la actualidad no existe una definición formal y universal de lo que es el delito cibernético o delito informático, por lo cual se han formulado conceptos a lo largo del mundo, respondiendo a las diversas realidades nacionales concretas, ésta no es una labor fácil, dar un concepto sobre este delito emergente, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de “delitos” en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión “delitos cibernéticos” esté plasmada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún, o se encuentran de manera implícita, en la mayoría de las materias.

Para efectos de esta tesis se define como delito cibernético la comisión de conductas delictivas cuyo objetivo es la utilización y aprovechamiento como medio o fin de las Tecnologías de Información y Comunicaciones (TIC), las cuales se traducen en la amenaza globalizada dirigida entre otros temas a:

- Sistemas Financieros.

[3] Núñez Ponce, Julio, Los Delitos Informáticos, en Revista Electrónica de Derecho Informático Nro. 15. http://biblioteca.uca.es/sbuca/bibcjer/detalle_rec.asp?codbib=DER&capbd=9&secbd=2&subbd=0&apabd=0&nombd=REDI.+Revista+Electr%F3nica+de+Derecho+Inform%E1tico&numreg=383

[4] Lima de la Luz, María, Criminalia N°1-6 Año L. Delitos Electrónicos, Ediciones Porrúa, Enero-Julio 1984, pág. 15.

- Bases de Datos.
- Difusión de códigos maliciosos.
- Obtención de secretos Industriales.
- Robo en propiedad intelectual.
- Usurpación de identidad.
- Pornografía Infantil.
- Entre otros.[5*]

El tema relativo a los ciberdelitos, ha captado la atención de diversas organizaciones internacionales, la Organización de las Naciones Unidas (ONU), por mencionar alguna, categorizándolos como delitos emergentes.

Cada cinco años, desde 1955, los encargados de la formulación de políticas y los profesionales que se ocupan de la prevención del delito y la justicia penal se reúnen para celebrar el Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal y colaborar en la elaboración de la agenda y las normas de las Naciones Unidas sobre esos temas.

En el Congreso de Doha de 2015, con el que se celebró el 60° aniversario de los Congresos sobre Prevención del Delito, se examinó el tema de la ciberdelincuencia, desde una óptica de la prevención del delito y la justicia penal en la agenda más amplia de las Naciones Unidas.

El tema general del 13° Congreso fue “La integración de la prevención del delito y la justicia penal en el marco más amplio del programa de las Naciones Unidas para

[5*] Cortés Becerril. José Héctor, Curso de Cibercriminalidad, Instituto Nacional de Ciencias Penales, Ciudad de México, mayo 2016.

abordar los problemas sociales y económicos y promover el estado de derecho a nivel nacional e internacional, así como la participación pública".

Acotando que en dicho Congreso se señaló, respecto al tema de la ciberdelincuencia, lo siguiente:

> Con unos dos mil millones de usuarios en todo el mundo, el ciberespacio es el lugar ideal para los delincuentes, ya que pueden permanecer en el anonimato y tener acceso a todo tipo de información personal que, a sabiendas o inconscientemente, guardamos en línea. Las amenazas a la seguridad en Internet se han disparado de forma espectacular en los últimos años, y el delito cibernético afecta ahora a más de 431 millones de víctimas adultas a nivel mundial.
>
> El delito cibernético existe en muchas formas, siendo los más comunes los relacionados con la identidad. Esto ocurre por *phishing* (engañar a los usuarios de Internet para que den sus datos personales), el *malware* (software instalado involuntariamente que recoge información personal) y *hacking* (acceso ilegal a la computadora de alguien de forma remota). Los delincuentes tienden a utilizar estos métodos para robar información de tarjetas de crédito y dinero. Por otra parte, Internet también se ha convertido en un lugar para los delitos relacionados con los derechos de autor y derechos de propiedad intelectual; y también delitos como la pornografía infantil y material de abuso.
>
> El delito cibernético ha ido creciendo más fácilmente a medida que avanza la tecnología y los autores ya no requieren grandes habilidades o técnicas para ser una amenaza. Por ejemplo, las herramientas de software que permiten al usuario localizar puertos abiertos o anular la protección de contraseña se pueden comprar fácilmente en línea. Lo que no ha crecido fácilmente, por desgracia, es la capacidad para encontrar a los responsables. Con el anonimato que ofrece el ciberespacio, es difícil para las fuerzas del orden identificar y localizar a los delincuentes. Lo que se sabe, sin embargo, es que más de tres cuartas partes de la delincuencia cibernética están hoy vinculadas a la actividad de la delincuencia organizada.

> La delincuencia cibernética ha crecido rápidamente convirtiéndose en un negocio que puede superar $3.000.000.000.000 al año. Sin una normativa adecuada y una capacidad insuficiente en muchos países, la lucha contra la delincuencia cibernética es difícil. Se necesita un esfuerzo mundial para proporcionar una mejor protección y regulaciones más firmes porque los delincuentes cibernéticos hasta ahora se han escondido dentro de vacíos legales en los países con menos reglamentación. Los autores y sus víctimas pueden ser localizados en cualquier lugar, pero los efectos se ven a través de las sociedades, destacando la necesidad de una respuesta internacional urgente y enérgica.[6]

1.3 CRIMINALIDAD INFORMÁTICA

Después de analizar la conceptualización de delito informático o cibernético desde diversas ópticas, resulta viable hablar sobre la criminalidad informática.

Por un lado tenemos el vocablo criminalidad que presenta tres usos, por un lado se llama así al conjunto de características que hacen que una acción sea considerada como criminal, por otro lado la criminalidad como el hecho de cometer crímenes, y por otro lado, se puede referir a la criminalidad como el número proporcional de crímenes en un tiempo y en un lugar determinado.

Por lo que resulta de gran importancia hablar un poco acerca de informática; vocablo que proviene del francés *automatique d'informations*, acuñado por el ingeniero Philippe Dreyfus para su empresa «*Société d'Informatique Appliquée*» en 1962.

Pronto adaptaciones locales del término aparecieron en italiano, español, rumano, portugués y holandés, entre otras lenguas, refiriéndose a la aplicación de las computadoras para almacenar y procesar la información. Es un acrónimo de las palabras *information* y *automatique* (información automática).

[6] 13 Congreso sobre Prevención del Delito y Justicia Penal, Organización de las Naciones Unidas, Doha, 2015, http://www.un.org/es/events/crimecongress2015/about.shtml, fecha de consulta 11 de agosto de 2016.

En lo que hoy día conocemos como informática confluyen muchas de las técnicas, procesos y máquinas (ordenadores) que el hombre ha desarrollado a lo largo de la historia para apoyar y potenciar su capacidad de memoria, de pensamiento y comunicación.

En el Diccionario de la Real Academia Española se define informática como "Conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento automático de la información por medio de computadoras."[7]

El concepto de criminalidad informática abarca una amplia variedad de delitos nuevos delitos y delitos tradicionales que se perfeccionan día con día mediante la implementación de la tecnología y la sociedad de la información. Todos ellos encaminados a la explotación de las redes de información y comunicación, aprovechando las ventajas de la no existencia de barreras geográficas, así como de la circulación de datos intangibles y volátiles de las personas, de las empresas e incluso de los gobiernos.

1.4 CLASIFICACIÓN DE LOS DELITOS CIBERNÉTICOS

En los delitos cibernéticos podemos realizar la clasificación de los mismos a partir de dos criterios; como instrumento o medio y como un fin u objetivo. Esta clasificación ha sido recogida por diversos juristas en sus obras, principalmente el Dr. Julio Alejandro Téllez Valdés.[8]

[7] Diccionario de la Real Academia Española, 2016, http://dle.rae.es/?id=LY8zQy3, fecha de consulta 17 de agosto de 2016.
[8] Cortés Becerril. José Héctor, Curso de Cibercriminalidad, Instituto Nacional de Ciencias Penales, Ciudad de México, mayo 2016.

1.4.1 CLASIFICACIÓN COMO INSTRUMENTO O MEDIO

En cuanto a la clasificación como instrumento o medio, están comprendidas aquellas conductas delictivas que se valen de las TIC's como medio o instrumento para realizar un ilícito, por ejemplo:

1.- Falsificación de documentos utilizando como medio sistemas de cómputo (tarjetas de crédito, cheques).
2.- Fraudes financieros a través de la red.
3.- Publicación de pornografía infantil a través de Internet.
5.- Espionaje a través de redes informáticas y/o telecomunicaciones.
6.- Robo de identidad.
7.- Alteración y robo de sistemas de bases de datos a través de una red informática.[9]

1.4.2 CLASIFICACIÓN COMO FIN U OBJETIVO

En este caso, nos referimos a las conductas criminales que van dirigidas de manera directa contra las TIC's, accesorios o programas como objetivo, como por ejemplo:

1.- Ataques que provocan negación de servicios.
2.- Ataques de bloqueo o *defacement* de páginas web.
3.- Destrucción o robo de los dispositivos que componen un sistema de cómputo o de telecomunicaciones.
4.- Sabotaje de centros de cómputo.[10]

[9] Ídem.
[10] Ídem.

1.5 SUJETOS QUE INTERVIENEN EN LA ACTIVIDAD CRIMINAL CIBERNÉTICA

Desde una óptica criminológica el estudio de los sujetos que intervienen en el ámbito de la cibercriminalidad, resulta de gran interés, la comisión de un acto o conducta criminal cibernética supone la existencia de dos sujetos, por un lado del sujeto activo o delincuente, y por otro, del sujeto pasivo o víctima.

> "De un lado el estudio de los sujetos activos o ciberdelincuentes cuyos perfiles y características resultan claves de cara a una adecuada prevención de los hechos delictivos. Pero igualmente el análisis de las víctimas de la cibercriminalidad; en efecto, distintos posicionamientos victimológicos han analizado el perfil y el papel que ocupa la víctima en la denominada delincuencia tradicional".[11]

1.5.1 SUJETO ACTIVO.

Hoy en día, se puede hablar de una nueva categoría de autores delictivos, ajena a los planteamientos clásicos existentes acerca de los delincuentes tradicionales y sus perfiles, un ciberdelincuente necesita esencialmente tener conocimientos y habilidades de las nuevas tecnologías de la información y comunicación, para llevarlo a cabo, sea como medio o como fin de sus actividades delictivas.

Siendo así, un factor criminógeno esencial en el estudio de los ciberdelitos, entre mayor sea el conocimiento y habilidad del ciberdelincuente, mayor podría ser el daño ocasionado, y mayor la eliminación de indicios para la investigación de la conducta delictiva que lleve a cabo.

[11] De la Cuesta Arzamendi. José Luis y Ana Isabel Pérez Machío, Capítulo III Ciberdelincuentes y Cibervíctimas, s.p.i., pág. 99, http://www.ehu.eus/documents/1736829/2010409/CLC+91+Ciberdelincuentes+y+cibervictimai9, fecha de consulta: 24 de agosto de 2016.

De acuerdo al profesor chileno Mario Garrido Montt, se entiende por sujeto activo o ciberdelincuente:

> Quien realiza toda o una parte de la acción descrita por el tipo penal. Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que "desvía fondos" de las cuentas de sus clientes. [12]

En este sentido, es importante mencionar algunos tipos de delincuentes cibernéticos, así como las actividades que llevan a cabo cada uno de ellos:

- *Hacker.*- Es quien intercepta un sistema informático, como un desafío personal para observar la información almacenada en computadoras pertenecientes a entidades públicas o privadas, son fanáticos de la información digital, generalmente jovenes, se caracterizan por no hacer daño a los sistemas interceptados, sino que lo hacen como reto.

  Cararacterizados por su alta capacidad para la programación creativa, la ingeniería inversa (copiar un programa informático sin tener el diseño) y la propiedad comunitaria del software. Se subdividen en:

[12] Acurio del Pino. Santiago, Delitos Informáticos: Generalidades, s.p.i., pág. 15, http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf, fecha de consulta: 24 de agosto de 2016, 19:41 hrs.

- *Old School hackers.-* dedicados a la producción y distribución de software libre que va desde sistemas operativos completos (Linux) hasta aplicaciones informáticas para diversos propósitos
- *Internet hackers.* - interesados en evaluar aspectos relacionados con las condiciones de seguridad de Internet. Escenarios como la intrusión informática, la evaluación de la seguridad de una red o la detección de un software malicioso son algunos campos de acción de su competencia. En los circuitos de seguridad informática también son conocidos como *white hat hackers* (hackers de sombrero blanco) a fin de diferenciarlos de los *black hat hackers* (hackers de sombrero negro, tambien conocidos como crackers), que buscan causar algun tipo de daño a las redes digitales.

- *Cracker.- Crack* o destructor, sus acciones pueden ir desde simples destrucciones, como el borrado de información hasta el robo de datos sensibles que pueden vender, es decir, presentan dos vertientes, el que se infiltra en un sistema informático y roba información y el que se dedica a desproteger programas.

Subgrupos *Cracker:*

- *Cracker* altamente motivados.- Ellos cuentan con un conocimiento experto en la intrusión informática, una gran cantidad de recursos informáticos y una sólida organización interna, con la cual persiguen fines económicos.

- *Crackers* competentes.- Poseen un conocimiento experto en intrusión informática, peo no cuentan con grandes recursos ni están organizados, usualmente trabajan en pequeños grupos o solos, tienen

como fin la recompensa económica, pero también la personal en el sentido de búsqueda de autosuperación y reconocimiento público.

- *Crackers* novatos (*script kiddies*).- Cuentan con poco conocimiento de las técnicas de intrusión y pocos recursos, principalmente operan en solitario a partir de programas desarrollados por los verdaderos crackers y su objetivo inmediato es obtener cuentas y datos personales de usuarios de Internet con muy poca cultura de seguridad informática.

- *Virii makers* patrióticos, mercenarios y aficionados.- Todos desarrollan virus, los primeros con fines de invasión territorial, los segundos con fines económicos y los últimos para probar su nivel de conocimiento en programación.

- *Warez.*- Están centrados en obtener todo tipo de software comercial para eliminar las protecciones anticopia que traen consigo y, posteriormente distribuirlo de manera gratuita en la red. Hoy en día comparte todo tipo de información: libros, música, revistas, películas, etc.

- *Lammers.*- Hace alusión a una persona falta de habilidades técnicas, sociabilidad o madurez; considerado un incompetente en una materia, actividad específica o dentro de una comunidad, a pesar de llevar suficiente tiempo para aprender sobre la materia, actividad o adaptarse a la comunidad que le considera un *lamme*r. Se trata de una persona que presume de tener unos conocimientos o habilidades que realmente no posee y que no tiene intención de aprender.

- *Virucker.*- Como lo indica la palabra, es un sujeto que crea programas (*malware*) insertándolos en forma dolosa en un sistema, destruye altera, daña o inutiliza un sistema informático, con o sin fines de lucro.

- *Phreacker.- Phreaking* es es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello.

- *Gurus.-* Son los maestros y enseñan a los futuros *Hackers*. Normalmente se trata de personas adultas, me refiero a adultas, porque la mayoría de *Hackers* son personas jóvenes, que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están de alguna forma ahí, para enseñar o sacar de cualquier duda al joven iniciativo al tema. Es como una especie de profesor que tiene a sus espaldas unas cuantas medallitas que lo identifican como el mejor de su serie. El *guru* no está activo, pero absorbe conocimientos ya que sigue practicando, pero para conocimiento propio y solo enseña las técnicas más básicas.

- Bucaneros.- En realidad se trata de comerciantes. Los bucaneros venden los productos crackeados como tarjetas de control de acceso de canales de pago. Por ello, los bucaneros no existen en la Red. Solo se dedican a explotar este tipo de tarjetas para canales de pago que los *Hardware Crackers*, crean. Suelen ser personas sin ningún tipo de conocimientos ni de electrónica o de informática, pero sí de negocios. El bucanero compra al *CopyHacker* y revende el producto bajo un nombre comercial. En realidad es un empresario con mucha afición a ganar dinero rápido y de forma sucia.

- *Newbie.-* Traducción literal de novato. Es alguien que empieza a partir de una WEB basada en *Hacking*. Inicialmente es un novato, no hace nada y aprende lentamente. A veces se introduce en un sistema fácil

y a veces fracasa en el intento, porque ya no se acuerda de ciertos parámetros y entonces tiene que volver a visitar la página *WEB* para seguir las instrucciones de nuevo. Es el típico tipo, simple y nada peligroso.[13]

1.5.2 SUJETO PASIVO

Hoy en día, las personas dotan a los ciberdelincuentes de oportunidades reales, facilitándoles la comisión de todo tipo de conductas cibernéticas delictivas. Un ejemplo claro sería no adoptar sistemas de seguridad o de controles informáticos y dar acceso público a un gran número de trabajadores de una compañía a determinados sistemas operativos, con una misma clave en común, son situaciones que verdaderamente vulneran y revelan la fragilidad de los sistemas informáticos de la actualidad.

En este ejemplo, bastaría con que el o los dueños de la compañía protegieran correctamente su sistema de seguridad, sus redes de información y su sistema operativo; asignando a todos los usuarios del mismo, una clave personal de acceso, con perfiles específicos, y con ello evitar un acceso libre para una pluralidad de personas.

Pero este no es el único tipo de víctimas que se generan en la esfera de la cibercriminalidad, ya que hoy en día numerosos delitos tradicionales se llevan a cabo utilizando como medio comisivo las Tecnologías de la Información y Comunicación, y es ahí donde surge un trabajo titánico por parte de las autoridades encargadas de investigar y sancionar estos delitos.

[13] Cortés Becerril. José Héctor, Curso presencial de Cibercriminalidad, Instituto Nacional de Ciencias Penales, Ciudad de México, mayo 2016.

En este sentido, y tomando en cuenta el continuo y creciente perfeccionamiento delictivo mediante las nuevas tecnologías de la información y la comunicación, es evidente que todas personas, las empresas, instancias públicas, privadas, escuelas, centros comerciales, etcétera. Pueden llegar a ser víctimas de la delincuencia cibernética, sobre todo cuando ellas mismas se colocan en un estado de vulnerabilidad, suministrando toda clase de información personal: ubicación, profesión, círculo social y familiar, estatus socioeconómico, horarios laborares, entre otros; sin ningún tipo de restricción, en aplicaciones y redes sociales.

Por otro lado, la falta de cultura de prevención se refleja incluso en grandes compañías, al tener una misma cuenta de usuario y contraseña para todo el personal, o todas las computadoras de la empresa, sin siquiera imaginarse todos los riesgos que eso implica.

Pero las víctimas de la ciberdelincuencia no sólo se asocian a estos supuestos, ya que hoy en día la gran mayoría de delitos tradicionales se están efectuando mediante el uso de las ya antes mencionadas tecnologías de la información y comunicación, y es ahí donde de manera particular se deben crear estrategias para prevenir la gran diversidad de actividades delictivas.

Dado lo anterior, hasta ahora ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables, sumando a esto la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas a denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionarle a su empresa así

como, las pérdidas económicas, traen como consecuencia que las estadísticas sobre este tipo de conductas se mantenga dentro de la cifra negra.

1.6 TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)

De manera general, las Tecnologías de la Información y la Comunicación (TIC), pueden conceptualizarse como "Dispositivos tecnológicos (hardware y software) que permiten editar, producir, almacenar, intercambiar y transmitir datos entre diferentes sistemas de información que cuentan con protocolos comunes".[14]

Estas aplicaciones, integran medios de informática, telecomunicaciones y redes, posibilitando tanto la comunicación y colaboración interpersonal (persona a persona) como la multidireccional (uno a muchos o muchos a muchos).

Estas herramientas desempeñan un papel medular en estas nuevas generaciones de intercambio, difusión, gestión y acceso al conocimiento, ya que la acelerada innovación e hibridación de estos dispositivos ha incidido en diversos escenarios, como de las relaciones sociales, las estructuras organizacionales, los métodos de enseñanza-aprendizaje, las formas de expresión cultural, los modelos negocios, las políticas públicas nacionales e internacionales, la producción científica, entre otros.

En el contexto de las sociedades del conocimiento, estos medios pueden contribuir al desarrollo educativo, laboral, político, económico, al bienestar social, entre otros ámbitos de la vida diaria, no obstante, se utilizan como medios para llevar a cabo actos delictivos.

Algunas características generales que se pueden señalar sobre las Tecnologías de la Información y la Comunicación son las siguientes:

[14] Cobo Romaní. Juan Cristóbal, El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento, s.p.i., pág. 312, http://www.ehu.eus/zer/hemeroteca/pdfs/zer27-14-cobo.pdf, fecha de consulta: 26 de agosto 2016.

- Son de carácter innovador y creativo, dan acceso a nuevas tendencias de comunicación.
- Favorecen a la educación, la hace más accesible y dinámica.
- Hoy en día son consideradas un tema de debate público y político, su utilización implica un futuro prometedor, están cada vez más inmersas en cualquier ámbito de la vida humana.
- Facilitan la comisión de conductas delictivas tradicionales, como el robo, la estafa o secuestros.

Actualmente no existe una clasificación general de las TIC, las mismas surgen y evolucionan conforme transcurre el tiempo y depende del espacio geográfico del que se esté hablando, algunos estudiosos las reagrupan o clasifican en:

- Redes**:** telefonía, banda ancha, telefonía móvil, redes de televisión, redes en el hogar.
- Terminales: computadora personal, navegador de internet, sistema operativo.
- Servicios: correo electrónico, búsqueda de información, banca en línea, audio y música, TV y cine, comercio electrónico, entre otros.[15]

1.7 PREVENCIÓN DEL DELITO

El concepto de prevención del delito ha pasado por diversas connotaciones a lo largo del tiempo, debido a que cualquier concepto derivado de las ciencias sociales es cambiante de acuerdo a la ubicación geográfica y época de que se trate.

[15] ** Idea sustraída del Blog en línea: Redes, Terminales y Servicios, https://bloginformaticasaia.wordpress.com/2014/12/02/redes-terminales-y-servicios/ fecha de consulta 29 de agosto 2016, 17:10 hrs.

Por ejemplo, a principios del siglo XX hablar de prevención del delito era hablar de "represión del delito a través de la justicia penal, donde los castigos o sanciones eran el instrumento para inhibir los actos delictivos".[16]

Así que los países adoptaron estrategias de represión que incluían fuertes castigos y maltratos físicos hacia los delincuentes, los cuales solo consiguieron llenar las cárceles y generarle altos costos al Estado, por la gran cantidad de población privada de su libertad. Dicha represión era aplicada también a los menores de edad que seguían el mismo proceso que los adultos.

Posteriormente, la Organización de las Naciones Unidas (ONU) decidió protagonizar desde 1955 hasta la fecha, la labor de promover la importancia de prevenir los orígenes de la problemática delictiva en el mundo, mediante planes y estrategias novedosas, evitando así la represión y los tratos inhumanos.

Siendo los Congresos y sus principales enfoques los siguientes:

- 1955. En el Primer Congreso se aprobaron las Reglas mínimas para el tratamiento de los reclusos.
- 1960. En el Segundo Congreso se recomendaron servicios especiales de policía para la justicia de menores.
- 1965. En el Tercer Congreso se analizó la relación entre la delincuencia y la evolución social.
- 1970. En el Cuarto Congreso se exhortó a que se mejorara la planificación de la prevención del delito para el desarrollo económico y social.
- 1975. En el Quinto Congreso se aprobó la Declaración sobre la Protección de Todas las Personas contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes.
- 1980. En el marco del tema "La prevención del delito y la calidad de la vida", en el Sexto Congreso se reconoció que la prevención del delito debía basarse en las circunstancias sociales, culturales, políticas y económicas de los países.

[16] REINTEGRA, Modelo para la Prevención Social del Delito con los Adolescentes y Jóvenes en Contexto Comunitarios, Ediciones REINTEGRA, México, 2011, Pág. 17.

- 1985. En el Séptimo Congreso se aprobó el Plan de Acción de Milán y varías reglas y normas nuevas de las Naciones Unidas, en el marco del tema “Prevención del delito para la libertad, la justicia, la paz y el desarrollo”.
- 1990. En el Octavo Congreso se recomendó la adopción de medidas contra la delincuencia organizada y el terrorismo, en el marco del tema “La cooperación internacional en materia de prevención del delito y justicia penal en el siglo XXI.”
- 1995. En el Noveno Congreso de las deliberaciones se centraron en la cooperación internacional y en la asistencia técnica de carácter práctico para fortalecer el estado de derecho, en el marco del tema “Menos crimen, más justicia: seguridad para todos.”
- 2000. En el Décimo Congreso se aprobó la Declaración de Viena en la que los Estados Miembros se comprometieron fortalecer la cooperación internacional en la lucha contra la delincuencia transnacional y la reforma penal.
- 2005. En el Onceavo Congreso se aprobó la declaración de Bangkok, un documento político crucial en el que se establecen los fundamentos de la coordinación y cooperación internacionales con miras a prevenir y combatir la delincuencia y se imparten directrices para fortalecer esa coordinación y cooperación.
- 2010. En el Doceavo Congreso se aprobó la Declaración de Salvador sobre estrategias amplias ante problemas globales: los sistemas de prevención de delito y justicia penal y su desarrollo en un mundo en evolución.[17]

En el Treceavo Congreso, celebrado en el año 2015, se habló particularmente de un tema relacionado con el presente trabajo de investigación, es decir, sobre la prevención de los delitos cibernéticos. La ONU comentó sobre la importancia de convertir los avances económicos, sociales y tecnológicos en un factor positivo para prevenir y combatir las nuevas formas de la criminalidad transnacional.

> Estudiar medidas concretas destinadas a crear un entorno cibernético seguro y resistente; prevenir y combatir las actividades delictivas realizadas por Internet, prestando especial atención a la detección del robo, la captación de personas con fines

[17] UNODC Oficina de las Naciones Unidas contra la Droga y el DELITO. (2010). Congreso de las Naciones Unidas sobre prevención del delito y justicia penal 1955-2010. 55 años de logros. Austria: *United Nations Information Service*. EN: Ibídem, Pág. 18.

> de trata y la protección de los niños contra la explotación y los abusos a través de Internet; reforzar la cooperación entre los organismos de aplicación de la ley en los planos nacional e internacional, incluso para identificar y proteger a las víctimas, entre otras cosas eliminando de Internet todo contenido pornográfico en que aparezcan menores, en particular imágenes de abusos sexuales contra niños; aumentar la seguridad de las redes informáticas y proteger la integridad de la infraestructura correspondiente, y procurar prestar asistencia técnica a largo plazo y crear capacidad a fin de que las autoridades nacionales puedan combatir con más eficacia la delincuencia cibernética, incluso mediante la prevención, la detección, la investigación y el enjuiciamiento de esos delitos en todas sus formas. Además, observamos las actividades del grupo intergubernamental de expertos de composición abierta encargado de realizar un estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, e invitamos a la Comisión de Prevención del Delito y Justicia Penal a que estudie la posibilidad de recomendar que el grupo de expertos, basándose en su propia labor, siga intercambiando información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales respuestas y proponer nuevas respuestas jurídicas o de otra índole frente al delito cibernético a nivel nacional e internacional.[18]

Con lo anterior se da un panorama claro del trabajo que ha venido desarrollando la ONU, en el tema de prevención del delito, así como la gran gama de aristas que deben ser consideradas en las políticas públicas de los países, las cuales no se limitan la justicia penal.

Ahora, para entender lo que es la prevención del delito, primero hay que entender que es prevenir y que es delito.

De acuerdo a diversos autores, diccionarios, enciclopedias y otras fuentes de consulta, prevenir es adelantarse, o anticiparse a algo, es decir que la prevención

[18] Naciones Unidas, Declaración de Doha sobre la integración de la prevención del delito y la justicia penal en el marco más amplio del programa de las Naciones Unidas para abordar los problemas sociales y económicos y promover el estado de derecho a nivel nacional e internacional, así como la participación pública, 13° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Doha, 2015, pág. 11.

es emplear las medidas necesarias para evitar que se presente o se realice un hecho futuro.

Por otro lado, delito en sentido dogmático es toda conducta ya sea de acción, omisión o comisión por omisión descrita en la ley, contraria a Derecho, es decir de naturaleza antijurídica y por tanto esa conducta típica debe ser sancionada por la autoridad.

Bajo este contexto, el Código Penal Federal define en su artículo séptimo como delito "es el acto u omisión que sancionan las leyes penales".[19]

Asimismo, el Código Penal del Distrito Federal en su artículo décimo quinto, establece que el delito "sólo puede ser realizado por acción o por omisión"[20] y, el Código Penal del Estado de México señala que el delito "es la conducta típica, antijurídica, culpable y punible".[21]

Es con ello que se entiende como prevención del delito la función del Derecho Penal moderno de emplear todas las acciones y medidas necesarias tendientes a evitar que se produzcan conductas delictivas dentro de una comunidad o grupo social.

Siguiendo con la definición y las características de la prevención del delito, es importante señalar que ésta "se ha contemplado desde diferentes puntos de vista, así los dos aspectos formales son la prevención general y la prevención especial, aplicables muy claramente a las funciones del derecho penal en general".[22]

A continuación se citan algunas de las razones por las que es de suma importancia aplicar diversas medidas de prevención del delito:

---

[19] Código Penal Federal, versión en línea, última reforma 18 de julio 2016, http://www.diputados.gob.mx/LeyesBiblio/pdf/9_180716.pdf, fecha de consulta 15 de marzo, 2017.
[20] Código Penal del Distrito Federal, versión en línea, última reforma 16 de junio 2016, http://www.aldf.gob.mx/archivo-d261f65641c3fc71b354aaf862b9953a.pdf , fecha de consulta 15 de marzo, 2017.
[21] Código Penal del Estado de México, versión en línea, http://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/cod/vig/codvig006.pdf, fecha de consulta 15 de marzo, 2017.
[22] Mendoza Bremauntz, Emma Carmen, Derecho Penitenciario, Mc Graw-Hill, México, 1998, Pág. 15

a) El incremento de la delincuencia en general.
b) El incremento de menores de edad que inciden en actividades delictivas o conductas violentas.
c) Los daños que se provocan en las víctimas de un delito.
d) Los daños que se ocasionan a la sociedad por el alto índice de comisión de delitos.
e) Los gastos y costos que la delincuencia genera al Estado y a la sociedad.
f) El fracaso del sistema penitenciario actual, al no lograr una correcta reinserción de las personas cuando salen de prisión.
g) El fracaso de las penas tradicionales.
h) El escaso personal investigador especializado en prevención del delito.

Bajo este orden de ideas, la forma más sencilla de clasificar las acciones encaminadas a la prevención del delito podría ser la siguiente:

Epidemiológicamente, la prevención se clasifica en:

- Primaria: tiene como objetivo a la población en general y entornos físicos.
- Secundaria: se centra en la población en riesgo de delinquir o ser víctimas.
- Terciaria: su objetivo son los sujetos, los delincuentes y las víctimas.

Bajo una visión sociológica, la prevención se clasifica en:

- Situacional: actúa sobre las situaciones predelictuales y en ocasiones abarca la administración, diseño y manipulación del entorno físico a modo de reducir las oportunidades para la comisión de delitos así como el control de instrumentos y objetos que puedan servir para la comisión de delitos.
- Social: actúa sobre infractores potenciales y sus disposiciones, a través de procesos sociales. Las medidas de este tipo se dirigen a la población escolar y grupos juveniles, creando principalmente oportunidades de estudio y de empleo.
- Comunitaria o mixta: combina tanto las medidas situacionales como las sociopreventivas.[23]

[23]Chipix Notz, Edwin, Prevención del Delito, http://www.policiasysociedad.org/userfiles/CHAT%20PREVEN%20DEL%20DELITO.pdf, archivo pdf, fecha de consulta: 5 de septiembre 2016, 11:12 am.

1.7.1 PREVENCIÓN GENERAL

De manera sencilla, la prevención general se entiende como la amenaza penal dirigida al conjunto de personas pertenecientes a una sociedad.

En sentido negativo según Von Feuerbach "la prevención del delito se establece mediante la amenaza de una sanción en caso de incumplimiento de las normas jurídicas que rigen a un grupo social".[24] Es decir la implantación del miedo en una población con el fin de evitar que dichas personas cometan actos delictivos.

En un sentido positivo por el contraste, Jakobs dice que se "busca prevenir los delitos de forma general mediante la asimilación y convicción de los miembros de una sociedad a acatar y no violentar lo establecido en su normatividad jurídica".[25]

1.7.2 PREVENCIÓN ESPECIAL

En otro contexto de la prevención del delito se puede hablar acerca de la prevención especial, la cual se refiere a la que está dirigida a la persona que ha cometido un delito y con la cual se pretende que tal persona no vuelva a cometer actos delictivos futuros.

Por tanto, esta prevención no va dirigida a toda la población de una sociedad, sino única y exclusivamente a aquellos que han vulnerado el ordenamiento jurídico previamente.

1.7.3 PREVENCIÓN SOCIAL

"El enfoque "social" (intervenciones no penales sobre delincuentes potenciales orientadas a atenuar su propensión criminal) está basado en las teorías etiológicas

[24] Villanueva Cabello Belinda Shaloom Peniel, Tesis de Licenciatura Nueva Política Criminológica de Prevención Social para Adolescentes que Inciden en Actividades o Conductas Violentas. México, 2013, pág. 12.
[25] Ídem.

del delito, según las cuales, la acción criminal se explica por la existencia de diversos factores anteriores a su perpetración".[26]

Dicha prevención solo puede presentar resultados a mediano y a largo plazo y todo depende de la responsabilidad social con la que se actúe.

Para complementar dicha idea la Ley General para la Prevención Social de la Violencia y la Delincuencia, en su artículo 2 señala que *la prevención social de la violencia y la delincuencia es el conjunto de políticas públicas, programas y acciones orientadas a reducir factores de riesgo que favorezcan la generación de violencia y delincuencia, así como a combatir las distintas causas y factores que la generan.*[27]

Dicho lo anterior se puede entender que la prevención social del delito es una pluralidad de acciones sociales encaminadas a la reducción e inhibición de actos delictivos que se presentan día a día en una sociedad.

Esta prevención destaca porque es 'concebida no como la función del derecho penal, sino como una práctica y una política desarrollada mediante estrategias específicas que pueden observarse desde los contextos sociales, culturales o económicos y que se planean y coordinan reviviendo y estimulando el interés de la comunidad […]' [28]

1.8 CIBERSEGURIDAD

Como se ha mencionado, el desarrollo de las Tecnologías de Información y Comunicación (TIC) ha generado una nueva forma de interacción a nivel mundial

[26] Peñaloza. Pedro José. Prevención Social del Delito: "Asignatura Pendiente", Porrúa, Tercera Edición, México, 2006, pág. 129.
[27] LEY GENERAL PARA LA PREVENCIÓN SOCIAL DE LA VIOLENCIA Y LA DELINCUENCIA, http://www.sep.gob.mx/work/models/sep1/Resource/f74e29b1-4965-4454-b31a-9575a302e5dd/ley_general_preven_soc_violencia.pdf, publicada en el Diario Oficial de la Federación el 24 de enero de 2012, fecha de consulta: 21 de agosto de 2016, 6:56 pm.
[28] John Graham, Crime Prevention Strategies in Europe and North America, HEUNI, Helsinki Institute for Crime Prevention and Control affilliated with United Natios, Finlandia, 1990, passim. EN: Mendoza Bremauntz, op. cit., Pág. 17.

en la que la rapidez y facilidad de los intercambios de información y comunicaciones han eliminado las barreras de distancia y tiempo.

Es decir, el llamado ciberespacio (nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información, incluida Internet, las redes y los sistemas de información y de telecomunicaciones), ha venido a quitar fronteras, haciendo partícipes a todos sus usuarios, dentro de esta globalización sin precedentes que propicia nuevas oportunidades, a la vez que comporta nuevos retos, riesgos y amenazas.

Por otro lado, es importante señalar que actualmente no hay una definición unánime de lo que es ciberseguridad, no obstante, es evidente que se trata de una condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas.

Los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, como el conjunto de políticas y técnicas destinadas a lograr dicha condición, pese a las medidas más drásticas y radicales de seguridad que se pueden tomar en este ámbito, siempre habrá, al menos, un grado mínimo de riesgo, todos los días surgen nuevas formas de llevar a cabo algún delito cibernético.

La ciberseguridad, como seguridad de la información tiene tres principios básicos, siendo estos: la confidencialidad, la integridad y la disponibilidad de la información, conocidos como CIA, por los vocablos en inglés *confidentiality, integrity y availability.*

> Como confidencial podemos entender que es la propiedad con la que cuenta la información que no se encuentre a disposición de cualquier persona o sea divulgada. La integridad puede ser definida la propiedad de conservar la exactitud y la complejidad

de los activos de información. Mientras que por disponibilidad entendemos que es la propiedad de ser accesibles y utilizables ante cualquier persona que los solicite.[29]

Actualmente, el manejo de casi toda la información existente en los diversos ámbitos sociales a nivel mundial, se maneja mediante la tecnología y en muchas ocasiones la información es o debería ser confidencial, por lo que al ser divulgada, mal utilizada, robada, borrada o saboteada, afecta su disponibilidad y la pone en riesgo.

Dentro de este controversial concepto de ciberseguridad o seguridad de la información existen dos vocablos muy importantes que son: riesgo y seguridad.

Riesgo: Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione.

Seguridad: Es una forma de protección contra los riesgos.

La ciberseguridad tiene como finalidad principal proteger la confidencialidad, integridad y disponibilidad de la información, involucrando la implementación de estrategias que cubran los procesos en donde la información es el activo medular.

Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas (peligro inminente), que puedan explotar vulnerabilidades y que pongan en riesgo tanto información como los sistemas que la almacenan y administran.

[29] Blog especializado en sistemas de gestión de seguridad de la información, iso 27001: Los Aspectos Básicos en la Ciberseguridad, http://www.pmg-ssi.com/2015/03/iso-27001-los-aspectos-basicos-en-la-ciberseguridad/, fecha de consulta 02 de septiembre de 2016, 18:12 hrs.

La ciberseguridad busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, siendo ésta un proceso continuo que se debe operar conociendo siempre las vulnerabilidades y las amenazas que atentan contra cualquier información que se encuentre almacenada y procesada mediante las TIC.

Finalmente, la importancia de la ciberseguridad radica en la rápida evolución del entorno técnico la cual requiere que tanto las organizaciones públicas como privadas, la sociedad civil, y los particulares adopten un conjunto mínimo de controles de seguridad para proteger su información y sistemas de información.

CAPÍTULO II. CIBERSEGURIDAD, ¿ESTAMOS PREPARADOS EN AMÉRICA LATINA Y EL CARIBE? INFORME CIBERSEGURIDAD 2016. ELABORADO POR LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS Y EL BANCO INTERAMERICANO DE DESARROLLO

2.1 EJES DE ESTUDIO

Desde varios años la Organización de los Estados Americanos (OEA), así como el Banco Interamericano de Desarrollo (BID) han realizado esfuerzos conjuntos a fin de brindar propuestas novedosas y eficaces a los Estados de América Latina y el Caribe en materia de ciberseguridad.

El informe más reciente es el del año 2016, en cual la OEA y el BID presentan una imagen completa y actualizada del estado de la seguridad cibernética de los países de América Latina y el Caribe.

Definitivamente los mejores estudios sobre algún fenómeno social, deben ser integrales y abarcar diversos enfoques o áreas de impacto de los mismos. En este caso, el Informe 2016, sustrajo aportaciones de las agencias gubernamentales de los países de las regiones analizadas, así como, de operadores de infraestructuras críticas, de las fuerzas militares, la policía, el sector privado, la sociedad civil y la academia.

De manera general, este informe consta de dos secciones principales; la primera sobre “Contribuciones de expertos”, que consta de ensayos sobre las tendencias actuales de la seguridad cibernética en la región.

La segunda sección, versa sobre el “Reporte de países”, aportando una visión general del estado actual de la seguridad cibernética en los países de la región sobre la base de la información obtenida a través de una herramienta en línea diseñada por la Universidad de Oxford, de entrevistas con funcionarios de los Estados Miembros y la investigación documental.

Los datos recogidos fueron agrupados en cinco dimensiones: 1) Política; 2) Sociedad; 3) Educación; 4) Legislación; y 5) Tecnología. Asimismo, cada dimensión se clasificó en cinco niveles de madurez: 1) Inicial; 2) Formativa; 3) Establecida; 4) Estratégica; y 5) Dinámica.

Este documento tiene la intención de generar una visión integral de la ciberseguridad en la región, incitando a las autoridades gubernamentales de las regiones estudiadas a utilizar esta información para comprender mejor la situación de la seguridad cibernética de su país en un contexto regional, ya que los resultados representados se pueden utilizar como punto de referencia a medida que los países continúen desarrollando sus capacidades de ciberseguridad.

2.2 APORTACIONES DE EXPERTOS

De acuerdo con la visión de los expertos involucrados en la elaboración de este informe, la maximización del valor de la Internet y el ciberespacio debe ser una parte central de la planeación de los gobiernos a nivel global, ya que las tecnologías de Internet aún no están maduras y eso las vuelve vulnerables a diversos riesgos.

Por ejemplo, hoy en día los delincuentes se han dado cuenta que pueden explotar fácilmente la inmensa gama de tecnologías de la información y la comunicación, y

a pesar de que este riesgo es manejable, requiere de la atención de los líderes nacionales.

Desde hace ya varios años, se ha generado un gran debate internacional sobre la importancia de la seguridad cibernética de las nuevas generaciones, lo que ha despertado el deseo de las naciones a reforzar la estabilidad y la seguridad de los recursos mundiales cibernéticos.

Según los expertos, la comunidad internacional se ha centrado en los temas de las normas de seguridad cibernética, las medidas de generación de confianza y la creación de capacidades. Cada uno se analizará en el capítulo siguiente.

Dentro de la agenda internacional para la seguridad cibernética merecen especial atención cuatro grupos de discusión. Se trata del Grupo de Expertos Gubernamentales de las Naciones Unidas (GEG), la Organización para la Seguridad y la Cooperación en Europa (OSCE), el Foro Regional de la Asociación de Naciones del Sureste Asiático (ASEAN, por sus siglas en inglés), y la OEA.

Se han realizado un total de cuatro reuniones, la última en la Haya, con el objetivo de generar un consenso sobre un comportamiento responsable en el ciberespacio, el principal logro es la creación del “Foro Mundial sobre Experticia Cibernética”. La OEA es el fundador.

El Foro facilitará el intercambio de experiencias, conocimientos y buenas prácticas entre los responsables políticos y expertos cibernéticos de diferentes países y regiones.

Otro aspecto a señalar por parte de los expertos, es que en América Latina y el Caribe, como en todas las regiones, los esfuerzos para lograr la estabilidad y la seguridad del ciberespacio están en una etapa inmadura, temprana, en consecuencia los principales desafíos de la región de América Latina y el Caribe en seguridad cibernética son el desarrollo de capacidades en todos los países, la mejora de la cooperación en delitos cibernéticos y el intercambio de información sobre mejores prácticas, amenazas y vulnerabilidades.

Para hacer frente a los desafíos que vulneran la esfera de la ciberseguridad, se requiere de esfuerzos diplomáticos y la cooperación internacional, por la naturaleza de la cibercriminalidad, ninguna nación por sí sola puede asegurar adecuadamente sus redes. “Esto hace que las gestiones regionales sean aún más importantes, especialmente teniendo en cuenta los vínculos entre la seguridad cibernética, el desarrollo y el crecimiento económico”.[30]

Las economías nacionales conectadas a la Internet global y que saben sacar ventaja del servicio de Internet crecen más rápidamente y se van enriqueciendo, razón por la cual garantizar la seguridad cibernética les ayuda a aprovechar al máximo este tipo de oportunidades.

Así, es útil considerar medidas complementarias enfocadas en cuatro ópticas, y no solo en el deber ser de los gobiernos, sino también a la comunidad académica, empresarial y social. En primer lugar, todos los gobiernos al menos de la región de América Latina y el Caribe deben perfilarse y crear una base jurídica armonizada para que atienda a los delitos cibernéticos, ya que los países que regulan estos delitos lo hacen de manera escasa e insuficiente, en consecuencia sufren mayores pérdidas económicas.

[30] Banco Interamericano de Desarrollo, Organización de los Estamos Americanos, Ciberseguridad. ¿Estamos Preparados en América Latina y el Caribe?, Informe Ciberseguridad 2016, file:///C:/Users/shaloom/Downloads/Ciberseguridad-Estamos-preparados-en-America-Latina-y-el-Caribe%20(4).pdf, fecha de consulta 21 de enero 2017.

En segundo lugar, es convincente seguir trabajando para llegar a un entendimiento homologado sobre las infraestructuras críticas y vulnerabilidades, incluyendo una definición única de infraestructuras cruciales.

En tercer lugar, resultaría benéfico contar con un enfoque regional más formal para la generación de confianza, el cual incluye un intercambio de documentos nacionales de políticas y leyes, reuniones periódicas entre diversos funcionarios, para discutir temas como: la estabilidad, comercio y seguridad y el fortalecimiento de redes de cooperación de autoridades responsables con disposición para brindar asistencia en caso de una emergencia.

Finalmente, una cuarta óptica, sería la formulación continua de estrategias nacionales de seguridad cibernética.

2.2.1 EL ESTADO ACTUAL DE LA LEGISLACIÓN SOBRE EL DELITO CIBERNÉTICO EN AMÉRICA LATINA Y EL CARIBE: ALGUNAS OBSERVACIONES

Los expertos señalan que la efectividad de la justicia penal es parte esencial de una estrategia adecuada de seguridad cibernética. Esto abarca la investigación, la fiscalización y la adjudicación de delitos en contra y por medio de datos y sistemas informáticos, de igual modo el obtener evidencia electrónica vinculada con cualquier hecho criminal, con fines del proceso penal.

Como es sabido, el delito cibernético tiene en sí mismo una naturaleza transnacional y la evidencia electrónica tiene una particular volatilidad, lo cual implica que la justicia penal será efectiva con una óptima cooperación internacional.

En este sentido, así como una correcta estrategia de ciberseguridad debe ser integral, de igual modo la legislación lo debe ser, ya que incluye el derecho sustantivo (la conducta a ser definida como delito) y el derecho procesal (los poderes investigativos para la aplicación de la ley).

Tal legislación debe cumplir con varios requisitos, entre éstos los expertos señalan los siguientes:

> Debe ser lo suficientemente neutral (tecnológicamente) como para responder a la evolución constante del crimen y la tecnología, ya que de no ser así corre el peligro de volverse obsoleta para cuando entre en vigor.
>
> Los poderes para la aplicación de la ley deben estar sujetos a salvaguardias con el fin de garantizar el cumplimiento de los requerimientos del Estado de derecho y de los derechos humanos.
>
> Debe operar con suficiente armonía o por lo menos ser compatible con las leyes de otros países para permitir la cooperación internacional; por ejemplo, el cumplimiento con la condición de la doble criminalidad. [31]

De acuerdo con la visión de los expertos, a través del Convenio de Budapest sobre el Delito Cibernético existe una vertiente internacional, utilizada ampliamente en América, que ha permitido y contribuido con los países a cumplir estos requerimientos.

Es indispensable, a criterio de los expertos que las partes penalicen el acceso ilícito, la interceptación ilegal, la interferencia de datos y de sistemas, así como el uso indebido de aparatos, la falsificación informática, el fraude informático, la pornografía infantil, entre otros delitos relativos a las infracciones en materia de derechos de autor y derechos vinculados.

[31] Ibídem, pág. 19.

Después de quince años de su adopción, las disposiciones establecidas en el convenio de Budapest, en relación con el delito cibernético siguen vigentes, pues en esencia fueron formuladas de manera neutral desde el punto de vista tecnológico.

Este documento comprende una diversidad de poderes específicos de Derecho Procesal, por ejemplo, órdenes para la búsqueda, captura, producción de datos o la interceptación de comunicaciones, además del poder para requerir la conservación de datos, como la evidencia electrónica relacionada con cualquier tipo de delito.

Este tratado busca garantizar la efectiva cooperación internacional en materia de la cibercriminalidad y evidencia electrónica, mediante la combinación de la asistencia legal mutua. El alcance de la cooperación no se limita al tipo de delito cibernético, sino que incluye la cooperación referente a la evidencia electrónica que se encuentre en un sistema informático derivado de la comisión de cualquier delito.

Hoy en día el Convenio de Budapest sigue abierto a la adhesión de cualquier Estado que esté preparado para implementar sus preceptos y varios países de América Latina y el Caribe han decidido seguir este camino y aunque varios ya lo han hecho, hasta el día de hoy México no lo ha hecho.

Considero que México debe adherirse a este convenio, a fin de fortalecer la cooperación internacional en la investigación de los delitos cibernéticos y armonizar un marco jurídico, en virtud de combatir de manera eficiente y eficaz estos delitos.

2.2.2 ECONOMÍA DIGITAL Y SEGURIDAD EN AMÉRICA LATINA Y EL CARIBE

Otro aspecto analizado por los expertos, fue lo referente a la economía digital vinculada con la seguridad cibernética en la región.

Como es sabido, en pocas décadas, Internet, también conocido como el ciberespacio, está presente en casi todos los aspectos de nuestra vida cotidiana, y por ende los riesgos cibernéticos a los que los que nos enfrentamos son cada vez más preocupantes y se están convirtiendo en un factor de mayores consideraciones en seguridad y formulación de políticas económicas.

La conciencia de seguridad cibernética ha ido creciendo a medida que se ha aceptado que tanto las amenazas como las vulnerabilidades tienen el potencial de detener la innovación y el crecimiento de la economía basada en Internet, y a su vez ponen en riesgo a las personas e instituciones públicas como privadas.

Los expertos señalan, que la mayoría de los países de América Latina y el Caribe reconocen la necesidad de contar con una estrategia de seguridad cibernética, pero muy pocos han dado un paso más allá de simplemente contar con un esquema.

En términos generales, sólo los países más grandes y más ricos de la región cuentan con distintas organizaciones dedicadas a la seguridad cibernética y falta una coordinación entre los sectores y organismos pero de los distintos Estados.

Incluso se afirma que el sector privado ha superado al sector público, según los expertos, parte del problema con respecto a la escasez de concienciación sobre la importancia de la ciberseguridad se deriva de la falta de infraestructura educativa en seguridad cibernética.

Por ejemplo, los expertos señalan que solo pocos países ofrecen programas educativos a nivel posgrado para la seguridad cibernética, y los que existen tienen deficiencias en cuanto a calidad. Es por ello que la diversidad de problemas que enfrentan la seguridad cibernética y la economía digital requieren un conjunto de respuestas innovadoras.

En este sentido, se afirma que ningún país, ya sea grande o pequeño, está inmune a los ataques cibernéticos, dentro del paisaje tecnológico en que se ve inmerso y está en constante evolución.

2.2.3 DESARROLLO SOSTENIBLE Y SEGURO: UN MARCO PARA LAS SOCIEDADES CONECTADAS RESILIENTES

Otro punto medular a tratar por los expertos en el informe, fue la cuestión vinculada al desarrollo sostenible y seguro de las tecnologías de la información y la comunicación (TIC), ya que la penetración de Internet y la adopción de estás impactan de manera global en las economías, los gobiernos y las sociedades.

Por ejemplo: la forma como se producen, distribuyen y consumen los bienes y servicios, o cómo los gobiernos prestan servicios y comparten información, hasta cómo las compañías y los ciudadanos interactúan y participan en el entorno social.

Actualmente muchas oportunidades se asocian con estar conectados y participando en la economía de Internet y el potencial impacto económico. Los expertos afirman que dos tercios de los usuarios de Internet viven en el mundo en desarrollo y están impulsando la mayor parte del crecimiento económico mundial.

Tanto la penetración de las TIC como del aumento de la conectividad, significa abrir nuevas oportunidades económicas y sociales para las poblaciones urbanas y rurales se han convertido en la plataforma de distribución más grande para la prestación de servicios públicos y privados, incluyendo los servicios bancarios, la educación y la atención en salud a millones de personas desatendidas .

Al provechar los beneficios derivados de la utilización de las TIC se estimula el crecimiento económico, mejora la prestación y la capacidad de servicios, impulsa las ganancias de la productividad y la innovación para promover el buen gobierno.

Buen gobierno, refiriéndose a que existe una agenda digital y una visión económica que promete generar tanto ingresos como empleos, así como proporcionar acceso a la información, aumentar la productividad y la eficiencia, así como permitir el aprendizaje electrónico para mejorar las habilidades de la fuerza laboral, facilitar las actividades del gobierno.

Por otro lado, en lo que respecta al tema de seguridad digital, la OEA y el BID han centrado muchos de sus esfuerzos en la creación y generación de una cultura de seguridad cibernética en la región y se han comprometido a trabajar con sus Estados Miembro para luchar contra la delincuencia cibernética, fortalecer la resiliencia cibernética y promover estrategias sostenibles de desarrollo de las TIC.

Principalmente, apoyando y fortaleciendo las estrategias de seguridad cibernética de los países de América Latina y el Caribe, y con ello prevenir y reaccionar ante las nuevas amenazas cibernéticas. Desafortunadamente, los expertos señalan que la mayoría de las naciones aún les falta hacer eso y si los países no invierten por igual en la seguridad de su infraestructura básica y la resiliencia de sus sistemas, su crecimiento económico se mermará.

El punto medular de este rubro, es general la estrategia idónea para aprovechar el poder económico de las TIC y al mismo tiempo evitar daños irreversibles a largo plazo a la economía, salud, seguridad y garantizando la resiliencia de sus países cuando la seguridad juega un papel igualmente importante dentro de esta estrategias de desarrollo.

Después pueden aprovechar las políticas, leyes, reglamentos, normas, incentivos de mercado y otras iniciativas para proteger el valor de sus inversiones digitales y preservar la seguridad de su conectividad. Pueden perseguir y financiar iniciativas de seguridad cibernética que disminuyen los riesgos y aumentan la resiliencia.

Los expertos señalan que adoptar un marco de seguridad y conocer el nivel de preparación cibernética de un país es ciertamente esencial y que el primer paso será articular una estrategia nacional de seguridad cibernética válida.

En términos generales. “la estrategia debe: describir el problema en términos económicos; identificar la autoridad competente que garantice la correcta ejecución de la estrategia; incluir objetivos específicos, medibles, alcanzables, basados en el tiempo y en los resultados del plan de implementación; y reconocer la necesidad de comprometer recursos limitados (por ejemplo, voluntad política, dinero, tiempo y personas) en un entorno competitivo para lograr los resultados económicos necesarios”.[32]

Otro elemento esencial señalado, son la posibilidad de los países de establecer y mantener tanto una capacidad nacional de respuesta a incidentes como un mecanismo de intercambio de información que permita la interacción entre la inteligencia procesable el gobierno y la industria.

[32] Ibídem pág. 33.

Muchos países de América Latina y el Caribe ya han establecido y puesto en funcionamiento los Equipos de Respuesta ante Emergencias Informáticas (CSIRT, por sus siglas en inglés) con capacidades y funciones reactivas, que incluyen servicios proactivos, preventivos, educativos y de gestión de la seguridad.

2.3 MARCO METODOLÓGICO

A partir del informe generado por el BID y la OEA, después de una amplia consulta a 200 expertos internacionales algunos del gobierno, otros de la academia, la industria y la comunidad técnica, la Profesora Sadie Creese, del Centro Global de Capacidad sobre Seguridad Cibernética de la Universidad de Oxford, señaló que ese Centro elaboró un modelo para entender la madurez de las capacidades de seguridad cibernética.

> El Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM, por sus siglas en inglés) toma en cuenta las consideraciones de seguridad cibernética a través de cinco diferentes áreas/ dimensiones de la capacidad, entendiendo que cada dimensión no es necesariamente independiente de las otras. Las cinco dimensiones son: Políticas y estrategia nacional de seguridad cibernética; Cultura cibernética y sociedad; Educación, formación y competencias en seguridad cibernética; Marco jurídico y reglamentario; y Normas, organización y tecnologías. Cada dimensión ofrece una serie de factores e indicadores de capacidad cibernética para que una nación comprenda la etapa de madurez en cada consideración específica. Se han identificado cinco etapas de madurez y estas varían desde una etapa inicial, en la cual una nación puede que haya apenas comenzado a considerar la seguridad cibernética, hasta un escenario dinámico, en el cual una nación es capaz de adaptarse rápidamente a los cambios en el panorama de la seguridad cibernética en relación a las amenazas, las vulnerabilidades, los riesgos, la estrategia económica o el cambio de las necesidades internacionales.[33]

[33] Ibídem, pág. 39.

Como se mencionó, el aumento de las tasas de penetración de Internet y la falta de capacidad de la seguridad cibernética preocupa a los gobiernos y a los interesados de la industria, y lo han vuelto una prioridad nacional.

A través del apoyo del BID y la OEA, la región de América Latina y el Caribe es la primera en el mundo en realizar un estudio para comprender de la capacidad de la seguridad cibernética en una región entera utilizando el modelo CMM.

> Los datos utilizados para este informe se recogieron a través de una encuesta en línea desarrollada en colaboración con el Centro Global de Capacidad sobre Seguridad Cibernética (GCSCC) sobre la base del Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM, por sus siglas en inglés) desarrollado por el GCSCC. La encuesta en línea fue traducida en dos idiomas (inglés y español) y se puso a prueba inicialmente con visitas a cuatro países piloto (Colombia, Costa Rica, Jamaica y Saint Kitts y Nevis), para luego ser administrada a un amplio sector de partes interesadas nacionales.[34]

Con base en estos parámetros de estudio, y como forma de ejemplificar, se desglosan los resultados obtenidos de algunos países de la región.

2.3.1 COSTA RICA

De acuerdo con el estudio realizado en el presente informe, en el caso de Costa Rica el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) es la autoridad responsable para resolver los problemas relacionadas con la seguridad cibernética nacional, así como generar políticas de desarrollo en este rubro.

[34] Ibídem, pág. 43.

Actualmente se encuentra en una etapa inicial de la planificación de una estrategia de seguridad cibernética nacional.

En febrero el año 2017, el Viceministro de Telecomunicaciones de Costa Rica, en una entrevista de prensa señaló que "actualmente ese país está desarrollando una estrategia en materia de ciberseguridad, que se encuentra en los últimos detalles para ser implementada en sector público pero a su vez que también sea una herramienta para las empresas privadas".[35]

Por otro lado, también cuenta con las contribuciones de la Secretaría Digital/ Gobierno Digital, la Sección de Delitos Informáticos del Poder Judicial, la Superintendencia de Telecomunicaciones, el Banco Central y la Agencia de Protección de Datos de los Habitantes (Prodhab).

Es de destacarse que el año 2012 fue decisivo para Costa Rica en el tema de la seguridad cibernética, con la aprobación de la Ley 9048 que incluyó formalmente el delito cibernético al código penal del país. "Costa Rica también reconoce la Convención Interamericana sobre Asistencia Mutua en Materia Penal (comúnmente conocida como la "Convención de Nassau") y regularmente coordina con la Interpol".[36]

Dentro del análisis sobre la situación que actualmente presenta este país, se señala que aunque la Fuerza Pública maneja un laboratorio forense digital, las autoridades judiciales tienen dificultades para trabajar con eficacia los delitos informáticos, ya que cuentan con un número limitado de fiscales y jueces capacitados y preparados en manejar casos que involucran evidencia electrónica.

[35] Pan y Agua Javier, ¿Cómo se encuentra Costa Rica en materia de ciberseguridad?, IT NOW, 9 de febrero, 2017, https://revistaitnow.com/como-se-encuentra-costa-rica-en-materia-de-ciberseguridad/, fecha de consulta 24 de julio 2017.
[36] Ibídem, pág. 66.

En mi experiencia, cuando tuve la oportunidad de estar en San José, Costa Rica y visité a la fiscalía responsable de la investigación de los delitos cibernéticos, me pude percatar que el intercambio de información es buena y eficaz, ya que como el país es pequeño y no tiene tantos habitantes, se agiliza la comunicación entre jueces, fiscales y policías.

No obstante al igual que México, se carece de personal capacitado en la investigación de estos delitos, y sobre todo de tecnología.

> Además, en 2012 el Gobierno de Costa Rica estableció el CSIRT-CR (bajo el MICITT). El CSIRTCR es el organismo nacional encargado no solo de la tarea de responder a los trastornos de la seguridad cibernética, sino también de coordinar las funciones nacionales de mando y control. La entidad ha recibido asistencia técnica de la OEA y de otros expertos regionales e internacionales y ha detectado y mitigado con éxito las principales amenazas de seguridad cibernética. Actualmente no existe un registro público de incidentes, aunque el gobierno está en el proceso de desarrollar uno.[37]

El estudio afirma que aunque Costa Rica no tiene ejército y la Fuerza Pública es de estructura y capacidades limitadas para desarrollar resiliencia cibernética, el sector público y las organizaciones de la infraestructura critica nacional han asumido y promovido normas de seguridad internacionales como la ISO/IEC 27001, la cual consiste en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) como apoyo en la identificación sistemática y el análisis de riesgos, que surgen con el uso de la información, hasta la implementación y el mantenimiento de mecanismos adecuados de vigilancia y control, no obstante el sector privado aún no las ha seguido y no contar con un marco normativo claro de riesgo para los proveedores del servicio de Internet retrasa el avance de la seguridad cibernética.

[37] Ídem.

Por otro lado, la sensibilización pública de la seguridad cibernética es baja, por lo que la sociedad toma pocas medidas de prevención sobre las amenazas cibernéticas. En el rubro académico, actualmente hay muy pocas instituciones que abarquen de manera extensa los temas relacionados con la seguridad cibernética.

En mi experiencia, tuve la oportunidad de hablar con algunos estudiantes de Ingeniería en Sistemas de diversas universidades en ese país y en mi opinión, aunque es una de las carreras de mayor demanda, los planes de estudio no contienen temarios bastos en seguridad cibernética, prevención, entre otros temas relacionados con la ciberseguridad.

De acuerdo al Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM), estos fueron los resultados obtenidos por dimensiones de análisis:

1.- Política y estrategia. De manera más detallada, esta dimensión comprende la estrategia nacional de seguridad cibernética ya sea oficial o documentada, como es su desarrollo, organización y contenido. Por otro lado, abarca lo referente a la defensa cibernética, tomando en cuenta su estrategia, organización y coordinación.

> Una estrategia nacional integral de seguridad cibernética identifica los intereses y roles de una gama de actores que contribuyen a, tienen la responsabilidad de o se ven afectadas por la seguridad cibernética con el propósito de crear un marco coordinado y cohesionado. Esta estrategia en ocasiones incluye varias áreas temáticas e identifica los roles y responsabilidades de varios actores que participan en la seguridad cibernética, incluida la industria, la sociedad civil y personas naturales, y destacará la importancia de los mecanismos para abordar sus necesidades y aprovechar su experiencia.[38]

[38] Ibídem, pág. 124.

En términos generales, Costa Rica se encuentra en una etapa de madurez inicial.

2.- Cultura y sociedad. Esta dimensión abarca la mentalidad de seguridad cibernética, la cual incluye valores, actitudes y prácticas, hábitos de los distintos actores dentro del ecosistema de la ciberseguridad, es decir, en el gobierno, sector privado y la sociedad en general, cada uno de estos actores con diferente mentalidad, pero con el mismo comportamiento responsable.

Asimismo, generar una conciencia de seguridad cibernética con especial énfasis en la percepción de los riesgos y amenazas cibernéticas, para así poderlos prevenir y mitigarlos.

Tener confianza en el uso de Internet, es de suma importancia sobre todo para que los usuarios puedan proporcionar su información en línea.

Finalmente, la privacidad en línea, como el intercambio de datos de carácter personal en el sector público y privado, ya que los países con estrategias sofisticadas de seguridad cibernética no comprometerán la libertad de expresión en línea en nombre de la seguridad de la red.

De manera genera, Costa Rica se encuentra en una etapa formativa.

3.- Educación. Se enfoca a la disponibilidad de la educación y la formación en seguridad cibernética. Esta disponibilidad debe reflejar las necesidades en el ámbito activo de la seguridad cibernética.

Asimismo, deben existir programas de educación en seguridad cibernética a nivel licenciatura, impartir cursos de temas actuales relacionados con la seguridad cibernética, así como, crear centros nacionales e internacionales cibernéticos de excelencia. Ya que como mencione, en carreras como ingenierías no se cuenta con asignaturas que contemplen temas de ciberseguridad, o de manera muy escasa, en carreras de la rama jurídico-social no se incluye en lo absoluto.

Por otro lado, esta dimensión de análisis no solo engloba la educación en el ámbito académico, sino también en el ámbito laboral. Y para ello, se requiere contar con programas destinados a mejorar las habilidades de los empleados del sector público y privado, para que puedan enfrentar los problemas de seguridad cibernética en los que se podrían ver inmersos.

Finalmente, esta dimensión de análisis, abarca la comprensión por parte de las juntas directivas de los riesgos que enfrentan las empresas, sus principales métodos de ataque y cómo su empresa se ocupa de asuntos cibernéticos.

De manera general, Costa Rica en la dimensión de educación, se encuentra en una etapa formativa, es decir, que tiene capacitación en seguridad de la información, pero es *ad hoc* y sin coordinación; hay seminarios disponibles y recursos en línea pero para grupos demográficos específicos y no existen medidas de efectividad.

“No hay transferencia de conocimientos por parte de los empleados de seguridad cibernética capacitados; debido a una formación limitada, solo hay uso informal de herramientas, modelos o plantillas existentes para la planeación de la seguridad cibernética de la organización, sin la integración automatizada de datos”.[39]

[39] Ibídem, pág. 145.

4.- Marcos legales. Esta dimensión incluye “los marcos jurídicos sobre las TIC, la privacidad, los derechos humanos y la protección de datos y el derecho sustantivo y procesal de delincuencia cibernética, y todos incluyen cooperación internacional.”[40]

En este rubro de análisis, Costa Rica refleja que sus autoridades han implementado los marcos legislativos de seguridad integral de las TIC que incluyen la seguridad cibernética; ha adoptado un marco normativo que protege los derechos humanos y a las organizaciones en el entorno digital.

Por otro lado, Costa Rica ha aplicado procedimientos reglamentarios y legislación de protección de datos integral; su legislación nacional engloba el derecho a la privacidad especificando el aviso, el propósito, el consentimiento, la seguridad, la divulgación, el acceso y la responsabilidad de la información personal.

En cuanto al derecho sustantivo de la delincuencia cibernética, su legislación tipifica algunos delitos relacionados con pruebas electrónicas que pueden ser objeto de una legislación específica o abordada en el código penal, por lo cual se consideró en este rubro que Costa Rica se encuentra en una etapa establecida.

De manera general, este país ha implementado el derecho procesal penal integral y los requisitos probatorios relacionados.

Dentro de la dimensión sobre los marcos legales, este estudio abarca la investigación jurídica, la cual se refiere a la capacidad de investigación para procesar las pruebas electrónicas y enfrentar la delincuencia cibernética, incluida la

[40] Ibídem, pág. 148.

forma de evaluar, obtener y tratar la evidencia digital, así como de usar los instrumentos procesales adecuados.

En este aspecto, Costa Rica muestra que ha establecido una capacidad institucional integral para investigar y manejar la delincuencia cibernética, así como, la prueba electrónica, que incluye “recursos humanos, procesales y tecnológicos, medidas exhaustivas de investigación, cadena de custodia digital y gestión integridad de las pruebas y mecanismos formales e informales de colaboración con interesados internacionales y nacionales (actores de los sectores privado y público).”[41]

Otro tema considerado dentro de esta dimensión es la divulgación responsable de la información, la cual proporciona directrices y declaraciones específicas que incluyen cómo puede manifestarse una vulnerabilidad y como mejorar la capacidad de seguridad mediante la mitigación de la misma y la prevención de cualquier daño futuro.

> Este factor se refiere a un modelo de divulgación de vulnerabilidades o metodología de informes en que una parte (el informador) da a conocer de forma privada la información relacionada con una vulnerabilidad descubierta a un proveedor de producto o proveedor de servicios (parte afectada) y le otorga tiempo a la parte afectada para investigar la reclamación e identificar y probar un remedio o recurso antes de coordinar la divulgación pública de la vulnerabilidad con el informador.[42]

Costa Rica no refleja la necesidad de una política de divulgación responsable en las organizaciones del sector público y privado.

De manera general, el desarrollo de la dimensión de marcos legales, refleja que Costa Rica se encuentra en una etapa de madurez establecida.

[41] Ibídem, pág. 152.
[42] Ibídem, pág. 155.

5.- Tecnología. Siendo la última dimensión de estudio dentro de este modelo de madurez, en la que se encuentra, entre otros, el factor de adhesión a las normas. Factor que se centra en la tecnología de infraestructura y la resiliencia de infraestructura nacional.

Ya que la tecnología de infraestructura se enfoca en la vida cotidiana y asegura que el país siga funcionando social y económicamente. Por lo tanto el gobierno y el sector privado deben lograr ser capaces de proteger los sistemas de información del país y los operadores de infraestructuras críticas para garantizar una mejor capacidad de recuperación nacional.

En el caso de Costa Rica, el modelo de madurez, refleja que se encuentra "identificado estándares de seguridad de la información para su uso y ha habido algunos signos iniciales de promoción y adopción del gobierno, sector público y organizaciones de la Infraestructura Crítica Nacional (ICN); hay una aplicación mínima de las normas nacionales e internacionales."[43]

Por otro lado, Costa Rica se encuentra discutiendo metodologías para los procesos de desarrollo de software que se centran en la integridad y la capacidad de recuperación, cuenta con evidencia suficiente que el sector público cuenta con organizaciones que suministran y adoptan normas de desarrollo y promoción gubernamental de prácticas seguras.

Dentro de esta dimensión del modelo de estudio, se encuentra la labor de las organizaciones de coordinación de seguridad cibernética, siendo un factor que "analiza la existencia y la actividad de los Equipos de Respuesta ante Incidentes de

[43] Ibídem, pág. 158.

Seguridad Informática (CSIRT, por sus siglas en inglés) y el Centro de Mando y Control en el ámbito nacional, en términos de capacidad de respuesta ante incidentes y mitigación de las amenazas".[44]

Aunque no todos los incidentes cibernéticos pueden ser mitigados, la identificación de los eventos que constituyen amenazas a nivel nacional ayuda a prevenir y limitar su alcance. Asimismo, mediante un enfoque organizado y coordinado de respuesta a incidentes asegura que las amenazas puedan ser manejadas de la manera más eficiente posible.

En este factor, Costa Rica ha logrado clasificar ciertas amenazas cibernéticas que se han registrado como incidentes o desafíos a nivel nacional.

La resiliencia de la infraestructura nacional es un factor dentro de la dimensión de la tecnología

> …que se enfoca en la tecnología de la infraestructura y la resiliencia de la infraestructura nacional. La tecnología de la infraestructura sustenta la vida cotidiana y asegura que el país siga funcionando social y económicamente. El gobierno y el sector privado pueden proteger los sistemas de información del país y los operadores de infraestructuras críticas para asegurar una mejor capacidad de recuperación nacional.[45]

Esta dimensión, también engloba la protección de la Infraestructura Crítica Nacional, ya que es importante que los gobiernos tomen las medidas adecuadas para proporcionar la seguridad cibernética necesaria para llevar a cabo una planeación y gestión adecuada del riesgo.

[44] Ibídem, pág. 161.
[45] Ibídem, pág. 166.

Asimismo, dentro de este rubro también se encuentra la Gestión de Crisis, siendo ésta más que la respuesta a incidentes. Por ejemplo, los ejercicios cibernéticos, pueden simular diversos roles, "desde atacantes a defensores, equipos de comunicación, organismos de coordinación y varios otros, todos los cuales son cruciales en caso de una crisis real. La planeación y la evaluación de las aplicaciones de gestión de crisis les ofrecen a los interesados la capacidad para hacerles frente a situaciones del mundo real".[46]

Según el Modelo de Madurez, Costa Rica debe desarrollar la gestión de crisis para la seguridad nacional.

Otro aspecto considerado dentro de la dimensión de la tecnología es considerar la redundancia digital, ya que en "el escenario donde se desactiva la comunicación por medios electrónicos, es fundamental la creación de vínculos de coordinación de respaldo entre los servicios de emergencia que no se basan en redes digitales de comunicación para mejorar la política y la estrategia cibernética".[47]

El mercado de la ciberseguridad es un factor dentro de esta dimensión que se refiere a la "disponibilidad de tecnologías de seguridad cibernética de la información y red y apoyo especializado para el despliegue, y también al seguro cibernético como una forma de protección contra las pérdidas que afectan directamente al titular del seguro o contra las pérdidas de otra organización o individuos afectados por una falla de seguridad".[48]

Costa Rica reflejó estar una etapa de madurez formativa, pues a pesar de que la tecnología y los procesos de seguridad en el gobierno y el sector privado están disponibles; "el mercado interno ofrece productos genéricos, no especializados; las

[46] Ibídem, pág. 173.
[47] Ibídem, pág. 175.
[48] Ibídem, pág. 177.

ofertas no están impulsadas por el mercado; consideraciones de seguridad están integradas en el software y la infraestructura".[49]

2.3.2 MÉXICO

De acuerdo al presente estudio, el Gobierno de México trabaja en la elaboración de una estrategia nacional de seguridad cibernética a cargo de las Fuerzas Armadas del país.

> El Equipo de Respuesta a Incidentes de Seguridad Informática del país, CERT-MX, es un miembro del Foro Mundial de Respuesta a Incidentes y Equipos de Seguridad (FIRST) y sigue un Protocolo de Colaboración con otras entidades gubernamentales. El CERTMX está muy involucrado en la protección de la Infraestructura Crítica Nacional (ICN). Los interesados coordinan la gestión de seguridad de infraestructuras y comparten información sobre los activos y las vulnerabilidades de la ICN. En todas las agencias gubernamentales, las tecnologías se actualizan regularmente, se realizan copias de seguridad y se adhiere a las disposiciones del Manual Administrativo de Aplicación General de Tecnologías de Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), el cual se desarrolló con base a normas internacionales como ISO 27001, ITIL *("Information Technology Infrastructure Library*" en inglés) y COBIT *("Control Objectives for Information and Related Technology*" en inglés), entre otras. Por otra parte, están en marcha planes de redundancia digital. La División Científica de la Policía Federal de México investiga los delitos cibernéticos nacionales. Trabaja en estrecha colaboración con el CERT-MX y ha recibido capacitación por parte de organizaciones sin ánimo de lucro y de varias organizaciones internacionales. Informes recientes indican un aumento de la suplantación de identidad (*phishing*) y amenazas persistentes avanzadas en el país y una disminución de los ataques de denegación de servicio DoS (por sus siglas en inglés, Denial of Service). Si bien las fuerzas del orden cuentan con una amplia capacidad de investigación, México aún está desarrollando una legislación integral sobre delincuencia cibernética, lo que dificulta el enjuiciamiento de tales actos. Con una tasa de penetración de Internet del 44%, se requiere emprender un esfuerzo para informar a la sociedad mexicana sobre los

[49] Ídem.

> problemas de seguridad cibernética. Instituciones gubernamentales y la academia ofrecen conferencias sobre seguridad cibernética. También están disponibles algunas oportunidades de capacitación para empleados, incluyendo programas de certificación a través del sector privado. Recientemente el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) inició una campaña proponiendo leyes más estrictas de protección de datos personales, así como una mayor transparencia y disponibilidad de información al público. Además de su labor de promoción, el INAI publica informes y conduce campañas de sensibilización para los ciudadanos sobre sus derechos como usuarios de las tecnologías de la información y la comunicación.[50]

De acuerdo al Modelo de Madurez, México refleja lo siguiente:

1.- Política y estrategia. En cuanto a su estrategia de defensa cibernética, se encuentra en una etapa formativa, es decir, que han identificado amenazas específicas a la seguridad nacional "en el ciberespacio, tales como actores de amenazas externas, amenazas internas, vulnerabilidades del sistema de suministro y amenazas a la capacidad operativa militar, pero aún no existe una estrategia de respuesta coherente".[51]

La organización de su defensa cibernética, refleja que sus unidades de operación se adhieren a las diversas ramas de las fuerzas armadas, pero no existe una estructura real central de mando y control.

Muestra coordinación en la capacidad de defensa cibernética entre el sector público y privado a fin de minimizar las amenazas que pudieran desestabilizar la seguridad nacional.

[50] Ibídem, pág. 86.
[51] Ibídem, pág. 127.

2.- Cultura y sociedad. Dentro de esta dimensión, México refleja tener una mentalidad de seguridad cibernética en etapa formativa en el gobierno, como en el sector privado, ya que en ambos sectores han comenzado a darle prioridad a la seguridad cibernética, mediante la identificación de los riesgos y amenazas.

Por otro lado, la sociedad también ha adoptado una mentalidad de seguridad cibernética, pero de manera inconsistente, y no generalizada; por lo que se sigue entrenando a la sociedad en mejorar las prácticas de seguridad cibernética.

En cuanto a la sensibilización para lograr una conciencia de seguridad cibernética, México refleja que se encuentra estableciendo campañas de sensibilización con objetivos definidos, pero son *ad hoc*, "no cubren necesariamente todos los grupos y no están estrechamente vinculadas a la estrategia de seguridad cibernética; están disponibles seminarios y recursos en línea para la población objetivo, pero no hay esfuerzos de coordinación o de medición".[52]

La confianza en el uso de Internet se identifica como una preocupación, por lo que los operadores de infraestructuras se encuentran tomando medidas para fomentar la confianza en los servicios en línea, sin que éstas se encuentren solidas aún.

México refleja que cuenta con un gobierno electrónico establecido, pues coordina "acciones para evitar ataques a la información personal y priorizan los delitos en Internet de alto nivel, además se promueve el cumplimiento de los estándares de Internet y de la web para proteger el anonimato de los usuarios".[53]

[52] Ibídem, pág. 135.
[53] Ibídem, pág. 137.

Pese a estos resultados, la realidad es que México sigue siendo vulnerable a los ciberataques, ejemplo de ello es el caso Pegasus:

> Entre 2015 y 201, varios periodistas y activistas mexicanos fueron objeto de ciberataques a través de un software malicioso que fue contratado por el gobierno mexicano, reveló un reporte hecho por la organización Red en Defensa de los Derechos Digitales (R3D), la oficina para México y Centroamérica de *Article 19* y *SocialTIC* y el cual se publicó en el diario *The New York Times*.
>
> Según el informe, en un año se registraron 76 nuevos intentos de infección a través del malware llamado *Pegasus*, el cual envía mensajes de texto a sus objetivos con un enlace que, al hacer clic sobre éste, permite el acceso a la información almacenada en el teléfono, como correos electrónicos y contactos, y activa los micrófonos y cámaras sin que el afectado se dé cuenta.[54]

Asimismo, el comercio electrónico se encuentra plenamente establecido, se considera seguro y por ende cada día se invierte más en él.

La privacidad en línea que refleja México es estratégica, es decir, que se adhiere a los estándares internacionales de derechos humanos, en relación con la privacidad. También se protege la privacidad de los trabajadores ya que los empleadores mantienen políticas de privacidad, ofreciendo un nivel mínimo de privacidad para sus empleados.

3.- Educación. El modelo de madurez indicó que en México existen ofertas educativas en seguridad cibernética por parte de escuelas e instituciones a nivel nacional, con una formación desde nivel elemental hasta posgrado.

[54] r. Fomperosa Mariana, ¿Qués es Pegasus? El malware usado para espiar en México, periódico Milenio, 19 de junio 2017, http://www.milenio.com/tendencias/pegasus-mexico-espionaje-que_es-malware-the_new_york_times-milenio-noticias_0_977902402.html, fecha de consulta 25 de julio 2017.

Cada vez son más los interesados en invertir en capacitación sobre seguridad cibernética, se conoce lo que se necesita para llevar a cabo dichas capacitaciones y se evalúa la eficacia de los modos y procedimientos de formación, estableciendo algunas métricas.

El desarrollo nacional de la educación de seguridad cibernética en México refleja que "existen incentivos para la formación y la educación; se identifican líneas presupuestales para la formación y la investigación y el desarrollo, con una oficina establecida para el desarrollo y ejecución del programa; se establece la participación de las partes interesadas para garantizar la continuidad"[55].

En mi experiencia, como estudiante hasta nivel posgrado y como profesionista en el sector público y privado, la educación en seguridad cibernética, no es un tema generalizado, ya que para obtener este tipo de capacitación debes pagar cursos especializados en la materia, o esperar a que haya una conferencia, seminario, o congreso que abarque este tema, no obstante estos eventos suelen ser pequeños y de nula o escasa difusión.

En el tema laboral, solo el personal que está directamente vinculado a estos temas llega a ser capacitado, aunque esto no es regla general y actualmente el sector privado impulsa más este tipo de capacitaciones, sobre todo en el sector financiero, que se tiene contacto con información sensible que puede ser utilizada para fines delictivos, mediante el uso de las TIC.

4.- Marcos legales. De acuerdo al Modelo de Madurez, México ha implementado los marcos legislativos y reglamentarios de seguridad cibernética, adoptando una

[55] Ibídem, pág. 144.

legislación que protege los derechos de los individuos y las organizaciones en el entorno digital.

Además, se cuenta con una legislación que abarca y garantiza la privacidad y protección de datos personales, con apego a derechos humanos.

Aunque en relación al derecho procesal penal, “se aplica ad hoc a la delincuencia cibernética, pero no ha comenzado el desarrollo de los delitos cibernéticos específicos”.[56]

En cuanto al derecho sustantivo de la delincuencia cibernética México refleja estar desarrollando una legislación que contiene algunos aspectos de los delitos cibernéticos.

En la investigación jurídica “existe alguna capacidad de investigación para indagar delitos que involucren pruebas electrónicas, así como para obtener dichas pruebas, de conformidad con el derecho interno; sin embargo, esta capacidad es mínima”.[57]

5.- Tecnologías. De acuerdo con el Modelo de Madurez, México en esta dimensión refleja estar en una etapa formativa, ya que aunque han identificado estándares de seguridad de la información para su uso, hay una aplicación mínima de las normas nacionales e internacionales en los sectores público, privado y social en general.

El presente informe, señala que el gobierno mexicano actualmente cuenta con un programa para “promover la adopción de estándares en el desarrollo de software, tanto para los sistemas del sector público como del sector privado, lo que incluye el

[56] Ibídem, pág. 151.
[57] Ibídem, pág. 152.

seguimiento de la observancia de las normas; están presentes los sistemas de alta integridad y técnicas de desarrollo de software dentro de la oferta educativa y de formación".[58]

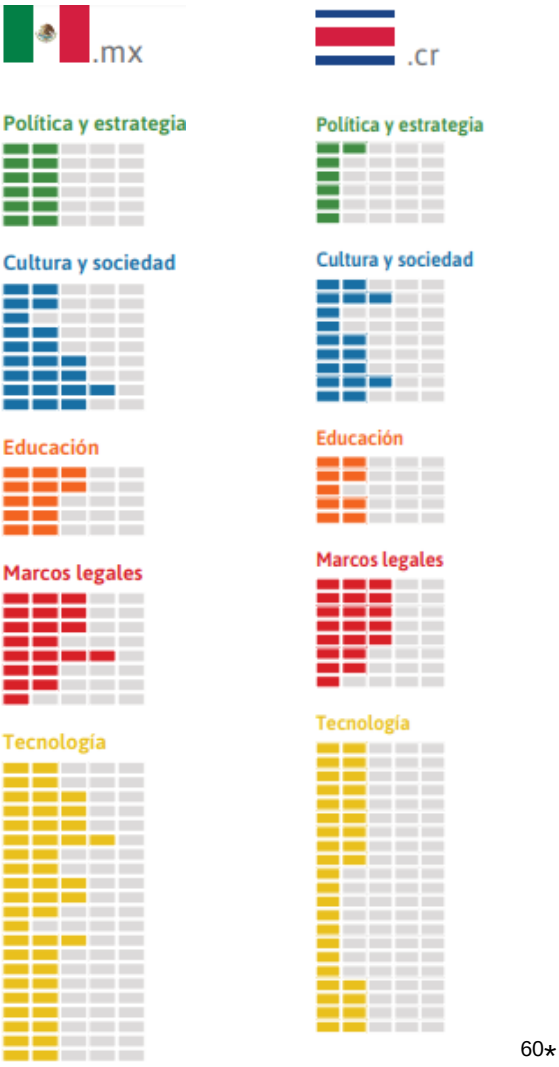
Por otro lado, México cuenta con una estrategia para registrar de manera regular y sistemática incidentes a nivel nacional, teniendo cierta capacidad para analizar y brindar respuesta a dichos incidentes.

Asimismo, se ha identificado la necesidad de un mercado para los seguros de delitos informáticos, "mediante la evaluación de riesgos financieros para los sectores público y privado; ahora se está discutiendo el intercambio de las mejores prácticas en materia de evaluación y reducción de riesgos, incluyendo el desarrollo y uso de estándares y productos variados apropiados".[59]

En general México refleja encontrarse en una etapa formativa por lo que respecta a esta última dimensión de estudio.

Para tener mayor claridad de los resultados obtenidos de Costa Rica y México en el Modelo de Madurez, se muestran las siguientes tablas:

[58] Ibídem, pág. 160.
[59] Ibídem, pág. 178.



60*

Lo que las gráficas reflejan es que de acuerdo al Modelo de Madurez, considerando los resultados de cada una de las 5 dimensiones evaluadas, tanto México como Costa Rica, se encuentran en una etapa de madurez formativa, es decir que se han construidos procesos, se están tomando iniciativas para atender todos los rubros que abarca una estrategia integral de ciberseguridad.

[60] *Gráficas obtenidas del informe en línea, BANCO INTERAMERICANO DE DESARROLLO, ORGANIZACIÓN DE LOS ESTAMOS AMERICANOS, op. cit. págs. 66 y 86.

CAPÍTULO III. MARCO JURÍDICO DE LA CIBERSEGURIDAD Y ACCIONES EMPRENDIDAS

3.1 MARCO JURÍDICO INTERNACIONAL

Si se parte de la idea de que el ciberespacio es un conjunto de interconexiones electrónicas en red, que en su conjunto constituye un espacio de relación e interacción, integrado por componentes materiales de tecnología e inmateriales sustentados en la información y el conocimiento, fundamentada en la sociabilidad del ser humano, siendo un medio óptimo para prestar servicios.

> …ha generado un nuevo marco espacio-cultural con efectos económicos, políticos, jurídicos, sociales, culturales y de seguridad; que tiene como límites la seguridad, el desarrollo y el respeto a los derechos humanos, y compartida la idea de la necesidad de establecer una estrategia internacional para su gestión, tal vez el paso siguiente en un proceso de profundización conceptual sea una aproximación jurídica.[61]

En este sentido, el ciberespacio se puede considerar como una realidad autónoma, pero con vinculaciones recíprocas con otras realidades tangibles e intangibles. Por ejemplo, con la geografía a través de la ubicación física de equipos, sistemas o nodos; con las instituciones, corporaciones, organizaciones y personas, a través del uso, posesión o titularidad de los equipos y servicios; y con intangibles como la información, el conocimiento, la antropología, la economía, la política o la cultura a través de la utilización de la red y sus servicios, que permite a los usuarios desarrollar todas sus potencialidades y proyectarse en el mundo globalizado de la actualidad.

[61] Molina Mateos José María, Aproximación Jurídica al Ciberespacio, Instituto Español de Estudios Estratégicos, España, 2015, pág. 3.

Derivado de la interacción entre el hombre y las TIC, surge la necesidad de ordenación, tanto para preservar su existencia, desarrollo y evolución, como para evitar el caos. A través de una regulación entre los sujetos que las crean y operan, garantizando derechos y estableciendo obligaciones o responsabilidades.

Bajo este orden de ideas, al realizar un acercamiento jurídico sobre el ciberespacio, el primer planteamiento que surge es sobre su delimitación y el alcance de su naturaleza jurídica.

En este sentido, se puede decir que la relación jurídica ciberespacial ordena las conductas de los sujetos que actúan en el ciberespacio en sus conexiones recíprocas y está constituida por el conjunto de poderes y facultades de unos con respeto a otros en forma reticular.

Como se ha mencionado, el ciberespacio tiene una naturaleza autónoma, “de derecho público y derecho privado, es compleja, dinámica, unitaria y con objeto propio”.[62]

Asimismo, una gran variedad de sujetos y relaciones tienen lugar en el ciberespacio abarcando organismos públicos, privados, civiles, militares, corporaciones, organismos internacionales, estados, empresas o individuos, provocando que regular de manera normativa al ciberespacio conlleve un alto grado de complejidad dentro de entornos de difícil gestión, pero que al mismo tiempo esa complejidad demande su ordenación.

[62] Ibídem, pág. 6.

“Las características del Ciberespacio, hacen que su seguridad (ciberseguridad) juegue un papel central en el contexto de un Estado de Derecho, así como en el juego de relaciones internacionales, llegando a ser una constante presente, de una u otra forma, en todos los intereses en juego del nuevo ámbito relacional actual”[63] ya sean técnicos, sociológicos, jurídicos, económicos, políticos, entre otros. Todos ellos que de una u otra forma emergen del ciberespacio o el ciberespacio de ellos, entrañando así un nuevo valor, un nuevo bien jurídico digno de protección, de carácter universal.

Toda estas estas nuevas formas de relaciones sociales, así como la necesidad de proteger este nuevo bien jurídico, trae consigo nuevas categorías jurídicas e, incluso, nuevos tipos penales, con independencia de los ya existentes en los códigos penales.

> Al ser Este fenómeno ha incidido de forma directa en las ciencias jurídicas, reguladoras de la conducta humana, que han acusado el impacto del mismo como factor de transformación social y han de dar respuesta —especialmente desde el Derecho Internacional— al sentimiento de considerar a la humanidad como titular de derechos sobre nuevos ámbitos que, hasta hoy, han tenido lugar respecto al Derecho del Mar, el Espacio Exterior o el Medio Ambiente, pero que no excluye otros entornos.[64]

En este sentido, si el concepto expansivo de patrimonio común de la humanidad engloba al ciberespacio, éste deberá ser reconocido en un Tratado internacional que así lo manifieste.

Es una realidad que el desarrollo del ciberespacio ha potenciado todas las actividades humanas, ya sea en el ámbito gubernamental, como comercial o social. En todos ellos se genera, procesa y se guarda demasiada información, en la

[63] Ibídem, pág. 8.
[64] Ibídem, pág. 9.

mayoría de los casos de gran valor, la cual necesita seguridad y por lo tanto una protección jurídica de índole internacional, por las características que se han descrito acerca del ciberespacio.

> La nueva situación demanda una respuesta adecuada de los ordenamientos jurídicos y de la normativa internacional, en un marco cívico, en el que se ha multiplicado toda clase de actividades, con una alta repercusión en todas las ramas del Derecho, de las que requiere su adecuación a la nueva realidad para hacer frente, especialmente, a las dimensiones informacionales, tecnológicas y securitarias incorporadas a las materias de su ámbito de ordenación, atendiendo al alcance global de los efectos de las nuevas tecnologías, su valor patrimonial, político y estratégico, su alto potencial como instrumento comisivo, y en la internacionalización de la vida en general.[65]

Actualmente y a nivel mundial, existe una insuficiencia normativa de la debida regulación del ciberespacio, como se ha mencionado, de los temas más críticos vinculados a éste, es la información y el conocimiento, por ello resulta esencial su aproximación al estudio y seguimiento de las iniciativas jurídicas que surjan en los derechos internos y en las normas internacionales.

3.1.1 CONVENIO SOBRE LA CIBERDELINCUENCIA, CONSEJO DE EUROPA

El Convenio sobre la Ciberdelincuencia del Consejo de Europa, mejor conocido como el Convenio de Budapest, porque fue elaborado en ese lugar, el 23 de noviembre del año 2001.

Surge con la necesidad de aplicar una política penal común, con el objeto de proteger a la sociedad frente a la ciberdelincuencia, mediante la adopción de una legislación adecuada de cooperación internacional.

[65] Ibídem, pág. 11.

Su importancia radica, en que fue el primer tratado internacional que buscó solucionar a la comisión de delitos informáticos, mediante la armonización normativa entre los países firmantes.

El tratado, abarca tanto derecho sustantivo, como procesal. En la sección de derecho sustantivo, se establecen los delitos que deben ser tipificados por las legislaciones nacionales.

Mencionando delitos como: el acceso ilícito, ataques a la integridad de los datos, abuso de dispositivos, falsificación informática, fraude informático, los relacionados con la pornografía infantil, relacionados con las infracciones de la propiedad intelectual y de los derechos a fines.

Por otro lado, la sección de derecho procesal, hace hincapié en la correcta investigación que deben llevar las autoridades para este tipo de delitos, garantizando la protección de los derechos humanos.

> …y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.[66]

Asimismo, el tratado en su artículo 16, señala que las autoridades competentes, deben llevar a cabo la conservación rápida de los dados electrónicos vinculados a

[66] Consejo De Europa, Convenio Sobre la Ciberdelincuencia, Serie de Tratados Europeos- n°185, Budapest, 2001, www.oas.org/juridico/english/cyb_pry_convenio.pdf, fecha de consulta: 13 de junio de 2017.

la investigación de que se trate, cuando existan motivos para creer que esos datos son susceptibles de perderse o de ser modificados.

Por otro lado, este tratado también contiene un capítulo referente a la cooperación internacional, en el cual cita los principios relativos a ésta. Dichos principios referentes a:

- La extradición en materia de los delitos informáticos previstos en este convenio y siempre que sean sancionados por los dos países implicados.

- La asistencia mutua entre los países firmantes, a efecto de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos, o con el fin de obtener pruebas en formato electro de un delito.

- Información espontánea; es decir, que dentro de los límites de su derecho interno y sin que exista denuncia previa, se pueden comunicar información obtenida de sus propias investigaciones, entre países involucrados en la comisión de este tipo de delitos, cuando dicha información pueda conducir una petición de cooperación en materia de delitos cibernéticos.

Otro aspecto a destacar que incluye el Tratado de Budapest, es la Red 24/7 que se menciona en su artículo 35. En el que se señala que:

> Cada Parte designará un punto de contacto localizable las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda acción que facilite las medidas que figuran a continuación, o su aplicación directa si lo permite el derecho y la práctica internos:
>
> a. Asesoramiento técnico.

b. Conservación de datos, de conformidad con los artículos 29 y 30; y

c. Obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos.[67]

El presente tratado entró en vigor el 1 de julio de 2004 y el 1 de marzo de 2006 el Protocolo Adicional a la Convención sobre el delito cibernético entró en vigor, respecto de la criminalización de actos de naturaleza racista y xenofóbica cometidos a través de sistemas de ordenador.

Actualmente "México es observador del Convenio de Budapest, lo cual lo obliga a actualizar sus leyes y a colaborar con autoridades internacionales para atrapar a los cibercriminales".[68]

Asimismo, el 13 de junio del año 2017, la Segunda Comisión de Relaciones Exteriores, Defensa Nacional y Educación Pública, sometió a consideración de la Comisión Permanente del H. Congreso de la Unión exhortar a las dependencias competentes del Gobierno Federal para que realizaran las acciones necesarias a efecto de que "el Estado Mexicano se adhiera y aplique las disposiciones del Convenio sobre Ciberdelincuencia conocido como Convenio de Budapest, su protocolo adicional, así como al Convenio 108 del Consejo de Europa, con objeto de fortalecer el marco jurídico en materia de ciberseguridad y reforzar la cooperación internacional para prevenir estos delitos."[69]

En este sentido, y como se mencionó en el capítulo anterior, traería grandes beneficios que México de adhiriera a este convenio, ya que sentaría las bases para

[67] Ibídem, pág. 21.
[68] Tech, 2016, "México, entre los 6 países más atacados por cibercriminales", Periódico El Financiero, 11 de junio de 2016, http://www.elfinanciero.com.mx/tech/mexico-entre-los-paises-mas-atacados-por-cibercriminales.html, fecha de consulta: 15 de junio de 2017.
[69] Solicitud de acuerdo de la Segunda Comisión de Relaciones Exteriores, Defensa Nacional y Educación Pública, pág. 8, http://www.senado.gob.mx/sgsp/gaceta/63/2/2017-06-21-1/assets/documentos/Dict_2da_Convenios_Ciberdelitos.pdf, fecha de consulta 02 de octubre de 2017.

armonizar el marco jurídico a nivel nacional, y se fortalecería la cooperación internacional, haciendo más eficiente y eficaz la investigación de los delitos cibernéticos.

Este convenio, hasta el día de hoy sigue siendo el único instrumento internacional existente que establece las tipologías y armoniza los elementos sustantivos penales relacionados con las conductas realizadas a través de sistemas de cómputo e internet.

Este convenio establece las atribuciones necesarias "en materia procedimental penal para que los países puedan identificar, investigar y obtener pruebas en relación a la información contenida en formato electrónico, así como establecer y fomentar medidas de cooperación internacional en forma ágil para contrarrestar y perseguir el crimen informático".[70]

3.2 COOPERACIÓN INTERNACIONAL PARA FORTALECER EL COMBATE DE LA CIBERCRIMINALIDAD

Como se ha citado en el desarrollo del presente trabajo de investigación, la cooperación internacional es uno de los componentes más importantes para combatir la ciberdelincuencia global, pues sin ella, sería una tarea realmente imposible adoptar medidas y políticas que ayuden a erradicar este latente problema de carácter transnacional, pues para combatirlo se necesita de la cooperación de diversos sectores sociales, de las autoridades y organismos.

> El cibercrimen y la ciberseguidad traen consigo un gran número de retos de naturaleza jurídica, técnica, organizativa e institucional que deben ser concentrados y dirigidos a

[70] Cristos Velasco, San Martín, La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet, Tirant lo Blanch, México, 2012, pág. 149.

través de estrategias viables que tomen en cuenta las actividades de cada organización y los roles de cada individuo en la mejora de la ciberseguridad y la lucha contra la ciberdelincuencia a nivel internacional. [71]

3.2.1 ORGANISMOS INTERNACIONALES Y ACCIONES EMPRENDIDAS

Hoy en día existen diversas iniciativas, planes y políticas de distintos organismos internacionales en materia de combate a la ciberdelincuencia, entre los que destacaremos los siguientes:

A. Unión Internacional de Telecomunicaciones (UIT)

La UIT es el organismo de las Naciones Unidas encargado de la creación de normas, estándares y políticas en el sector de las telecomunicaciones, así como de diversos aspectos de seguridad en donde participan las agencias gubernamentales de 191 países miembros.

La UIT fungió como el organismo rector de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) que se organizó en dos fases, la primera en Ginebra, Suiza en 2003 y la segunda en Túnez, Túnez en 2005. Durante esa cumbre mundial, gobiernos, sector privado, sociedad civil y expertos de todo el mundo intercambiaron ideas y experiencias acerca de la necesidad de abordar las cuestiones relacionadas con el desarrollo de una sociedad de la información mundial. Lo que incluía la definición de normas, legislación y políticas públicas.[72]

En esa cumbre mundial, se destacó la importancia de la adopción de medidas para combatir el ciberdelito y generar la confianza y seguridad al utilizar las TIC, así como la necesidad de promover la cooperación internacional para mitigar la ciberdelincuencia.

[71] Ibídem, pág. 151.
[72] Ibídem, pág. 161.

Derivado de un Memorando de Entendimiento entre la UIT y la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD), firmado con ocasión del Foro de la CMSI celebrado en mayo de 2011 en Ginebra, ambas organizaciones colaboran para ayudar a los Estados Miembros de la UIT y de las Naciones Unidas a mitigar los riesgos que plantea la ciberdelincuencia. Cabe señalar que esa fue la primera vez que dos organizaciones del sistema de las Naciones Unidas convienen oficialmente en cooperar a escala mundial en materia de ciberseguridad.

> En consonancia con su larga tradición de asociación entre los sectores público y privado, la UIT también ha firmado un Memorando de Entendimiento con Symantec, uno de los principales proveedores de soluciones de gestión de seguridad, almacenamiento y sistemas. La UIT utiliza la información de Symantec sobre seguridad, es decir, sus informes trimestrales sobre las amenazas contra la seguridad de Internet, con el fin de aumentar el conocimiento que se tiene de los riesgos para la ciberseguridad e incrementar la capacidad de hacerles frente.
>
> Como refuerzo adicional de las actividades de la UIT en este ámbito, la colaboración y las relaciones de la UIT con la Alianza Internacional Multilateral contra las Ciberamenazas (IMPACT) siguen cobrando impulso, y ya son más de 130 los Estados Miembros de la UIT que forman parte de la coalición UIT-IMPACT.
>
> UIT-IMPACT es la primera iniciativa de cooperación a nivel global que divulga conocimientos y recursos sobre ciberseguridad para que los Estados Miembros interesados puedan detectar, analizar y responder eficazmente a las ciberamenazas. Esta coalición, que es particularmente provechosa para los países que no tienen la capacidad ni los recursos necesarios para desarrollar sus propios centros avanzados de ciberrespuesta, también ayuda a los países técnicamente avanzados proporcionándoles una visión mundial de las amenazas en línea potenciales y reales.[73]

[73] Texto en línea, Ciberseguridad, Creando un mundo en línea más seguro, Actualidades de la UIT, Junio 2011, http://www.itu.int/net/itunews/issues/2011/05/38-es.aspx, fecha de consulta, 25 de julio 2017.

De manera general, la UIT actualmente se encuentra trabajando en iniciativas dirigidas a proteger a los menores que hacen uso de la red, además ofrece a sus países miembros conocimientos, facilidades y recursos técnicos necesarios para eficientar su labor en la prevención y combate de las ciberamenazas, así como, capacitar y entrenar a personal en materia de ciberseguridad.

B. Organización de las Naciones Unidas (ONU)

La ONU ha tenido un papel muy importante en el desarrollo de políticas y resoluciones relacionadas con la prevención y control de delitos informáticos desde el año 1990.

Ese organismo internacional, a través de su Asamblea General ha adoptado un amplio número de Decisiones, Resoluciones y Recomendaciones relacionadas con delitos cometidos a través del uso de las TIC, incluyendo aspectos sobre terrorismo, narcotráfico y protección de los menores en internet. [74]

Como es sabido, la ONU organiza cada cinco años, a partir del año 1955, el Congreso sobre Prevención del Delito y Justicia Penal en donde se han aprobado declaraciones relacionadas con la lucha contra la ciberdelincuencia y los delitos transnacionales.

Cabe señalar que dentro de las actividades más importantes en materia de prevención y combate al ciberdelito y la explotación de menores en internet, la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC) por sus siglas en inglés, se encuentra trabajando con otras organizaciones internacionales, gobiernos y el sector privado con el fin de facilitar programas de capacitación y entrenamiento de autoridades ejecutoras, incluyendo el poder judicial con el propósito de combatir el crimen organizado transnacional cometido a través del uso de sistemas de cómputo y redes de telecomunicaciones.

[74] Ibídem, pág. 163.

C. GRUPO DE LAS OCHO NACIONES (G-8)

> El origen del Grupo de los Ocho G-8 se establece en Marzo de 1973, cuando, a petición del Secretario de Tesoro Estadounidense se reunieron los Ministros de Finanzas de las seis potencias económicas mundiales, un grupo conformado en ese entonces por 6 países: Estados Unidos, Japón, Alemania, Italia, Francia y el Reino Unido. En 1976, ese grupo pasó a ser de 7 miembros con la incorporación de Canadá, en la Cumbre de San Juan, Puerto Rico formándose el G-7; y finalmente en la Cumbre de Kananskis, Canadá en 2002, el grupo se convirtió definitivamente en el G-8, con la admisión de Rusia como miembro de pleno derecho en todas las negociaciones y discusiones.[75]

En la reunión del año 1997 el G-8 estableció un subgrupo sobre Delitos de Alta Tecnología, que tenía como objetivo primordial luchar contra el ciberdelito. En esa reunión, celebrada en Washington D.C. Estados Unidos, los Ministros de Justicia y del Interior adoptaron Diez principios y un Plan de Acción que contiene diez acuerdos para combatir los delitos de alta tecnología.

Estos principios han servido como base para la adopción de políticas relacionadas con el cibercrimen y otras formas de crimen organizado para organismos internacionales como la ONU, y la Organización de los Estados Americanos.

Uno de los logros más importantes del Grupo de Expertos del G-8 hasta ahora ha sido la creación de la red internacional de puntos de contacto, que opera las 24 horas del día, los 7 días de la semana. Esta red exige que los países participantes establezcan coordinadores de las investigaciones transnacionales que se llevan a cabo y deben estar accesibles y disponibles las 24 horas, loas 7 días de la semana.

[75] Ibídem, pág. 169-170.

El G-8 ha abordado el tema de la ciberdelincuencia y los delitos cometidos a través del uso de las tecnologías en diversas reuniones y talleres de trabajo.

Asimismo, los Ministerios de Justicia e Interior del G-8 han elaborado y acordado una serie de documentos, recomendaciones, principios y mejores prácticas relacionadas con la intercepción de comunicaciones transfronterizas para llevar a cabo investigaciones derivadas de delitos, en las que se incluyan lineamientos para el acceso, recolección, retención y el intercambio de datos e información relacionada con el crimen transfronterizo y la interacción con las víctimas de ciberdelitos.

D. ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO (OCDE)

La Organización para la Cooperación y el Desarrollo Económico (OCDE) es un organismo internacional establecido en 1960, del cual forman parte los gobiernos de 31 países, de entre ellos México y Chile de Latinoamérica. Este organismo tiene como mandato discutir políticas públicas, buscar soluciones a problemas comunes entre sus miembros, identificar mejores prácticas y coordinar las políticas domésticas e internacionales en distintos sectores de la economía, incluyendo el área de tecnologías de información y comunicación.

La OCDE tiene conformado un Grupo de Trabajo sobre Seguridad de la Información y Privacidad (WPISP) que tiene como mandato crear políticas de seguridad y privacidad en Internet para reforzar la confianza de los usuarios en la sociedad de la información entre los países miembros. Este Grupo de Trabajo mantiene una red activa de expertos del gobierno, industria y sociedad civil y sus miembros se reúnen periódicamente para seguir las tendencias, compartir experiencias y analizar el impacto de la tecnología en la seguridad de la información y la privacidad y desarrollar políticas de orientación.[76]

[76] Ibídem, págs. 171-172.

La OCDE ha sido una de las organizaciones internacionales más proactivas en el combate al *spam* y el correo comercial no solicitado, asimismo, ha publicado algunos reportes y libros relacionados con ciberdelitos tales como el *malware* y virus informáticos, usurpación y robo de identidad, entre otros principalmente para fomentar la concientización entre sus Estados miembros sobre la necesidad de combatir las amenazas existentes en internet.

E. ORGANIZACIÓN INTERNACIONAL DE POLICÍA CRIMINAL (INTERPOL)

Como es bien sabido la INTERPOL, es la mayor organización policial internacional del mundo, cuya misión consiste en facilitar la cooperación policial transfronteriza, apoyar y asistir a todas las organizaciones, autoridades y servicios que tienen como fin combatir y prevenir la delincuencia.

> La sede de su Secretaría General se encuentra ubicada en Lyon, Francia y además, en cada uno de sus países miembros existe una Oficina Central Nacional (OCN), cuyo personal está compuesto por funcionarios de policía altamente cualificados para responder a las solicitudes de ayuda, localización y detención de prófugos.
>
> Además, INTERPOL ha estado involucrada de manera activa desde los años 90´s en la lucha contra la delincuencia cometida a través del uso de las tecnologías de la información y actualmente tiene conformados Grupos Regionales de Trabajo integrados por expertos, directores y personal experimentado de las unidades nacionales especializadas para combatir la delincuencia informática.[77]

Las actividades de los Grupos Regionales de Trabajo consisten en coordinar con el resto de los grupos y subgrupos de INTERPOL aspectos relacionados con la

[77] Ibídem, pág. 174.

delincuencia informática, promover la cooperación policial internacional con otros países y compartir experiencias prácticas en la investigación de ciberdelitos.

Una de las funciones esenciales de INTERPOL es la operación de su sistema mundial de comunicación policial denominado I-24/7, para que los 190 países miembros puedan solicitar y compartir datos policiales vitales, de manera remota e instantánea, para combatir los crímenes transnacionales a nivel mundial.

> Hoy en día, la mayoría de los delitos cibernéticos son de carácter transnacional, por lo que INTERPOL es el socio natural de cualquier organismo encargado de hacer cumplir la ley que busque investigar estos crímenes a nivel cooperativo. Trabajando con la industria privada, INTERPOL puede proporcionar a la policía local información cibernética centrada, derivada de la combinación de insumos a escala mundial.

Sus principales iniciativas en torno a la ciberdelincuencia se centran en:

- Apoyo operativo y de investigación.
- Inteligencia cibernética y análisis.
- Forense digital.
- Innovación e investigación.
- Creación de capacidad.[78]

Cabe señalar que INTERPOL se ha comprometido a ser un organismo de coordinación mundial para la detección y prevención de delitos digitales a través del Complejo Mundial para la Innovación (IGCI) de INTERPOL en Singapur. Este centro de investigación y desarrollo de vanguardia, que abrió sus puertas en 2014,

[78] Texto extraído de la página oficial de INTERPOL https://www.interpol.int/es/Crime-areas/Cybercrime/Cybercrime, fecha de consulta 07 de julio de 2017.

aprovecha la experiencia cibernética global de las fuerzas del orden público y de los principales asociados del sector privado.

Hoy en día, INTERPOL está en una posición única para avanzar en la lucha contra el ciberdelincuencia a escala mundial a través de una investigación proactiva sobre los crímenes emergentes, las últimas técnicas de formación y el desarrollo de nuevas herramientas policiales innovadoras.

F. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA)

La Organización de los Estados Americanos (OEA) es un organismo regional constituido formalmente en 1948 y conformado por 35 países del continente Americano. La OEA ha venido ocupándose activamente de las cuestiones del ciberdelito y terrorismo en la región desde 1999 dentro del mandato y alcance de la Reunión de Ministros de Justicia o Ministros Procuradores Generales de las Américas (REMJA).

En marzo del año 1999 los Ministros de Justicia de REMJA recomendaron establecer un Grupo de Expertos Intergubernamentales sobre Delito Cibernético con el mandato de hacer un diagnóstico de la actividad delictiva vinculada a las computadoras y la información en los Estados miembros; hacer un diagnóstico de la legislación, las políticas y las prácticas nacionales con respecto a dicha actividad; identificar las entidades nacionales e internacionales que tienen experiencia en la materia; e identificar mecanismos de cooperación dentro del sistema interamericano para combatir el ciberdelito.

Como se analizó en el capítulo anterior de este trabajo de investigación, la OEA, es uno de los organismos internacionales que ha hecho gran labor en materia de ciberseguridad, al hacer informes anuales sobre la situación de los Estados de

América Latina y el Caribe, en los que no solo se presentan las problemáticas actuales que enfrentan estos países, sino que busca incentivar a los Estados ha crear y fortalecer sus estrategias en materia de ciberseguridad.

> Cabe señalar que con el fin de apoyar a los Estados Miembros en su lucha contra el crimen cibernético, la OEA, a través del Comité Interamericano contra el Terrorismo (CICTE) y del Programa de Seguridad Cibernética, está trabajando en el desarrollo de una agenda sobre seguridad cibernética en las Américas. En cooperación con una amplia gama de entidades nacionales y regionales de los sectores público y privado, tanto en asuntos políticos como técnicos, la OEA fomenta y fortalece las capacidades de seguridad cibernética entre los Estados Miembros a través de asistencia técnica y capacitación, mesas redondas sobre política, ejercicios de gestión de crisis e intercambio de mejores prácticas para el uso de tecnologías de la información y la comunicación.[79]

3.3 ESTUDIO ANALÍTICO DE LOS DELITOS INFORMÁTICOS REGULADOS EN MÉXICO

Dentro de este análisis, resulta necesario señalar, que en la legislación mexicana no existe un apartado específico que trate como tal de los delitos informáticos, por eso, es que no existe una definición en los marcos normativos de México, de conceptos como “cibercrimen” o “ciberdelito”.

No obstante, actualmente existen distintas leyes federales y locales para perseguir los delitos que utilizan las TIC como medio o fin para su comisión.

Cabe aclarar que la República Mexicana, compuesta por 32 Estados, cada Estado cuenta con la facultad de adoptar sus propios Códigos Civiles y Penales, así como

[79] Información extraída de la página oficial de la OEA http://www.oas.org/es/temas/seguridad_cibernetica.asp, fecha de consulta 07 de julio de 2017.

expedir sus propias reglas y legislación procesal. Tradicionalmente los Estados usan como modelo para crear sus legislaciones las leyes federales. No obstante, esto no es regla general y por lo tanto no existe una unificación en los Estados en cuanto a los tipos penales relacionados a los delitos cibernéticos, e incluso algunos códigos locales ni siquiera engloban los mismos tipos penales.

Aunque se ha intentado numerosamente conformar un Código Penal para todos los Estados de la República Mexicana, se han obtenido resultados infructuosos en virtud de que se ha requerido mantener la soberanía de cada Estado integrante de la Federación, los valores de sus habitantes.

> De manera recurrente, en el ámbito académico, existe la inquietud entre los noveles egresados de la Licenciatura en Derecho, para considerar como probable objeto de investigación el tema de los Delitos Informáticos, es decir, sugieren su inclusión, ya sea en el Código Penal Federal o en uno de carácter estatal, en razón a que perciben la ausencia de un Capítulo o un delito con tal denominación.[80]

En mi opinión, aunque en México actualmente gran parte de los delitos cibernéticos se encuentran previstos y sancionados en diversos ordenamientos jurídicos, ya sea en códigos penales, leyes federales, entre otros, no es de manera unánime, por lo que desde mi punto de vista es necesario crear una ley general, para atender a los delitos cibernéticos, de manera que aplique para todos los Estados de la República Mexicana, ya que como se ha mencionado, estos delitos tienen la peculiaridad de que su comisión puede llevarse a cabo en cualquier lugar, y para facilitar y eficientar la investigación de estos delitos así como de la cooperación que amerite cada caso, lo más factible sería tener una ley general que contenga todas las tipologías posibles, establezca conceptos básicos, y señale una metodología de investigación unificada para estos delitos.

[80] Piña Libien, Hiram Raúl, Los Delitos Informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano, documento en línea, pág. 7, http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf, fecha de consulta: 13 de julio de 2017.

3.3.1 BIENES JURÍDICOS PROTEGIDOS EN LOS DELITOS CIBERNÉTICOS

A lo largo de la evolución del Derecho se han ido distinguiendo diversos conceptos de lo que representa el bien-jurídico. “El concepto dogmático de bien jurídico, acuñado por Birnbaum a mediados del S. XIX, se refiere a los bienes que son efectivamente protegidos por el Derecho”.[81]

> Según Von Liszt, y bajo una concepción material del bien jurídico, su origen reside en el interés de la vida existente antes del Derecho y surgido de las relaciones sociales. El interés social no se convierte en bien jurídico hasta que no es protegido por el Derecho.
>
> En otras palabras el bien jurídico es la elevación a la categoría del bien tutelado o protegido por el derecho, mediante una sanción para cualquier conducta que lesione o amenace con lesionar este bien protegido, de esta reflexión se puede decir que el bien jurídico obtiene este carácter con la vigencia de una norma que lo contenga en su ámbito de protección, más si esta norma no existiera o caduca, éste no deja de existir pero si de tener el carácter de jurídico.
>
> Esta característica proteccionista que brinda la normatividad para con los bienes jurídicos, se hace notar con mayor incidencia en el derecho penal, ya que es en esta rama del derecho en que la norma se orienta directamente a la supresión de cualquier acto contrario a mantener la protección del bien jurídico, por ejemplo el delito de espionaje informático busca sancionar los actos que difunden en forma irregular la información privilegiada industrial o comercial a través de medios electrónicos.
>
> En la actualidad la conceptualización del bien jurídico, no ha variado en su aspecto sustancial de valoración de bien a una categoría superior, la de bien tutelado por la ley,

[81] Díaz García Alexander, El Bien Jurídico Tutelado de la Información y los Nuevos Verbos Rectores en los Delitos Electrónicos, Universidad Santiago de Cali, documento en línea, http://www.redipd.es/noticias_todas/2011/tribuna/common/1/EL_BIEN_JURIDICO_TUTELADO_DEL_DATO_Y_LOS_NUEVOS_VERBOS_RECTORES_DE_LOS_DELITOS_ELECTRONICOS_USC.pdf

> en cuanto a ciertos criterios como el origen, o como el área del derecho que deba contenerlos. El Derecho penal tiene su razón de ser en un Estado social porque es el sistema que garantiza la protección de la sociedad a través de la tutela de sus bienes jurídicos en su calidad de intereses muy importantes para el sistema social y por ello protegibles por el Derecho penal. [82]

Asimismo, hoy la tendencia en lo que respecta a los delitos informáticos es que la protección de los bienes jurídicos, se haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales que ya existen, para subsanar las actuales lagunas legislativas originadas por los novedosos comportamientos delictivos.

> Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente. De otro lado otra vertiente doctrinaria supone que la emergente Sociedad de la Información hace totalmente necesaria la incorporación de valores inmateriales y de la INFORMACIÓN misma como bienes jurídicos de protección, esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la intangible.
>
> En conclusión podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como:

- EL PATRIMONIO, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar.

[82] Ídem.

- LA RESERVA, LA INTIMIDAD Y CONFIDENCIALIDAD DE LOS DATOS, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos.
- LA SEGURIDAD O FIABILIDAD DEL TRÁFICO JURÍDICO Y PROBATORIO, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.
- EL DERECHO DE PROPIEDAD, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático. Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere. [83]

3.3. 2 ELEMENTOS DEL TIPO EN LOS DELITOS INFORMATICOS

El delito es "aquella acción del hombre, típica, antijurídica y culpable, que es lo que los alemanes han denominado el *unrecht* (ilícito), del cual se desprenden tres elementos fundamentales, a saber: la acción, el tipo y la tipicidad y la justificación".[84]

En este sentido, de manera general se puede decir que el tipo es la descripción de una conducta prohibida por la norma, la tipicidad por su parte es la cualidad de una conducta de adecuarse al tipo penal.

> La función del tipo es ver si la norma controla la conducta determinada. De esta forma los componentes del elemento objetivo del tipo recaen especialmente sobre la protección del bien jurídico y las modalidades de acción. En lo que respecta a la acción, para la concepción causal naturalista, la ilicitud tiene su acento en la lesión que se ha producido con independencia de cual sea la voluntad. En cambio para los finalistas, el acento se pone en la intencionalidad y eventual conocimiento de las circunstancias concomitantes.

[83] Acurio del Pino, Santiago, op.cit., pág. 22.
[84] Huerta Miranda, Marcelo y Libano Manzur Claudio, Delitos Informáticos, Editorial Jurídica ConoSur Ltda, Segunda Edición, Santiago de Chile, 1998, pág. 181.

> El tipo contiene la acción a través de los distintos verbos rectores, según los cuales los tipos pueden ser de mera actividad o de resultado. Los tipos de mera actividad […] son aquellos que se consuman por una simple acción del hombre, que basta por si sola para violar la ley, por ejemplo, las injurias y los allanamientos. Por su parte, los tipos de resultado […] son aquellos cuya consumación la ley requiere que se haya verificado el resultado querido por el agente y consistente en la ofensa de hecho del bien para cuya protección se ha creado la normal penal.[85]

Por lo anterior, se entiende que la regla general es que los delitos sean de mera actividad. No obstante en lo que se refiere a los delitos informáticos, la situación no puede salvarse en términos generales. Por lo que se debe analizar cada tipo penal en particular y ver si se trata de un delito de mera actividad, un ejemplo sería el fraude, o de resultados como el *hacking.*

Dentro de los elementos de los tipos penales se encuentran los elementos objetivos y subjetivos. Asimismo, los elementos objetivos abarcan los siguientes:

1.- Elementos descriptivos. Se integran por una enunciación precisa del objeto de la prohibición o del mandato contenido en el tipo legal inserto en los preceptos de la ley. Además, en ellos se definen de forma concreta las hipótesis de hecho a las que se asignan penas determinadas. Los elementos descriptivos del tipo son captables por los sentidos.

2.- Elementos normativos. Son aquellos no susceptibles de ser captados por nuestros sentidos, sino que tienen que ser comprendidos por el razonamiento, ya que llevan implícito un juicio de valor, por ejemplo, cuando se habla de la “buena fama”.

[85] Ídem.

“En lo que respecta a los delitos informáticos el elemento descriptivo es esencial, debido a su extraordinaria complejidad, principalmente enfocada a las conductas que realiza el delincuente de estos delitos.”[86]

Por otro lado, en lo que respecta al elemento normativo de tipo delictivo informático, la condición valorativa es esencial, debido a la disparidad de opiniones y criterios y la casi inexistencia de lenguajes y conceptos comunes generalmente aceptados, el rol valorativo, auxiliado por lo jurídico o por lo cultural, presenta un papel preponderante.

Los elementos subjetivos por su parte, se encuentran gobernados por el principio de los actos humanos finales y previsibles. Es decir que solo que es factible de preverse es, a la vez, susceptible de penalizarse. Quedado excluidos los casos fortuitos y de fuerza mayor.

Los actos previsibles pueden ser dolosos o culposos. Esto es lo que determina la fase subjetiva del tipo penal del que se trate. En los actos dolosos, además de ser previsibles, el delincuente había realizado en su mente la configuración de un fin determinado, es decir, que quería la acción y el resultado.

En los culposos, el delincuente no previó el resultado, es decir quería la acción pero no el resultado.

3.3.3 LOS DELITOS CIBERNÉTICOS EN LA LEGISLACIÓN MEXICANA, UN BREVE ACERCAMIENTO

[86] Ibídem, pág. 182.

A continuación, se realiza el análisis de algunos delitos tradicionales regulados en el Código Penal Federal vigente, en donde el tipo penal incluye de manera explícita o implícita la posibilidad de que se utilicen las TIC ya sea como medio o como fin para llevar a cabo su comisión.

Es importante señalar que existen una serie de delitos especiales contenidos en Leyes Federales, independientemente de las legislaciones locales que también regulan delitos informáticos.

Los primeros delitos que se señalan dentro del Código Penal Federal son los que están en contra de la seguridad de la Nación. Aquí se encuentran "varios delitos que se comenten a través de Internet, redes sociales, correos electrónicos y mensajes instantáneos, los cuales desafortunadamente pueden poner en riesgo incluso la seguridad y soberanía de nuestro país".[87]

Ejemplo de ello, es el delito de traición a la patria mencionado en el artículo 123 del presente código, en el que se podría dar fuga de información y la organización de grupos, a través de las TIC para llevar conductas mencionadas en este artículo tales como:

> *Artículo 123.- Se impondrá la pena de prisión de cinco a cuarenta años y multa hasta de cincuenta mil pesos al mexicano que cometa traición a la patria en alguna de las formas siguientes:*
>
> *I.- Realice actos contra la independencia, soberanía o integridad de la Nación Mexicana con la finalidad de someterla a persona, grupo o gobierno extranjero;*
>
> *II.- Tome parte en actos de hostilidad en contra de la Nación, mediante acciones bélicas a las órdenes de un Estado extranjero o coopere con éste en alguna forma que pueda perjudicar a México […]*

[87] Lira, Arteaga Óscar Manuel, Cibercriminalidad, Fundamentos de Investigación en México, INACIPE, Segunda Edición, México, 2014, pág. 151.

III.- Forme parte de grupos armados dirigidos o asesorados por extranjeros; organizados dentro o fuera del país, cuando tengan por finalidad atentar contra la independencia de la República, su soberanía, su libertad o su integridad territorial o invadir el territorio nacional, aun cuando no exista declaración de guerra;

V.- Reclute gente para hacer la guerra a México, con la ayuda o bajo la protección de un gobierno extranjero;

VI.- Tenga, en tiempos de paz o de guerra, relación o inteligencia con persona, grupo o gobierno extranjeros o le dé instrucciones, información o consejos, con objeto de guiar a una posible invasión del territorio nacional o de alterar la paz interior;

VII.- Proporcione dolosamente y sin autorización, en tiempos de paz o de guerra, a persona, grupo o gobierno extranjeros, documentos, instrucciones o datos de establecimientos o de posibles actividades militares;

VIII.- Oculte o auxilie a quien cometa actos de espionaje, sabiendo que los realiza;

XI.- Invite a individuos de otro Estado para que hagan armas contra México o invadan el territorio nacional, sea cual fuere el motivo que se tome; si no se realiza cualquiera de estos hechos, se aplicará la pena de cuatro a ocho años de prisión y multa hasta de diez mil pesos;[88]

Asimismo, se indica en el artículo 127 el espionaje, delito que actualmente es bien entendido gracias a las noticias en medios de comunicación relacionadas con la publicación de información clasificada, como confidencial de distintos gobiernos alrededor del mundo, producto incluso del espionaje de agencias del gobierno de Estados Unidos publicadas por Edward Snowden, así como de la plataforma mundial Wikileaks, donde se difundió información incluso del gobierno mexicano, "y que dan sustento a la importancia de identificar conductas que se lleva a cabo mediante la utilización de códigos maliciosos (virus), ingeniería social y quebrantamiento de sistemas (hackeo)."[89]

Otro delito interesante a comentar dentro de los delitos contra la seguridad de la Nación vulnerable a llevarse a cabo mediante las TIC es el delito de sabotaje, mencionado en el artículo 140 de este código, "vale la pena aclarar que lo que se identifica como negación de servició en el argot técnico en realidad es un sabotaje,

[88] Código Penal Federal, Diario Oficial de la Federación, última reforma del 26 de junio de 2017.
[89] Lira Arteaga, Óscar Manuel, op. cit. pág. 153.

ya que, por ejemplo, los ataques a los servidores que alojan las páginas de las distintas instituciones gubernamentales a nivel nacional e internacional". [90]

Este código define el delito de sabotaje como:

> *Artículo 140.- Se impondrá pena de dos a veinte años de prisión y multa de mil a cincuenta mil pesos, al que dañe, destruya, perjudique o ilícitamente entorpezca vías de comunicación, servicios públicos, funciones de las dependencias del Estado, organismos públicos descentralizados, empresas de participación estatal, órganos constitucionales autónomos o sus instalaciones; plantas siderúrgicas, eléctricas o de las industrias básicas; centros de producción o distribución de artículos de consumo necesarios de armas, municiones o implementos bélicos, con el fin de trastornar la vida económica del país o afectar su capacidad de defensa.*

Bajo este orden de ideas, y ampliando el concepto de sabotaje, para Romeo Casabona el sabotaje informático consiste en la destrucción o inutilización del soporte lógico, esto es, de datos y/o programas contenidos en un ordenador (en sus bandas magnéticas).[91]

Dentro de esta modalidad de sabotaje, se encuentra la intervención en los sistemas de teleproceso, la cual consiste en una forma de sabotaje informático por medios telemáticos. Esta modalidad permite llevar a cabo un sabotaje a distancia, a través del acceso a las redes de telecomunicaciones.

Ulrich Sieber "cita el increíble, pero veraz caso de los pequeños estudiantes primarios de una escuela neoyorquina que en 1980, a través de su computador escolar de práctica, se introdujeron en bancos de datos de compañías canadienses

[90] Ibídem, pág. 158.
[91] Huerta Miranda, Marcelo y Libano Manzur Claudio, op.cit. pág. 139.

y del gobierno federal, logrando en algunos casos destruir las informaciones que allí se contenían."[92]

Dentro de los delitos contra la salud que señalados el presente código, desafortunadamente tanto el internet como la telefonía celular se han convertido en un medio idóneo y de fácil acceso, para comerciar, publicitar e incluso financiar todo tipo de sustancias ilegales, considerando los artículos referentes a la producción, tenencia, tráfico, proselitismo y otros actos en materia de narcóticos.

Artículo 194.- Se impondrá prisión de diez a veinticinco años y de cien hasta quinientos días multa al que:

I.- Produzca, transporte, trafique, comercie, suministre aun gratuitamente o prescriba alguno de los narcóticos señalados en el artículo anterior, sin la autorización correspondiente a que se refiere la Ley General de Salud;

Para los efectos de esta fracción, por producir se entiende: manufacturar, fabricar, elaborar, preparar o acondicionar algún narcótico, y por comerciar: vender, comprar, adquirir o enajenar algún narcótico.

Por suministro se entiende la transmisión material de forma directa o indirecta, por cualquier concepto, de la tenencia de narcóticos.

.

III.- Aporte recursos económicos o de cualquier especie, o colabore de cualquier manera al financiamiento, supervisión o fomento para posibilitar la ejecución de alguno de los delitos a que se refiere este capítulo; y

IV.- Realice actos de publicidad o propaganda, para que se consuma cualesquiera de las sustancias comprendidas en el artículo anterior.

Otros delitos interesantes que su ejecución se lleva a cabo mediante las TIC, son los delitos contra el libre desarrollo de la personalidad.

Siendo un hecho desafortunado que el internet y la telefonía celular sean medios utilizados para el comercio y distribución de material pornográfico, sitios en donde con frecuencia se exponen imágenes de menores de edad. Lo anterior implica no sólo la publicación de dichas fotografías a través de Internet y teléfonos celulares, sino la

[92] Ibídem, pág. 144.

explotación, secuestro e incluso la desaparición y muerte de cientos de miles de menores, alrededor del mundo. [93]

Artículo 200.- Al que comercie, distribuya, exponga, haga circular u oferte, a menores de dieciocho años de edad, libros, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter pornográfico, reales o simulados, sea de manera física, o a través de cualquier medio, se le impondrá de seis meses a cinco años de prisión y de trescientos a quinientos días multa.

Artículo 202.- Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa.

A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito.

Dentro de los delitos más relevantes que se señalan en este código, que utilizan las TIC, en su ejecución, se encuentra el delito de revelación de secretos y acceso ilícito a sistemas y equipos de informática. Estos versan “específicamente de sistemas informáticos; al respecto, cabe señalar que se habla de robo de secretos

[93] Lira Arteaga, Óscar Manuel, op. cit. pág. 163 y 164.

industriales, acceso no autorizado a un equipo de cómputo al cual se está autorizado".[94]

Artículo 210.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- 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 cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

[94] Ibídem, pág. 168.

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 3.- 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 ocho 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 cuatro 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 cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. 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 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Por otro lado, encontramos el delito de falsificación de documentos, por ejemplo, con la capacidad que existe hoy en día de procesamiento y la calidad de impresión de computadoras y equipos de impresión, permiten que los delincuentes los utilicen a su favor, para falsificar documentos oficiales como los títulos profesionales, documentos de identidad como la credencial para votar, licencias de manejo, papel moneda, entre otros.

Como se ha analizado, casi cualquier delito tradicional puede llevarse a cabo mediante las TIC, o al menos valerse de ellas para llevar a cabo parte de la ejecución de la conducta delictiva.

Inclusive, en los delitos contra la vida y la integridad corporal se utiliza el internet y la telefonía celular para hostigar, amenazar, extorsionar y/o falsificar documentos con la finalidad de usurpar nuestra personalidad, entre otros. Por ejemplo "las lesiones psicológicas se encuentran en nuestra legislación y me parece responsable hacer comprender que las palabras, fotos y videos de los cuales los delincuentes se valen para martirizar a sus víctimas a través de redes sociales, correos electrónicos y mensajes de texto pueden dejar cicatrices en la personalidad de las víctimas que en ocasiones no terminan de sanar".[95]

El delito de operaciones con recursos de procedencia ilícita, mejor conocido como el lavado de dinero, en el que

[95] Ibídem pág. 176.

> "Ante la facilidad de realizar transferencias en sistemas financieros mediante dispositivos móviles e Internet, la movilización de recursos de procedencia ilícita, que utilizan para ello cuentas bancarias de otras personas sin su consentimiento, se realiza con tal velocidad y sigilo que incluso para las instituciones financieras es difícil detectar dichos movimientos, pues en ocasiones son realizadas por personal que trabaja en las propias instituciones". [96]

Como se ha analizado, casi cualquier delito tradicional puede llevarse a cabo mediante las TIC ya se con el uso de códigos maliciosos, la ingeniería social, correos electrónicos, telefonía celular, uso de redes sociales, entre otros.

Este análisis, fue tan solo de una legislación a nivel nacional, pero existen otras legislaciones no solo en materia penal como la Ley Federal de Telecomunicaciones, donde resulta de gran importancia la regulación de los distintos proveedores de servicios, así como la importancia de colaborar con las autoridades en la investigación de los delitos, por ejemplo: en la localización geográfica, en tiempo real, de los equipos de comunicación móvil asociados a una línea que se encuentra vinculada a un delito de delincuencia organizada, secuestro, extorsión o amenaza.

El Código de Comercio, en relación con la firma electrónica y los aspectos legales que se deben tomar en cuenta para poder emplearla como instrumento de comunicación confiable. Así como de la regulación del comercio electrónico.

La Ley Federal del Derecho de Autor, en vinculación del uso de las redes informáticas para sustraer y distribuir obras protegidas por el derecho de autor, ya que hoy en día la tecnología permite hacer mucho más fácil el robo y la distribución de programas de computación, obras musicales, entre otros.

[96] Ibídem, pág. 182 y 183.

Finalmente, por mencionar una más, la Ley de la Propiedad Industrial, cuando se habla por ejemplo del espionaje industrial, el cual es un delito que se comete básicamente en los sistemas informáticos.

CAPÍTULO IV ESTRATEGIA INTEGRAL DE CIBERSEGUIDAD PARA AMÉRICA LATINA Y EL CARIBE

4.1 ARMONIZACIÓN LEGISLATIVA EN AMÉRICA LATINA Y EL CARIBE

Como se mencionó en el capítulo anterior de este trabajo, México al igual que otros países de América Latina y el Caribe, deben buscar la adhesión al Convenio de Budapest en materia de cibercrimen, a modo de coordinar esfuerzos a nivel internacional y trabajar en conjunto para la armonización legislativa.

Esto fortalecerá la cooperación internacional, optimizando la labor de las autoridades responsables en la investigación de los delitos cibernéticos en los países de la región.

En la actualidad tanto los patrones de conducta como las modalidades delictivas de los delincuentes en el ciberespacio han evolucionado, perfeccionando la comisión de los delitos tradicionales mediante el uso de las TIC, de igual forma propician el surgimiento de nuevas formas de delinquir.

> La actuación policial y judicial de los Estados en materia de ciberseguridad deberá adecuarse, a este cambio social.
>
> Para afrontar adecuadamente estas amenazas, que traspasan en muchos casos las fronteras de los Estados, es imprescindible el fortalecimiento de la cooperación judicial y policial internacional, articulando los instrumentos adecuados de colaboración e intercambio de información y la armonización de las legislaciones nacionales, con el desarrollo y mantenimiento de una regulación sólida y eficaz. Igualmente, se hace necesario fomentar la colaboración ciudadana, facilitando los procedimientos de acceso y transmisión de la información de interés policial. El éxito en la lucha contra el terrorismo y la delincuencia en el ciberespacio exige la articulación de los mecanismos

> necesarios que mejoren las capacidades de las instituciones policiales y los organismos judiciales competentes.[97]

A partir de mi experiencia en México, considero que falta mayor coordinación entre las autoridades encargadas de investigar este tipo de delitos, además de una deficiente comunicación entre los organismos federales y estatales, no existe un adecuado intercambio de información o apoyo que se pueden necesitar de un organismo a otro, e incluso de proveedores de servicios de internet, como consecuencia de esta situación no se atienden con oportunidad los casos que se presentan.

De tal manera que la adhesión de México al convenio de Budapest, así como de la totalidad de los países de América Latina y el Caribe, sería un parteaguas, para el fortalecimiento de la cooperación internacional y el debido proceso en la investigación de los delitos cibernéticos.

De acuerdo, a un informe de la ONU en febrero de 2013.

> A nivel mundial 82 países han firmado y/o ratificado un instrumento obligatorio sobre el delito cibernético. Además de contar con miembros oficiales que los aplican directamente, los instrumentos multilaterales han influido indirectamente en las legislaciones nacionales en forma indirecta, al ser adoptados como modelo por países que no son parte en ellos, o las legislaciones de los Estados Partes han influido en otros países.
>
> La adhesión a un instrumento multilateral sobre el delito cibernético coincide con la percepción de una mayor suficiencia de las leyes nacionales penales y procesales, lo que indica que, generalmente, las disposiciones multilaterales vigentes en la materia se

[97] Gobierno de España, Estrategia de Ciberseguridad Nacional 2013, Departamento de Seguridad Nacional, pág. 24, https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf, fecha de consulta 26 de julio 2017.

> consideran eficaces. En opinión de los más de 40 países que suministraron información, el Convenio sobre el delito cibernético, del Consejo de Europa, es el instrumento multilateral más utilizado para elaborar legislación sobre este tema. En total los instrumentos multilaterales de otros "grupos" se utilizaban en la mitad de ese número de países.[98]

La armonización legislativa penal y procesal para perseguir sancionar delitos cibernéticos en América Latina y el Caribe, es una propuesta viable, para que los países de esa región, puedan hacer frente, de manera eficiente, a los retos actuales y futuros que traen consigo esta nueva era de criminalidad a nivel global.

Para llevar a cabo debidas investigaciones de delitos cibernéticos, y considerando que en su mayoría estas investigaciones requieren no solo de la "reacción inmediata de las autoridades del país o países donde él o los presuntos responsables se encuentran ubicados, sino también de la cooperación jurídica internacional, a través de los mecanismos e instrumentos para tal fin".[99]

Algunos instrumentos jurídicos más comunes utilizados por los países para lograr la cooperación judicial en forma bilateral y multilateral son: los Tratados de asistencia mutua, Acuerdos de Asistencia Mutua, Acuerdos Ejecutivos y Comisiones Rogatorias, entre otros.

[98] UNODC, Resumen del Estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, Viena, 2013, pág. 5, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_S.pdf, fecha de consulta 29 de julio 2017.
[99] Cristos Velasco, San Martín, op.cit. pág. 284.

4.2 LA INVESTIGACIÓN EN LOS DELITOS CIBERNETICOS

Dentro de los retos que tiene la investigación de los delitos cibernéticos a nivel global, es la dificultad en la identificación, rastreo o seguimiento de la información, que se deriva del funcionamiento de los sistemas informáticos, concretamente de la estructura de Internet, que tiene las siguientes características:

- Es una estructura mundial, cuyos canales de comunicación no son físicos sino digitales, lo que dificulta el control fronterizo y la ubicación territorial de actividades, conexiones y operaciones.
- La arquitectura de Internet favorece un alto nivel de opacidad en las conexiones y facilita el anonimato de los internautas, lo que hace difícil la identificación y rastreo de los datos de navegación.
- La determinación de responsabilidad, estrechamente vinculada a los problemas de autoría, viene dificultada por la falta de una reglamentación común a nivel internacional sobre la actividad de los intermediarios, empresas y prestadores de servicios en las actividades presuntamente delictivas.
- La tecnología informática, especialmente la pretendida invulnerabilidad de los sistemas, constituye en la actualidad una marca de calidad en la actividad de las empresas y operadores financieros, de tal suerte que la violación de tales sistemas raramente se denuncia dado el peligro que ello supondría para su credibilidad y para la confianza de los clientes.
- Bajo el índice de denuncias deriva también la clandestinidad que con frecuencia acompaña la actividad de los *hackers* o piratas informáticos, de modo que la víctima raras veces conoce o detecta la vulneración de su sistema informático.
- Por último, las técnicas de encriptado y firma digital, que progresivamente se van imponiendo entre los usuarios, dificultan en gran medida los procesos de investigación e interceptación de contenidos delictivos, así como de la identificación de destinatarios y remitentes de la información. [100]

[100] Flores Prada Ignacio, Criminalidad Informática (aspectos sustantivos y procesales), Tirant lo blanch, México, 2012, pág. 310 y 311.

Bajo este tenor, no resulta difícil advertir la necesidad constante de especialización en los técnicos y en las técnicas de investigación policial y judicial, además de los instrumentos legislativos, como: las fuentes y medios de prueba.

Dentro de las necesidades preponderantes para poder llevar a cabo una debida investigación de los ciberdelitos, se señalan las siguientes:

- Dotación de unidades policiales especializadas en la investigación de delitos informáticos.
- Fortalecimiento de los sistemas de cooperación internacional entre los cuerpos policiales de los distintos países, funcionamiento de órganos de coordinación entre ellos, y creación de unidades policiales internacionales dependientes de agencias intergubernamentales de la investigación.
- Medidas legislativas comunes sobre la creación de programas informáticos y sistemas de conexión, que permitan la existencia de <<puertas traseras>> por las que pueda canalizarse la investigación criminal.
- Constitución de escalas especiales de peritos informáticos al servicio de cuerpos policiales, fiscales y tribunales de justicia, así como de centros o institutos de investigación y análisis de procesos y sistemas informáticos relacionados con la actividad delictiva.
- Creación de fiscalías especiales con formación de fiscales especializados en la investigación y persecución de la delincuencia informática.
- Modificaciones legislativas en los ordenamientos procesales tendentes a recoger y prever medidas de interceptación de las comunicaciones informáticas, datos de navegación por la Red, rastreo de contenidos delictivos, confección de páginas web o utilización de programas de suministro de información criminal en Internet.
- Acuerdos y convenios internacionales para el reconocimiento y ejecución de sentencias relativas a los delitos informáticos, para la ejecución de sentencias relativas a delitos informáticos, para la cooperación entre jueces y fiscales de

distintos países y para la fijación y ejecución de la responsabilidad civil derivada del delito. [101]

El fenómeno actual de la cibercriminalidad, no solo es un desafío para el Derecho penal sustantivo, sino también para el Derecho procesal, al ser éste, el responsable de diseñar y poner en funcionamiento los medios e instrumentos para la investigación de los delitos cibernéticos.

4.2.1 CADENA DE CUSTODIA

Uno de los aspectos más delicados en la investigación de los delitos cibernéticos, es la volatilidad de los indicios, ya que éstos se pueden borrar, alterar, o simplemente perderse los datos que estén contenidos en medios electromagnéticos o electrónicos; también se puede alterar con mucha facilidad el lugar de los hechos, por ejemplo: las variantes del entorno donde se encontró el hecho delictivo, los equipos a analizar, sistemas operativos utilizados, políticas de seguridad aplicadas, entre otros.

"Para reducir estos factores de riesgo de pérdida de evidencia, los peritos en la materia de TIC, deben aplicar técnicas y metodologías de investigación científica, las cuales serán fundamentales al momento de integrar el expediente de una investigación judicial".[102]

En México se utiliza la cadena de custodia como técnica de investigación por excelencia y tiene su fundamento jurídico en el artículo 227 del Código Nacional de Procedimientos Penales, que a la letra señala lo siguiente:

[101] Ibídem, pág. 312.
[102] Lira Arteaga, Óscar Manuel, op.cit. pág. 251.

Artículo 227. Cadena de custodia La cadena de custodia es el sistema de control y registro que se aplica al indicio, evidencia, objeto, instrumento o producto del hecho delictivo, desde su localización, descubrimiento o aportación, en el lugar de los hechos o del hallazgo, hasta que la autoridad competente ordene su conclusión. Con el fin de corroborar los elementos materiales probatorios y la evidencia física, la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, empaque y traslado; lugares y fechas de permanencia y los cambios que en cada custodia se hayan realizado; igualmente se registrará el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos.[103]

4.2.2 EL MINISTERIO PÚBLICO

Cabe señalar, que en este ordenamiento jurídico también se establece en su artículo 127, que el Ministerio Público es el competente de conducir la investigación de los delitos, coordinar a las policías y a los peritos durante la investigación.

Artículo 127. Compete al Ministerio Público conducir la investigación, coordinar a las Policías y a los servicios periciales durante la investigación, resolver sobre el ejercicio de la acción penal en la forma establecida por la ley y, en su caso, ordenar las diligencias pertinentes y útiles para demostrar, o no, la existencia del delito y la responsabilidad de quien lo cometió o participó en su comisión.

De igual modo, la Constitución Política de los Estados Unidos Mexicanos en el artículo 21, señala que es competencia del Ministerio Público llevar a cabo la investigación de los delitos.

[103] Código Nacional de Procedimientos Penales, última reforma publicada en el DOF el 17 de junio de 2016, versión digital, http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_170616.pdf , fecha de consulta 31 de julio de 2017.

Artículo 21. La investigación de los delitos corresponde al Ministerio Público y a las policías, las cuales actuarán bajo la conducción y mando de aquél en el ejercicio de esta función.

Con lo anterior, se asume que de acuerdo a la legislación mexicana, el único "responsable de una investigación, y de la integración del expediente de la misma, es el Agente del Ministerio Público, cuyo conocimiento de las leyes y su correcta interpretación permite tipificar y dar cauce a una investigación ministerial".[104] Cabe aclarar que las investigaciones sobre posibles comisiones de delitos informáticos, pueden ser a nivel local o federal, según sea el caso en particular. Por lo que serán competencia de Ministerios Públicos Federales o Locales.

4.2.3 LA POLICÍA

Por otro lado, tal y como se señala en los artículos citados con anterioridad, la policía también tiene un papel muy importante dentro de las investigaciones de posibles hechos delictivos, es responsable de auxiliar al agente del Ministerio Público en sus labores de investigación, los policías deben tener conocimientos y habilidades suficientes "para preservar los indicios encontrados en el lugar de los hechos en caso de no contar con peritos especialistas en una determinada materia".[105]

La actuación de los policías tiene gran relevancia, resguardan el lugar del hecho presuntamente delictivo y emiten su informe de actuaciones. No obstante, los policías no emiten dictámenes periciales, los cuales dan sustento científico a la posible evidencia.

[104] Lira Arteaga, Óscar Manuel, op.cit. pág. 252.
[105] Ibídem, pág. 256.

4.2.4 LA CRIMINALÍSTICA Y LOS PERITOS

Antes de hablar de la función de los peritos, considero importante hondar un poco sobre el origen, desarrollo y concepto de la criminalística.

El término Criminalística fue empleado por primera vez en 1892 por el juez de instrucción Hans Gross en su obra *El manual del juez*. Este texto sienta las bases de la Criminalística con las materias de Antropometría, Argot Criminal, Contabilidad, Criptografía, Dibujo Forense, Documentoscopía, Explosivos, Fotografía, Grafología, Hechos de Tránsito Ferroviario, Hematología, Incendios, Medicina Legal, Química Legal e interrogatorio.

A nivel mundial la Criminalística se consolida a finales del siglo XIX y principios del XX. En el caso de México, en 1926, Benjamín Martínez y Carlos Roumagnac iniciaron la fase científica de la policía con la creación del Gabinete de Identificación y el Laboratorio de Investigación Criminalística, dependiente de la Jefatura del Distrito Federal.

> En 1941, el maestro Alfonso Quiroz Cuarón, quien es reconocido como la máxima figura en la materia en nuestro país, por haber identificado al espía que asesinó a Trotsky, fundó la Sección de Investigadores Especiales del Banco de México, realizando la selección técnica y procurando la capacitación del elemento humano que constituye el cuerpo de investigadores. Para 1964, logró que la Facultad de Medicina impartiera el curso de adiestramiento de Medicina Forense.[106]

Actualmente, en México la Agencia de Investigación Criminal de Procuraduría General de la República cuenta con una Coordinación General de Servicios

[106] Ibídem, pág. 9.

Periciales, que es líder a nivel nacional en la generación de metodologías de investigación forense.

“Cuenta con las siguientes especialidades: análisis de voz, antropología forense, asuntos fiscales y financieros, audio y video, balística forense, delitos ambientales, documentos cuestionados, fotografía forense, genética forense, incendios y explosiones, informática, telecomunicaciones”,[107] entre otras.

Por otro lado, el concepto de Criminalística varía de acuerdo al tiempo y el espacio en el que nos situemos, no obstante al día de hoy considero que la manera en que define a la Criminalística el Dr. Alfonso Quiroz Cuarón, sigue siendo sencilla y muy basta.

“La Criminalística es la disciplina auxiliar del Derecho penal que se ocupa del descubrimiento y verificación científica del delito y del delincuente”.[108]

La criminalística aplica fundamentalmente los conocimientos, métodos y técnicas de investigación de las distintas ciencias naturales, con el fin de determinar, en auxilio de las autoridades responsables de administrar justicia, la existencia, reconstrucción, o bien determinar la intervención de uno o más sujetos en un posible hecho delictivo.

Su objeto de estudio son los indicios o evidencia física relacionada con los hechos posiblemente delictivos que se investiguen. Las personas especializadas en las distintas áreas de esta disciplina se conocen como peritos, los cuales tienen la labor

[107] Ibídem, pág.10.
[108] Ibídem, pág. 11.

de emitir dictámenes, que darán soporte a la investigación que lleve a cabo el Ministerio Público para el esclarecimiento de la posible comisión de un delito.

De acuerdo con la legislación mexicana, el artículo 25 de la Ley Orgánica de la Procuraduría General de la República:

> *Artículo 25.- Los peritos actuarán bajo la autoridad y mando inmediato del Ministerio Público de la Federación, sin perjuicio de la autonomía técnica e independencia de criterio que les corresponde en el estudio de los asuntos que se sometan a su dictamen.*[109]

A manera de síntesis, la investigación criminal es la parte primordial, para llevar a cabo el esclarecimiento de los hechos posiblemente constitutivos de un delito. Sin una adecuada legislación que regule los métodos y mecanismos correctos de investigación, así como de la preparación que debe tener cada uno de los que intervienen en las investigaciones, difícilmente se podría garantizar una correcta impartición de justicia.

La investigación de los delitos cibernéticos, resulta a veces mucho más compleja, por los tecnicismos utilizados, por la volatilidad de la evidencia, y por la falta de capacitación y especialización de las autoridades responsables de llevar a cabo este tipo de investigaciones.

No obstante, si se parte desde un buen ordenamiento jurídico, cooperación entre las autoridades e involucrados en investigar estos delitos, así como de una correcta inversión en tecnología que facilite y optimice las investigaciones, definitivamente se verán mejoras en el tema de la ciberseguridad de los países, de la región de

[109] LEY ORGÁNICA DE LA PROCURADURÍA GENERAL DE LA REPÚBLICA, última reforma del 29 de mayo de 2009, http://www.oas.org/juridico/spanish/mesicic3_mex_anexo23.pdf, fecha de consulta 31 de julio 2017.

América Latina y el Caribe, lo cual impulsará y fortalecerá la cultura de ciberseguridad a la que todos los países deben aspirar, con el fin de tener un mundo más seguro.

4.3 CENTROS DE RESPUESTA A EMERGENCIAS DE CÓMPUTO (CERT´S)

Los Centros de Respuesta a Emergencia de Cómputo, conocidos por sus siglas en inglés como CERT´s (*Computer Emergency Response Team*) o CSIRT *(Computer Security Incident Response Team)*, para referirse al mismo concepto.

Las siglas CSIRT se suelen usar en Europa en lugar del término protegido CERT, que está registrado en EEUU por el CERT *Coordination Center* (CERT/CC).

Los CERT´s tienen como "función principal monitorear la seguridad de las redes y sistemas de información, con el objeto de coordinar, facilitar y ofrecer servicios de respuesta inmediata tanto a víctimas del delito como a organizaciones e instituciones encargadas de la administración y control de sistemas de seguridad y cómputo".[110]

Desde mi punto de vista, los CERT´s tienen una función muy importante en la identificación de nuevas amenazas cibernéticas, además son un conducto para facilitar información para la prevención y resolución de incidentes y problemas derivados de ataques cibernéticos, como virus, *spam, malware*, troyanos, entre otros. Y sirven como punto nacional de contacto para coordinar las respuestas y estrategias vinculadas con la seguridad en las TIC.

[110] Cristos Velasco, San Martín, op.cit. pág. 369.

Se tiene registro de que el primer CERT fue creado en Estados Unidos en el año 1988, en respuesta a las necesidades expuestas durante el incidente en el que el primer ejemplar de malware autorreplicable llamado el Gusano Morris afectó a Internet. Se sabe que aproximadamente 6000 de los 60 000 servidores conectados a la red fueron infectados por este gusano informático.

De manera general las funciones, pues, de un CERT/CSIRT son:

- Ayudar al público objetivo (*constituency*) a atenuar y prevenir incidentes graves de seguridad.
- Ayudar a proteger informaciones valiosas.
- Coordinar de forma centralizada la seguridad de la información.
- Guardar evidencias, por si hubiera que recurrir a pleitos.
- Apoyar y prestar asistencia a usuarios para recuperarse de las consecuencias de los incidentes de seguridad. objetivo (sector comercial, público, nacional, militar, entre otros) establece sus prioridades
- Dirigir de forma centralizada la respuesta a los incidentes de seguridad - Promover confianza, que alguien controla la situación.
- Ayuda a difundir la cultura de seguridad informática y crear medios de difusión para organizaciones e individuos.

Cada CERT es diferente y en función de sus recursos y su público y aportar servicios diferentes como:

- Avisos de seguridad.
- Búsqueda de vulnerabilidades.
- Auditorías o evaluaciones de seguridad.
- Configuración y mantenimiento de herramientas de seguridad, aplicaciones e infraestructuras.
- Desarrollo de herramientas de seguridad.

- Propagación de información relacionada con la seguridad.

Actualmente, no todos los países de América Latina y el Caribe, cuentan con CERT´s, no obstante los países que si cuentan con al menos uno, están fortaleciendo su estrategia de ciberseguridad, ya que los CERT´s son de gran utilidad.

Por ejemplo, en México se cuenta con el UNAM-CERT, que fue oficialmente reconocido para operar en el 2001.

> UNAM-CERT funciona como un centro de investigación para diseminar información, proporcionar asesoría y servicios de seguridad, así como para intercambiar experiencias y puntos de vista en torno a políticas de seguridad de sistemas de información y cómputo para ayudar a disminuir la cantidad y gravedad de los problemas de seguridad, así como para difundir una cultura de la seguridad en cómputo en México.[111]

Asimismo, México cuenta con el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX) de la Policía Federal, perteneciente al área de la División Científica. El CERT-MX "es la única institución acreditada a nivel federal para el intercambio de información con las policías cibernéticas nacionales e internacionales, además de contar con la capacidad de identificar y atender posibles ataques en agravio de la infraestructura gubernamental o contra la ciudadanía en general"[112].

[111] Cristos Velasco, San Martín, op.cit. pág. 370.
[112] Comisión Nacional de Seguridad, Fortalece CNS Estrategias para la Protección del Ciberespacio Mexicano, comunicado de prensa, 25 de febrero 2015, http://www.denuncia.gob.mx/portalWebApp/wlp.c;jsessionid=n2wmJxvJv1KY2J5cWQLBTfcQrdJ4tcvV11fqhw1JQpvGGvzwLJ2s!-1886721534?__c=f7130, fecha de consulta 01 de agosto 2017.

Países como Chile, Colombia, Brasil, Argentina también cuentan con CERT´s, que sin duda fortalecen su estrategia de ciberseguridad a nivel nacional, no obstante, lo idóneo sería que todos los países de la región contaran con CERT´s, a fin de fortalecer la cooperación internacional y la cultura de ciberseguridad, ya que son una herramienta para combatir y prevenir amenazas vinculadas a las TIC.

4.3.1 CIBERINTELIGENCIA COMO ESTRATEGIA PARA PREVENIR LAS AMENZAS Y ATAQUES INFORMÁTICOS

Dentro de los servicios que ofrece un CERT, se encuentran: el análisis de tráfico de red, análisis de vulnerabilidades y pruebas de penetración, análisis de riesgos, creación de políticas de seguridad de la información, programas de capacitación, respuesta a incidentes de seguridad de la información, entre otros.

La seguridad de la información está vinculada con la administración de riesgos, y riesgo se puede definir como la probabilidad de que una amenaza explote una vulnerabilidad, ocasionando un impacto a la organización. Es decir, que si no hay amenaza no hay riesgo, y si no hay vulnerabilidades, aunque haya amenaza tampoco hay riesgo, y aun si hay amenazas y vulnerabilidades, si no hay impacto tampoco hay riesgo.

En la actualidad, las estrategias de ataque implementadas son muy complejas y de largo plazo, ya que utilizan múltiples pasos estructurados, a los que se les conoce como ciclo de vida de un ataque, el cual se puede sintetizar de la siguiente manera:

1. Preparación. Abarca la identificación, selección del objetivo a atacar y recolección de toda la información que sea posible acerca de la víctima, así como la creación o adquisición del arsenal de ciberarmas.

2. Obtención de acceso. Envío de las ciberarmas por diversos medios, siendo el correo electrónico (*spearphishing*), sitios Web infectados y dispositivos USB los tres más comunes para explotar vulnerabilidades en el sistema de la víctima y evadir los sistemas de seguridad que tenga.

3. Creación de persistencia. Los atacantes buscan afirmar y ampliar su presencia y control en la red de la víctima, realizando el reconocimiento de la red, diversos movimientos laterales y robo de credenciales de administradores.

4. Ejecución de acciones. Considera la selección y recolección de la información buscada hasta lograr la extracción de la misma (*exfiltration*).

5. Eliminación de rastros**.** Una vez logrados sus objetivos, el intruso buscará eliminar todos los rastros e indicios que pudieran revelar las acciones tomadas, sus tácticas, técnicas y procedimientos.[113]

Lo mencionado, definitivamente son acciones que de manera implícita llevan la labor de inteligencia.

Bajo este tenor, resulta ilustrativo definir brevemente lo que es inteligencia, entiendo por ésta la capacidad de elegir entre varias posibilidades, aquella opción más acertada para la resolución de un problema.

[113] Polanco Marcos, La ciberinteligencia como habilitador de la ciberseguridad, MAGAZCITUM, 21 de abril 2016, http://www.magazcitum.com.mx/?p=3205#.WYJB9YQ1_IW, fecha de consulta 02 de agosto 2017.

Por lo que la ciberinteligencia es “la adquisición y análisis de información para identificar, rastrear, predecir y contrarrestar las capacidades, intenciones y actividades de los ciberactores (atacantes), y ofrecer cursos de acción con base en el contexto particular de la organización, que mejoren la toma de decisiones”.[114]

La ciberinteligencia puede apoyar a la ciberseguridad en cada una de las etapas del ciclo de vida de los ataques:

> En la etapa de preparación del ataque, la ciberinteligencia apoya con la investigación en fuentes abiertas, monitoreo de *DeepWeb* y *Darkweb*, canales IRC, etc., en búsqueda de posibles campañas que se estén orquestando en contra de la organización, conocimiento de nuevas amenazas, identificación de toda aquella información que permita anticiparse a un posible ataque.
>
> En las etapas de obtención de acceso y creación de persistencia entra en juego una de las áreas de la ciberinteligencia conocida como *Cyber Threat Intelligence* (inteligencia de ciberamenazas), la cual se define como el conocimiento acerca de los adversarios y sus motivaciones, intenciones y métodos, que es recolectado, analizado y difundido en formas tales que ayudan al personal de seguridad y de negocio a proteger los activos críticos de la organización.
>
> Lo anterior significa realizar el monitoreo y análisis de malware, la identificación de posibles vectores de ataques, la identificación de TTP (técnicas, tácticas y procedimientos) de los atacantes.
>
> En las etapas de ejecución de acciones y eliminación de rastros, la ciberinteligencia complementa a través del monitoreo activo en *DeepWeb* y *DarkWeb* para identificar cuándo se pone a la venta o se hace pública, de forma no legítima, la información que es propiedad de la organización.[115]

[114] Ídem.
[115] Ídem.

Una actividad que apoya a todas las etapas es el establecimiento de una estrategia de colaboración con diversas entidades (autoridades del gobierno, CERT´s, empresas, sociedad civil en general, entre otros) que complemente la estrategia de ciberinteligencia.

Esto con el fin de realizar el intercambio de información de inteligencia relativa a las amenazas de seguridad y así potencializar mutuamente sus capacidades de protección, detección y respuesta, fortaleciendo la capacidad de análisis y vigilancia de amenazas e incidentes, y con ello mejorar en la toma de decisiones y acelerar la ejecución de acciones de respuesta y remediación, así como mejorar la conciencia situacional.

Ante este nuevo contexto de ciberamenazas, contar con una estrategia de ciberinteligencia es uno de los elementos esenciales para combatirlas. De manera que la ciberinteligencia debe formar parte integral de cualquier estrategia de ciberseguridad.

4.4 LA VICTIMOLOGÍA EN LOS DELITOS INFORMÁTICOS

Antes de empezar a desarrollar los aspectos generales de la victimología, se considera importante definir de manera general el vocablo víctima, Luis Rodríguez Manzanera lo define como “el sujeto que padece un daño por culpa propia, ajena o por causa fortuita”[116].

En el Derecho penal la víctima es la persona física que sufre un daño provocado por un sujeto, este daño puede ser físico, moral, material o psicológico. También se

[116] RODRÍGUEZ Manzanera Luis, Victimología, Estudio de la Víctima, Porrúa, sexta edición, México, 2000, pág. 57.

puede ser víctima de delitos que no hayan producido un daño corporal físico, por ejemplo, en un robo o una estafa, siendo entonces el daño únicamente patrimonial.

La victimología por su parte, se puede definir como el estudio de las causas por las que algunas personas son víctimas de un delito, y de cómo el estilo de vida conlleva una mayor o menor probabilidad de que una determinada persona sea víctima del mismo. La victimología estudia tanto a la víctima y su papel en el hecho delictivo.

Cabe señalar que el estudio de las víctimas es multidisciplinario, es decir, que no se refiere sólo a las víctimas de un delito, sino también a las que lo son por consecuencia de accidentes, desastres naturales, crímenes de guerra y abuso de poder.

Por ende, los profesionistas de la victimología son expertos en distintas ramas, por ejemplo: científicos, operadores jurídicos, sociales o políticos.

Asimismo, el estudio de las víctimas puede realizarse desde la perspectiva de una víctima en particular o de manera general, analizando las causas por las que grupos de individuos son vulnerables y susceptibles de resultar afectadas.

El estudio de la victimología no se limita sólo a la víctima, por lo que podría analizarse en tres niveles:

1.- Individual. Su objeto de estudio es la víctima, su personalidad y características.

2.- Conductual. En este nivel se estudia la conducta aislada de la víctima con relación a la conducta criminal.

3.- General. En este nivel debe estudiarse el fenómeno victimal, como suma de víctimas y victimizaciones.

Ahora, la cibercriminalidad abarca cualquier delito mediante el uso de las TIC, por lo que existe una variedad de delitos de naturaleza distinta, así como diferentes tipologías de cibercriminales y por ende existe una multiplicidad de víctimas de los ciberdelitos.

Cualquier usuario de Internet y cualquier persona que tenga acceso a un sistema informático que esté conectado a una red, ya sea en una biblioteca, una institución pública, en el trabajo, la casa, la escuela, hoteles, entre otros sitios, puede ser víctima de diferentes ciberdelitos "dependiendo de la motivación del sujeto que realiza el ataque pero, también, del tipo de actividad que el propio usuario realice."[117]

No solo a motivación criminal es la que define el ámbito de oportunidad en el ciberespacio, sino que la propia víctima con su conducta también construye los ámbitos de riesgo. Por lo tanto "hay ámbitos de victimización específicos definidos por el actuar de la víctima en el ciberespacio, que conformarán un ámbito de oportunidad criminal al interaccionar con el ciberagresor motivado".[118]

Por ejemplo, en las redes sociales, cuando el usuario crea un perfil público y sube toda su información personal: nombre completo, fecha de nacimiento, domicilio, pasatiempos, trayectoria escolar y profesional, fotografías, etc. Entonces el ciberdelincuente que está buscando suplantar la identidad de otra persona para llevar a cabo a su vez otros actos delictivos, tiene prácticamente todo lo que necesita a su alcance para realizarlo.

[117] Miro Llinares Fernando, El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio, Marcial Pons, España, 2012, pág. 261.
[118] Ibídem, pág. 262.

La víctima y su comportamiento son siempre elementos determinantes del evento criminal acontecido. Es decir, ella misma "determina desde un primer momento, al incorporar determinados bienes y esferas de su personalidad al ciberespacio, los márgenes genéricos del ámbito de riesgo al que va a estar sometida."[119]

Entonces, se podría afirmar que el comportamiento cotidiano de la víctima en el ciberespacio es un importante predictor de su victimización. Otro ejemplo, sería cuando una persona entra a diversos sitios web, para descargar música y descargue involuntariamente un virus.

También hay otros factores que aumentan el riesgo de victimización, por ejemplo el tiempo que una persona pasa en Internet, es decir, a mayor número de horas en Internet, mayor riesgo de victimización. Por otro lado, el interactuar con extraños a través de redes sociales, realizar compras en línea, entre otras actividades que se pueden realizar en la web.

Y es que casi cualquier tipo de delito se puede dar hoy en día, mediante el uso del Internet, por ejemplo los delitos sexuales, como el ciberacoso. Cuando hice una estancia en Costa Rica, tuve la oportunidad de visitar el Organismo de Investigación Judicial (OIJ), y al conversar con el encargado del área de la investigación de delitos cibernéticos, me comentó que un delito que empieza a propagarse es la extorsión mediante el uso de redes sociales, siendo el *modus operandi* el siguiente: una mujer muy atractiva contacta a un hombre de buen *status* social, con familia y empiezan a conversar por medio del chat, empiezan a tener conversaciones con insinuaciones sexuales, para posteriormente tener lo que se conoce como *sexting* (consiste en el envío contenidos de tipo sexual, principalmente fotografías y/o vídeos), para posteriormente usar esos contenidos para extorsionar a la víctima, pidiendo grandes

[119] Ibídem, pág. 263.

cantidades de dinero, a fin de que no reenvíe los contenidos sexuales a sus familiares, a la empresa donde trabaja o simplemente hacerlos públicos en las redes sociales.

Lo que recomiendan las autoridades cuando la víctima acude a pedir ayuda, es no acceder a las peticiones de los extorsionadores, pues una vez que entregan la cantidad de dinero solicitada, lo seguirán haciendo de manera reiterada, saben que la víctima está dispuesta a hacer cualquier cosa con tal de que no hagan públicos los contenidos sexuales proporcionados por la propia víctima.

Sin duda, todos los sectores de la población tienen cierto grado de vulnerabilidad, de acuerdo al uso que le den al Internet y a las diversas TIC que existen hoy en día, por lo tanto se necesita realizar estudios minuciosos no solo de prevención del delito desde el enfoque de los distintos perfiles criminales que pueden existir, sino también de las potenciales víctimas.

Por lo referido es necesario crear y fortalecer una estrategia de ciberseguridad más amplia en los países de América Latina y el Caribe, en la que exista un intercambio de estudios, información y buenas prácticas, enfocados en la óptica de la victimología.

CONCLUSIONES

A partir del análisis realizado se comprobó la hipótesis planteada inicialmente , en la que se establece la necesidad de crear una estrategia integral en América Latina y el Caribe en materia se ciberseguridad, basada en la armonización legislativa, mediante la adhesión de todos los países de la región al Convenio sobre la Ciberdelincuencia del Consejo de Europa, con la finalidad de fortalecer la cooperación internacional entre las autoridades responsables de investigar los delitos cibernéticos.

En atención a las consideraciones siguientes:

PRIMERA.- Las Tecnologías de Información y Comunicación (TIC) han generado una nueva forma de interacción a nivel mundial, la que la rapidez y facilidad de los intercambios de información y comunicación han eliminado las barreras de distancia y tiempo, hacen partícipes a todos los usuarios de esa interacción, dentro de esta globalización sin precedentes se propician nuevas oportunidades en todos los ámbitos, incluida la de delinquir, a la vez que genera nuevos retos, riesgos y amenazas.

De modo que los Estados, al menos de la región de América Latina y el Caribe deben perfilarse y crear una base jurídica armonizada para que atienda a los delitos cibernéticos, ya que los países en los que actualmente se regulan estos delitos se hace de manera escasa e insuficiente.

SEGUNDA.- La efectividad de la justicia penal es parte esencial de una estrategia adecuada de seguridad cibernética. Esto abarca la investigación, la fiscalización y la adjudicación de delitos en contra y por medio de datos y sistemas informáticos,

de igual modo el obtener evidencia electrónica vinculada con cualquier hecho criminal, con fines del proceso penal.

TERCERA.- La esencia del Convenio de Budapest radica en fortalecer la cooperación internacional en materia de la cibercriminalidad, mediante la combinación de la asistencia legal mutua. Dado que el alcance de la cooperación no se limita al tipo de delito cibernético, incluye la cooperación referente a la evidencia electrónica que se encuentre en un sistema informático derivado de la comisión de cualquier delito.

La importancia de que la totalidad de los países de América Latina y el Caribe se adhieran a este convenio, radica en que hasta el día de hoy sigue siendo el único instrumento internacional existente que establece las tipologías y armoniza los elementos sustantivos penales relacionados con las conductas realizadas a través de sistemas de cómputo e internet.

Para construir y fortalecer una buena estrategia de ciberseguridad en América Latina y el Caribe la cooperación internacional es uno de los componentes más importantes para combatir la ciberdelincuencia global, pues sin ella, sería una tarea realmente imposible adoptar medidas y políticas que ayuden a erradicar este latente problema de carácter transnacional, pues para combatirlo se necesita de la cooperación de diversos sectores sociales, de las autoridades y organismos, por lo que es recomendable que México se adhiera al Convenio de Budapest, así como la totalidad de los países de la región.

A continuación se establece una propuesta de clasificación de algunos delitos que emplean las TIC para su comisión, así como algunas posibles medidas que se podrían adoptar para su prevención.

CLASIFICACIÓN DE ALGUNOS DELITOS QUE EMPLEAN LAS TIC PARA SU COMISIÓN.

Delito	**TIC´s utilizadas**	***Modus operandi***	**Finalidad de la comisión de este delito**	**Tipo de víctima**	**Factores de riesgo**	**Prevención**
Falsificación de documentos.	Redes sociales, software, hardware	Búsqueda de perfiles en redes sociales, de los que se obtengan mayor información personal: lugar y fecha de nacimiento, fotografías, grado de estudios, etc. Falsificación de documentos oficiales.	Robo/usurpación de identidad.	Cualquier persona	Perfiles públicos en redes sociales, *hackeo* de cuentas, robo de celulares, pérdida o robo de documentos oficiales: INE, licencia de manejo, acta de nacimiento, pasaporte, entre otros.	Restringir el acceso a sus redes sociales, no proporcionar información confidencial, establecer código de seguridad para dispositivos. Hacer campañas públicas de prevención, a través de diversos medios de comunicación como radio, T.V. y redes sociales.
Fraude	Correo electrónico, telefonía celular, entre otros	Se contacta a la víctima de manera amistosa, o se finge ser un familiar o persona cercana, solicita información de cuentas bancarias, o pide que realice depósitos,	Delincuencia organizada, lavado de dinero.	Cualquier persona	Mostrar Confianza hacia desconocido, no cerciorarse de que sus familiares se encuentran bien.	No confiar en desconocidos, cerciorarse que sus familiares se encuentren fuera de peligro. Hacer campañas públicas de prevención, a través de diversos medios de comunicación como radio, T.V. y redes sociales.

Espionaje	Códigos maliciosos, correos electrónicos, intervención de comunicaciones.	Se intervienen las conversaciones telefónicas, o medios electrónicos con el fin de obtener información sensible, que será utilizada en contra de la víctima.	Secuestro, extorsión, robo de información, robo de secretos industriales, entre otros.	Gobierno, empresas, cualquier persona en general.	Falta se sistemas de seguridad confiables en dispositivos tecnológicos.	Proteger sistemas tecnológicos usados, verificar la autenticidad de los sitios web a los que se acceso. Hacer campañas públicas de prevención, a través de diversos medios de comunicación como radio, T.V. y redes sociales.
Trata de personas	Redes sociales, teléfonos celulares, correos electrónicos.	Se crea perfiles falsos en redes sociales, compañías ficticias, con el fin de contactar a la víctima.	Explotación sexual, explotación laboral, tráfico de órganos, entre otros.	Cualquier persona, principalmente mujeres y niños.	Falta de atención de los padres hacia sus hijos. Contactar extraños en redes sociales.	Que los padres o tutores se cercioren a los sitios web a los que acceden los niños. No contactar desconocidos en redes sociales. Verificar que las compañías que ofrecen empleos realmente existan. Hacer campañas públicas de prevención, a través de diversos medios de comunicación como radio, T.V. y redes sociales.

Fraudes financieros	Correo electrónico, telefonía, códigos maliciosos	Cuando la víctima cree haber hecho una transacción o compra en línea.	Operaciones con recursos de procedencia ilícita, delincuencia organizada.	Personas con solvencia económica, que tiene cuentas bancarias, empresas, gobierno.	No cerciorarse sobre la autenticidad del sitio web. Dejar guardada información de cuentas bancarias en sitios no confiables.	Verificar la autenticidad de los sitios web a los que se accede antes de realizar cualquier transacción o compra en línea. Hacer campañas públicas de prevención, a través de diversos medios de comunicación como radio, T.V. y redes sociales.
Operaciones con recursos de procedencia ilícita.	Hardware, software, telefonía, redes sociales, entre otros.	La sobrefacturación en establecimientos y empresas, abrir diversas cuentas Bancarias y realizar actividades sospechosas, utilizar fundaciones, operaciones en casinos, hipódromos, casas de cambio, entre otros.	Financiamiento al terrorismo, narcotráfico, tráfico de armas, contrabando, entre otros.	El Estado, la economía nacional.	No implementar correctos mecanismos para la prevención de este delito. Falta de legislación o falta de claridad en la misma.	Hacer campañas públicas de prevención dirigidas a los sectores más vulnerables, a través de diversos medios de comunicación como radio, T.V. y redes sociales.

Sabotaje.	Códigos maliciosos, correos electrónicos, intervención de comunicaciones, uso de software, hardware, entre otros.	Se destruya, perjudique o ilícitamente entorpezca vías de comunicación, servicios públicos, funciones de las dependencias del Estado, organismos públicos descentralizados, empresas de participación estatal, órganos constitucionales autónomos o sus instalaciones.	Terrorismo, genocidio, ataques a las vías de comunicación, entre otros.	Dependencias del gobierno, proveedores de servicios de internet, telefonía, entre otros.	Falta se sistemas de seguridad confiables en dispositivos tecnológicos.	Proteger sistemas tecnológicos usados, verificar la autenticidad de los sitios web a los que se acceso. Hacer campañas públicas de prevención, a través de diversos medios de comunicación como radio, T.V. y redes sociales.
Pornografía infantil.	Hardware, software, telefonía, redes sociales, entre otros.	Se contacta a niños mediante redes sociales, aplicaciones para citas o encontrar el amor, se tiene charlas con ellos y se les empieza a inducir realizar actos sexuales, para ser fotografiados y/o grabados y después subirlos a la red, imprimirlos y distribuirlos.	Turismo sexual, corrupción de menores, violación, secuestro, etc.	Cualquier menor de 18 años.	Falta de atención de los padres hacia sus hijos. Contactar extraños en redes sociales	Que los padres o tutores se cercioren a los sitios web a los que acceden los niños. No contactar desconocidos en redes sociales. Hacer campañas públicas de prevención, a través de diversos medios de comunicación como radio, T.V. y redes sociales, o físicamente en escuelas.

MESOGRAFÍA

BIBLIOGRAFÍA:

1. ACURIO DEL PINO. Santiago, Delitos Informáticos: Generalidades, s.p.i., http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

2. BRAMONT- ARIAS TORRES, Luis Alberto, El Delito Informático en el Código Penal Peruano, Fondo Editorial de la Pontificia Universidad Católica del Perú, Lima, 1997.

3. BRENNER, Susan W, Cybercrime, Criminal Threats from Cyberspace, Greenwood, United States of America, 2010.

4. COBO ROMANÍ. Juan Cristóbal, El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento, s.p.i., pág. 312, http://www.ehu.eus/zer/hemeroteca/pdfs/zer27-14-cobo.pdf.

5. CRISTOS VELASCO, San Martín, La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet, Tirant lo Blanch, México, 2012.

6. DE LA CUESTA ARZAMENDI. José Luis y Ana Isabel Pérez Machío, Capítulo III Ciberdelincuentes y Cibervíctimas, s.p.i., pág. 99, http://www.ehu.eus/documents/1736829/2010409/CLC+91+Ciberdelincuentes+y+cibervictimai9, fecha de consulta: 24 de agosto de 2016.

7. DÍAZ García Alexander, El Bien Jurídico Tutelado de la Información y los Nuevos Verbos Rectores en los Delitos Electrónicos, Universidad Santiago de Cali, documento en línea, http://www.redipd.es/noticias_todas/2011/tribuna/common/1/EL_BIEN_JURIDICO_TUTELADO_DEL_DATO_Y_LOS_NUEVOS_VERBOS_RECTORES_DE_LOS_DELITOS_ELECTRONICOS_USC.pdf

8. FLORES Prada Ignacio, Criminalidad Informática (aspectos sustantivos y procesales), Tirant lo blanch, México, 2012.

9. HUERTA Miranda, Marcelo y Libano Manzur Claudio, Delitos Informáticos, Editorial Jurídica ConoSur Ltda, Segunda Edición, Santiago de Chile, 1998, pág. 181.

10. LIMA de la LUZ, María, Criminalia N°1-6 Año L. Delitos Electrónicos, Ediciones Porrúa, Enero-Julio 1984.

11. LIRA, Arteaga Óscar Manuel, Cibercriminalidad, Fundamentos de Investigación en México, INACIPE, Segunda Edición, México, 2014.

12. MENDOZA BREMAUNTZ, Emma Carmen, Derecho Penitenciario, Mc Graw-Hill, México, 1998.

13. MIRO Llinares Fernando, El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio, Marcial Pons, España, 2012, pág. 261.

14. MOLINA Mateos José María, Aproximación Jurídica al Ciberespacio, Instituto Español de Estudios Estratégicos, España, 2015.

15. PEÑALOZA. Pedro José. Prevención Social del Delito: "Asignatura Pendiente", Porrúa, Tercera Edición, México, 2006.

16. PIÑA Libien, Hiram Raúl, Los Delitos Informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano, documento en línea, http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf.
17. REINTEGRA, Modelo para la Prevención Social del Delito con los Adolescentes y Jóvenes en Contexto Comunitarios, Ediciones REINTEGRA, México, 2011.

18. RODRÍGUEZ Manzanera Luis, Victimología, Estudio de la Víctima, Porrúa, sexta edición, México, 2000.

19. TELLEZ VALDEZ, Julio, Derecho Informático, Universidad Nacional Autónoma de México, 1991.

20. VILLANUEVA Cabello Belinda Shaloom Peniel, Tesis de Licenciatura, Nueva Política Criminológica de Prevención Social para Adolescentes que Inciden en Actividades o Conductas Violentas. Ciudad Universitaria, México, 2013.

LEGISLACIÓN:

1. CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, última reforma publicada en el Diario Oficial de la Federación el 24 de febrero de 2017, versión en línea http://www.diputados.gob.mx/LeyesBiblio/pdf/1_240217.pdf

2. CONSEJO DE EUROPA, Convenio Sobre la Ciberdelincuencia, Serie de Tratados Europeos- n°185, Budapest, 2001, www.oas.org/juridico/english/cyb_pry_convenio.pdf.

3. CÓDIGO PENAL FEDERAL, Diario Oficial de la Federación, última reforma del 26 de junio de 2017, versión en línea, http://www.diputados.gob.mx/LeyesBiblio/pdf/9_070417.pdf.

4. CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES, última reforma publicada en el DOF el 17 de junio de 2016, versión digital, http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_170616.pdf , fecha de consulta 31 de julio de 2017.

5. LEY GENERAL PARA LA PREVENCIÓN SOCIAL DE LA VIOLENCIA Y LA DELINCUENCIA,
http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPSVD.pdf
6. , publicada en el Diario Oficial de la Federación el 24 de enero de 2012.

7. CÓDIGO PENAL DEL DISTRITO FEDERAL, versión en línea, última reforma 16 de junio 2016, http://www.aldf.gob.mx/archivo-d261f65641c3fc71b354aaf862b9953a.pdf.

8. CÓDIGO PENAL DEL ESTADO DE MÉXICO, versión en línea, http://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/cod/vig/codvig006.pdf.

9. LEY ORGÁNICA DE LA PROCURADURÍA GENERAL DE LA REPÚBLICA, última reforma del 29 de mayo de 2009, http://www.oas.org/juridico/spanish/mesicic3_mex_anexo23.pdf.

CIBERGRAFÍA**:**

1. 13° Congreso sobre Prevención del Delito y Justicia Penal, Organización de las Naciones Unidas, Doha, 2015, http://www.un.org/es/events/crimecongress2015/about.shtml.
2. Naciones Unidas, Declaración de Doha sobre la integración de la prevención del delito y la justicia penal en el marco más amplio del programa de las Naciones Unidas para abordar los problemas sociales y económicos y promover el estado de derecho a nivel nacional e internacional, así como la participación pública, 13° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Doha, 2015, pág. 11.

3. BANCO INTERAMERICANO DE DESARROLLO, ORGANIZACIÓN DE LOS ESTAMOS AMERICANOS, Ciberseguridad. ¿Estamos Preparados en América Latina y el Caribe?, Informe Ciberseguridad 2016, texto en línea, file:///C:/Users/shaloom/Downloads/Ciberseguridad-Estamos-preparados-en-America-Latina-y-el-Caribe%20(4).pdf.

4. Blog en línea: Redes, Terminales y Servicios, https://bloginformaticasaia.wordpress.com/2014/12/02/redes-terminales-y-servicios/.

5. Blog Especializado en Sistemas de Gestión de Seguridad de la información, ISO 27001: Los aspectos básicos en la ciberseguridad, http://www.pmg-ssi.com/2015/03/iso-27001-los-aspectos-basicos-en-la-ciberseguridad/.

6. CHIPIX NOTZ, Edwin, Prevención del Delito, texto en línea, http://www.policiasysociedad.org/userfiles/CHAT%20PREVEN%20

7. COMISIÓN NACIONAL DE SEGURIDAD, Fortalece CNS Estrategias para la Protección del Ciberespacio Mexicano, comunicado de prensa, 25 de febrero 2015,

http://www.denuncia.gob.mx/portalWebApp/wlp.c;jsessionid=n2wmJxvJv1KY2J5cWQLBTfcQrdJ4tcvV11fqhw1JQpvGGvzwLJ2s!-1886721534?__c=f7130.

8. Diccionario de la Real Academia Española, 2016, http://dle.rae.es/?id=LY8zQy3.

9. GOBIERNO DE ESPAÑA, Estrategia de Ciberseguridad Nacional 2013, Departamento de Seguridad Nacional, texto en línea, https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf .

10. NACIONES UNIDAS, Proyecto de Declaración de Doha sobre la integración de la prevención del delito y la justicia penal en el marco más amplio del programa de las Naciones Unidas para abordar los problemas sociales y económicos y promover el estado de derecho a nivel nacional e internacional, así como la participación pública, 13° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Doha, 2015, https://www.unodc.org/documents/congress/Declaration/V1504154_Spanish.pdf.

11. NUÑEZ PONCE, Julio, Los Delitos Informáticos, en Revista Electrónica de Derecho Informático Nro. 15. http://biblioteca.uca.es/sbuca/bibcjer/detalle_rec.asp?codbib=DER&capbd=9&secbd=2&subbd=0&apabd=0&nombd=REDI.+Revista+Electr%F3nica+de+Derecho+Inform%E1tico&numreg=383

12. Página oficial de INTERPOL https://www.interpol.int/es/Crime-areas/Cybercrime/Cybercrime.

13. Página oficial de la OEA http://www.oas.org/es/temas/seguridad_cibernetica.asp.

14. PAN Y AGUA Javier, ¿Cómo se encuentra Costa Rica en materia de ciberseguridad?, IT NOW, 9 de febrero, 2017, https://revistaitnow.com/como-se-encuentra-costa-rica-en-materia-de-ciberseguridad/, fecha de consulta 24 de julio 2017.

15. POLANCO Marcos, La ciberinteligencia como habilitador de la ciberseguridad, MAGAZCITUM, 21 de abril 2016, http://www.magazcitum.com.mx/?p=3205#.WYJB9YQ1_IW.

16. R. FOMPEROSA Mariana, ¿Qués es Pegasus? El malware usado para espiar en México, periódico Milenio, 19 de junio 2017, http://www.milenio.com/tendencias/pegasus-mexico-espionaje-que_es-malware-the_new_york_times-milenio-noticias_0_977902402.html.

17. TECH, 2016, "México, entre los 6 países más atacados por cibercriminales", Periódico El Financiero, 11 de junio de 2016, http://www.elfinanciero.com.mx/tech/mexico-entre-los-paises-mas-atacados-por-cibercriminales.html.

18. Texto en línea, Ciberseguridad, Creando un mundo en línea más seguro, Actualidades de la UIT, Junio 2011, http://www.itu.int/net/itunews/issues/2011/05/38-es.aspx.

19. UNODC Oficina de las Naciones Unidas contra la Droga y el DELITO. (2010). Congreso de las Naciones Unidas sobre prevención del delito y justicia penal 1955-2010. 55 años de logros. Austria: *United Nations Information Service*, https://www.unodc.org/documents/data-and-analysis/Crime-statistics/Manual_Victimization_surveys_2009_spanish.pdf.

20. UNODC, Resumen del Estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, Viena, 2013, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_S.pdf.

OTRAS FUENTES:

1. CORTÉS BECERRIL. José Héctor, Curso de Cibercriminalidad, Instituto Nacional de Ciencias Penales, Ciudad de México, mayo 2016.