



**Universidad de Quintana Roo**

División de Ciencias Sociales y Económico Administrativas.

**Policía Cibernética: Una  
propuesta para Seguridad  
Pública en Quintana Roo.**

**TRABAJO DE TESIS  
para obtener el título de:**

**Licenciada en Seguridad Pública.**

**PRESENTA:**

**Mitzi Aureny Cab Caamal.**

**DIRECTOR DE TESIS:**

**M.C. Kinuyo Esparza Yamamoto**



**Chetumal, Quintana Roo; Junio del 2013**



UNIVERSIDAD DE QUINTANA ROO

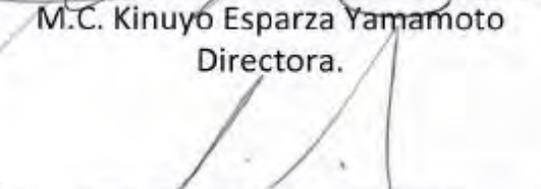
**División de Ciencias Sociales y Económico  
Administrativas.**

Trabajo de Tesis elaborada bajo la supervisión del Comité de  
Asesoría y Supervisión. Aprobado como requisito para obtener  
el título de:

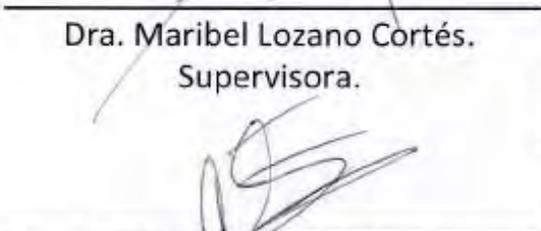
Licenciada en Seguridad Pública

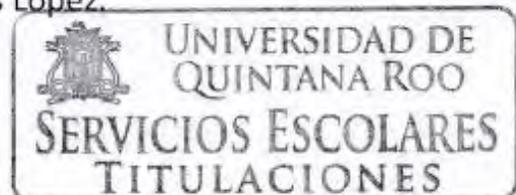
**Comité:**

  
M.C. Kinuyo Esparza Yamamoto  
Directora.

  
Dra. Maribel Lozano Cortés.  
Supervisora.



  
M.C. Enrique Cercas López.  
Supervisor.



Chetumal, Quintana Roo; Junio de 2013

## AGRADECIMIENTOS

A Dios:

Por darme la oportunidad de vivir, pensar y analizar cada una de las cosas que he logrado, por darme la capacidad de poder estudiar y lograr el triunfo de la vida, por poner en mi camino a personas especiales que me acompañaron en el momento de la lucha.

A mis padres:

Quienes han sido mi fuerte en todo momento; Madre gracias por tu infinita paciencia, por tu tierna compañía y tu inagotable apoyo, si hay algo que sé hacer bien es por ti, te amo con todo mi corazón. Padre; detrás de este logro se encuentra usted, te agradezco por su apoyo, confianza y cariño, gracias por alentarme a hacer una triunfadora en la vida, te adoro; este logro también lleva sus nombres porque fueron los que me enseñaron a que la mejor manera de crecer en la vida es la formación.

Familia:

A mi tía, que me alentó y acompañó en este camino de dificultad, a la que hizo posible mis asistencias al centro escolar, mis logros son los tuyos. Recordando siempre juntas, hasta el final. A mi hermana, a la que me ha enseñado a luchar, por regalarme agradables momentos y por tu cariño. A mi Abuelita por cada una de las bendiciones que me diste al salir de casa, por tus oraciones encomienda a mis estudios, gracias por estar a mi lado.

# Índice

## Capítulo I: La Internet.

1.1 Qué es una red.....	8
1.2Historia del internet. ....	8
1.3La complejidad del internet.....	11
1.4 Manejo de internet. ....	12
1.5Ciberespacio. ....	14
1.6 Redes sociales. ....	17
1.6.1 Antecedentes .....	19
1.6.2Concepto de Red Social.....	20
1.6.3Origen de las Redes Sociales .....	20
1.6.4 Representación de las Redes Sociales .....	21
1.6.5 Tipos de redes sociales.....	25

## Capítulo II: La Policía

2.1Definición de Policía.....	27
2.2La policía en México. ....	30
2.3La seguridad pública: antecedentes. ....	31
2.4Funciones primordiales de la policía. ....	37

## Capítulo III: La Cibernética.

3.1 Definición de cibernético.....	41
3.2Antecedentes.....	45
3.3Policía cibernética: .....	46
3.3.1Qué es la policía cibernética.....	46
3.3.2 Funciones. ....	50
3.3.3 Modus operandi.....	53
3.3.4 Perfil del policía cibernético.....	55

## **Capítulo IV: Investigación de los delitos ocasionados por el Internet.**

<b>4.1 Pornografía infantil vía internet.....</b>	<b>58</b>
<b>4.2 Fraudes.....</b>	<b>62</b>
<b>4.3 Cyberbullying.....</b>	<b>64</b>
<b>4.4 Pedofilia vía internet.....</b>	<b>67</b>
<b>4.5 Crimen organizado.....</b>	<b>70</b>
<b>4.6 Delitos informaticos.....</b>	<b>72</b>

## **Capítulo V: Importancia de la propuesta de la aplicación de la policía cibernética en Seguridad Pública.**

<b>5.1 Importancia de la policía cibernética en Quintana Roo.....</b>	<b>76</b>
<b>5.2 Recomendaciones de prevención para la sociedad.....</b>	<b>77</b>
<b>5.3 Implementación de programas de auto cuidado.....</b>	<b>83</b>
<b>Conclusión.....</b>	<b>87</b>
<b>Anexos.....</b>	<b>88</b>
<b>Glosario.....</b>	<b>93</b>
<b>Bibliografías.....</b>	<b>95</b>

## **Introducción**

Los delitos cibernéticos constituyen actos criminales que pueden llegar a afectar al gobierno y su estabilidad, la economía y la paz social; resultados de las encuestas presentadas por el Instituto Nacional de Estadística, Geografía e Informática (INEGI), México se encuentra situado en unos de los primeros lugares en el mundo con violencia.

Hoy día el INEGI refleja que en nuestro país el 38.9 millones de personas son usuarios de la computadoras y el 32.8 millones tienen acceso a internet, esto quiere decir que más del 50% de nuestra población puede ser objeto o víctima de algún delito cibernético.

Algunos Estados de la República Mexicana como por ejemplo Chihuahua cuentan con una policía cibernética, que como resultado ha favorecido al combate de los delitos cibernautas; sin embargo, en Quintana Roo no existe una policía capacitada para combatir este tipo de delitos que van en incremento.

Derivado de esto, existe la necesidad responder la incógnita de ¿Sería conveniente para combatir los delitos cibernéticos mediante la implementación de una policía especializada en Quintana Roo?; es necesario tener una respuesta confiable y fundamentada mediante conceptos y experiencias de distintos lugares, en los cuales la implementación de programas para la erradicación de esta problemática.

Las redes sociales en los últimos años han evolucionado a tal grado, que ya no únicamente son utilizadas para contactar amigos, además de ser una plataforma comercial, sino que muchos las utilizan para delinquir. La población juega un papel importante para poder prevenir los delitos cibernéticos, ya que en un día normal los usuarios consumen una gran cantidad de información extraída de medios de la red.

La Policía de Cibernética contará con elementos estrictamente capacitados, los cuales se encargarán del monitoreo en línea en aquellos problemas que se presenten mediante las redes de internet e indagar y dar solución a los crímenes online, por lo cual también se dará la tarea de fomentar la cultura de prevención del delito cibernético.

Esta propuesta tiene implicaciones prácticas y reales la cual reconocerá qué tipos de estrategias utilizan las personas que operan en estas bandas cibernéticas, aplicando identificación de los autores del delito;

proporcionando conocimiento a la sociedad, autoridades nacionales, autoridades federales, autoridades locales, en base del conocimiento del resultado de la investigación.

Esto es con la finalidad de tener personal mejor capacitado, en los cuerpos policiacos con elementos dispuestos a trabajar con equipos de nueva generación tecnológica proporcionando, un buen resultado, tomar medidas y presentar alternativas para reducir la vulnerabilidad en la que se desenvuelven los ciudadanos al tener contacto con la red.

Este trabajo de investigación pretende analizar las problemáticas que hoy día están ocurriendo con relacionas a las páginas de internet, de manera que al crear una policía cibernética, como cuerpo de prevención del delito, brindará grandes avances para combatir los índices de violencia en la red que se presentan en el Estado de Quintana Roo, demostrando la necesidad de contar con un cuerpo capacitado para acabar con los índices de peligrosidad.

Los resultados de esta investigación aportarán datos y propuestas que puedan ser tomados en cuenta para garantizar una adecuada prevención y combate a los delitos cibernéticos, y pueda igualmente inspirar a otros investigadores a aunar sobre el tema aportando propuestas para resolver este problema que impacta en nuestra realidad. Igualmente, la presente investigación aporta un valor teórico, contribuyendo en el desarrollo de posturas y conceptos nuevos dentro del tema de la cibernética que es muy contemporáneo.

Por último se hará mención acerca de los beneficios que conlleva crear un departamento que permita la seguridad en la comunidad cibernética y en la sociedad usuaria en general, así como las recomendaciones sobre la importancia de establecer una unidad de policía cibernética en el Estado.

El primer capítulo nos habla del internet; fundamentalmente los elementos más importantes de la historia del internet, de donde proviene, como se desarrollaron, las redes sociales y su importancia en pro y contra de la sociedad, cual es su origen y cuáles son los tipos de redes sociales, que existen hoy en día.

En el segundo capítulo nos menciona a la policía, empezando por saber cuál es la definición exacta de lo que es un policía, los cambio que ha ido recibiendo durante los últimos años, sus antecedentes, y lo más importante las funciones principales que debe de cumplir un policía en la ciudad.

De esta manera el tercer capítulo nos explica la importancia de la cibernética, como va surgiendo esta materia, describiendo lo más importante de este tema, los antecedentes y la creación de la policía cibernética, sus funciones principales, el modus operandi, y el perfil que debe cumplir un policía cibernético.

El cuarto capítulo nos habla de la investigación de los delitos principales causantes de las redes de internet; especificando los delitos por los cuales es importante conocer y a los que una persona puedes estar expuestos a ser víctimas, con solo consultando internet.

Por último el quinto capítulo nos refleja la importancia de poder contar con una policía cibernética, demostrando que la necesidad de combatir los delitos en nuestro estado es la mejor manera de capacitar a nuestros cuerpos policiacos; demostrando que implementar unos programas de prevención para la sociedad es de gran ayuda para reconocer como actuar en caso de acoso cibernético

# **CAPÍTULO I**

## **La Internet.**

### **1.1 Qué es una red.**

Una red se define como un conjunto de computadores, equipos de comunicaciones y otros dispositivos informáticos y software que se pueden comunicar entre sí, a través de un medio en particular, como un dispositivo físico que envía y recibe impulsos electrónicos. La red de contactos, que mantiene un o unos usuarios es simplemente aquella conexión unificada de sus ordenadores, que se mantiene viva por las máquinas que tienen algún enlace; como lo son impresoras, faxes, módems, servidores y en ocasiones, también desde un teléfono.

La red informática permite que sus recursos tecnológicos como lo es la conexión entre las personas hablen entre sí y establezcan una comunicación a grandes distancias; conectar a empresas con la Internet, aportándole numerosos beneficios adicionales como teleconferencia, actividad multimedia, transferencia de archivos de vídeo y archivos gráficos a gran velocidad, servicios de información de negocio en línea, etc.

### **1.2 Historia del internet.**

Los antecedentes del Internet marcaron los avances del mundo de las redes que hoy en día existe y que representa un sistema mundial de enorme conexiones entre computadoras que globalizan al mundo; la información que nos brinda este sistema de enlace es manera fácil de adquirir, que permite que todo aquel que necesite de información puede tenerla de forma gratis. Nunca antes en la historia de la humanidad el saber había estado tan desarrollado y abarcado gran parte de una sociedad, teniendo al alcance de todos como es ahora la Internet.

Los grandes cambios realizados en el manejo de la información han hecho que algunos estudiosos lleguen a plantear la superación de la modernidad (Lyotard, 1987), nos dice que el manejo de la tecnología está sufriendo grandes cambios en el mundo. Sin llegar a discutir la veracidad de dicha aseveración, la llegada de una comunicación remota y a la vez instantánea, y fácil de adquirirla junto con una capacidad de computo nunca antes vista con la disponibilidad de información a escala mundial han significado cambios en la estructura social del mundo entero, lo que ha sido planteado como un cambio de paradigma (Castells, 2000).

El nacimiento del Internet nos remonta a los años 60; Estando en tiempos de la guerra fría, Estados Unidos crea una red exclusivamente militar, con objetivos de lograr que, en el caso de un ataque ruso, se pudiera tener acceso a la información militar de cualquier movimiento y amenaza desde cualquier punto del país; esta red de nombre *ARPANET* se creó en 1969, para poner en evidencia al enemigo.

En principio, esta red contaba con pocos ordenadores distribuidos entre distintas universidades del país. Pasando dos años, ya contaba con unos 40 ordenadores conectados que trasladaban esta información. Tanto fue el crecimiento de la red que su sistema de comunicación se quedó obsoleto. Entonces dos investigadores se dieron la tarea de crear el Protocolo *TCP/IP*, que se convirtió en el estándar de comunicaciones dentro de las redes informáticas.

*ARPANET* con el paso del tiempo siguió creciendo y abriéndose al mundo, siendo así que cualquier persona con fines académicos o de investigación podía tener acceso a la red. Las funciones militares, fueron a parar a *MILNET*, una nueva red creada por los Estados Unidos. Esta manera el desarrollo de las redes fue abismal, creando nuevas redes de libre acceso que más tarde se unen a *NSFNET*, una red que se dedicó a la información de investigación y educación formando el núcleo de lo que hoy conocemos como *INTERNET*.

Gibson, nos menciona que el Internet ya era una tecnología establecida, aunque conocida por unos pocos e hizo una revelación: sobre el término "*ciberespacio*", realidad simulada por los ordenadores creada por las redes de información. (Gibson, 1985)

En ese tiempo la red era básicamente textual, y Gibson lo relaciono todo lo que ya había investigado con videojuegos. Con el tiempo la palabra "ciberespacio" terminó vista como sinónimo de Internet, fue tal que hacia el año 1990 ya se contaba con muchos servidores.

Tim Berners reclutado en el centro de investigación nuclear, interesado en la búsqueda de un sistema de almacenamiento y recuperación de datos, retomó la idea de Ted Nelson un investigador de la red de grandes conocimientos que se adentró a *un proyecto llamado "Xanadú"* de usar hipervínculos. Robert Caillau quien cooperó con el proyecto, nos dice que en 1990 deciden ponerle un nombre al sistema y lo llamarón *World Wide Web (WWW)* o telaraña mundial.

Esta fórmula permitía vincular información en forma lógica y a través de las redes, su contenido se programaba en un lenguaje de hipertexto con "etiquetas" que asignaban una función a cada parte del contenido. Luego, un programa de computación, un intérprete, eran capaz de leer esas etiquetas para desplegar la información. Ese intérprete sería conocido como "navegador" o "browser".

Andreesen, produjo la primera versión del navegador "*Mosaic*", que permitió acceder con mayor naturalidad a la *WWW*. La interfaz gráfica iba más allá de lo previsto y la facilidad con la que se podía manejar con programas de red a los legos. Desde entonces Internet comenzó a crecer más rápido que otro medio de comunicación, convirtiéndose en lo que hoy todos conocemos. (Andreesen, 1993).

Podemos definir a Internet como una "*red de redes*", es decir, una red que no sólo interconecta computadoras, sino también interconecta redes de computadoras entre sí. Una red de computadoras es un conjunto de máquinas que se comunican a través de algún medio (cable coaxial, fibra óptica, radiofrecuencia, líneas telefónicas, etc.) con el objeto de compartir recursos de información.

De esta manera, Internet sirve de enlace entre redes más pequeñas y permite ampliar su cobertura al hacerlas parte de una "*red global*". Esta red global tiene la característica de que utiliza un lenguaje común que garantiza la intercomunicación de los diferentes

participantes; este lenguaje común o *protocolo* (lenguaje que utilizan las computadoras al compartir recursos) se conoce como *TCP/IP*.

Así pues, Internet es la "red" que utiliza TCP/IP como su protocolo de comunicación. Internet es un acrónimo de *INTERconnected NETWORKS* (Redes interconectadas). Para otros, Internet es un acrónimo del inglés *INTERNational NET*, que traducido al español sería *Red Mundial*.

### **1.3 La complejidad del internet.**

El Internet es una red de computadoras conectadas entre sí, permitiendo el intercambio e interacción de información. A fin de poder compartir enlaces entre diferentes computadoras ubicadas en distintas partes del mundo, utilizando un lenguaje común a todas las máquinas.

A su vez, este intercambio de información crea un universo virtual, diferente del universo físico conocido. Este espacio universal o ciberespacio no tiene la localización fija, es decir, no se puede ubicar el lugar en donde se asienta.

Una de las características de este ciberespacio es que está formado por información contenida en medios electrónicos de almacenamiento y que estos medios de almacenamiento son de orden físico, por lo que en última instancia esa información esa ubicada en cierto lugar físico territorial, pero puede ser accedida desde cualquier parte del mundo.

Dentro del ciberespacio o del espacio virtual, es decir dentro de la red, existen diferentes métodos de comunicación, cada uno de ellos acorde con una finalidad. Así como el mail que funciona como un correo tradicional, el (FTP) que funciona como el sistema de intercambio de libros de la biblioteca.

Existe uno de estos servicios que ha cobrado más fuerza que los demás y es el servicio web, consiste en una "página" en la que se coloca cierto tipo de información sobre algún tema en

particular. El servicio funciona como un tabloide de anuncios o como un sistema de reparto de propaganda.

Un ejemplo de lo anterior son los esfuerzos de las empresas e instituciones privadas por blindar sus sistemas de acceso a la información y así evitar fugas o desvíos de numerario, las instituciones que a nuestro modo de ver han puesto especial énfasis en esa autoprotección y en defensa de sus clientes son las instituciones de crédito.

#### **1.4 Manejo de internet.**

Al producirse la interacción mundial a través del Internet, es necesario para algunos establecer reglas básicas de comportamiento por parte del usuario, así como de los prestadores del servicio; por el contrario, existe quienes piensan que al ser el Internet un bien de la humanidad debe seguir un patrón de comportamiento libre en el que el recorrido por lo que se ha denominado la supercarretera de la información no se limite, y sólo esté sujeta a la habilidad de cada usuario para conducirse en ese mundo virtual; a nuestro modo de ver estimamos que sí deben existir reglas de etiqueta del comportamiento por parte de los usuarios.

Un sistema de comunicación mundial, como los es el internet comprende una gran variedad de cultura, edad, y educación, no tan sólo es congruente sino indispensable crear un manual del comportamiento del usuario, manual que no debe limitarse a un estadio nacional, sino a un plano internacional, con la distinción de que no debe encontrarse elevado a la categoría de una norma con todos sus atributos legales, pero que sí debe servir de patrón para una mejor interacción en el Internet, y para desmotivar en principio, conductas reprobables, así como conductas lesivas.

Uno de los aspectos a destacar y que más se queja el usuario, es la recepción del correo no deseado (spam), se parte de la base que el correo electrónico se diseñó para permitir una comunicación fluida, sencilla y a bajo costo, esa ausencia de discriminación entre mensajes solicitados o no solicitados, dio lugar a ofertar productos en forma masiva, que generó el spamming, en el que se abusaba el uso de las páginas de internet.

En algunos países como lo es Estados Unidos, se creó la ley federal de control del ataque de pornografía y mensaje no solicitado, viendo de esta manera que el internet es un medio de comunicación masivo de comunicación que controla casi todos los accesos de información importante; siendo esta manera el usuario el responsable del manejo de las páginas.

La regulación del Internet es un enorme reto en razón de su carácter internacional y de la enorme cantidad de sitios que existen de tan variada índole e interés; es decir que el manejo de la red no está visto como un problema para la sociedad, y que hasta la fecha muchos desconocen del peligro al que se enfrentan al estar dentro de las páginas de internet.

Lo anterior da una idea de lo grave que resulta carecer de reglas de comportamiento en el Internet; por ello, consideramos que los valores fundamentales de la sociedad, con independencia de la raza, credo, cultura y educación, son necesarios para la interacción en ese mundo virtual, por lo que consideramos que al darse de alta una persona en el Internet debe ser consciente y actuar de buena fe, expresando los datos que corresponden a su identidad, de igual manera los prestadores de servicio deben exigir mayores requisitos para la autorización de direcciones electrónicas.

Por ello se deben tener en cuenta ciertos puntos básicos para el uso correcto de las páginas;

- ♣ Las personas son los que usualmente utilizan los medios benéficos de la red; es decir que las personas son responsables de las páginas que visitan, a que vínculos acceden y a que canal de chat ingresan.
- ♣ La necesidad de tener acceso a las páginas es porque se requiere el uso de información que se maneja en ellas, razón por la cual del que está entrando a la red tiene el control de cuánto tiempo va a tardar y que es lo que piensa investigar.
- ♣ Los medios compiten entre sí, esto da como resultado que cada página de internet tiene su objetivo, tratar de conquistar al navegador con el fin de llegar a tener el control de su atención.
- ♣ Metodológicamente la atención que tiene las páginas de internet suelen llamar la y distraer al usuario de tal manera que pierda su tiempo entrando a otras conexiones provocando la experimentar de sitios no adecuados.

Cierto es, que solicitar lo anterior parece mínimo y poco trascendente, pero debemos recordar que en un principio la relación entre usuario e internet se generó bajo el principio de la buena conexión, axioma que debe rescatarse para el vertiginoso mundo de las relaciones a través del Internet.

### **1.5 Ciberespacio.**

Dentro de los conocimientos de internet, es importante saber, que el mundo en donde se transmite el enlace de información es parte importante para un usuario que tiene acceso a las redes y por lo tanto debe conocer; el ciberespacio es una realidad simulada que se encuentra dentro de aquellos ordenadores y de aquellas redes digitales que se conocen en todo el mundo

Para Walker el ciberespacio es una alucinación consensual que proporciona experimentos diarios desconocidos como la sensación de transporte desde el mundo físico a otros mundos de la imaginación, cambia el modo en que se perciben los humanos en un nivel muy fundamental y personal (Walker, 1989)

Gibson nos da un término sencillo del ciberespacio como aquellos datos que son controlados por poderosas máquinas de información tridimensional, que permiten al usuarios navegar o conectarse a través de equipos especiales; lugar donde se mantiene una comunicación real de conexión, brindando un enlace con todo el mundo; transfiriendo información de un lugar a otro.

El ciberespacio en los usuarios es visto como el (espacio de interacción virtual) que maneja enlaces de grandes distancias que es utilizado por varios usuarios a fin de conseguir tener una comunicación en un área determinada; en donde existe solamente como espacio relacional; se construye a través del intercambio de información; es decir, es *espacio* y es *medio*.

Es importante reconocer que una red sin interacción entre sus miembros deja de ser una red; una red existe porque existen relaciones entre sus integrantes y al no ser así pierde su valor como conexión.

El carácter esencial del Ciberespacio determina su emergencia: con la idea de comunicación, ya que surge en y por la comunicación, de ahí su doble naturaleza de espacio y medio. Es, por tanto, un espacio que se genera cuando se producen ciertos tipos de comunicación que se transfiere por enlaces.

El argumento de Theodor Nelson, menciona que este sistema interactivo de una serie de presentaciones destinadas a afectar en cierta manera la mente del usuario. Dicha afectación es llamada virtualidad que trata del espacio donde ocurre el argumento; Realidad virtual que habla de una estructura de la apariencia cuyas creaciones se sustentan en la percepción conceptual. (Nelson, 1987)

La identificación del ciberespacio con el internet no es relativamente igual; ambos carecen de diferentes componentes cibernéticos, necesarios para justificar los datos que adquiere cada uno, garantizando información de diferentes fuentes.

La acción activa que presenta un usuario en el ciberespacio se sustenta en lo que mejor hacemos los humanos: detectar modelos, hacer evaluaciones, percibir sutiles cambios de contexto, descarga de información y hacer uso de ellos a fin de darle uso necesario a los diferentes conocimientos, ya que fue creada en y por la comunicación.

Esto nos demuestra que el uso que se le tiene a esta rama de comunicación es de vital importancia, ya que son los medios en los cuales se realiza todo tipo de trabajo, manteniendo una directa conexión misma que agiliza la manera de trabajar, dando los mismos resultados.

La realidad fáctica en la realidad virtual simulada del ciberespacio puede trazarse desde varias rutas; este diseño tridimensional con vista múltiple, genera grandes conocimientos de modos de trabajar, creativamente haciendo del mundo una forma rápida de adquirir conocimientos.

No obstante, lo fundamental de este diseño de página es la producción de contenidos exactos que brinda el sistema a fin de generar mediaciones sociales.

Algo muy importante que se debe recordar al manejar este tipo de conocimiento; es reconocer que tipo de comunicación existe entre una posibilidad para superar la barrera de la alfabetización digital.

Hoy día ya no alcanza la oralidad secundaria, es decir saber leer y escribir. Con las tecnologías de información se necesita leer y escribir sobre símbolos hospedados en aparatos de comunicación que no necesariamente son personales. Y como nivel superior, una alfabetización multimedia que se plantea esta incógnita es saber ¿por qué y para qué usar las tecnologías y sus aparatos de comunicación? Con este nivel de alfabetización se comprende el uso de los nuevos medios digitales para construir identidades virtuales a fin de construir comunidades. No es solo el hecho saber que existe este tipo de herramienta, sino, reconocer que es necesario capacitarse para poder tener acceso a este tipo de enlace a fin de formar parte de los grandes avances de la tecnología.

El espacio virtual de interacción reconoce que se ha creado un ámbito de conocimiento en donde el ser humano se desarrolla de una manera más rápida junto con sus potenciales de conocimientos, básicamente por la ampliación de la capacidad de comunicación e interacción.

Se entiende el Ciberespacio como una gran acumulación de información, pero no es lo todo lo necesario para un usuario. Lo básico son las posibilidades de interacción que puede lograr una persona; esta capacidad de interactuar se ve también ampliada respecto a otras formas más limitadas anteriores. A diferencia de otros medios -el Ciberespacio es también *medio*-, permite la convivencia, la construcción de relaciones de diversos tipos y grados.

Lo importante de este espacio virtual, es la manera del actuar de las personas, el punto de encuentro, lugar de convivencia, es la comunicación, el intercambio de información, es el área de relación que se tiene para lograr una buena comunicación el espacio. Es el efecto, en todos los sentidos, aunque sea virtual.

Joaquín Aguirre establecen que existen tres niveles de comunicación los cuales básicamente son: a) las relaciones de intercambio de información entre máquinas; b) las

relaciones de intercambio de información entre hombres y máquinas; y) las relaciones de intercambio de información entre seres humanos a través de las máquinas. (Aguirre, 2004)

El Ciberespacio es el un espacio relacional *cibernético*, en el que una máquina, que constituye un red, es el medio para que se establezcan unas comunicaciones entre humanos. La realidad en el Ciberespacio quienes se comunican directamente son las máquinas las que actúan como mediadoras para posibilitar nuestras comunicaciones interpersonales

Básicamente estos tres tipos de comunicaciones, forman parte de un *proceso* que mantienen un propósito de: a) para establecer contacto con otros seres humanos que están en otros puntos de la red, b) nosotros nos comunicamos con las máquinas, c) que se comunican entre sí.

Finalmente se debe tener lectura crítica de conocimiento con relación a las tecnologías y ante todos sus contenidos, de esta manera reconocer lo necesario para identificar que contenidos debe seguir un usuario reconociendo que términos puede utilizar. El Ser reafirma su existencia por fuera de las tecnologías y, por tanto, lo cultural y lo social no pueden estar excluidos sino integrados a partir de la propuesta de un ciudadano activo.

## **1.6 Redes sociales.**

Las redes sociales se definen como un conjunto finito de actores como lo son; individuos, grupos, organizaciones, comunidades, sociedades, etc. Que están vinculados unos a otros a través de una relación o un conjunto de relaciones sociales. Las redes sociales se apoyan en el Análisis de Redes Sociales (ARS) el cual se centra en tomar las relaciones entre actores como el material sobre cual se construye y se organiza el comportamiento social de actores.

Una red social básicamente es una estructura que está conformada por grupos de individuos, a los cuales se les llama nodos, los cuales están conectados mediante algún tipo de relación; amistad, negocios, parentesco, etc. Este tipo de estructuras son frecuentemente utilizadas para modelar una situación social.

El surgimiento de nuevas tecnologías basadas en Web, han permitido que la comunicación e interacción entre usuarios sea cada vez más cercana. Es por eso que hoy en día podemos encontrar diferentes servicios Web que permiten a los usuarios interactuar con personas en diferentes partes del mundo. Este tipo de tecnología ha venido a cambiar la forma en que interactúan los usuarios, ya sea mediante la compartición de archivos, el envío de mensajes, publicaciones en blogs, etc.

La Web hace referencia a una segunda generación de Web basada en comunidades de usuarios y un conjunto de utilidades como las redes sociales, los blogs, o los wikis, donde la colaboración y el intercambio ágil de información juegan un papel importante. El estudio de las redes sociales a gran escala representa un gran reto para los investigadores del Análisis de Redes Sociales (ARS), ya que estas redes poseen propiedades que no pueden ser obtenidas por simple escalamiento de las redes pequeñas estudiadas por los sociólogos.

La tendencia de la gente para formar grupos y crear nuevas relaciones es fundamental en la estructura de la sociedad y la forma en que tales grupos se van desarrollando a través del tiempo y como este crecimiento afecta directamente el comportamiento de la estructura de la sociedad.

El Análisis de Redes Sociales (ARS), nace en los años 70 con la fundación de la International Network for Social Network Analysis, la cual es una asociación profesional para investigadores interesados en el análisis de redes sociales aplicada en diferentes áreas del conocimiento.

Las redes sociales son representadas mediante grafos, y utiliza técnicas de la teoría de grafos para estudiar la estructura de las redes sociales. Sin embargo, existen diferencias en la forma en cómo se aplican los distintos conceptos de la teoría de grafos sobre el ARS.

### **1.6.1 Antecedentes**

La teoría de redes tiene sus orígenes e influencias en diferentes corrientes del pensamiento como la antropología, psicología, sociología y las matemáticas. La sociometría se interesó por la estructura de los grupos de amigos aunque sus principales razones fueran terapéuticas.

En los últimos años diversas áreas del conocimiento han desarrollado estudios enfocados a la estructura y comportamiento de estos sistemas, y principalmente en la relación entre usuarios utilizando el ARS (análisis de redes sociales) como un conjunto de técnicas para el estudio formal de las relaciones entre usuarios y las estructuras sociales que se presenten.

Recientemente los servicios de redes sociales en línea han adquirido gran popularidad y se encuentran dentro los sitios más importantes en la Web en cuestión de generar tráfico en la red. Por ejemplo, sitios como MySpace, Facebook, twitter, Youtube y Flickr poseen una gran cantidad de usuarios que van desde los millones hasta los cientos de millones como en el caso de Facebook y Youtube que en los últimos años han tenido un alto crecimiento y a medida que pasa el tiempo incorporan nuevas tecnologías en base a la aceptación de los usuarios.

Sin embargo, las redes sociales van más allá de solo generar nuevos sistemas y aplicaciones; Distintos grupos de investigadores han visto a las redes sociales en línea como una oportunidad de poder obtener información y poder plantear nuevas problemáticas a diversas áreas del conocimiento. Trabajos recientes han propuesto el uso de redes sociales para mitigar el correo SPAM, mejorar la eficiencia de los motores de búsqueda, para encontrar organizaciones de terroristas y traficantes, entre otros.

### **1.6.2 Concepto de Red Social.**

Para indicar que las redes sociales han tenido un impacto positivo tanto en la vida de las personas, como para las empresas, es decir que se involucran en las actividades del ser humano de diferente índole: social, económico, que se desarrollan en la red. Ambos (personas y empresas) conforman la red de redes a nivel mundial.

Para las personas, las redes sociales han sido un medio que ha cambiado la forma de educación, socialización y comunicación tradicional; dándoles oportunidad de conocer nuevas culturas, nuevas personas y mantener un contacto más rápido, efectivo y constante con familiares y conocidos.

Las redes sociales es el medio por el cual las relaciones entre personas y el contenido que crean y comparten. En un contexto más simple, las redes son páginas de internet que permiten que las personas se relacionen entre sí.

En el año 1997 surge la primera red social, de nombre Six Degrees, en la que se permitía a los usuarios describir sus características principales, tales como los son: (sexo, fecha de nacimiento, etc.) y tener un círculo de amigos, y fue la red social que impulsó el concepto y creación de las demás redes sociales.

Ya con el paso del tiempo y de las tecnologías; En el año 2003 empiezan a surgir las redes sociales que hoy en día se conocen globalmente tales como Facebook, MySpace, Twitter, LinkedIn, Last.fm, Sónico, Hi5, Tumblr, YouTube.

### **1.6.3 Origen de las Redes Sociales**

Una red social es una estructura social en la que las personas se mantienen conectados mediante algún tipo de relación amistad, negocios, y parentesco a distancia; Este tipo de estructuras son frecuentemente utilizadas para modelar una situación social.

Fue en 1930 cuando aparece la sociometría como una manera de formalizar las ciencias sociales, donde se utilizaba la estadística para estudiar las poblaciones y a la teoría de grafos servía para modelar la relación entre personas.

En años recientes la teoría basada en la estructura de las redes sociales fue retomada, debido al alto número de sistemas en la Web que permiten generar comunidades virtuales que pueden ser representadas como una estructura de red social.

La distancia entre las redes es una medición de la teoría de grafos que permite definir propiedades más complejas sobre la posición de los individuos y sobre la estructura de la red en uso. La trayectoria que tiene la estructura de una red, es el número de enlaces que existen entre dos nodos en el grafo. La distancia geodésica es el número mínimo de enlaces que llevan de un nodo a otro (trayectoria mínima), esta medida es muy utilizada en el ARS, ya que nos permite obtener el camino más eficiente entre dos actores que tienen comunicación.

Sin embargo, para el caso de las redes sociales el camino más corto no siempre es el buscado y dependerá del tipo de red social para determinar el tipo de distancia a utilizar. El diámetro de un grafo está definido como el máximo geodésico de todos los vértices dentro de un grafo. El diámetro representa el tamaño del grafo y permite saber que tan grande es la comunicación que se está implementando.

#### **1.6.4 Representación de las Redes Sociales**

En una red social cada nodo, también llamado actor o vértice, puede ser representado como un individuo o grupo de individuos. Una arista, también llamada relación o vínculo, conecta a dos nodos y representa el enlace entre dos individuos en una red social. Las redes pueden tener pocos o muchos actores y uno o más tipos de relaciones entre pares de actores.

El ARS usa dos tipos de herramientas de las matemáticas para representar información de las relaciones entre actores sociales, los grafos y las matrices, una razón para usar métodos

formales para representar redes sociales es que la representación matemática permite utilizar computadoras para dicho análisis.

El ARS usa un tipo de representación, estructura que consiste de puntos (o nodos) para representar actores y líneas (o aristas) que representan lazos o relaciones. Sin embargo, cuando los sociólogos empezaron con el análisis de redes tomaron esta representación y la llamaron sociograma. Es decir Matemáticamente los sociogramas son conocidos como grafos dirigidos hacia la conexión que se tiene con otras personas. (1.1)



### 1.1 Sociograma. (Mejía, 2010)

No solo nos hemos vuelto adictos a la Red. El mundo se ha convertido en la Red; esto es para indicar que el internet ha tenido un impacto positivo tanto en la vida de las personas, como para las empresas, de tal manera que muchas de las actividades del ser humano de diferentes índole, se desarrollan mediante la red por causas del nivel mundial que tiene.

Para las personas, el internet ha sido un medio que ha cambiado la forma de educación, socialización y comunicación tradicional; dándoles oportunidad de conocer nuevas culturas, nuevas personas y mantener un contacto más rápido, efectivo y constante con familiares y allegados que se encuentran en otro lugar.

Por otro lado, el internet ha funcionado como un medio alternativo a lo tradicional para que las empresas puedan dar a conocer y vender sus productos y servicios; Gracias al surgimiento de estas páginas, han permitido que algunas empresas mejoren las relaciones con los clientes, proveedores e intermediarios con los que comparten comunicación, teniendo ventajas e imagen de presentación virtual.

En los años 90 en que las compañías las utilizaban para dar a conocer los bienes que comercializaban se vivía un momento donde sólo existía una vía de comunicación y los consumidores no tenían voz.

A medida que fueron pasando los años, fue surgiendo un nuevo enfoque para este medio de comunicación, un internet más social y rápido, el cual buscaba darles a los usuarios y consumidores participación y derecho a expresarse mediante esta herramienta. Tiempo después esta posibilidad de expresión, y voz se logró con los portales sociales o páginas de redes sociales.

El nacimiento de las redes sociales en los últimos cinco años se han realizado múltiples investigaciones al respecto, dentro de las cuales cabe destacar el estudio publicado por la consultora Tendencias Digitales donde expresan que el uso de las redes sociales es cada vez más popular en las regiones latinoamericanas.

De acuerdo a un análisis realizado por el Tecnológico de Monterrey y el World Internet Project para el año 2009, en México existen cerca de 52.3 millones de internautas a lo largo y ancho del territorio, por lo que el porcentaje de población con acceso a internet se ubica en 46 por ciento. Este número no sólo demuestra un crecimiento exponencial en los últimos años, sino que también coloca al país en el lugar número 12 dentro de las naciones con mayor índice de penetración en la red.

El “Estudio 2012 Hábitos y Percepciones de los Mexicanos sobre Internet y Diversas Tecnologías Asociadas” acota que de ese total, aproximadamente 38.1 millones son personas menores de 32 años, agregando también que el 49 por ciento de usuarios son mujeres y el 51 pertenece al género masculino.

La capital mexicana y sus zonas conurbadas registran la mayor cantidad de penetración de internet con un 55% de la población es decir: 11 millones de usuarios involucrados en la red, mientras que el norte y el noroeste cuentan con 46 y 45 % respectivamente.

Por otro lado, (Monzón, 2009), nos da a conocer en el artículo “Redes Sociales aumentan posibilidades de las Pymes”, publicado en el Listín Diario. (Extraído de <http://www.listin.com.do>), expresa claramente que las redes sociales son medios eficientes y eficaces siempre y cuando se exploten adecuadamente.

De esta manera podemos decir que hay tipos de usuarios que frecuentan las redes sociales que se clasifican de dos maneras de forma activa y pasiva;

- Un usuario activo es aquel que, en las redes sociales, comparte información y realiza actividades como enviar mensajes, publicar mensajes o actualizar su estatus y compartir fotos y videos, mientras que.
- los usuarios pasivos son aquellos que se dedican a consumir información sin realizar publicaciones, ven fotos, revisan noticias de sus contactos y buscan personas.

Lo que conlleva a que la privacidad en Internet es uno de los grandes temas que se tratan hoy día, quedando la Sociedad digital como el punto clave de las circunstancias y, sin duda, será objeto de reflexión y disputas legales en los próximos años. Los datos personales que se brindan en la red tienen una dimensión económica y ética de suma relevancia, es decir que en la sociedad digital constituye el insumo a través del cual se gestionan electrónicamente asuntos gubernamentales y comerciales, disminuyendo costos administrativos e incrementando la eficiencia esta.

Los internautas en el mundo que accedemos a más de 200 millones de sitios web de la más diversa índole, empresas millonarias que a causa de nuestros datos personales se traducen en un gran importante de insumo económico. Toda esta dinámica no sería posible sin la confianza y responsabilidad que nos acompaña cada vez que escribimos en una pantalla nuestra información personal a cambio de algún servicio o entretenimiento.

Las redes sociales son las plataformas ideales para compartir contenidos, el 86% de los usuarios comparte fotografías y solamente el 42% comparte videos. La red social donde más fotografías se publican es Facebook, hasta el 96% de los usuarios lo hace, Twitter tiene el segundo lugar con un 32%. En cuanto a los videos la herramienta preferida es Youtube con 75%, seguido de cerca por Facebook con el 71%.

Estas plataformas sociales, la que cuenta con más usuarios es Facebook con más de 33 millones de usuarios, le siguen de lejos Twitter en el cual están registrados hasta el 58% de los usuarios de redes sociales, hi5 con 35% pero con pérdidas continuas de usuarios y Google con 33% de usuarios. Cabe destacar que cada usuario en México está registrado en promedio en 3.26 redes sociales diferentes. (social, 2013) 1.2.



## **1.2 Redes sociales. (Social, 2013)**

### **1.6.5 Tipos de redes sociales.**

A lo largo del tiempo y con el avance de la tecnología, los usuarios de internet han hecho del mundo una red de redes, que hizo que los pensadores actualicen las páginas sociales y con ello la creación de las diferentes páginas que hoy día existen, como lo son:

- Facebook: Creado en marzo de 1997 en E.U.A usado con blogs, con aplicaciones de chat, la idea de crear una comunidad basada en la Web en que la gente compartiera sus gustos.
- Youtube: Creado en febrero de 2005 en E.U.A, pagina web con contenidos de videos, usa un reproductor en línea basado en Adobe Flash para reproducir.
- Windows Live: Creado en diciembre de 1994, pagina que comparte archivos y aplicaciones de diferentes programas: conjunto de servicios online de Software de Microsoft, en uso desde el navegador, con programas de instalación.
- Wikipedia: Creado Enero de 2001, organización sin anónimo de lucro, con información de datos, y acceso de proyectos con información sustentada.
- Twitter: Creado en Enero de 2000, microblogging personal, con notificaciones en tiempo real, y aplicaciones de archivos en carga.
- MySpace: Creado en Febrero de 1996, uso personal de blogs con algunas aplicaciones de chat y aplicaciones, lugar de origen E.UA.
- Hi5: Creado en junio del 1996, en México usado como fuente personal, en donde se compartían archivos y aplicaciones de archivos adjuntos.
- LinkedIn: Creado en Noviembre del 2002 en E.U.A, como una fuente para los usuario de personalidad profesional con el fin de buscar, publicar y ofrecer cuestiones de trabajo.

Paginas sociales que son utilizadas por millones de cibernéticos con el fin de incrementar sus conocimientos y popularidad, servicios que ofrecen a los usuarios el trafico rápido de de información en grandes cantidades y mantener contacto con personas de distintos lugares.

## **Capítulo: 2**

### **La policía.**

#### **2.1 Definición de Policía.**

Encontramos que la policía en la mayoría de las veces se define como el personaje que hace cumplir la ley mediante las sanciones administrativas sin embargo consultaremos varios autores importante que se acercan a lo que es en si la definición exacta de policía.

La policía es una fuerza de seguridad encargada de mantener el orden público y la seguridad de los ciudadanos y sometida a las órdenes de las autoridades políticas. Su administración puede ser centralizada a nivel nacional, o descentralizada, con fuerzas de policía local autónomas en gran medida. Se llama también policía a cada agente perteneciente a dicha organización. Los reclutas suelen recibir formación especializada y deben presentarse a un examen de admisión.

La policía viene Del latín *politīa* (que procede un vocablo griego), la policía es una fuerza estatal que se encarga de mantener el orden público y garantizar la seguridad de los ciudadanos de acuerdo a las órdenes de las autoridades políticas.

Hanlon, nos plantea que la policía es una de las funciones más habituales del Estado impartiendo poder de una manera de organización socio-política que mantiene en práctica el uso de la fuerza en el mismo Estado en el que el ciudadano puede hacer uso de la fuerza de un policía. (Hanlon, 2006)

El Estado le otorga policía la facultad de disuadir, reprimir e investigar delitos que estén en contra de las personas o sus propiedades privadas, que si en un momento dado se presente algún tipo de daño el policía puede implementar y proceder al uso de la fuerza con ayuda de las autoridades competentes, es normal que el policía lleve a cabo un trabajo preventivo que actué en un determinado momento ayudando a la ciudadanía implementando sus conocimientos.

Desde el punto de vista terminológico, la palabra policía deriva de la voz latina *politia* procedente de la griega *politeia*, que significa constitución de la ciudad, constitución del Estado y, en un sentido aplicable a la administración pública, gobierno. Se llega a entender con esta palabra el ordenamiento político del Estado, cualquiera fuese su régimen. Llega a identificarse con el conjunto de la actividad del Estado, comprendiendo el gobierno en un concepto más amplio de administración estatal (Durand, 2004).

Durand, opina que la policía es de poder público en donde el uso de la fuerza es de amplio criterio sobre el actuar del hombre y las cosas, durante los tiempos pasados la policía era vista como el poder supremo del Estado que era equivalente al gobierno del mismo Estado en la época de la edad media del feudalismo. El poder del Estado era relacionado con el poder de la policía en donde el policía tenía un poder máximo en el cual podía castigar sin ningún problema teniendo un poder absoluto ligado en la forma de actuar y regir un país con orden, en si la policía era objeto del gobierno.

Para Laporta, existe un mecanismo, a través de una “agencia”, para controlar y administrar este uso legítimo de la fuerza en el Estado de Derecho. Una agencia centralizada de coacción con el monopolio del uso de la fuerza. La existencia de esa agencia y sus actos de administración de la fuerza, determina que las eventuales conductas agresivas, al sentirse amenazadas con sanciones coactivas y, en su caso, castigadas queden prevenidas y limitadas. (Laporta, 2002)

Laporta declara, su actuación debe regirse indiscutiblemente, por tres ideales:

1. El imperio de la ley,
2. Los derechos del hombre y
3. El principio democrático.

La agencia de la que el autor menciona es denomina Policía, y la podemos definir como un órgano civil y profesional del Estado, con la facultad de hacer cumplir la ley de manera

imparcial y reiterada con el estricto respeto de no violentar los derechos humanos, sujeta a llevar un control, obligada a rendir cuentas y capaz de fomentar una convivencia democrática ante la sociedad expuesta a las faltas administrativas con el único fin de salvaguardar los intereses de un país y los que lo conforman.

Otra definición es que la Policía “es un organismo civil armado, que tiene a su cargo velar porque se cumpla la Constitución, las leyes y los reglamentos que de ella emanan, protegiendo la vida humana y la propiedad, para hacer más segura, agradable y cómoda la convivencia social (Sotelo, 2000).

De igual manera Sotelo nos demuestra la acción en la que debe cumplir un modelo de policía actual ante las situaciones que se presenten, las acciones de aquellas personas que cometen faltas corren el riesgo de ser sancionadas por la ley cumpliendo de esta manera con el reglamento que lo amerite ante la autoridad. La Policía es parte del sistema de control del Estado y específicamente, del control formal, es pieza importante de la intervención del Estado sobre los ciudadanos teniendo un efectivo control: la Policía constituye el órgano inmediato de aplicación del control penal y uno de los más importantes del control en general.

Un estado requiere poner a la Policía en relación con los derechos humanos y con los derechos fundamentales. (Bustos, 1986) opina que la función de la Policía tiene dos vertientes dependiendo del tipo de Estado en el que se ejerza el poder policial:

- Un Estado absoluto o autoritario, la Policía es un órgano del sistema penal, en el que se devuelve mal por mal a los malos ciudadanos. Incluso cuando tal función sea justa, no es posible castigar mal con mal.
- Un Estado Democrático es necesario que la función policial esté legitimada y para ello se requiere que de alguna manera todos los ciudadanos estén de acuerdo con ella y acorde con sus propios fines” (Bustos, 1986).

## **2.2 La policía en México.**

La institución policial en la Ciudad de México se inició a mediados del siglo XIX. El reglamento y aplica una regla y obliga a instruir a todos sus elementos, desde el soldado policía hasta el comandante.

Las reglas y obligaciones básicas incluían el conocimiento de las ordenanzas y leyes sobre el respeto a las autoridades jerárquicas, normas acerca de nombramientos, separación del empleo, reglamentación de servicios y conocimiento de penas impuestas por incumplimiento, manejo de armas y operaciones tácticas.

En la época presidencial de Francisco I. Madero en 1912 se creó el primer Centro Social y Educativo de la policía del Distrito Federal, en las calles de Juárez y Balderas. Y fue durante el Gobierno del General Álvaro Obregón 1923, que se expidió el decreto con el que nace la Escuela Técnica de Policía, en la calle de Bucareli, teniendo como primer director al Profesor Gonzalo García trabéis. Es en esta época se modifica el plan de estudios con la intención de dar instrucción a los diversos puestos, desde gendarmes y técnicos hasta agentes de policía judicial.

Para 1930 esta Institución cambia de Escuela Técnica de Policía a Academia de Policía Científica en la que se tiene un especial interés a la planeación de programas y selección de asignaturas para la preparación de policías.

Entre los años 70's y 80's se presentan una gran cambios, la desaparición de la Academia de Policía, para incorporarse al Centro de Capacitación y Formación Balbuena como la Dirección de Educación Policial, posteriormente Academia de Policía y Tránsito del Distrito Federal, después Colegio de Policía y para el 12 de julio de 1993, que se publicó en el Diario Oficial de la Federación el decreto que instituye la Ley de Seguridad Pública del Distrito Federal, que en su artículo 22, determina la creación del Instituto Técnico de Formación Policial estructura y nombre que conserva hasta nuestros días

### **2.3 La seguridad pública: antecedentes.**

El actual Sistema Nacional de Seguridad Pública, que en su momento renovó las políticas e instituciones en esta materia, tiene uno de sus primeros antecedentes en las reformas realizadas al artículo 115 constitucional, en los años ochenta, durante el sexenio del presidente Miguel de la Madrid.

Ernesto López Portillo nos comenta que desde entonces se precisó la forma de organización de los municipios y sus obligaciones, para incluir la prestación del servicio de seguridad pública, lo cual originó, a su vez, la creación de leyes estatales en esta materia.

El crecimiento de la delincuencia, que tuvo uno de sus principales repuntes en los años noventa, fue el contexto para que, en las postrimerías del sexenio del presidente Carlos Salinas de Gortari, se creara la Coordinación de Seguridad Pública de la Nación (Diario Oficial de la Federación, 26 de abril de 1994).

El Plan Nacional de Desarrollo 1995-2000 definió a la seguridad pública como un asunto prioritario y enfatizó la necesidad de contar con un marco jurídico adecuado para garantizar justicia, seguridad y bienestar social. Una de las estrategias definidas para poner en marcha nuevas acciones fue establecer la coordinación entre los tres niveles de gobierno

En los años 1500 aparecieron los primeros personajes que representaban autoridad los denominados calpullec, encargados de mantener el orden de los calpulli; los teachcacuhtin, tipo guerreros que se encargaban de la situación interna de los barrios en tiempos de guerra; y los tianquizpan, guardianes de los mercados importantes.

En 1524, ya con los españoles establecidos en tierras mexicanas, aparece la primera cárcel provisional en la Ciudad de México al Poniente de la Plaza Mayor; y el primer plano en

que se basó la policía; ya para el año siguiente 1525 se conforma el primer cuerpo de alguaciles de la ciudad.

En 1529 se expide el lineamiento policiaco en forma de un Reglamento de Policía, que entre otras cosas, asentaba la prohibición a los indios de habitar dentro del casco urbano destinado a los españoles.

Para el 30 de marzo de 1531, mediante la Cédula Real, se faculta a los cuerpos policiacos, entonces denominados alcaldes y alguaciles de diferentes categorías, a aprehender a infractores dando ahí por primera vez el poder de castigar.

En 1631 fue construida la prisión mayor en el Real Palacio de Virreyes, con calabozos de castigo y la tan temida sala de tormentos.

Con el paso del tiempo y con los grandes cambios de poder y mediante un acuerdo de las Reales Audiencias del 22 de mayo de 1722, se creó un nuevo cuerpo policiaco al que se le llamó *La Acordada* que estuvo al mando durante muchos años.

Posteriormente en los años siguientes ya para 1789, ya con el Virrey Conde de Revillagigedo, se creó la Policía de Seguridad y Ornato, que se encargaba de preservar la seguridad, pero también de cuidar el buen aspecto de la ciudad.

Para el año siguiente aparecen los guardias de faroles mejor conocidos como *serenos*, que de acuerdo al nuevo Reglamento para Alumbrado y para los Guardas, se encargaban de cuidar los 93 faroles instalados, la vigilancia se desarrollaba en un entorno de cercanía, en donde cada vigilante conocía perfectamente su territorio y todos los habitantes del vecindario los reconocían.

Marzo de 1812, en la Constitución de Cádiz se ordena la desaparición de *La Acordada* en donde se otorga un amplio poder político a los miembros del Ayuntamiento, poniendo en sus manos la fuerza de seguridad. En el mismo apartado de la constitución se ordena en

junio del siguiente año la Instrucción deposita en los jefes políticos la facultad y responsabilidad de vigilar por la seguridad de bienes y de las personas en la ciudad, así como de hacer cumplir el reglamento de policía.

En 1821, se conforma un cuerpo de vigilantes voluntarios en la ciudad para subsanar la falta de policía, cada voluntario portaba un sable con tahalí ellos representaban la autoridad de la misma forma que un policía instituido.

En 1827, se establece la primera República con la ciudad como residencia de los poderes supremos es ahí donde la ciudad se divide en cuarteles. El reglamento establece nuevas bases para el régimen policial, convirtiendo a los vigilantes en soldados de policía a quienes les llamaron gendarmes, pero este sistema no tuvo el mayor éxito así desapareció muy pronto y un nuevo reglamento dejó otra vez la vigilancia en manos de los propios vecinos de barrios o cuarteles; no obstante, el sustantivo de gendarme se mantuvo por décadas para referirse a las personas encargadas de la seguridad.

Diez años después para la vigilancia de la ciudad, quedó bajo la responsabilidad de los prefectos y subprefectos que luchaban contra la delincuencia y los guardaríos que tenían como responsabilidad la vigilancia de los ríos, las acequias, los caños y la limpieza de las calles.

Se creó posteriormente el cuerpo de la Policía Montada, que tenía como objeto de contribuir a la preservación de la seguridad pública con buena vigilancia en las calles; la guardia de policía quedó conformada por escuadrones de infantería y caballería que sumaban mil hombres; de manera simultánea desaparecen los guardias voluntarios, que participaban en la vigilancia de la ciudad desde 1821.

Se expide la Ley sobre la Policía General del Imperio en 1865, en donde se designan comisarios imperiales, prefectos y la guardia municipal, misma que se dividía en guardias diurnos y nocturnos, todos ellos responsables de hacer cumplir la Ley y reglamentos de la policía.

El gobierno federal encabezado por Benito Juárez para la caída del segundo imperio emite un decreto el 21 de enero de 1869, en donde se conforma un nuevo cuerpo de policías rurales dependiente de la Secretaría de Gobernación del mismo modo, se reestructura el sistema policiaco, determinando que en la Ciudad de México se había elevado, más que en ninguna otra parte, el índice de hechos delictivos.

El Gobernador del Distrito Federal de nuevo tiene al mando la autoridad policial junto con un inspector general de policía, como responsable directo de la corporación.

Tiempo después los cuerpos de la policía seguían agrupados bajo el mando de un inspector general del que dependían todas las; ya luego cambia el nombre de gendarme por el de Policía Urbana. En enero de 1878, se implanta un nuevo Reglamento de Policía, en donde las comisiones de seguridad pasan a ejecutar funciones reservadas a la policía judicial, con atribuciones para auxiliar a jueces y al inspector general de la policía en la captura de delincuentes.

A principios del siglo XX, Porfirio Díaz inaugura el Palacio de Lecumberri el 28 de septiembre de 1900, edificio que de alguna manera terminó con el antiguo sistema carcelario, tres años después aparecen las leyes que analizan la creación de los cuerpos de gendarmes judiciales y fiscales

Con los avances de la Revolución la ciudad es puesta en estado de sitio y el ejército se hace cargo de la seguridad pública con consecuencias en donde los miembros de la gendarmería son involucrados en las fuerzas regulares y otros regresan a sus lugares de origen para incorporarse a filas revolucionarias y los demás elementos que quedan se dedican a auxiliar en servicios médicos.

El Presidente Francisco I. Madero, da a conocer una nueva guardia especial con el nombre de Batallón de Seguridad (1912); y también que los cuerpos de gendarmes aumentaron. La inestabilidad general en la Ciudad de México, entre la década de 1910 a 1920, se observa

que en los cuerpos policiacos, hubo un total de veinte directores de la Policía, tal situación implicaba y demostraba que la inseguridad en la ciudad se agudizará notablemente, aparecieron bandas organizadas y surge el secuestro como uno de los delitos más recurrentes. El 30 de diciembre del mismo año, Madero inaugura el Casino de la Escuela de Policía y a finales de esta década de nuevo se reorganiza el cuerpo responsable de la seguridad en el Distrito Federal, creando de esta manera la Inspección General de Policía, con el General Pedro J. Almada, al frente de ella.

El 20 de noviembre de 1932, entra en funcionamiento el primer semáforo eléctrico en la Ciudad de México, en el cruce de Avenida Juárez y San Juan de Letrán. En este mismo año se aprueba el escuadrón de moto patrullas, que dieciséis años después pasa a ser parte de la Policía Preventiva.

El 31 de diciembre de 1938, se aprueba la Ley Orgánica del Departamento del Distrito Federal en donde la ciudad queda dividida en doce delegaciones, en las cuales queda instalada una agencia del Ministerio Público y una Compañía de Policía. Con el cambio La Policía del Distrito Federal se convierte en Preventiva y se instalan casetas de policía en cada una de las entradas y salidas de la ciudad se hace una mejora en las instalaciones y en el cuidado interno de la ciudad de México.

El 1 de septiembre de 1941, se crea la Policía Bancaria e Industrial y el 12 de noviembre se aprueba el nuevo Reglamento de la Policía Preventiva, mismo que establece que el Jefe de la Policía, debe tener grado de general de división y sus principales subalternos también grados militares; pasando un mes exactamente el 12 de diciembre del mismo año, la policía se divide en dos especialidades:

- La Policía Preventiva del Distrito Federal, encargada de la vigilancia y
- La Dirección General de Tránsito como responsable de la vialidad.

A inicios de la década de los sesenta, el cuerpo policiaco está integrado por 4,380 policías a pie, el batallón motorizado con 638 patrullas, una compañía de granaderos compuesta por

240 policías, un batallón de transportes con 50 jeeps, 8 julias, 6 moto patrullas y 66 vehículos de diferentes tipos.

Oficialmente el 17 de enero de 1984 la Institución Policial, se denomina Secretaría General de Protección y Vialidad.

En septiembre de 1995, la institución cambia su nomenclatura por la de Secretaría de Seguridad Pública del Distrito Federal.

A principios de este milenio, fueron creadas las setenta Coordinaciones Territoriales de Seguridad Pública y Procuración de Justicia del Distrito Federal, mismas que por representantes del Gobierno del Distrito Federal, Delegaciones, Secretaría de Seguridad Pública, Agencias del Ministerio Público, Juzgados Cívicos, Defensores de Oficio, Médicos Legistas, Participación Ciudadana y Comités Vecinales.

Estas coordinaciones ya mencionadas tienen como objetivo prevenir y combatir la criminalidad, así como procurar e impartir justicia dando un enfoque integral que permita reducir la incidencia delictiva, mediante planes y programas de prevención de delitos y la instrumentación de acciones conjuntas apoyadas en una política social de alto impacto.

La seguridad pública es una función a cargo del Estado que tiene como fines salvaguardar la integridad y derechos de las personas, así como preservar la libertad, el orden y la paz pública, de acuerdo con la Constitución Política de los Estados Unidos Mexicanos.

Se establece que el Estado, a través de las autoridades competentes alcanzarán los fines de la seguridad pública mediante la prevención, persecución y sanción de las infracciones y delitos, así como la reinserción social del delincuente y del menor infractor. Para ello se necesita:

- La actuación legal e imparcial de la autoridad y de los cuerpos policíacos.
- El respeto a las instituciones.

- La confianza de la población en la autoridad y el respeto a la corporación policial.
- La cooperación de la comunidad en el mantenimiento de la seguridad pública.
- Capacitación adecuada de los cuerpos policiacos.

Se considera que “la Policía, se encargada de la aplicación de las leyes y del mantenimiento del orden público, es la parte de la administración de la justicia penal que se encuentra constantemente en contacto directo no solamente con el crimen y el criminal sino también con el público en general”. En México, la actuación de la Policía está lejos de ser ligada con las características anteriores, por lo que durante los últimos años el sistema policial ha sufrido reformas más o menos significativas, hasta la del año 2006.

Se describen las características generales de la política pública que configura el Nuevo Modelo Policial de la presente administración federal, desde 2006 a 2008, haciendo énfasis en los apartados que sobre capacitación policial se perfilan en los mismos, todo ello con base en los documentos oficiales. Esto permitirá establecer cómo se concibe la reforma policial en México y permitirá configurar el modelo desde la perspectiva oficial.

Para Ernesto López Portillo, existen dos tipos de policía: “una que ve al ciudadano como un igual, al que le da un servicio; y otra que lo ve como una amenaza al orden establecido y como fuente de oportunidades para el beneficio propio” (2005:97). En este contexto es que se propone un marco teórico también de la reforma policial, y en las siguientes líneas, el contexto en el que se considera necesario una reforma y las características de ella.

#### **2.4 Funciones primordiales de la policía.**

Como finalidad la Policía tiene parte integrante de las autoridades de la República como cuerpo armado permanente de naturaleza civil a cargo de la Nación principalmente instituida para proteger a todas las personas que conforman un país en la vida, bienes, creencias y demás derechos y libertades para asegurar el cumplimiento de los deberes sociales del Estado y de sus particulares. Así mismo para el cumplimiento del

mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas y para asegurar a todo los habitantes conviviendo en paz.

En si actividad de la Policía está destinada para proteger los derechos fundamentales tal como está contenido en la Constitución Política y en pactos, tratados y convenciones internacionales de Derechos Humanos, suscritos y ratificados en el país.

El fin de la policía está íntimamente dirigida al mantenimiento del orden público interno dicho orden resulta de la prevención y la eliminación de aquello que pueda perturbar la tranquilidad, la seguridad, la salubridad, el urbanismo, la moral pública y algunos aspectos económicos ligados al orden público.

En principio el servicio público de policía se presta con fundamento de igualdad, imparcialidad control ciudadano y publicidad mediante la descentralización, la delegación y la desconcentración de funciones. Por ello el interés por mantener la armonía social, la convivencia ciudadana, el respeto entre las personas y estas hacia el Estado, le da a la actividad policial un carácter eminentemente comunitario, preventivo, educativo, solidario y de apoyo judicial.

Es decir que toda persona tiene el derecho a recibir inmediata protección contra cualquier manifestación delictiva o contravenciones que afecte directamente a su persona o sus bienes debiendo así cooperar con las autoridades. De esta manera la Policía es un cuerpo armado, instituido que presta un servicio público de carácter permanente, de naturaleza civil y a cargo de la Nación teniendo como fin primordial el mantenimiento de las condiciones necesarias para el ejercicio de los derechos de un estado y libertades públicas para asegurar la paz ciudadana.

La actividad policial es una profesión en la que sus servidores deberán recibir una formación académica integral y adecuada de forma que les permita una promoción profesional, cultural y social, en la instrucción ética, de liderazgo y de servicio comunitario.

Cada miembro de la Policía de acuerdo a su rango, será capacitado en academias y centros de formación especializada integral en donde su formación técnica y académica abarcará nociones de derecho y entrenamiento de salvamento y ayuda ciudadana es decir que el personal uniformado de la Policía cualquiera que sea su especialidad o circunstancia en que se halle, tiene la obligación de intervenir frente a los casos de policía, de acuerdo con la Constitución Política, el presente Estatuto y demás disposiciones legales.

De manera que la policía tiene a su cargo gran poder sobre un estado y que de ello depende la estabilidad de seguridad del país con forme a esto se deben de cumplir con un orden de trabajo para poder mantener su principal función:

- La policía como poder: El poder de policía puede definirse como la facultad del Estado para limitar los derechos y las libertades individuales, en beneficio de la comunidad.
- La policía como función: La función de policía es la actividad que ejercen los funcionarios llamados normalmente *de Policía*, con el fin garantizar el desarrollo de las actividades dentro del orden, preservando la armonía social. Es la potestad del Estado para el ordenamiento de las actividades individuales, con el fin de garantizar los elementos sociales necesarios al desarrollo y el bienestar de la actividad humana.
- La policía como norma: La función de policía es regulada por la ley. Las normas de policía son dictadas para hacer efectivos los derechos y libertades y nunca para vulnerarlos o negarlos.
- La policía como profesión: El ejercicio de la actividad policial constituye una profesión, ya que se trata de un oficio permanente para la que sus miembros deben prepararse adecuadamente.

El término Profesionalización de la Policía es uno de los puntos primordiales cuando se habla de reforma policial. Para los efectos de este trabajo es importante establecer la definición de este término, vinculado con la función policial.

- Servicio permanente y que responda a las necesidades y perfil de personas, organizaciones y sociedad.
- Requisitos de ingreso en función de necesidades operativas y expectativas.
- Procedimientos de selección técnicos, transparentes y rigurosos.
- Formación en sus diferentes niveles.
- Estabilidad laboral.
- Dignificación (remuneraciones coherentes calidad/riesgo)
- Tareas definidas
- Mecanismos de supervisión, control y evaluación.
- Estructura organizacional.
- Fuertes líneas de conducta ética.
- Estrecha vinculación con la sociedad.
- Registros.
- Certificación.

Adicionalmente, son elementos indirectos de la profesionalización:

- Políticas, planes, programas, reglamentos, procedimientos y manuales.
- Acopio de información, resguardo, análisis y emisión de estrategia.
- Integración de tecnología moderna.
- Asimilación de experiencias nacionales y extranjeras.
- Vinculación con otras personas, organizaciones e instituciones.

La definición de este término, profesionalización abarca elementos que por sí mismos representan procesos complejos dentro de una organización policial, y la interrelación entre ellos. Es decir, la profesionalización se trata de un complejo sistema que permite otorgar un servicio, la seguridad pública, con calidad y en congruencia al marco de principios y valores de una sociedad democrática que convive en un Estado de Derecho.

## **CAPÍTULO: 3**

### **La cibernética.**

#### **3.1 Definición de cibernético**

Cibernética proviene del griego kyberneees ('timonel' o 'gobernador'). El concepto fue aplicado por primera vez en 1948 por el matemático Norbert Wiener a la teoría de los mecanismos de control relacionado con los discursos contemporáneos sobre una sociedad de información con el fin de estudiar la sociedad de la información por medio de las avenidas teóricas edificadas desde el origen mismo de la comunicación como disciplina científica.

Ciencia que surgió en base de los problemas planteados durante la Segunda Guerra Mundial en donde se ha trabajado en la teoría de los mensajes. Además de la parte electrotécnica de su transmisión, existe un campo muy amplio que incluye, no solo el estudio del lenguaje, sino además el estudio de los mensajes como medio de manejar aparatos o grupos humanos, el desarrollo de las maquinas de calcular y otros autómatas similares, algunas reflexiones sobre la psicología y el sistema nervioso y una tentativa de enunciar una nueva hipótesis del método científico. Esta teoría más amplia de los mensajes es probabilística y parte intrínseco de aquella corriente que debe su origen a Willard Gibbs.

En el momento de desarrollar los denominados cerebros electrónicos y los mecanismos de control automático para los equipos militares, así como los visores de bombardeo.

La cibernética también contempla los sistemas de comunicación y control de los organismos vivos que los de las máquinas. Para obtener la respuesta deseada en un organismo humano o en un dispositivo mecánico, para proporcionarle la información necesaria.

Cuando alguien se pone en contacto con otra persona, le da un mensaje y cuando responde, tiene que tener relación con lo primero que se dijo; lo cual tiene una relación entre hombres y maquinas, entre maquinas y hombres y entre maquina y maquina.

Cuando se da una orden a una maquina, la situación no difiere esencialmente de la que se produce cuando mando algo a una persona. La señal en sus etapas intermedias, haya pasado por una maquina o por una persona carece de importancia y de ninguna manera cambia esencialmente mi relación con señal. Así la teoría de la regulación en ingeniería, sea humana, animal o mecánica, es un capítulo de la teoría de los mensajes.

Naturalmente, existen diferencias de detalle en los mensajes y en los problemas de regulación, no solo entre un organismo vivo y una maquina, sino también dentro de cada clase más especializada de seres.

El propósito de la cibernética es desarrollar una lengua y unas técnicas que nos permitan, no solo encarar los problemas más generales de comunicación y regulación sino además establecer un repertorio adecuado de ideas y métodos para clasificar sus manifestaciones particulares por conceptos.

El propósito principal del matemático estadounidense (Norbert, 1948) como fundador de la cibernética nos menciona que el objetivo fue fundar una filosofía general de la tecnología, para esto se propuso reunir teóricamente y de manera lógica un conjunto de conocimientos disciplinarios.

De igual manera la cibernética también se aplica al estudio de la psicología, la inteligencia artificial, los servomecanismos, la economía, la neurofisiología, la ingeniería de sistemas y los sistemas sociales. La palabra cibernética ha dejado de identificar un área independiente de estudio y la mayor parte de la actividad investigadora se centra ahora en el estudio y diseño de redes neuronales artificiales.

Después de la segunda guerra mundial la cibernética fue definida como el estudio teórico de los procesos de comunicación y de control en sistemas biológicos, mecánicos y artificiales

Breton, opina que la palabra Cibernética, se derivada del griego “Kybernetes” traducida como timonel o gobierno en lo que la comunicación es asociada con las nociones de control, regulación y dominio, conocido mediante Platón, usada en el siglo 19 por André Marie Ampere refiriéndose a los modos de Gobierno fundamentalmente la cibernética consiste en una ciencia de leyes generales de comunicación que se aplican en diversas entidades en la que ocupa una principal función de comprender al ser humano y sus relaciones de ambiente, según el enfoque cibernético la comunicación representa el modo de ser como elemento común de todas las disciplinas.(Breton, 2000)

De la misma manera Bowker, menciona que la cibernética es la coyuntura histórica en la cual las maquinas eran lo suficientemente complejas e intensamente relacionadas con el ser humana creando un nuevo lenguaje de comunicación cibernético. (Browker, 1993)

La cibernética es el estudio interdisciplinario de la estructura de los sistemas reguladores, que está estrechamente relacionado a la teoría de control y a la teoría de sistemas (siglo XX), la cibernética es aplicable a los sistemas físicos y sociales abarcando su ambiente externo en términos técnicos, es decir que se centra en funciones de control y comunicación. Esta capacidad es natural en los organismos vivos y se ha imitado en máquinas y organizaciones de gran importancia.

Wiener nos dicen que la cibernética es una ciencia, nacida en el año 1942 que en su inicio tenía como objeto el control y comunicación en el animal y en la máquina o desarrollar un lenguaje y técnicas que nos permitirán abordar el problema del control y la comunicación en general. (Wiener, 1963)

Laposky, crea los oscilones o abstracciones electrónicas por medio de un ordenador analógico considerando esta posibilidad de manipular ondas y de registrarlas

electrónicamente como el despertar de lo que habría de ser denominado computer graphics recibiendo luego el nombre de computer art e infoarte. (Laposky, 1950)

La cibernética con el paso de sus grandes aportaciones dio gran impulso a la teoría de la información a mediados de los 60, en donde la computadora digital sustituyó la analógica en la elaboración de imágenes electrónicas, con esos avances en los siguientes años aparecen la segunda generación de computadoras (con transistores en 1960) concretándose por entonces los 1º dibujos y gráficos de computadora, y la tercera (con circuitos integrados en 1964) así como los lenguajes de programación de la época.

En 1965 tuvo lugar en Stuttgart la exposición "Computer-graphik". Pero lo que consagró la tendencia fue la que tuvo lugar en 1968 bajo el título "Cybernetic Serendipity" en el Instituto de Arte Contemporáneo de Londres.

En ese mismo año se destacó la exposición "Mindextenders" del Museum of Contemporary Crafts de Londres. En 1969 el Museo Brooklin organizó la muestra "Some more Beginnings" en el mismo año pero en Buenos Aires y en otras ciudades de Argentina, se presentaba Arte y cibernética, organizada por Jorge Glusberg donde se inauguraría los principios de la relación arte e imagen digital en ese país.

Pero en España la primera manifestación fue la de "Formas computables" en 1969, "Generación automática de formas plásticas" en 1970 ambas organizadas por el Centro de Cálculo de la Universidad de Madrid.

Estas fueron las primeras experiencias de lo que luego se llamaría net.art que se remontan al año 1994. De todas formas se puede establecer, que las primeras experiencias donde la tecnología informática puesta al servicio de la comunidad funcionó como soporte estético que trascurrieron por aquellos años.

Puedo decir que el estudio de la cibernética en su sentido actual comienza con los mecanismos de teleológica (del griego τέλος o telos para el final, meta o propósito) en máquinas con fechas de retroalimentación correctiva de finales de 1700 cuando aparece el motor de vapor de James Watt.

### **3.2 Antecedentes.**

Durante muchos años han existido grupos y personas encargadas de nuestra protección en las calles, pero la violencia y la inseguridad que existe en nuestro país, que a lo largo del tiempo han crecido tanto que jamás pensamos que necesitaríamos un equipo especial que cuidara de nosotros, de nuestros hijos y familiares mientras estamos en la comodidad de nuestro hogar, navegando a través de las máquinas en la infinita carretera de la información.

Las diferentes agencias policíacas alrededor del mundo crearon una unidad especializada contra crímenes cibernéticos. Su principal objetivo es realizar minuciosas operaciones de patrullaje anti hacker para atrapar a todas las personas que dañan a la sociedad y organizan sus actividades delictivas en la red.

Con el término Cyber policías podemos imaginarnos muchas cosas con respecto a los daños que se pueden suscitar mediante un ordenador, pero la verdad que las personas están entrenadas específicamente para encontrar y desmantelar redes criminales y bloquear sitios ilegales.

La inseguridad fue aumentando con el paso del tiempo fue por ello que la policía como una medida de seguridad para combatir delitos cibernéticos y proporcionar las condiciones de prevención para el desarrollo integral de la red Internet, en el año 2000 se creó en México la Policía Cibernética.

Los delitos que ocurren con más frecuencia en nuestro país son como piratería, hackeo, fraudes con tarjetas bancarias, pederastia y otros; sin darnos cuenta nuestro país fue formando sitio de de los primeros lugares en las estadísticas a nivel mundial en estas problemáticas de esta forma fue que se le tomo más importancia a los problemas que se estaban dando a través de las máquinas a las que tenían acceso toda la población.

Por ello que los cuerpos policíacos toman una gran decisión de poder combatir estos problemas de inseguridad en nuestro país adoptando de manera segura nuevo cuerpo llamado Policía cibernética, en cual serán capacitados para disminuir los índices de

inseguridad a través de los monitores de computadoras y los manejos que se hacen por medio de las líneas telefónicas y bancos.

### **3.3 Policía cibernética:**

#### **3.3.1 Qué es la policía cibernética.**

Durante mucho tiempo el mal uso del Internet en nuestro país, ha provocado una problemática nueva entre la sociedad, por lo que el cuerpo policiaco ha hecho que se genere un programa llamado Policía Cibernética.

Con el objetivo de ayudar a proteger las normas de seguridad en la red; La Policía Cibernética perteneciente a la Dirección General de Tráficos y Contrabandos, que además de las acciones preventivas en materia de delitos cometidos en Internet usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores; todo esto es con la finalidad de poder disminuir los problemas que se presentan por medio de redes sociales en las cuales tienen acceso casi todo el mundo.

Este cuerpo policiaco, es el primero en su tipo en América Latina y que depende de la Secretaría de Seguridad Pública (SSP) tiene registrados 497 casos de menores desaparecidos que, se presume, fueron ubicados vía Internet por sus plagiarios. De ese total, 51 por ciento son varones y el 49 por ciento mujeres cuyas edades van de los cinco a los 17 años y que en el 72 por ciento de los casos (357), desaparecieron en el Distrito Federal.

Cabe señalar que si bien entre sus funciones está la de combatir la pornografía infantil vía Internet, la Policía Cibernética también busca prevenir otros delitos que se cometen en y a través de una computadora, principalmente aquellos que atentan contra las instituciones y la población vulnerable.

De acuerdo con la dirección de Inteligencia de la PFP, dicha Policía trabaja actualmente en la conformación de un banco de datos sobre pedofilia y agresiones sexuales.

Esa base de datos servirá para identificar patrones, rangos, preferencias y modus operandi de los casos reportados en México, para lo cual se intercambia información con organizaciones no gubernamentales nacionales, que en 2002 denunciaron 118 casos de menores desaparecidos. (El siglo de torreon)

El objetivo es conformar el primer banco de datos de bandas mexicanas dedicadas al tráfico de prostitución infantil y que utilizan la Internet para promover este delito. Además, se intercambian datos con organizaciones internacionales como el National Center For Missing and Exploited Children, de Estados Unidos, que ha ayudado identificar grupos de pedófilos en el estado de California.

La Policía Cibernética opera a través de "patrullajes antihacker por el ciberespacio, a través de computadoras, con lo que han comprobado el "alarmante crecimiento de organizaciones de pedófilos que transmiten pornografía infantil y promueven la corrupción de menores vía Internet".

Dicho "ciberpatrullaje" sirve también para atrapar a los delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red, sin que necesariamente se dediquen a la pornografía infantil.

Según datos de la PFP, luego del "ciberpatrullaje" se analiza la información recolectada para combatir los delitos que tienen lugar en Internet y que son cometidos de manera particular contra menores.

También, de manera encubierta, se realizan operativos en la denominada "Supercarretera de la Información" para detectar sitios donde se transmite pornografía infantil y donde un menor puede ser contactado por los delincuentes para conducirlo a actos inmorales.

De igual manera, la Policía Cibernética de la SPP recibe la colaboración de organismos no gubernamentales, quienes por su cuenta realizan ciberpatrullaje en la Red, que han localizado sectas satánicas que utilizan menores y animales en sus sacrificios.

De acuerdo con la información de la Dirección de Inteligencia de la PFP, ello demuestra que los delitos cometidos en contra de menores a través de una computadora y otros medios han tenido un incremento sin precedentes en México y todo el mundo.

"Internet ha sido utilizado por organizaciones criminales de pedófilos que promueven y transmiten pornografía infantil".

También se han detectado "bandas internacionales de prostitución, que utilizan sistemas informáticos como medio de promoción y sobre todo de reclutamiento", señaló la misma fuente.

Con la Policía Cibernética, la PFP busca identificar y desarticular bandas dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como la elaboración, distribución y promoción de pornografía infantil, por cualquier medio.

La Policía Cibernética está adscrita a la Coordinación General de Inteligencia para la Prevención de la SSP y patrulla Internet mediante software convencional para rastreo de hackers y sitios de Internet, comunidades y chat rooms en los que promueven la pornografía y el turismo sexual infantil.

Con ello se busca hacer de Internet en México "un lugar seguro para el intercambio de información, además de analizar y atacar los diferentes tipos de delitos cibernéticos que se presentan en el ciberespacio, así como su modus operandi.

Sin embargo, la PFP aclaró que "la supervisión de los padres no sustituye ningún precedente de seguridad que podamos ofrecerle", por lo que emitió algunos consejos para evitar que sus hijos sean víctimas de toda clase de delincuentes a través de Internet.

Así, se debe tomar en cuenta que las personas con quienes se comunican en línea no siempre son quienes dicen ser, y que la información en línea no es privada ni confiable. "Es decir, alguien que dice ser una "niña de 12 años", podría ser en realidad un hombre de 40 años".

También deben asegurarse que "sus hijos comprendan lo que usted considera apropiado en Internet. Qué tipo de sitios pueden visitar, Estipule reglas claras y castigos por romperlas". De igual manera, se recomienda convertir el ciberespacio en una actividad familiar, por lo que el hecho de instalar la computadora en la sala o en el cuarto de estar permite que los padres vigilen lo que hacen sus hijos.

Los padres de familia deben instalar también "programas o servicios en línea que filtran materiales y sitios ofensivos, como: SmartFilter, SurfWatch, Net Nanny, CyberPatrol, X-Stop y PureSnoop" que permiten el control de acceso a Internet para menores.

Además, algunos proveedores de Internet, ofrecen bloqueo de sitios y restricciones en cuentas para niños.

La Policía Cibernética de la PFP, que opera desde el año 2001, a la vista de que los delitos cibernéticos fueron aumentando con el tiempo, fue que se implemento la propuesta de crear este cuerpo policiaco.

### 3.3.2 Funciones.

A lo largo de las últimas décadas, la sociedad se han visto enfrentada a una serie de desafíos estructurales que están contribuyendo a transformar a muy diferentes niveles las relaciones que mantienen los ciudadanos con los Estados, así como el papel tradicional que éstos últimos desempeñaban

Las estructuras estatales recelosas de la pérdida de poder y dispuestas a ejercer su influencia con el objetivo de mantener su presencia, han ido dejando paso a otras formas en las que la ciudadanía está adquiriendo conciencia de su papel en la gestión de su propio desarrollo y persecución de intereses.

Sin embargo, la transformación de la globalización ha sido de gran impacto de gran impacto, que de forma paralela se están registrando otras dinámicas que se caracterizan por la incertidumbre que introducen en nuestros escenarios actuales.

De esta manera los grandes cambios que se ha sufrido por los abusos de poder, por los mismos delincuentes; el empleo intensivo de las nuevas tecnologías de la comunicación y el conocimiento de los nuevos autores de las redes, entre otros, están sentando las bases para el surgimiento de nuevas oportunidades de progreso y de desarrollo humano, en cual se pueden utilizar para enfrentar la delincuencia que se presenta hoy día por los medios de comunicación; pero también contribuyen a crear condiciones propicias para la emergencia de dramáticos desequilibrios económicos, sociales y políticos que se traducen en pobreza, guerras y deterioro ecológico de nuestro entorno, para manifestarse finalmente a través del terrorismo, la delincuencia organizada o el incremento generalizado de la inseguridad.

Es precisamente en este nuevo contexto en el que actúa la actual policía de las sociedades democráticas. Constituyen fuerzas de seguridad que han superado la exclusiva defensa de los intereses políticos de los Estados clásicos a través del mantenimiento del orden público como función preferente, para comprometerse en un proceso de reconversión que ha de

situarla en vanguardia de una nueva concepción del servicio público mediante el desarrollo y la profundización en conceptos como son la seguridad ciudadana.

Esta nueva realidad global adquiere un particular significado cuando hablamos de México puesto que en nuestra sociedad la transformación ha sido de doble cara ante las situaciones de violencia en los avances de la tecnología.

Al proceso de transformación planetaria es necesario añadirle la derivada unos años antes de un cambio político, que fue lo que detono los grandes cambios de los movimientos de poder que ya había obligado a los ciudadanos y a la Administración a realizar un esfuerzo suplementario de adaptación al nuevo contexto.

Las fuerzas de seguridad han afrontaron la necesidad de introducir cambios en los cuerpos policiacos, dando como resultados dificultades ante la falta de un modelo y de medios para acometer una transformación estructural de las formas de trabajos de las instituciones a cargo del orden público. La paulatina adaptación ha sido consecuencia de la esforzada voluntad de los propios policías y de su capacidad para adaptarse a los nuevos contextos.

En la actualidad nos enfrentamos a nuevos retos que han de ser profundamente conocidos y abordados, tanto en lo que se refiere a la propia articulación de la estructura de seguridad interior como en lo que hace referencia a los nuevos riesgos y amenazas que se presentan en los diferentes países.

Los nuevos procesos y riesgos a las sociedades complejas, así como la eficaz gestión de la seguridad pública, exigen un conocimiento profundo de los escenarios del presente y de futuro.

La toma de decisiones a realizarse en función de la toma en consideración de muy numerosos factores cuya importancia fluctúa en función de condicionantes coyuntural y estructural cuyo impacto varía según los cambios que se presenten en la sociedad.

Esta realidad exige un conocimiento teórico que permita visualizar los problemas y analizarlos con el fin de aportar soluciones globales o parciales para este tipo de abuso

cibernético. Para ello es necesaria la existencia de este Instituto capacitado que tendrá la voluntad inequívoca de constituir un ámbito de referencia en el abordaje de todas aquellas cuestiones que afectan a la seguridad interior y exterior de un país que, sin duda, condicionará el devenir de la sociedad mexicana el futuro.

La voluntad que presenta este instituto es la de realizar un considerable esfuerzo en el ámbito de la investigación en aquellas materias que afectan a la seguridad interna, conformando de esta manera unos instrumentos de apoyo para el desarrollo y fomento de aquellas disciplinas vinculadas a lo que se denomina Ciencia Policial.

De esta manera las bases que se presentan en la forma de trabajar de esta institución policial, sea en el futuro una fuente de información ineludible sobre materias policiales y de seguridad interior en el mundo latinoamericano gracias al acceso facilitado a través de Internet y los medios de comunicación.

Todo este esfuerzo redundará en un mejor conocimiento de nuestra Policía, así como de los escenarios en los que tienen que intervenir, lo que sin duda permitirá velar más eficazmente por la seguridad de todos, contribuyendo asimismo a elevar los niveles de calidad de vida en nuestro país.

- Sus funciones está la de combatir la pornografía infantil vía Internet.
- Conformar el primer banco de datos de bandas mexicanas dedicadas al tráfico de prostitución infantil y que utilizan la Internet para promover este delito.
- La policía cibernética es que los agentes revisan programas prohibidos de la web y ellos investigan de dónde eres para detenerte por estar en sitios probados de la web un ejemplo estar apostando en un juego de casino en la web ellos rastrean de donde lo juegan y pasan al arresto de la persona.
- Se dedican a la persecución de delitos informáticos, son policías judiciales.
- La Policía Cibernética también busca prevenir otros delitos que se cometen en y a través de una computadora, principalmente aquellos que atentan contra las instituciones y la población vulnerable.

- La policía cibernética también se encarga de combatir el terrorismo virtual.
- La policía cibernética opera mediante patrullas anti hacker por el ciberespacio mediante computadoras con las cuales sirven para poder monitorear el gran crecimiento que han tenido los pedófilos que se dedican a la distribución de la pornografía infantil, así como los que promueven la corrupción de los menores proel internet.
- El ciberpatrullaje se utiliza para buscar y atrapar delincuentes que cometen fraudes, instituciones y organizaciones delictivas en la red sin que se dediquen forzosamente a la pornografía infantil.
- Esta policía de manera encubierta realiza operativos por la carretera del internet, para detectar sitios donde se trafica con pornografía infantil y donde un menor puede ser contactado por personas con malas intenciones.
- La Policía Cibernética de la SPP recibe la colaboración de organismos no gubernamentales, quienes por su cuenta realizan ciberpatrullaje en la Red, que han localizado sectas satánicas que utilizan menores y animales en sus sacrificios.

### **3.3.3 Modus operandi.**

A lo largo de las últimas décadas, las sociedades se han visto enfrentadas a una serie de desafíos estructurales de parte de los grandes cambios de la tecnología que contribuyen a transformar a muy diferentes niveles las formas de cómo manejar las redes de internet ante las personas y su misma integridad.

Un nuevo modus operandi que se suma a la lista de tareas por atender de la recién lanzada Policía Cibernética de la Secretaría de Seguridad Pública con capacidad de bloquear, y prevenir los delitos que se cometen en y a través de una computadora, principalmente aquellos que atentan contra las instituciones y la población vulnerable.

Este cuerpo policiaco opera a través de “patrullajes antihacker” por el ciberespacio, a través de computadoras, las cuales tienen enlace con los sitios de información, en dicho patrullaje, se analiza la información recolectada para combatir los delitos que tienen lugar en Internet.

Las acciones que realiza este cuerpo policiaco se caracterizan por Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, elaboración y distribución y promoción de pornografía infantil, el análisis y desarrollo de investigaciones de campo sobre actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.

La localización y puesta a disposición ante autoridades de personas dedicadas a cometer delitos utilizando computadoras. En lo cual Integrar equipo especializado en delitos cibernéticos a fin de hacer de este medio electrónico un lugar seguro para el intercambio de información.

Utilizar Internet como un instrumento para identificar a los delincuentes que cometen este tipo de delitos. Realizar "patrullajes" en la red a fin de localizar sitios que hayan podido ser vulnerados, de esta manera analizar y desarrollar estrategias para la identificación de los diversos delitos ocurridos en Internet.

Todo esto se trata de que los criminales instalen en las computadoras con la capacidad de bloquear el equipo desde una ubicación remota. El bloqueo del ordenador es la parte más importante de la estafa a los usuarios del mundo del internet; sin embargo, no en todos los casos se presenta de la misma forma.

El objetivo es buscar hacer de Internet en México un lugar seguro para el intercambio de información, además de analizar y atacar los diferentes tipos de delitos cibernéticos que se presentan en el ciberespacio, así como su modus operandi.

Este cuerpo policiaco está conformado por trabajadores de la SSP que han sido constantemente capacitados, para la correcta manipulación de las herramientas informáticas para el combate de delitos; y que tienen además, el deber de analizar páginas de Internet sospechosas.

La policía cibernética se dedica principalmente a combatir la prostitución y pornografía infantil, desarticulando las bandas que se dedican a estas situaciones de delito, detectando a los compradores de esta, a los vendedores y a las víctimas. Por medio de una base de datos

con información de las personas involucradas en relacionan a las víctimas, que comúnmente son niños robados o desaparecidos.

Este cuerpo policiaco comparte información con diversas organizaciones de seguridad, no necesariamente dependientes del gobierno mexicano, la información es compartida con diversos países del mundo, los cuales tiene el mismo objetivo de disminuir las cifras de delitos cibernéticos que se presentan en las redes sociales con datos estrictamente confidenciales que fundamente la necesidad de la misma.

El avance de los tiempos en las tecnologías cambian, las maneras de delinquir se adaptan a las mismas, así como las leyes y sanciones, pero para cerciorarse de que las anteriores se cumplan, es necesario contar con un grupo de personas especializado que vigilen la realidad creada dentro de las computadoras y las redes.

### **3.3.4 Perfil del policía cibernético.**

La tecnología es un tema importante en la actualidad entre la sociedad, quienes por el fácil acceso a las redes sociales están expuestos a conductas que si bien para ellos no son malas, pero que puede orillarlos a ser presa fácil de la delincuencia. Es por ello que un policía cibernético tiene que contar con una capacidad de combatir tipos de delito en red; por lo cual debe presentar un perfil adecuado.

"El perfil de los elementos que componen esta nuestra unidad son licenciados, ingenieros y técnicos en informática, estas personas elegidas utiliza la lógica de programación en aplicaciones para la toma de decisiones.

Saben construir proyectos de tecnología computacional. Aprende a usar lenguajes y técnicas de programación vigentes, así como la construcción de compiladores e interfaces computacionales, además de de tener el conocimiento de construir redes de computadoras.

Por lo cual las instituciones policiacas dependientes de la Secretaria de Seguridad Pública pretenden que los elementos elegidos para formar parte de estos cuerpos tenga los suficientemente conocimientos en Sistemas Computacionales con una formación

interdisciplinaria que les permita el manejo de relaciones del contexto informático y de la Ingeniería en sistemas computacionales, involucrados en una organización; que tenga la capacidad para analizar situaciones reales y plantear soluciones a los problemas detectados en el desarrollo del procesamiento de datos en una organización, que favorezca el planteamiento del escenario de la organización y mejore su estado actual, reflejándose en un incremento en la calidad y productividad de la misma.

Se busca que los elementos estén comprometidos con la problemática nacional, actúen como agentes de cambio en su área.

Para lograr que los elementos cumplan con el objetivo de este nuevo cuerpo policiaco deben de estar estrechamente vinculación institucionalizada con conocimientos de específicos.

Una preparación de formación en el campo básico de la Ing. en Sistemas Computacionales que permite profundizar o ampliar en algún conocimiento o campo de aplicación específicos para atender las distintas demandas del entorno; su revisión periódica permitirá actualizarlo en sus contenidos y orientación.

Personal con una mejora académica continua que tenga como uno de sus parámetros las tendencias internacionales de tipo de profesionistas con conocimientos de programas de equipo básico y software que permita realizar prácticas actualizadas y acordes a la problemática que se presente.

El sistemas de apoyo para tener información actualizada y de distintas fuentes y países debe contener el desarrollo de actividades que fomenten la creatividad en el terreno de los Licenciados en Sistemas computacionales y que fortalezcan su trabajo cumpliendo un perfil adecuado para combatir este tipo de delito cibernético, por lo cual tiene que cumplir con un perfil de conocimientos básicos como lo son:

- Crear e implantar sistemas de información particulares en alguna actividad específicas o de aplicación global en la organización, permitiendo obtener

beneficios como una operación sencilla y eficiente de los datos y una explotación rica y variada de la información que el sistema de investigación.

- Conformar y adecuar eficientemente las estructuras creando, innovando, operando las bases de datos de los sistemas, para responder a los requerimientos operativos, de cálculo, investigación y de información requeridas.
- Administrar la explotación, mantenimiento y operación de los sistemas de información, así como todos los elementos que son parte de estos.
- Realizar estudios de factibilidad operativa, técnica y económica para proyectos informáticos y computacionales, selección de equipo, desarrollo de sistemas de información, instalación y mantenimiento de redes y la adquisición de productos y herramientas de programación.
- Establecer comunicaciones con profesionales de otras disciplinas dentro y fuera de la organización para identificar áreas de oportunidad para el procesamiento de recopilación de datos.
- Conocer y aplicar las disposiciones de carácter legal en la organización relacionadas con la función informática. Comprender el funcionamiento y alcance de los recursos de software utilizados en el desarrollo y uso de sistemas de información.
- Colaborar en la solución de problemas de la comunidad, aplicando conocimientos informáticos y Computacionales.
- Integrar conocimientos para especializarse en el desarrollo de software de vanguardia en diversas áreas de aplicación, tales como graficación, la multimedia, las comunicaciones y el diseño.

## **Capítulo 4**

### **Investigación de los delitos ocasionados por el Internet.**

#### **4.1 Pornografía infantil vía internet.**

En los años 1990, la distribución de pornografía vía Internet prácticamente se reducía al porno. No fue hasta entonces que el Internet se convirtió en una herramienta más accesible al público en general cuando la pornografía en la red se convirtió en un fenómeno de enormes dimensiones.

A sus inicios, la distribución online de pornografía a menudo consistía en la colaboración de los propios usuarios que subían imágenes que escaneaban de revistas para adultos a los, este estilo era generalmente gratuito, y proporcionaba un considerable anonimato. Dicho anonimato permitía saltarse las restricciones de copyright algo relativamente sencillo, y que al mismo tiempo que protegía la identidad tanto de los usuarios que subían contenidos como de quienes lo descargaban.

Sin embargo, no fue hasta la aparición de la Red Informática Mundial cuando se produjo el verdadero empujón a la distribución de pornografía en Internet, tanto gratuita como comercial, teniendo un acceso más fácil a las páginas.

El surgimiento de sitios web ofreciendo fotografías de las temáticas más variadas imaginables, vídeos descargables y contenidos vía multimedia incluyendo cámaras webs en directo, permitieron un mayor acceso a la pornografía.

Aunque inicialmente lo más habitual eran adaptaciones digitales de emporios pornográficos ampliamente asentados en el mercado, como los contenidos exclusivos online y el aumento de interactividad con los usuarios fueron aumentando progresivamente, distanciándose de otras divisiones que hizo más grande este mal hábito, creando de esta manera que aumente del números de usuarios.

Durante el 2000 la pornografía en Internet volvió a sufrir nuevas evoluciones. Por un lado, la aparición de redes de intercambio de documentos potenció la libertad a la hora de

intercambiar pornografía entre los propios usuarios. Por otro lado, las redes sociales en Internet modificaron los hábitos diarios de los internautas, en busca de una mayor interactividad y de la potenciación de las relaciones entre los propios usuarios, bien virtuales y reales, a través de sitios web de contactos.

Pornografía en Internet ha creado en el mundo uno de los problemas más destacados que abarca gran parte de la sociedad de esta manera colocando a la pornografía que se distribuye a través de las distintas tecnologías sobre las que Internet se apoya, principalmente vía sitios web, intercambio de ficheros o grupos de noticias.

Si bien la pornografía ha formado parte de Internet desde los años 1980, pero fue la invención de la Red Informática Mundial en 1991, así como la apertura de Internet al público general lo que detonó a una explosión de la pornografía online, destacando al igual las cintas de vídeo y los DVD, que son las que tienen más visitas de usuarios.

Internet se ha hecho popular en la distribución de pornografía permitiendo que la gente vea pornografía de forma anónima en el confort y la privacidad de sus hogares. Con lo cual también permite el acceso a la pornografía a gente cuyo acceso estaría restringido legalmente o por condiciones sociales.

Sin embargo, la relación entre el porno e Internet no es unilateral. La industria del porno ha ayudado en el desarrollo de Internet, dirigiendo la popularización o creación de nuevas tecnologías, entre las que pueden contarse en multimedia de audio y vídeo, la geolocalización, los distintos sistemas de pago o la validación de usuarios frente a software automatizado.

Fundamentalmente el marco conceptual lo que comprende esta problemática aborda en la investigación puntos importantes y definiciones, tales como: niño, niñez, menor, adolescencia, delito, y las distintas conductas delictivas que atacan la integridad sexual y física de los menores, y personas que son vulnerables a abuso sexual, pederastia, atentados al pudor, corrupción de menores, estupro, prostitución.

El Marco Jurídico Actual a nivel Federal, nos dice que la reforma de distintos ordenamientos federales, tiene como fin de que las niñas, niños y adolescentes de nuestro país tengan una mayor protección en relación a los delitos relacionados con abuso sexual el cual expone los instrumentos jurídicos nacionales e internacionales que brindan protección al menor en lo cual al avance de la tecnología se ha incrementado los diferentes tipos de abusos contra las personas.

Cabe mencionar que La cámara de diputados propone endurecer las penas contra las personas que explotan y abusan sexualmente de menores de edad, puesto que el marco legal vigente de México ha sido rebasado por las bandas criminales, que hacen uso inadecuado de las páginas de internet.

Por lo cual se presentó una iniciativa de reformas a la constitución y adecuaciones al artículo 201 bis del Código Penal Federal, para tipificar con precisión, federalizar y penalizar como grave la prostitución infantil, la pornografía infantil y el turismo sexual con menores de edad. Todo esto con el debido apego a estándares internacionales y a los documentos que el Estado mexicano ha firmado. Existen diversos tipos de abusos, en los cuales muchos no conocen sus términos como los son los siguientes:

- Abuso Sexual: es aquella situación definida como cualquier actividad sexual entre dos o más personas sin el consentimiento de una de ellas. El abuso sexual puede producirse entre adultos, de un adulto a un menor e incluso entre menores; teniendo dos clasificaciones las cuales son:

- El primer tipo se describe cuando ocurre una penetración de órganos genitales en contra de la voluntad, o aprovechando la incapacidad de un menor para comprender ciertos actos. También se incluye el inducir u obligar a tocar los órganos genitales del abusador.
- El segundo es la acción que incite al menor a escuchar o presenciar contenido sexual impropio; así como observar al adulto desnudo o mientras mantiene

relaciones sexuales con otras personas, ver material pornográfico o asistir a conversaciones de contenido sexual.

- Acoso Sexual: es aquella acción que consta de una serie de conductas compulsivas sexuales con distintas formas, sin el consentimiento de la personas. Se puede presentar en personas de ambos sexos o personas del mismo sexo; pero la que mas predomina comúnmente en los hombres que se mueven en ambientes de relaciones laborales, académicas, estudiantiles, que incluyen hasta el hogar
- Atentados al Pudor: delito de tipo sexual que protege el pudor de los individuos que se lleva a cabo cuando una persona realiza actos de tipo sexual en el cuerpo de otra, sin que ésta haya prestado su consentimiento para hacerlo. Es diferente a la violación según el caso, la legislación y las distintas épocas. Se distingue entre atentado al pudor simple y atentado al pudor con violencia
- Corrupción de Menores: los delitos que afectan a quienes promovieren la práctica sexual rentada o utilización de personas en material pornográfico. En el caso prostitución es en realidad el proxenetismo y este no tiene requisitos de edad.
- Estupro: es una violencia sexual considerada como un delito que generalmente es confundido con el abuso sexual infantil, sin embargo tiene una diferencia sustancial, en cuanto el estupro se puede cometer en contra de una persona en edad de consentimiento sexual y menor de 18 años.
- Lenocinio: es aquella acción en la cual una persona que explote el cuerpo de otra por medio del comercio carnal, se mantenga de este comercio u obtenga de él un lucro cualquiera; al que induzca o solicite a una persona para que con otra, comercie sexualmente con su cuerpo o le facilite los medios para que se entregue a la prostitución, y/o, administre o sostenga directa o indirectamente, prostíbulos, casas de cita o lugares de concurrencia expresamente dedicados a explotar la prostitución, que tenga de por medio beneficio con sus productos.

## **4.2 Fraudes.**

El avance de la tecnología agiliza y facilita la mayor parte de nuestras actividades cotidianas. Sin embargo, también lo hace con los actos delictivos que se aprovechan de la falta de información e ingenuidad de los usuarios.

El fraude es uno del delito más creativo, que requiere de las mentes más audaces ya que es una acción en la que podemos decir que es prácticamente imposible dejar de hacer. Esta acción de fraude, se presenta como la manera muy antigua de conseguir beneficios mediante la utilización de la inteligencia, viveza y creatividad del ser humano, considerado hoy día como un delito, mostrando la manera en que son afectados diversos sectores empresariales, y personales mediante los medios más vulnerables.

Esta actividad que se presenta con más frecuencia ha generado pérdidas económicas considerables tanto al sector empresarial como en los particulares durante los últimos años.

El phishing o robo de datos personales es el que ha presentado una gran giro en las pérdidas entre los usuarios que manejan una cantidad de recursos, que se han visto afectados en los últimos años; se caracteriza por intentar adquirir información confidencial de forma fraudulenta así como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria.

El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas; por lo regular los estafadores no se conocen personalmente ante el usuario por lo que es un poco más difícil detectar en el momento la acción del fraude.

De acuerdo a los estudios del INEGI de 2010 al 2013 han incrementado las quejas a los diferentes tipos de fraudes que existen y se presentan han la sociedad.

<b>Categorías Principales</b>	<b>Número de Quejas</b>	<b>Porcentaje</b>
<b>1) Robo de Identidad</b>	246,035	36%
<b>2) Compras desde el Hogar   Ventas por Catálogo</b>	46,995	7%
<b>3) Premios   Sorteos y Loterías</b>	45,587	7%
<b>4) Quejas sobre Servicios de Internet y Computadoras</b>	41,243	6%
<b>5) Subastas en Internet</b>	32,832	5%
<b>6) Ofrecimientos de Dinero Extranjero</b>	20,411	3%
<b>7) Préstamos con Cargo Adelantado y Protección   Reparación de Crédito</b>	10,857	2%
<b>8) Clubes de Compradores y de Revistas</b>	8,924	1%
<b>9) Servicios Telefónicos</b>	8,165	1%
<b>10) Atención Médica</b>	7,467	1%
<b>11) Oportunidades de Negocio y Planes de Trabajo en Casa</b>	7,460	1%
<b>12) Viajes, Vacaciones y Tiempos Compartidos</b>	6,712	1%
<b>13) Artículos y Servicios para Oficinas</b>	5,723	1%
<b>14) Subsidios: Becas/Educativas y No-Educativas</b>	5,310	1%
<b>15) Agencias de Empleo/Asesores Laborales/Trabajo en el Exterior</b>	4,485	1%
<b>16) Inversiones</b>	3,630	1%
<b>Otras quejas codificadas</b>	12,399	2%

Las extorciones van de la mano junto con los fraudes ya que de ahí se delimitan las acciones que causan los integrantes de estafadores; teniendo en cuenta que estas personas estudian los movimientos de las personas para de ahí actuar y saber en qué momento lanzar las amenazas del ataque.

Una extorción en si es aquella amenaza de difamación pública o daño semejante que se hace contra alguien, con la finalidad de obtener de él o ella, dinero u otro provecho; es la presión que, mediante amenazas, se ejerce sobre una persona para obligarle a obrar en determinado sentido, es decir al que sin derecho obligue a otro a hacer, tolerar o dejar de hacer algo, obteniendo un lucro o beneficio para sí o para otro.

Estas personas que son causantes de este tipo de anomalías hacen llamadas telefónicas que lo confunden y presiona para obtener dinero u otro beneficio, su mayor ataque es:

- ◆ Hacen creer que son un familiar en peligro (fingiendo voz de angustia), un servidor público o cualquier persona ajena que lo amenaza directamente.
- ◆ Lo amenazan con el secuestro de un familiar.
- ◆ Le ofrecen ayuda para salir de un problema legal.
- ◆ Lo hacen creer que es beneficiario de un sorteo o rifa.
- ◆ Es amenazado con la difamación pública o con sufrir daños.
- ◆ Le exigen un depósito en cuentas bancarias, órdenes de pago o compra de tarjetas telefónicas.

### **4.3 Cyberbullying.**

En la sociedad actual el ser humano se, caracterizada fundamentalmente por la capacidad de poder adentrarse en el mundo de la información y, lo que es más importante, hacer un buen uso de ello, sabiendo utilizar adecuadamente estas herramientas.

Edreira, nos dice que este problema de acoso es el proceso por el cual un individuo o grupo de individuos aplican violencia; psicológica o moral que empiezan con pequeñas dosis de agresión a otro individuo con la intención de desestabilizarlo y hacerlo dudar de sus propios pensamientos y afectos provocar el arrebatada de identidad. (Edreira, 2012)

El objetivo de esta conducta de acoso es paralizar a la víctima evitando que esta reaccione, para que no pueda pensar ni comprender, y mantener de esta forma la disposición del agresor. El proceso pretende pervertir moralmente a la víctima y destruirla lentamente para conseguir un crimen perfecto, y en dado caso cuando se provoca y se induce a la víctima al suicidio o violencia física.

Las nuevas tecnologías de la comunicación han sido un punto importante ante el mundo globalizado en el que vivimos. El desarrollo de los aparatos móviles y de las redes sociales ha impulsado nuevas modalidades de maltrato o acoso entre nuestros jóvenes que en su mayor dimensión se presenta en las comunidades escolares, conocido como Ciberacoso o Cyberbullying.

El Ciberacoso, ahora conocido como el Cyberbullying por su traducción al inglés; es el uso de información electrónica entre los medios de comunicación tales como redes sociales, blogs, mensajería instantánea, correos electrónicos, mensajes de texto, teléfonos móviles, y whatsapp, programas difamatorios para acosar a un o unos individuos, mediante los ataques personales; si se hace cotidianamente o con grado de persecución hacia una persona se constituirá como un delito penal.

Este problema no es una acción voluntaria ya que implica un daño recurrente y repetitivo infligido a través del medio del texto electrónico llámese (amenazas o difamaciones), provocando de esta manera angustia emocional, preocupación, y no tiene propósito legítimo para la elección de comunicaciones. El Ciberacoso se presenta de un modo simple como continuar mandando e-mails a alguien a fin de incrementar la inseguridad de una persona que ha dicho que no quiere permanecer en contacto con el remitente o de manera más agresiva como las amenazas, connotaciones sexuales, etiquetas con discurso de odio.

La particularidad de este problema es el uso principalmente de Internet, debido al alcance, y difusión que estas páginas tiene al tener acceso a distancia, es por eso que el ciberacoso prácticamente ocurre en todos los ámbitos en los que se mueve una persona relativamente hoy en día como lo son las siguientes áreas:

- Académico: en la vida de una persona durante la etapa de crecimiento va, pasando por diferentes escuelas adicionales, facilidad que tienen las redes sociales que dan la opción de clasificación a sus usuarios según los colegios, escuelas, universidades donde se ha estudiado o se estudia actualmente, de forma que mediante el buscador interno de la red social, se localizan a las personas, consiguiendo acceder de forma

ilegal a su cuenta, obteniendo de esta manera cuantiosa información privada y del entorno de la víctima.

- Profesional: en el área laboral donde actualmente, la mayoría de las empresas tienen páginas web, dirección de contacto, en donde se trabaja con los ordenadores conectados en red, donde estas personas violan los accesos para poder introducirse a documentos con información valiosa.
- Social y amoroso: este modo más particular que daña con dolo a las personas de las redes sociales relacionando el ámbito académico, donde los miembros más jóvenes de la familia hacen uso de Internet.

Las víctimas que sufren este tipo de acoso en la vida real, sufren problemas de estrés, humillación, ansiedad, depresión, ira, impotencia, fatiga, enfermedad física, pérdida de confianza en sí mismo, pudiendo derivar al suicidio; viéndolo de esta manera las víctimas se clasifican en dos tipos.

♣ Víctimas pasivas:

- Se deprimen y piensan en el suicidio mucho más frecuentemente.
- Personas que son prudentes, sensibles, tranquilos, retraídos y tímidos.
- Tendencia a sufrir ansiedad, son inseguros, infelices y poseen una baja autoestima.
- El caso de los chicos, suelen ser físicamente más débiles que sus compañeros.
- Con frecuencia huyen de los conflictos.
- Tienen rasgos físicos que resaltan: más jóvenes, más pequeñas, más gordas, tienen gafas, son parte de minorías étnicas, etc.
- Tienen dificultades de aprendizaje o, al contrario, tienen un comportamiento de muy buenos resultados académicos.

♣ Víctimas provocadoras o acosadores:

- Las víctimas provocadoras se caracterizan por un retraso escolar y por su dificultad para permanecer atentos a las tareas escolares, rebeldía.
- Estas personas se caracterizan por unos comportamientos y reacciones agresivas.
- A menudo, su forma de comportarse puede causar irritación y tensión a su alrededor y ser considerado como una provocación por parte de los compañeros.

Informe Nacional del 2010 sobre Violencia de Género en la Educación Básica en México, elaborado por la Secretaría de Educación Pública nos dice que un 30% de las víctimas pasivas no se atreven a denunciar su situación de acoso, ya sea por el miedo a represalias y al recibir violencia más grave. (Rayuela, 2010)

Las víctimas pasivas a menudo se encuentran encerradas en el círculo vicioso de la ley del Silencio, con el sentimiento de incapacidad de poder enfrentar los problemas; cosa contraria de las víctimas provocadoras que apenas se les llama la atención se quejar de ser agredidos.

Las víctimas agresivas provocan fácilmente a otras víctimas, respondiendo a la agresión a la que son sometidas, pueden ser hiperactivas y tener un temperamento fuerte; mientras que las víctimas pasivas no provocan situaciones de violencia y, por lo general, prefieren huir del conflicto a responder de la misma forma suele ser tímidas, sensibles y cautelosas.

#### **4.4 Pedofilia vía internet.**

Pedofilia es una patrón de comportamiento sexual que consiste en la acción de un individuo que se presenta una atracción sexual hacia niños o niñas pre adolescentes, la persona de, al menos, 16 años que siente atracción sexual hacia menores de 13 y respecto de los que mantiene una diferencia de edad de, por lo menos, cinco años, lo que se observa de este delito es que la atracción de una persona hacia niños preadolescentes, no se engloba al acto sexual realizado con dichos niños, que en su mayoría los destacan que muchos pedófilos no cometen ningún tipo de abuso sexual y que estas acciones las confunden con abusadores de niños y que no son pedófilos.

Etimológicamente, la palabra deriva del término griego, (muchacho o niño). Paidophilia fue acuñada por los poetas griegos como un sustituto de (pederastia) o viceversa.

Este término estudiado por Krafft, en el que nos dice que el interés sexual dirigido sólo hacia jóvenes se les denomina prepubescente, sin incluir a adolescentes, un interés que desaparecería con la aparición de los primeros signos de vello púbico. (Krafft, 1886)

A los que Krafft los clasifica de tres formas:

- Pedófilos.
- De sustitución, cuando los jóvenes prepubescente son visto como objetos que sustituyen a un adulto.
- Sádicos.

La pedofilia es un rasgo multifactorial en la personalidad del individuo, en este sentido, se suelen distinguir dos tipos de pedofilia: una primaria o esencial, muy arraigada en el sujeto, y otra secundaria, que aparecería motivada por factores circunstanciales; del que la padece, y se compone de aspectos mentales, institucionales, de actividad, de educación sexual, de violencia, de control de las pulsaciones, etc.

La personalidad y las conductas pedófilas son muy heterogéneas, desde casos casi inofensivos, hasta aquellos en que alcanzan niveles que entran dentro de lo criminal; esto es si en algún caso de actividad sexual de un pedófilo con un menor se lo conoce con el nombre de abuso sexual infantil o pederastia.

Estudios de los especialistas en estos casos lo ven desde una perspectiva de que, son, sujetos con una orientación sexual dirigida primariamente a niños, sin interés por los adultos, y con conductas compulsivas no mediatizadas por situaciones de estrés, El pedófilo suele ser hombre. Las mujeres pedófilas suelen ser o bien personas con trastornos mentales o bien personas muy solitarias y que viven al margen de la sociedad.

La personalidad del pedófilo se pueden distinguir dos grandes tipos: los primarios y los secundarios o situacionales:

- ◆ Los primarios muestran una inclinación sexual casi exclusiva por los niños y su conducta compulsiva es independiente de su situación personal. Se trata, clínicamente, de pedófilos en un sentido estricto del término que presentan distorsiones cognitivas específicas: consideran su conducta sexual como apropiada planifican sus acciones, pueden llegar a atribuir su conducta a un efecto de la seducción por parte del menor o pueden justificarla como un modo de educación sexual para este, esta persona no se siente culpable de su modo de actuar, y no se avergüenza de lo que haya hecho.
- ◆ En cuanto a los secundarios o situacionales, estos se caracterizan por que su conducta; viene inducida por una situación de soledad o estrés en algunos casos, la experimentación de relaciones sexuales con menores suele ser un medio de compensar la baja autoestima o de liberarse de cierta hostilidad, y no son estrictamente pedófilos, por lo que su inclinación natural es hacia los adultos, con los que mantienen normalmente relaciones.

Las necesidades emotivas de los pedófilos se pueden dar de diferentes maneras; se puede decir como primer punto de que casi siempre el tener relaciones sexuales con un menor de edad es el único modo de alcanzar para ellos la excitación sexual.

Como segundo punto, les permite sentirse poderosos a través del control ejercido sobre el menor, algo más complicado que si se tratase de lidiar con adultos.

En tercer lugar, la consecuencia de lo anterior, les sirve para aumentar su autoestima; creyendo de esta manera que ellos son los únicos que tienen el control de poder manejar a su víctima.

Como cuarto lugar, al repetir escenas traumáticas vividas por ellos (en los casos en los que se hayan dado), el contacto pedófilo les permite superar sus propios traumas personales y tomarse una especie de revancha al enfrentarse según a sus escenas de miedos a los que pudieron ser expuestos y situarse ahora en la posición del dominante.

En quinto lugar, la relación con menores consigue para el pedófilo consolar sus privaciones de competencia social o de cohibición en la relación con los adultos; se trata, pues, no solo de algo relacionado con su vida sexual sino con la propia realización como persona.

- Causas

No existe consenso entre los especialistas respecto del origen de la pedofilia. Muchos psicólogos y psiquiatras, dicen que los pedófilos tendrían una personalidad inmadura, problemas de relación o sentimientos de inferioridad que no les permitirían mantener una relación amorosa adulta e igualitaria.

#### **4.5 Crimen organizado.**

La delincuencia organizada se caracteriza por la actividad de un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la Convención de Palermo con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material.

Las bandas del crimen organizado utilizan el Internet para extorsionar a los jóvenes y reclutarlos en sus redes, al enviarles correos electrónicos en los que se les invita a entregar documentos o servicios de paquetería ignorando su contenido.

Los contactan vía chat o messenger en el que se les ofrece una gama de nuevos “medicamentos de promoción a fin de llamar la atención de los usuarios” como son para inhibir el apetito, relajarse, activar sus músculos, quitar el estrés, etc., que en realidad son diversas drogas que dañan la salud y su desarrollo personal, conduciéndolos a la privación de su libertad y en casos extremos a la muerte.

El narcomenudeo es la posesión, comercio o suministro de estupefacientes o psicotrópicos, cuya distribución se hace en dosis individuales. Que hoy día está tipificado como delito federal contra la salud.

Las drogas en México han presentado un crecimiento a gran escala en las últimas décadas. Es importante reconocer que el tráfico de drogas ha sido un brutal desarrollo de la Violencia.

Conforme creció la industria del crimen organizado ha logrado que la cocaína se consolidara como el producto más importante de entre los que movían las organizaciones mexicanas, la violencia se tornó más sistemática.

El mundo criminal, en los negocios ilícitos, ha respondido con entusiasmo al modernismo, y ha explotado las oportunidades brindadas por la globalización; es decir que de esta manera se ha presentado un bance en otros rubros de crecimiento para esta problemática, que se ha mantenido firmemente medieval.

El autor Williams nos da una pequeño concepto de que es para un grupo criminal definiéndolo de esta manera “Los líderes de la delincuencia son como barones medievales: con frecuencia se ven enfrascados en luchas de poder y en alianzas endebles caracterizadas por defección y traiciones frecuentes”. (Williams, 2012)

El crimen organizado y el tráfico de drogas han sido guardianes de muchas características distintivas provenientes de la cultura, la política y la cercanía del país con Estados Unidos, que ha resultado ser una maldición geográfica, puesto que ellos son los que más predominan mas en este tipo de anomalías de poder.

Sin embargo, la similitud tanto en el contexto como en el *modus operandi*, de estas organizaciones, son parte de un patrón más generalizado del crimen y no requieren ni de la imposición de caracterizaciones simplistas como el narco-terrorismo, ni de nuevos conceptos como el de insurgencia criminal.

De nuevo el autor Williams nos menciona que en la primera década del siglo XXI, el crimen organizado en México guardó muchas similitudes con su contraparte rusa de los años 1990. El colapso de la Unión Soviética y el Partido Comunista removió mecanismos de control político y social que habían permitido que una élite se beneficiara del crimen organizado a la vez que mantenía los niveles de violencia bajo control. (Williams, 2012).

De hecho, la debilidad del Estado ruso en los noventa dio cabida al florecimiento del crimen organizado, mientras que el cambio hacia una economía de mercado ofrecía oportunidades sin precedente para los delincuentes de espíritu emprendedor.

En Rusia durante los años noventa, fue común que la violencia se diera en forma de asesinatos por encargo, los líderes criminales tradicionales, se enfrentaron a una nueva especie de criminales, más emprendedores, y la competencia se desató entre los grupos étnicos. De ese modo las organizaciones rivales pelearon por el dominio de sectores de la economía, así como de instalaciones industriales.

El narco mexicano se ha comportado de manera similar o lo anterior mencionado, presentando ejecuciones en contra de periodistas, policías de bajos y altos rangos, miembros del ejército y de grupos rivales. En este rubro, la violencia criminal y las ejecuciones por encargo en ambos países fueron instrumentales y resultaron ser una continuación de sus negocios ilícitos por otros medios.

#### **4.6 Delitos informáticos.**

Se entiende por delito informático, toda aquella acción o conducta ilícita susceptible de ser sancionada por el derecho penal, que consistente en el uso indebido de cualquier medio informático.

Para Téllez los delitos informáticos son las actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento a fin de dañar con conductas típicas, antijurídicas y culpables en que tiene el acceso a las computadoras con el que se realiza el delito informático; conducta delictiva de cuello blanco, en la que se requiere conocimientos técnicos; acciones ocupacionales por realizarse cuando el sujeto activo labora, y son acciones de oportunidad pues se aprovecha la ocasión o el universo de funciones y organizaciones de un sistema tecnológico y económico. (Téllez, 2011)

Los delitos informáticos también conocidos como “delitos cibernéticos” acciones que tienen que ser conocidos por los millones de usuarios de la red y conocer con ello la importancia de poder tener un control sobre sus cuentas de información personal, mantenerse al tanto de lo puede llegar a pasar si en dado caso se les presenta un acoso cibernético, de esta manera saber actuar ante lo que pueda pasar.

El delito cibernético implica el uso de equipos tecnológicos (celulares, computadoras de escritorio y portátiles o cualquier dispositivo que implique el uso de la internet) como instrumento para llevar a cabo actos delictivos; que a su vez es el servicio de internet el cual es utilizado como una herramienta entre todas las personas independientemente de la edad que en ocasiones no saben cómo explotarla y aprovecharla al máximo y limitan su uso a actividades de esparcimiento y diversión, que en muchas ocasiones son víctimas de estos delitos.

Las principales actividades que los usuarios realizan comúnmente en Internet son: uso del servicio de correo electrónico, mensajes instantáneos, visitas de chat, envío de postales, escuchar música, bajar música, juegos on-line, visita de páginas de chistes y humor, visitas a páginas de uso exclusivo para mayores de 18 años, investigación y por ultimo sitios de educación y aprendizaje.

Es importante mencionar y destacar que los delincuentes cibernéticos cuentan con habilidades para el manejo de sistemas informáticos y generalmente, por su situación

laboral, se encuentran en lugares estratégicos donde se maneja información sensible o bien son hábiles en el uso de los sistemas.

Actualmente el Internet es utilizada por organizaciones criminales que promueven, transmiten y operan pornografía infantil; fraude; piratería de software, intromisión a sistemas de cómputo; hackeo, venta de armas y drogas, además del Cyber terrorismo, constituyéndose en auténticas amenazas para la sociedad, ya que actualmente es muy fácil acceder a estas tecnologías desde celulares o aparatos móviles como lap tops y Cyber cafés; Siendo los sectores más vulnerable de la población los niños y los jóvenes.

Una de las posibilidades de que un usuario sufra un daño o una pérdida en Internet se incrementa al reunir tres factores principales:

- Algo que tiene valor, es decir, la información de nuestra computadora, archivos, información personal, contraseñas, que sea de gran importancia para estas personas etcétera.
- Amenaza, como un evento generado por una persona maliciosa que puede causar un daño o robo.
- Vulnerabilidad, como la falla de un sistema o programa informático.

La Organización de las Naciones Unidas, nos presenta las acciones que son reconocidas como delitos informáticos y que se dividen en tres rangos de peligrosidad:

1. Fraudes cometidos mediante manipulación de computadoras:

- a) Manipulación de los datos.
- b) Manipulación de programas.
- c) Manipulación de datos de salida.
- d) Fraude efectuado por manipulación informática.

2. Falsificaciones informáticas:

- a) Utilizando sistemas informáticos como objetos.
  - b) Utilizando sistemas informáticos como instrumentos.
3. Daños o modificaciones de programas o datos computarizados.

- a) Sabotaje informático.
- b) Virus.
- c) Gusanos.
- d) Bomba lógica o cronológica.
- e) Acceso no autorizado a sistemas o servicios.
- f) Piratas informáticos o hackers.
- g) Reproducción no autorizada de programas informáticos con protección legal

Entre los potenciales e importantes adversarios de las autoridades se encuentran: los usuarios de sistemas, empleados, hackers, intrusos, el espionaje corporativo, el crimen organizado y el terrorismo.

Dentro de este último apartado se ubican el tráfico de drogas, personas y armas, entre otros; secuestro, delincuencia organizada, piratería, pornografía infantil, estafas electrónicas y delitos tradicionales cometidos a través de medios electrónicos.

Incluye hacking, ataques destructivos a información estratégica gubernamental y financiera, manipulación de datos y programas, falsificaciones informáticas, creación de virus, sabotaje informático, estafas electrónicas, intrusiones, modificaciones, interceptación, copia de información no autorizada, interrupción de las comunicaciones electrónicas, violaciones a los derechos de autor, spam y robo de identidad.

Nos damos cuenta que el eje central de los delitos informáticos se da en la manipulación de los datos de entrada, programas y salidas de computadoras, así como la falsificación de los sistemas informáticos, y el espionaje de información, este conjunto de elementos produce en el sujeto pasivo un daño en su patrimonio; por ello se estima que los ilícitos cometidos a

través de Internet afectan el patrimonio de un usuario que en su mayoría desconoce de las acciones que se le presentaron.

## Capítulo 5

### 5.1 Importancia de la policía cibernética en Quintana Roo.

Recordemos que México fue el primer país latinoamericano en conectarse a Internet, lo cual es más vulnerable a los delitos que se presentan hoy día en las páginas de internet.

Recordemos que en el país el 38.9 millones de personas son usuarios de la computadoras y el 32.8 millones tienen acceso a la red, esto quiere decir que más del 50% de nuestra población puede ser objeto o víctima de algún delito cibernético

La creación de una **Policía Cibernética** es una propuesta que permanece estancada en el **Congreso del Estado**, pero a consideración de la población es un mecanismo que atenta contra la libertad de expresión en contra de las personas que han sido víctimas de estas anomalías

La propuesta tiene como objetivo abarcar distintas áreas como los son Preventiva, jurídica, Informática, psicológica, social, con el fin de abordar la gran mayoría de los movimientos que pueda realizar un delincuente, y con ello estudiar las maneras de poder combatir y disminuir los índices de delitos cibernético.

De manera general lograr que los padres de familia, alumnos, docentes y sociedad en general eviten ser víctimas o parte activa de un delito relacionado con el uso inapropiado de las tecnologías informáticas (internet).

Es necesario que se analice y se legisle la operación de la policía cibernética, con el fin de sancionar a los hackers que realicen fraudes financieros, utilicen la información

confidencial de las personas y los castigos que se pudieran dar contra quien difame, calumnie o dañe moralmente a otra persona a través de cuentas falsas o clonadas.

El uso de Internet ha sido el banco perfecto para diversas investigaciones; el conocer mejor las características y el desarrollo del ciberespacio y sus usuarios, elementos que son poco estudiados debido al tiempo de vida que tiene la red.

México no es la excepción al uso del internet y mucho menos hacer víctima de algún abuso cibernético: la Asociación Mexicana de Internet nos dice que en el 2003 más del 50% de los cibernautas mexicanos tienen acceso a las páginas inadecuadas es decir que más de la mitad de la población tiene una computadora en sus manos. Por lo cual nos damos cuenta que cada vez somos más vulnerables hacer víctimas a estas situaciones de delitos. Por ello es conveniente que nuestro Estado sea uno de los que cuenten con una policía especializada de tal manera que estos delitos sean prevenidos antes que sea demasiado tarde.

## **5.2 Recomendaciones de prevención para la sociedad.**

La implementación de la policía cibernética brindara que los docentes, padres de familia, alumnos y sociedad en general se capaciten en el uso adecuado de la internet de esta manera tener la gran importancia de que los padres de familia y cualquier persona sigan y apliquen estas estrategias en su hogar.

- ❖ Tener en cuenta que en el trabajo o cualquier lugar en donde usen un equipo con conexión a internet, las medidas y recomendaciones que permitan prevenir que sean víctimas de un delito relacionado con el uso de la tecnología.
- ❖ Conseguir que los padres de familia influyan e instruyan favorablemente a sus hijos y conocidos con la finalidad de prevenir cualquier tipo de delito cibernético.
- ❖ Lograr que el padre de familia identifique las conductas que caracterizan a un menor o persona que esté siendo víctima por el uso incorrecto de las tecnologías informáticas.

- ❖ Motivar a los alumnos que padezcan algún tipo de amenaza o acoso para que comuniquen inmediatamente el suceso a sus padres, autoridades escolares o autoridades de la Secretaría de Seguridad Pública.
- ❖ Contribuir para que los padres de familia, alumnos, docentes y cualquier persona desarrollen la capacidad de denunciar cualquier situación delictiva derivada del uso de las tecnologías de comunicación como: las computadoras de escritorio o portátiles, el celular y cualquier herramienta que implique el uso de internet, ya sea para diversión, trabajo o servicios.
- ❖ Desarrollar en los menores de edad que utilizan la internet, la capacidad de aplicar efectivamente las medidas preventivas que les auxilien a evitar que sean víctimas o parte actora de un delito relacionado con el uso incorrecto de los servicios programas y los equipos implicados en las tecnologías de las comunicaciones.

Es importante hacer comprender a la sociedad que el uso diario de la tecnología, también genera una vulnerabilidad de poder ser víctimas de algún delito cibernético de forma que cada uno de los que a diario utilizan esta herramienta básica, conozcan a que se enfrentan al usar una maquina que contenga datos personal de gran valor; y reconocer que los delitos cibernéticos se clasifican en dos rangos de peligrosidad que son:

#### ♣ Delitos cibernéticos I.

Los que se consideran de menor peligrosidad par el usuario, como lo es el robo o manipulación de datos o servicios por medio de piratería o virus, el robo de identidad y fraudes en el sector bancario o del comercio electrónico.

Los que en cierto modo el usuario no es dañado físicamente a su persona, pero que al igual debe tomar precaución ante estos abusos, y evitar ser una víctima más de estos delinquentes. Por tanto brindar de este modo las medidas necesarias para los usuarios.

1. No abrir correos electrónicos de remitentes desconocidos.
2. Su banco no le enviará correos electrónicos en dónde solicite sus datos como: nombre, clave de acceso, número de tarjeta o cualquier otra información comercial.

3. Realice un monitoreo periódico de sus estados de cuenta.
4. Compruebe que el sitio de su banco de la tienda virtual donde desea comprar, cuente con las señales de seguridad.
5. Utilice herramientas de eliminación de software malintencionado para buscar, prevenir, detectar y eliminar este tipo de programas maliciosos como por ejemplo un antivirus y firewall. Este último es un programa que monitorea la entrada y salida de información entre su computadora e Internet.
6. Actualice regularmente los programas instalados (anti-virus, anti-intrusos, etc.) en su máquina para evitar que exista cualquier vulnerabilidad.
7. Al comprar en línea, conserve el número de identificación de compra, identificación del vendedor y los correos electrónicos enviados entre usted y el vendedor en caso de que se presente algún problema.
8. Evite bajar software gratuito ya que la mayoría contiene spyware (programas espía) que se instala automáticamente en su computadora.
9. Revise su máquina periódicamente por técnicos especializados para que la limpien de todo tipo de software malicioso.
10. Evite utilizar el servicio de banca en línea en cafés Internet o centros de negocios en hoteles, toda vez que esos equipos no siempre cuentan con software de seguridad y son blanco fácil de personas que tratan de obtener datos confidenciales.

#### ♣ Delitos cibernéticos II.

Son aquellas actividades que presentan una gravedad mayor, toda vez que el objetivo central es atacar a la población más vulnerable; como lo es el acoso en Internet, turismo sexual, extorsión, chantaje, espionaje, terrorismo, abuso de menores, explotación sexual comercial infantil, robo o sustracción de menores, etc.

En especial las recomendaciones son para los padres con referencia a los niños y jóvenes en el hogar para que no sean presas de este tipo de delitos:

Cuando se está en una computadora personal:

1. Utilice programas que ayudan a filtrar el contenido de sitios de Internet.

2. Procure ubicar la computadora en un área visible para la familia, a fin de que pueda supervisar lo que hacen y ven sus hijos, y así evitar cualquier uso inadecuado.
3. Conozca los hábitos en Internet de los niños.
4. Establezca, junto con sus hijos, la hora y reglas del uso de Internet y procure que naveguen bajo su supervisión.
5. Enseñe a los menores a no proporcionar información personal o comunicarse con extraños en línea.
6. Promueva la importancia de mantener su privacidad y la de la familia.
7. Solicite a los menores que avisen cuando reciban mensajes que los hagan sentirse incómodos o con miedo.

Si usan una computadora que presta el servicio de internet lo que deben hacer es:

1. Tratar de conocer qué programas de seguridad son ofrecidos por el proveedor.
2. Es recomendable acompañar al menor cuando necesite buscar información.
3. Entérese más visitando los sitios que le informan, para prevenir que sean víctimas de la delincuencia informática.

Por ello es necesario presentar recomendaciones para los usuarios de visitas contantes a estas grandes redes de comunicaciones, con un solo fin de que reconozcan y tengan la precaución necesaria.

Nos damos cuenta que, un alto porcentaje de los internautas se conectan a Internet desde su casa, lo que nos hace suponer que cualquier miembro del hogar es una víctima en potencia, teniendo una mayor posibilidad de ser presa de algún tipo de delito cibernético, si no toma las precauciones debidas.

La mejor recomendación que se les puede brindar a los usuarios es que tengan bloqueado a las personas que les presentan algún problema y el cambio constante de contraseña, para evitar ser víctima de un acosador en las redes sociales.

Tomar en cuenta que ya es necesario aplicar un bloqueo de las cuentas que se tiene por uso, lo cual se puede hacer fácilmente en las páginas de Facebook y Twitter, así como restringir sus direcciones de correo electrónico y nombres de usuario de cualquier servicio de mensajería instantánea que no se reconozca.

Algo muy importante que los usuarios deben de saber en caso de que las personas cuenten con un blog, se recomendó modificar la configuración de éste, para evitar los comentarios anónimos, los acosadores crean nuevos nombres de usuario para eludir tu bloqueo en los servicios de mensajería, en lo cual es donde se tiene que estar atentos a las anomalías de estos autores del delito.

De cierto modo los que se encuentran más vulnerables a este tipo de acoso son los jóvenes que se pasan horas en las maquinas de la tecnología y que presentan gran parte de su infamación personal y que desconocen que pueden ser víctimas de algún delito cibernético.

#### Recomendaciones para los jóvenes:

- Reconocer que no todo lo que se ve por Internet o la Web, no es real. De hecho hay servicios y propuestas falsas y peligrosas. El estar conectados a la red por largas horas todos los días podría generarnos comportamientos antisociales y de aislamiento.
- Recordar que una vez que se coloque información en línea no la puedes retirar tan fácilmente.
- Antes de asociarte a un sitio de redes sociales, analiza detenidamente las diferentes opciones que te ofrecen.
- Coquetear o seducir en línea con extraños puede tener graves consecuencias.
- Piensa bien antes de colocar tu foto en el sitio Web ya que podría ser alterada y difundida, y ello te podría causar más de un dolor de cabeza.

- Hay que ser muy cautos y prudentes si un nuevo amigo que has conocido por la red desea conocerte personalmente, si lo haces anda acompañado de un adulto, que la reunión sea de DÍA y en un lugar público, aunque esto no es nada recomendable.
- Están los "Ciberbullying", que es la “Cyber-intimidación” realizada por compañeros del entorno escolar o social que intimidan o amenazan por mail anónimos.
- Cuando veas o recibas algo en Internet que te haga sentir incómodo/a o amenazado/a, debes hablar inmediatamente con tus padres.
- Por ningún motivo respondas a mensajes o avisos de boletines electrónicos que sean desconocidos, sugestivos, obscenos, agresivos o amenazantes o que te hagan sentir incómodo, o mensajes atractivos que indiquen que eres ganador de un sorteo para evitar fraudes y proteger tu intimidad e integridad.
- Si recibes mensajes en los cuales buscan seducirte, te ilusionan, te amenazan, te chantajean o te intimidan, pláticalo con un adulto de tu confianza.
- Si recibes un mensaje en tu celular que donde te digan que eres ganador de un vehículo, premios en efectivo y más, comunícaselo a tus padres, anota el número de teléfono y repórtalo al 089, no respondas a las llamadas que te hagan de ese número ni respondas los mensajes con mensaje ni llamadas porque se trata de una extorsión comprobada.
- Nunca debes publicar información personal como número telefónico familiar o celular, dirección o nombre de tu escuela.
- Comparte tus contraseñas solo con una persona de tu confianza.
- Observa siempre un buen comportamiento en línea y no hagas nada que pueda molestar o enojar a otras personas o que sea ilegal.
- Nunca hagas nada en Internet que cueste dinero sin que lo sepan tus padres.
- Deja que tus padres sepan tu nombre de inicio de sesión en Internet y las direcciones de los chats que visitas.

Sugerimos cuidarte ante todo de páginas donde:

- Te pidan que envíes fotografías o que te despojes de tu ropa ante una Web Cam
- Te pidan datos personales como tu domicilio, edad, teléfono, nombre, etc.

- Traten de solicitarte información sobre tu condición económica.
- No utilices tu nombre ni tu fecha de correo electrónico para nombrar tu dirección de correo electrónico.
- Existen números telefónico de emergencia que se pueden consultar, para que este tipo de problema sea tomado en cuenta y que de algún modo se pueda actuar como corresponde.

#### Recomendaciones para una contraseña segura:

- La selección de una contraseña difícil de adivinar es el primer paso a la hora de mantener las contraseñas a salvo y lejos de las manos equivocadas.
- Las contraseñas fuertes están formadas por ocho caracteres como mínimo y utilizan una combinación de letras, números y símbolos (p. ej. 7#0%&/). No utilice ninguna de las siguientes opciones para su contraseña: su nombre de inicio de sesión, cualquier término relacionado con sus datos personales, como su apellido, o palabras que puedan encontrarse en el diccionario. Intente seleccionar contraseñas muy sólidas y exclusivas para proteger actividades como las operaciones bancarias en Internet.
- Guarde sus contraseñas en un lugar seguro e intente no utilizar la misma contraseña para todos los servicios de los que disponga en la red.
- Cambie las contraseñas con regularidad, al menos cada tres meses a fin de tener un control de mi información. De este modo, es posible limitar el daño causado por alguien que ya haya accedido a su cuenta. Si observa algo sospechoso con alguna de sus cuentas en línea, lo primero que debe hacer es cambiar su contraseña.

### **5.3 Implementación de programas de auto cuidado.**

Implementación de programas que se ha propuesto mediante los cambios que se han presentado a causa de los grandes avances de la red; es decir que cada día aparecen nuevas expresiones de la criminalidad y actualmente muchas de ellas están vinculadas al uso de las

nuevas tecnologías, por lo que las autoridades de Seguridad Pública se actualizan con el objetivo de informar e instrumentar acciones preventivas que contribuyan con la seguridad de las familias, padres, alumnos, instituciones educativas, empresas y sociedad en general que utilizan los instrumentos fabricados para el uso y aprovechamiento de las herramientas relacionadas con la comunicación y la informática.

Esta propuesta viene con el solo objetivo de hacer notar que contar con un cuerpo policiaco como lo es la policía cibernética es de primera necesidad para los estados vulnerable en caso de los delitos cibernéticos, de esta forma la misión de este cuerpo de prevención es de: la identificación, localización y desarticulación de organizaciones y personas quienes utilizan la Internet como un instrumento para cometer fraudes, intrusiones, actividades delictivas dedicadas al robo, al fraude electrónico, al robo de tarjetas e información personal, al lenocinio, al tráfico y corrupción de menores, a la prostitución infantil, al narcotráfico, a la elaboración, distribución y promoción de pornografía infantil, al Cyber terrorismo, a la extorsión e infinidad de delitos que tienen su origen en cualquier instrumento de comunicaciones y actividades informáticas.

El fin de esta propuesta es implementar un programa de prevención del delito que se da por el internet, a fin de que los usuarios tengan un breve conocimiento a lo que se encuentran expuestos cuando se encuentran utilizando una página con acceso a internet.

La Policía Cibernética se ocupara, de la prevención de los delitos cometidos por la nueva tecnología, mediante la red de comunicación haciendo continuamente una revisión de las herramientas que utiliza un usuario, de este modo se implementaran estudios por cada movimiento que se frecuente extraño, por lo que este cuerpo de prevención tendrá acceso abierto a todas las paginas a fin de estar a la orden del día tomando las medidas preventivas para no ser víctima de delitos a través de internet y generando algunos de los tips o recomendaciones importantes que se deben tomar los ciudadanos.

Propuesta:

Esta implementación de un programa de prevención de delitos cibernéticos; teniendo como campo a trabajar centros educativos y sociedad para los usuarios que tienen acceso a las páginas sociales con un solo objetivo de disminuir el índice de violencia y delito cibernético, al igual impartir información en los centros recreativos como parques, museos o áreas públicas, con el fin de lograr que la sociedad en general tenga conocimientos de la información necesaria a la que se encuentra al tener un aparato móvil con internet.

- Como objetivo general: Que los cibernautas conozca, comprenda y replique las acciones que le permitan detectar e identificar el delito cibernético, así como transmitir a los usuarios tales como son (niñas, niños y jóvenes) recursos de protección para navegar en Internet de forma segura.
- Objetivos específicos: Conocer las particularidades del delito cibernético sus antecedentes, modalidades y otras conductas antisociales o ilícitas con las que se vincula; Identificar los factores de riesgo que existen al navegar en Internet.

Como primer término, se implementara visitas de programación en los centros educativo de tal manera que se lleve un control de las fechas especificas de las visitas en escuelas, de esta manera impartir la información de necesaria a los jóvenes que se encuentran vulnerables a estos tipos de delitos.

La implementación de las técnicas que se abordaran serian:

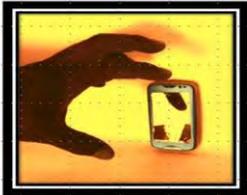
- ⌚ Que es el internet.
- ⌚ Como utilizar el internet.
- ⌚ Concepto de delitos.
- ⌚ Tipos de delitos cibernéticos.
- ⌚ Conductas de riesgo.
- ⌚ Conductas antisociales.
- ⌚ Actividades preventivas.

- ⌚ Talleres.
- ⌚ Denuncias.

Las placitas que se implementaran en escuelas con el nombre de “prevención de delito cibernético” tendrán un valor de poder disminuir los índices altos de ser víctimas de los acosadores cibernéticos de tal manera que al detectar un problema, la policía cibernética se dedique a seguir todo lo que corresponde con ello.

De esta manera la policía cibernética se presentara como una manera de que la sociedad, se sienta un poco más segura, al poder contar con un cuerpo policiaco que en se puede confiar y que se enfoque a los problemas de la red, de tal manera que la población enfrente sus opiniones y puede ser asesorada para reconocer en qué momento se encuentra en riesgo y actuar de manera precisa ante lo que ocurre.

Los programas de prevención que se implementaran en la sociedad también serán de gran ayuda para la atención de toda la sociedad en general, abarcando de esta manera todo el usuario de internet. El resultado de todo el trabajo que se quiere realizar será a fin de que se tenga un control de todas las actividades a realizar, y seguir constantemente valorando los resultados de las inquietudes de la población. Por lo cual se brindara información de los siguientes temas importantes.

<p><b>TALLER DE PREVENCIÓN CONTRA EL DELITO CIBERNÉTICO</b></p> 	<p><b>OBJETIVO</b></p> <p>Fomentar una cultura de prevención en la población infantil, juvenil y adulta al navegar en Internet.</p> 
---	--



## Conclusión

El Internet ha tenido y continuará teniendo un gran impacto mundial, abarcando muchos niveles, tanto social, económico y político: que gracias a sus avances de tecnología, han hecho del mundo un elemento muy importante para el desarrollo de un país.

Partiendo del estudio de las medidas que se han adoptado a nivel internacional para atender esta problemática y de la operación internacional en la esfera del delito cibernético y las medidas que se han tomado para poder combatirla han hecho del mundo una esfera vulnerable del acoso del delito.

La falta de conocimiento parte primordialmente de quienes hacen cumplir la ley, ya que han provocando una dificultad de carácter confuso ante la sociedad, haciéndoles falta armonización para investigaciones y castigos de los delitos informáticos.

La cultura de reconocer que existen delitos graves a los que se puede estar expuestos al manejar las páginas de redes de internet es lo que hace que nuestro país sea uno de los principales lugares que no se tomen en cuenta para poner en forma la seguridad.

Un usuario que se pasa más de un tiempo considerable en las páginas de internet, se presenta como una persona que no reconoce en realidad a que es lo que se encuentra expuesto, y mucho menos a lo que se puede llegar enfrentar.

Los delitos cibernéticos son el tema principal de este trabajo de investigación; como propuesta dar a conocer la importancia de un cuerpo capacitado para combatir los delitos a los que se encuentran expuestos todos los usuarios que se encuentran inscritos en páginas de redes sociales a fin de no tener un uso adecuado de la misma.

### Anexos

El Consejo de Europa ha llamado a una implementación en todo el mundo de su Convención sobre el delito cibernético para combatir el creciente problema del crimen económico en la web.

Durante la quinta conferencia anual del Consejo de Europa sobre delito cibernético en Estrasburgo realizada en el mes de junio de 2013, los participantes se pronunciaron a favor de una mayor cooperación internacional en el intercambio de herramientas, instrumentos y mejores prácticas e iniciativas.

Durante la conferencia también se pidió una mayor cooperación entre la policía y las industrias nacionales e internacionales.

Los delegados también respaldaron las peticiones de la ICANN (La **Corporación de Internet para la Asignación de Nombres y Números**), para reforzar los procesos de registro de nombres de dominio para hacer la vida más difícil a los spammers y otros riff-raff. Se sugirió que la policía debería poder utilizar la base de datos para combatir el crimen

cibernético, al mismo tiempo que se protegiera la privacidad de los solicitantes individuales sin duda un objetivo de la competencia.

Tanto Rusia como China recientemente reforzaron su proceso de registro de dominio, ya que ahora requieren identificación con foto antes de que las autoridades asignen nuevos dominios, por ejemplo. Las medidas han sido bien aceptadas por los observadores de la seguridad, a pesar de los rumores sobre los servicios de obtención de ID diseñados para eludir los nuevos controles que han surgido.

La Conferencia también consideró la seguridad y las implicaciones de privacidad de un mayor uso de tecnología basado en nube, haciendo una serie de recomendaciones.

Para hacer frente a la aplicación de la ley y los retos relacionados con la privacidad informática, instrumentos de computación basados en nube existentes en materia de cooperación internacional - como el Convenio de Protección de Datos (CETS 108) y el Convenio de Budapest se necesitan aplicar más ampliamente y de manera eficiente.

Otras normas internacionales sobre la aplicación de la ley de acceso a los datos almacenados en las "nubes" deben considerarse.

Estándares y políticas de privacidad global y protección de datos, encargados de poner en marcha esas cuestiones en el Consejo de Europa, fueron encomendados de seguir abordando estas cuestiones en sus actividades normativas, así como por el Proyecto Global sobre crimen cibernético.

Eurócratas piden una próxima convención de la ONU sobre los delitos informáticos en Salvador, para que Brasil adopte el enfoque de Europa como un plan de acción aplicado a nivel mundial para la lucha contra los delitos informáticos, el espionaje electrónico y las amenazas relacionadas.

El Secretario General Adjunto del Consejo de Europa, Maud de Boer-Buquicchio, dijo a los delegados: "El Congreso de las Naciones Unidas sobre el crimen en abril de 2010 será una oportunidad para reforzar nuestra respuesta mundial a la amenaza mundial de la delincuencia y el terrorismo cibernético.

"Creo que tendremos más oportunidad de éxito si nos unimos alrededor de un instrumento internacional que ya existe a saber, la Convención del Consejo de Europa sobre la delincuencia informática".

Un total de 29 países, principalmente europeos, pero también incluyendo los Estados Unidos, han ratificado la Convención de Budapest desde su adopción en 2001. Portugal y Montenegro, anunciaron la ratificación de la Convención, mientras que Argentina hizo una petición para adoptar el tratado.

Diecinueve países han firmado pero no han ratificado el Tratado, incluyendo el Reino Unido y España. El convenio establece una guía para cualquier país en desarrollo de una legislación nacional integral contra el delito cibernético, así como marco para la cooperación internacional.

Alrededor de 300 expertos en delincuencia informática de unos 60 países participaron en la conferencia de la delincuencia cibernética del Consejo de Europa. Temas en la agenda incluyeron el mapeo de las redes y la lucha contra la pornografía infantil en línea, así como de formación para jueces y fiscales. Los derechos humanos y la privacidad ya han sido dibujadas en la agenda de la conferencia del año próximo.

Es importante recalcar que tener una policía especializada en estos trabajos de informática brindan a un país la seguridad de estar protegido, transitar de una manera mas segura y lograr tener la confianza de la población con un solo fin lograr no temer a lo sucede en el mundo.

Es importante recordar que los delitos cibernéticos se cometen a través de Internet y son la causa de afectación a bienes jurídicos de diversa naturaleza, dependiendo de la gravedad del delito se clasifican de la siguiente manera:

#### **A. Delitos patrimoniales**

De acuerdo con la información que proporciona, el fraude electrónico es una las causas de afectación a los usuarios que tienen cuenta con la banca, los ataques informáticos se generan en contra de los clientes y no en contra de la institución crediticia, lo que obedece a

los sistemas de protección que gozan las instituciones bancarias, el solo propósito de esos programas es hacerse de los recursos del usuario de la banca, aprovechándose de los dos factores básicos que toman en consideración los defraudadores, los cuales son el nivel cultural del usuario y la natural curiosidad del ser humano, tales ataques se llevan a cabo a través de dos programas que se denominan: Phising y Pharming,

## **B. Delitos de pornografía**

De acuerdo al Código Penal Federal visto en el artículo 201 Bis establece que el tipo descriptivo en que al que procure o facilite por cualquier medio, el que uno o más menores de dieciocho años, con o sin su consentimiento de ello, lo o los obligue o induzca a realizar actos impropios de exhibicionismo corporal, lascivos o sexuales, a fin de video-grabarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro se clasificara como un acción de pornografía.

(Alfaro, 2002) nos menciona que el fenómeno de la pornografía en Internet, se engloba dentro de los denominados delitos computacionales, al suponer una nueva manifestación del delito ofensas al pudor, cuya comisión afecta el bien jurídico de la libertad sexual de una persona.

## **C. Delincuencia organizada**

La terminación delincuencia es aquella cualidad de una persona que comete delitos que por lo tanto, viola la ley, término utilizado para nombrar al conjunto de los sujetos que delinquen y mantienen conductas anti sociales contrarias al derecho.

La delincuencia organizada trata de un grupo social con una cierta estructura de miembros que se organizan para cometer acciones delictivas, esta a diferencia del delincuente que actúa en solitario, los individuos que forman parte de una banda de delincuencia organizada deben responder a la estructura y cumplir con una determinada función.

La delincuencia organizada suele dedicarse a tareas más complejas que robos comunes o hurtos. Estos grupos del crimen organizado se involucran en actividades como el tráfico de drogas o armas, la trata de blancas, el contrabando o la falsificación.

Estas organizaciones delictivas estén regidas por un orden jerárquico. Los miembros de las capas más bajas deben hacer méritos para ascender y mostrar su lealtad a los jefes, decir que si alguno de los integrantes de estos grupos llega a fallar o dar un paso en falso, puede llegar a convertirse en una víctima más del crimen organizado.

## Glosario

- ⌚ ARPANET: Red de computadoras Advanced Research Projects Agency Network (ARPANET) fue creada por encargo del Departamento de Defensa de los Estados Unidos, fue el medio de comunicación para los diferentes organismos del país.
- ⌚ TCP: Protocolo que inicio el nodo de transferencia de información que se creó en 1983.
- ⌚ CIBERESPACIO: También conocido ciberinfinito, realidad simulada que se encuentra implementada dentro de los ordenadores y de las redes digitales de todo el mundo.
- ⌚ PROYECTO DE XANADU: Primer proyecto de Hipertexto, que usa hipervínculos, fundado en 1960.
- ⌚ NAVEGADOR: También conocido como navegador web, aplicación que opera a través de Internet, interpretando la información de archivos y sitios web para que éstos puedan ser leídos.
- ⌚ MOSAIC: Fue el primer navegador gráfico disponible para visualizar páginas web y el primer navegador gráfico para Microsoft Windows.
- ⌚ PROTOCOLO: Conjunto de reglas que se siguen en un proyecto de determinados actos oficiales o formales, y que han sido establecidas por decreto o por costumbre.
- ⌚ SPAMMING: Se le determina con varios términos como Spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido, correo anónimo, habitualmente de tipo publicitario.
- ⌚ TCP/IP: Lenguaje que utilizan las computadoras al compartir recursos.

- ⌚ PREPUBESCENTE: Es cuando a los jóvenes prepubescente son vistos como objetos que sustituyen a un objeto adulto que es el preferido pero que no está disponible.

## **Bibliografías**

1. ALIAGA, Andrea. (2010). Delitos informaticos.
2. ARREGUIN, Amelia. (2010). Pornografía, internet, medios y política. Hudson: Routledge.
3. AYALA, Cristian. (2007). Relación entre el Uso de Internet y el Logro Académico. México.
4. AZAOLA, Elena (2000). La trata de personas en México. México.
5. CARRASCO, R; NAVAS, O. (2013). El acoso escolar a través de las nuevas tecnologías, el Cyberbullying. México.
6. CASSOU, Jorge (2013). Delitos informáticos en México. México.
7. DELGADO, Víctor (2012). Policía, derechos humanos y libertades individuales. México.
8. DE LOS CABALLEROS, Santiago (2010). Impacto de la promoción realizada por las empresas dominicanas a través de las redes sociales facebook y twitter, desde la perspectiva de los usuarios. Republica dominicana.
9. FIGUEROA, Carlos; SÁNCHEZ, Oliver. (2010). La policía cibernética en México y el combate a delitos informáticos. Universidad Loyola del Pacifico.
10. GONZALES, Christian (2008). Cyber policía.
11. GUTIÉRREZ, Miriam. (2010). Los Delitos sexuales contra los menores de edad. México.
12. IÑIGO, Alejandra (2000). Bitácora de un policía. México. México.
13. LÓPEZ, Portillo (2003). Educación y entretenimiento policial para la democracia. México.
14. MARTÍNEZ, Beatriz. (2007). La policía en México. Reforma policial.
15. MASANA, Sebastián (2010) El ciberterrorismo: una amenaza real para la paz mundial. Argentina.
16. MEJÍA, Cristian (2010). Análisis de Redes Sociales a Gran Escala. México.
17. MÉNDEZ, Ana. (2013) Policía cibernética. Interesante, Notimex. México.
18. MIRANDA, Carla (2009). Los retos de la reforma policial y la capacitación en el marco del estado de derecho y democracia. México: Flasco.
19. MONTIEL, Oscar (2009). Trata de personas. México, D.F.

20. MUÑOS, Porras (1928). La policía en la historia de la ciudad de México. México.
21. NORBERT, Wiener. (1942). El origen de la cibernética. México.
22. PINED, María (2009). Ciberbullying la nueva manera de acoso escolar. México.
23. SANTONI, Pedro (1983). La policía de la ciudad de México en el porfiriato. 2 Edición. México
24. TORRES, Pedro. (2012). Aspectos generales de los delitos informáticos y el combate a los mismos. México.
25. URETA, Laura (2009) Retos a superar en la administración de justicia ante los delitos informáticos en el ecuador. Ecuador
26. VARENIK, Robert. (2005). Pólíce Reform in México. México.
27. WILLIAMS, Phil. (2012). El crimen organizado y la violencia en México: una perspectiva comparativa. México.
28. Arroyo, M., (2010). Historia de la cibernética. Recuperado el 17 de junio de 2012. <http://www.monografias.com/trabajos4/cibernetica/cibernetica.shtml#ixzz2JzdblWu>  
1. Consulta realizada el 20 de abril de 2013.
29. Gonzales, Javier G. (2013). Trafico de drogas online. Recuperado el 19 de marzo de 2013.
30. Hernández, C. (1999). Los piratas del chip y de internet. Recuperado el 23 de Junio de 2001. <http://perso.wanadoo.es/snickers>. Consulta realizada el 14 de abril 2013.
31. Hernández, Erick. (2013). México ocupa el numero 12 a nivel mundial en penetración de internet. Muy interesante, fayerwayer.  
<http://www.delitosinformaticos.com/03/2013/delitos/la-venta-de-drogas-online#.UYXiY0aI7IU>.