UNIVERSIDAD DE QUINTANA ROO

División de Ciencias Sociales y Económico Administrativas

El uso de las Tecnologías de Información y Comunicación en la producción de conductas delictivas.

TRABAJO MONOGRÁFICO
Investigacion documental

Para obtener el grado de
LICENCIADO EN SEGURIDAD PUBLICA

PRESENTA

C. Oscar Abraham Montesinos Jimenez

ASESORA:

Dra. Luz Margarita Gonzalez Lopez

Chetumal, Quintana Roo, México, Julio del 2017.

UNIVERSIDAD DE QUINTANA ROO

División de Ciencias Sociales y Económico Administrativas

Trabajo Monográfico elaborado bajo la supervisión del comité
y aprobada como requisito para obtener el grado de:

LICENCIADO EN SEGURIDAD PUBLICA

COMITÉ DE TRABAJO MONOGRÁFICO

Asesor: _____

Dra. LUZ MARGARITA GONZALEZ LOPEZ

Asesor: _____

MA. CARLOS ENRIQUE HERNANDEZ TAPIA

Asesor: _____

MD. CARLOS MOISES HERRERA MEJIA

Chetumal, Quintana Roo, México, Julio 2017.

Agradecimientos

Me gustaría que estas líneas sirvieran para expresar mis más profundos y sinceros agradecimientos a todas aquellas personas que con su ayuda y colaboración se realizó el presente trabajo, en especial a mi padre y a mi madre, sobre todo por la motivación y el apoyo recibido a lo largo de estos años, a mis hermanos por ser un claro ejemplo a seguir, a mi enamorada por su motivación y apoyo incondicional, a mis profesores les agradezco su digna labor por fomentar la educación inculcando valores y sembrando el conocimiento, en especial a la Doc. Luz Margarita González López por el gran papel que desempeño en esta hermosa etapa de mi vida, a mis amigos y conocidos universitarios por todos y cada uno de los momentos vividos a su lado. Y, por último, pero no menos importante a la Universidad de Quintana Roo por haberme dado la oportunidad de escalar un peldaño más en el campo del conocimiento, MUCHAS GRACIAS.

Índice

Introducción.

Vivimos en la era en la cual la tecnología ha logrado grandes avances, un claro ejemplo son los avances Tecnológicos de información y comunicación, las tecnologías modifican nuestra forma de vida cotidiana, un claro ejemplo es la forma de comunicación, que a lo largo de los años se ha ido modificando e innovando, desde el uso de cartas y telegramas, hasta en la actualidad con el uso de la mensajería instantánea.

Simbólicamente el Internet y las TIC fueron construidas como herramientas al servicio de la comunidad para facilitar y mejorar la calidad de vida de los seres humanos. Para otras personas de manera más concreta, representa la promesa del bienestar en distintos ámbitos del desarrollo, como la educación, la superación de la pobreza, el mejoramiento de la gestión pública a través del e-gobierno, la protección de los derechos humanos, el fortalecimiento de la democracia, entre muchas otras.

> *"Diferentes países de la región han procurado hacer realidad la promesa de desarrollo y bienestar asociada a la difusión de las nuevas TIC, mediante la implementación de iniciativas nacionales tendientes a lograr la universalización del acceso a la Internet"*. (Villatoro, 2005).

Crear y divulgar información sin tomar algunas medidas de seguridad no es muy conveniente, puesto que los flujos de información, las comunicaciones y los mecanismos de coordinación se están digitalizando en muchos sectores de la sociedad, proceso que se traduce en la aparición progresiva de nuevas formas de organización social.

Un claro ejemplo es la delincuencia cibernética que en los últimos años ha crecido rápidamente convirtiéndose en un amplio mercado, afectando de forma directa y volviéndonos vulnerables exponiendo la información que enviamos de un lugar a otro.

Cada día aparecen nuevas expresiones de la criminalidad y actualmente muchas de ellas están vinculadas al uso de las nuevas tecnologías, el flujo de información personal y confidencial que nosotros mismos proporcionamos circula todos los días por el ciber espacio, de tal manera la delincuencia organizada ha visto al ciber espacio como el lugar ideal para cometer delitos, ya que se puede permanecer en el anonimato y así conseguir acceso a todo tipo de información personal, que en la mayoría de los casos son para fines malintencionados, o en su defecto alcanzar algún lucro.

Organizaciones a nivel mundial se centran en la divulgación, expansión y globalización de las TIC, sin embargo, deberían concentrarse en la seguridad de la misma puesto que los países que tienen acceso a estos medios presentan altas incidencias en fraudes, extorciones o delitos cometidos a través de los diferentes medios tecnológicos de información.

En la Cumbre Mundial sobre la Sociedad de la Información en Ginebra los líderes mundiales declararon: "*Estamos plenamente comprometidos a convertir la brecha digital en una oportunidad digital para todos, especialmente aquellos que corren peligro de quedar rezagados y aún más marginados"* (CMSI, 2003).

Justificación.

En las últimas décadas el uso excesivo de las tecnologías de información y comunicación ha aumentado, en este caso específicamente las redes sociales se han globalizado utilizando al ciber espacio, por este medio se propaga todo tipo de información, propiciando así la producción de ciertas conductas delictivas, un claro ejemplo son los delitos que se llevan a cabo a través de redes sociales o páginas de internet como el robo de identidad o extorsión, y la mayoría se encuentran claramente tipificadas en los códigos penales federales de sus correspondientes países, incluso la Organización de las Naciones Unidas, reconoce a ciertos delitos como delitos informáticos.

De tal forma el Internet se ha vuelto una parte casi esencial en nuestra vida , donde cada individuo suministra información de todo tipo, que abarca desde su ubicación, cuentas de banco e incluso su información personal, información circula diariamente por los diferentes medios tecnológicos y de comunicación, lo que no tenemos en cuenta es que esta información en algunos casos se usa de forma mal intencionada, recolectan la información y con ella se realizan actividades ilícitas , la era moderna trae consigo este tipo de delitos que se vieron sujetos a la necesidad de adaptarse ante los nuevos entornos y sociedades, que de cierta manera les facilita cometer un acto o conducta delictiva desde la comodidad de su casa o algún lugar con acceso a internet.

> La influencia de la tecnología sobre la sociedad ha sido claramente explicitada por Kranzberg, en su ley sobre la relación entre tecnología y sociedad*: "La tecnología no es buena ni mala, ni tampoco neutral"* (1985: 50)

Importancia del tema.

Es importante conocer y aprender a proteger tu identidad e información personal, así como los datos que suministras todos los días en los diferentes medios tecnológicos.

El impacto social de los avances tecnológicos, de información y comunicación, son de suma importancia, la finalidad de prevenir a las actuales y futuras generaciones son primordiales, puesto que día con día se proporciona información privada y confidencial en todos los diferentes medios de comunicación, dejando así expuesta tu información, la de amigos y familiares con los que te relacionas en los diferentes medios a diario.

Contribución del tema.

Con la información recolectada en este trabajo se busca informar y prevenir a la sociedad ante el hecho de las conductas delictivas y delitos cibernéticos, de tal manera se expone esta problemática lo más digerible posible para que cualquier persona se vea beneficiada con esta información, sabemos que en la actualidad existen organizaciones encargadas de la seguridad informática, sin embargo, se tienen que hacer enormes ajustes a las estructuras y políticas de privacidad por todo el ciber espacio, dado que no son muy eficientes y la demanda de los usuarios por usar los diversos medios de comunicación son muy altos, tanto que sobre pasan las medidas de seguridad y administración de los medios de comunicación.

De tal forma este articulo busca colaborar con la sociedad, informando de las consecuencias de suministrar información personal en los diferentes medios tecnológicos y así reducir el índice de personas vulneradas ante este tipo de delitos

y conductas ilícitas, es importante mencionar que ya existen leyes en los diferentes países del mundo que buscan reducir el índice de personas vulneradas ante estos delitos, en el caso de México se pueden encontrar algunos de estos delitos ya tipificados en el Código Penal Federal.

Descripción sintética del contenido de los capítulos del trabajo.

En los siguientes capítulos se explica de manera comprensible que son las tecnologías de información y comunicación, cuáles son sus características, como estas fueron cambiando e innovándose a lo largo del tiempo, cuáles fueron sus antecedentes, las ventajas y desventajas que estas presentan, así como una explicación de las conductas delictivas y como estas se han ido incluyendo y adaptando a la actual sociedad, cuales son los factores que propician las conductas delictivas (factores endógenos y exógenos de las conductas delictivas), la globalización de los delitos cibernéticos, su penalización por parte de cada país, así como una lista de los delitos cibernéticos más comunes que se realizan por medio de las diversas tecnologías de comunicación y las medidas que se están tomando o deberían tomarse para la prevención de las mismas.

Capítulo I.

Tecnologías de información y comunicación.

1.1 Delitos Cibernéticos.

Los delitos cibernéticos implican el uso de equipos tecnológicos (celulares, computadoras de escritorio y portátiles o cualquier dispositivo que contenga el uso de la internet) como instrumento para llevar a cabo actos delictivos; el servicio de internet es una herramienta que las personas independientemente de la edad no saben cómo explotarla y aprovecharla al máximo y limitan su uso a actividades de esparcimiento y diversión.

Las principales actividades que los usuarios realizan comúnmente en Internet son: uso del servicio de correo electrónico, mensajes instantáneos, visitas a páginas web, envió de postales, escuchar música, descarga de música, juegos online, visitas a páginas de uso exclusivo para mayores de 18 años, investigación y por ultimo sitios de educación y aprendizaje.

Sin embargo, los delitos informáticos o también conocido como delitos cibernéticos implican actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurtos, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera.

Debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

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

La posibilidad de que un usuario sufra un daño o una pérdida en Internet se incrementa al reunir tres factores:

1.- Algo que tiene valor, es decir, la información de nuestra computadora, archivos, información personal, contraseñas, etcétera.

2.- Amenaza, como un evento generado por una persona maliciosa que puede causar un daño o robo.

3.- Vulnerabilidad, como la falla de un sistema o programa informático.

Según el rol de las Tecnologías de Información y Comunicación utilizadas para la comisión de un delito cibernético, la Unidad de Investigación Cibernética (UIC) los clasifica en dos grupos:

- **Cuando las TIC son un instrumento o medio comisivo.**
- **Cuando las TIC son el fin u objeto del delito.**

En esta categoría se contemplan las conductas probablemente delictivas que se valen de las computadoras como medio (utilizan métodos electrónicos para llegar a un resultado ilícito), en la comisión del delito, por ejemplo, las siguientes actividades:

Tabla 1.- **Delitos cibernéticos y conductas delictivas, como un instrumento o medio.**

Delitos cibernéticos y conductas delictivas, como un instrumento o medio	Extorsiones, fraudes electrónicos y amenazas.
	Exhibición, publicación, difusión, intercambio y comercialización de pornografía infantil.
	Falsificación de documentos vía computarizada, Negociaciones de secuestros
	Robo, sustracción o copiado de información confidencial.
	Aprovechamiento indebido o violación de seguridad para ingresar a sistemas.
	Variación del destino de sumas de dinero a otras cuentas (transferencias electrónicas).

Fuente: Elaboración propia con información del Manual de Prevención del Delito, SSP del estado de Veracruz, 2006.

En la mayoría de los casos, los delitos cibernéticos se adecuan a tipos penales vigentes. Por ejemplo, en el caso de un fraude bancario cometido por Internet, se perseguirá con apego al tipo penal para el “fraude”, en donde Internet fue sólo el medio por el cual se llevó a cabo el hecho ilícito.

Tabla 2.- Delitos cibernéticos y conductas delictivas, como fin u objeto.

Delitos cibernéticos y conductas delictivas, como fin u objeto	Manipulación de datos e información privada contenida en archivos o soportes físicos informáticos ajenos.
	Accesos forzados sin autorización alguna, y obtención de información confidencial
	Utilización de programas y equipos de otras personas, sin autorización, con el fin de obtener algún lucro o para algún fin malintencionado
	Introducción de virus o programas ajenos, para la destrucción de información o datos privados, con fines mal intencionados.
	Utilización de las tecnologías de información y comunicación con fines fraudulentos.

Fuente: Elaboración propia con información del Manual de Prevención del Delito, SSP del estado de Veracruz, 2006.

Por otro lado, Internet es una fantástica tecnología de información y comunicación cuyo potencial no se limita a servir únicamente a usuarios bien intencionados.

Es necesario reconocer que algunos usuarios también aprovechan este gran poder para cometer actividades ilícitas, como la trata de menores, el lenocinio de menores, el turismo sexual y la pedofilia, el abuso informático incluye una diversidad de ofensas, tanto penales como administrativas; algunas de éstas constituyen delitos que ya se castigan en diversas legislaciones; sin embargo, quedan conductas que aún no encuentran tipificadas en legislaciones penales.

1.2 Introducción a las tecnologías de información y comunicación.

El autor Cabero hace referencia a las TIC de la siguiente manera: "*En líneas generales podríamos decir que las nuevas tecnologías de la información y comunicación son las que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo de manera interactiva e interconexionada, lo que permite conseguir nuevas realidades comunicativas*" (Cabero, 1998).

Las Tecnologías de Información y Comunicación, son todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos, tales como:

1. Computadoras.
2. Teléfonos móviles.
3. Televisores.
4. Reproductores portátiles de audio y video.
5. Consolas de juego.
6. Tabletas
7. Entre otros.

Los cuales ofrecen muchos servicios como lo son las siguientes: Mensajería instantánea, correo electrónico, búsqueda de información, banca online, descarga de música y cine comercio electrónico, video conferencias, etc.

Las TIC nos presentan muchas oportunidades para los países en desarrollo, ya que el hecho de que las TIC y las prácticas digitales tengan beneficios que van más allá de la esfera económica y sean aplicables en el ámbito de la salud, la política, la administración pública, la educación e investigación, así como en actividades

culturales, sociales e incluso religiosas, demuestra el potencial el desarrollo tecnológico a nivel mundial.

El término brecha digital se puede resumir en lo que la CEPAL afirma: "*la brecha digital es la línea divisoria entre el grupo de población que ya tiene la posibilidad de beneficiarse de las TIC y el grupo que aún es incapaz de hacerlo"*. En otras palabras, es una línea que separa a las personas que ya se comunican y coordinan actividades mediante redes digitales de quienes aún no han alcanzado este estado avanzado de desarrollo. También se describe como *"la línea divisoria entre la población de clase alta y clase baja en información, donde la clase alta es capaz de cosechar beneficios sociales y económicos del acceso a la infraestructura mundial de la información y las comunicaciones".* Esta forma de exclusión se identifica también como brecha digital internacional (abismo que separa a las regiones y a los países) y brecha digital doméstica (divide a los grupos de ciudadanos de una sociedad). (CEPAL, 2003)

En la Cumbre Mundial sobre la Sociedad de la Información en Ginebra, organizada por la Organización de Naciones Unidas (ONU) y la Unión Internacional de Telecomunicaciones (ITU), los líderes mundiales declararon:

> *Nuestro deseo y compromiso comunes de construir una sociedad de la información centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos.* (CMSI, 2003)

Vulgarmente suele escucharse que en el presente año se está viviendo la revolución de información y comunicación, y ha sido propiciada por la aparición de la tecnología digital.

La tecnología digital, unida a la aparición de ordenadores cada vez más potentes, ha permitido a la humanidad progresar muy rápidamente en la ciencia y la técnica desplegando nuestra arma más poderosa: la información y el conocimiento.

En un mundo cada vez más tecnológico, las TIC están en constante evolución y adaptación al cambio de sociedades, mantenerse informado es clave para conocer y aprovechar los nuevos servicios, y ser competitivos.

Las características que presentan las tecnologías de información y comunicación que diferentes autores especifican como representativas de las TIC, a continuación, son recopiladas por Cabero (1998), son:

Inmaterialidad: En líneas generales podemos decir que las TIC realizan la creación (aunque en algunos casos sin referentes reales, como pueden ser las simulaciones), el proceso y la comunicación de la información. Esta información es básicamente inmaterial y puede ser llevada de forma transparente e instantánea a lugares lejanos.

Interactividad: La interactividad es posiblemente la característica más importante de las TIC para su aplicación en el campo educativo. Mediante las TIC se consigue un intercambio de información entre el usuario y el ordenador. Esta característica

permite adaptar los recursos utilizados a las necesidades y características de los sujetos, en función de la interacción concreta del sujeto con el ordenador.

Interconexión: La interconexión hace referencia a la creación de nuevas posibilidades tecnológicas a partir de la conexión entre dos tecnologías o más. Por ejemplo, la telemática es la interconexión entre la informática y las tecnologías de comunicación, propiciando con ello, nuevos recursos como el correo electrónico y los mensajes instantáneos, etc.

Instantaneidad: Las redes de comunicación y su integración con la informática, han posibilitado el uso de servicios que permiten la comunicación y transmisión de la información, entre lugares alejados físicamente, de una forma rápida, llegando hasta los lugares más remotos del mundo.

Elevados parámetros de calidad de imagen y sonido: El proceso y transmisión de la información abarca todo tipo de información: textual, imagen y sonido, por lo que los avances han ido encaminados a conseguir transmisiones multimedia de gran calidad, lo cual ha sido facilitado por el proceso de digitalización.

Digitalización: Su objetivo es que la información de distinto tipo (sonidos, texto, imágenes, animaciones, etc.) pueda ser transmitida por los mismos medios al estar representada en un formato único universal.

Por otro lado, un sujeto no sólo dispone, a partir de las TIC, de un conjunto de información para construir su conocimiento, sino que, además, puede construirlo en forma colectiva, asociándose a otros sujetos o grupos.

Estas dos dimensiones básicas (mayor grado de protagonismo por parte de cada individuo y facilidades para la actuación colectiva) son las que suponen una modificación cuantitativa y cualitativa de los procesos personales y educativos en la utilización de las TIC.

Penetración en todos los sectores: (culturales, económicos, educativos, industriales, etc). El impacto de las TIC no se refleja únicamente en un individuo, grupo, sector o país, sino que, se extiende al conjunto de las sociedades del planeta. *"Los propios conceptos de "la sociedad de la información" y "la globalización", tratan de referirse a este proceso. Así, los efectos se extenderán a todos los habitantes, grupos e instituciones conllevando importantes cambios, cuya complejidad está en el debate social hoy en día" (Beck, U. 1998).*

Innovación: Las TIC están produciendo una innovación y cambio constante en todos los ámbitos sociales. Sin embargo, es de reseñar que estos cambios no siempre indican un rechazo a las tecnologías o medios anteriores, sino que en algunos casos se produce una especie de simbiosis con otros medios. Por ejemplo, el uso de la correspondencia personal se había reducido ampliamente con la aparición del teléfono, pero el uso y potencialidades del correo electrónico ha llevado a un resurgimiento de la correspondencia personal.

Tendencia hacia automatización*:* La propia complejidad empuja a la aparición de diferentes posibilidades y herramientas que permiten un manejo automático de la información en diversas actividades personales, profesionales y sociales. La necesidad de disponer de información estructurada hace que se desarrollen gestores personales o corporativos con distintos fines y de acuerdo con unos determinados principios.

Diversidad: La utilidad de las tecnologías puede ser muy diversa, desde la mera comunicación entre personas, hasta el proceso de la información para crear informaciones nuevas, se tiene al alcance de toda la sociedad en general haciendo de esta muy accesible a todo tipo de información que se requiere en la vida cotidiana.

"Los ordenadores sirven como herramienta para acceder a información, a recursos y servicios prestados por ordenadores remotos, como sistema de publicación y difusión de la información y como medio de comunicación entre seres humanos". (Castells ,1997)

Para una mayor comprensión de las tecnológicas de información y comunicación tenemos que hablar sobre el internet, al cual me refiero como el medio por el cual se suministra y fluye toda la información haciendo posible la transferencia de datos con todo tipo de información.

El Internet es más que una plataforma tecnológica para el intercambio de información. *"Más específicamente, consiste en una tecno-estructura cultural comunicativa, que permite la "resignificación" de las experiencias, del conocimiento y de las prácticas de interacción humana". (*Cabrera, 2004)

A continuación, se presentan algunas de las características los cuales definen al Internet:

Extensa: En su mayoría destacan los usuarios de computadoras, sin embargo, los teléfonos móviles o inteligentes no se quedan atrás.

Cambiante: se adapta continuamente a las nuevas necesidades y circunstancias que la sociedad presenta.

Diversa: Con todo tipo de equipos y usuarios, fabricantes, redes, tecnologías, medios físicos de transmisión, etc.

Descentralizada: no existe un controlador oficial sino más bien está regulada por los miles de administradores de pequeñas redes que hay en todo el mundo, sus políticas de seguridad y privacidad. Por lo tanto, es casi garantizado que es un medio democrático e independiente de grupos de presión (políticos, económicos o religiosos). Sin embargo, carece de comportamientos éticos: En su mayoría no se respeta la intimidad de los diversos usuarios.

1.3 Evolución histórica de las Tecnologías de Información y Comunicación.

Las tecnologías de información y comunicación se desarrollan a partir de los avances científicos producidos en los ámbitos de la informática y las telecomunicaciones, por tal motivo son el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido,). El elemento más representativo de las nuevas tecnologías es el Internet supone un salto cualitativo de gran magnitud, cambiando y redefiniendo los modos de conocer y relacionarse del hombre.

Abarcan un abanico de soluciones muy amplio, Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes.

En un mundo cada vez más avanzado y tecnológico, las TIC están en constante evolución y adaptación al cambio de sociedades, mantenerse informado es clave para conocer y aprovechar los nuevos servicios, y ser competitivos.

Como han llamado recientemente la atención Tiffin y Rajasingham (1997, 119): *Se han realizado muchos intentos por solucionar los problemas de la educación con las tecnologías de la comunicación. Durante los años cuarenta y cincuenta se produjeron la introducción del cine y la radio, y en los sesenta y setenta, el auge, decadencia y el nuevo auge de la televisión educativa. Los ochenta constituyeron la década de los ordenadores personales en las escuelas.*

La siguiente información fue recopilada del autor: Angel L. Rubio Moraga en su Investigación con el Dpto. de Historia de la Comunicación, Fac. de Ciencias de la Información, Universidad Complutense de Madrid:

El internet surge con base a un proyecto americano denominado ARPANET (con sus siglas en inglés Advanced Research Project Agency Net). cuyo objetivo era la construcción de un sistema de comunicación entre computadoras altamente flexible y dinámico, que permitiera utilizar cualquier tipo de medio y tecnología de transmisión y que siguiera funcionando incluso ante la eventualidad de la destrucción de algunas de sus partes de la red.

Los ordenadores conectados a ella disponían de diversas rutas por las que alternar las comunicaciones, con el fin de continuar funcionando, aunque alguno de ellos fuese destruido como consecuencia de algún ataque. Ya en los años setenta comenzaron a unirse a la Red empresas e instituciones educativas, desmarcándose así del ámbito estrictamente militar. De forma paralela iban surgiendo redes similares a ARPANET a lo largo del planeta. Sin embargo, éstas no podían comunicarse entre sí, al utilizar protocolos para la transmisión de datos diferentes. Este obstáculo se salvó en 1974 cuando Vinton Cerf junto con Bob Kahn publicó el Protocolo para Intercomunicación de Redes por paquetes, en el que se detallaban las características del nuevo protocolo TCP/IP (Transfer Control Protocol/Internet Protocol), cuya definición como estándar culminó en 1982. La nueva especificación se concibió, así como el idioma común de todos los ordenadores conectados a la Red. De este modo, diversas redes pudieron conectarse a una única, la cual pasó a denominarse Internet. Durante la década de los 80, la Red se expandió en gran medida gracias a la conexión de un gran número de ordenadores. Fue entonces cuando se creó el sistema de denominación de dominios (DNS, Domain Name System).

Internet se encuentra aún en un gran proceso de expansión y modificación, por lo que, a medida que se produzca la modernización de las infraestructuras de comunicaciones y las nuevas tecnologías vayan generalizándose entre el público, a lo que hay que unir una progresiva racionalización y estructuración de los recursos en grandes áreas temáticas, es de esperar que los resultados sean más rápidos, pertinentes y satisfactorios.

Internet ha revolucionado por completo el sistema de trabajo y las posibilidades de información en muchos ámbitos profesionales. A pesar de encontrarse en permanente estado de adaptación y mejora. Sin embargo, es evidente que aún encontramos muchas limitaciones, pero que con el paso del tiempo habrán de solucionarse para hacer más factible y confiable la información que esta nos proporciona.

Por otro lado, la web ha evolucionado desde su creación de forma rápida en diferentes aspectos:

Ámbitos de aplicación. El uso de las redes de comunicación ha ido aumentando exponencialmente desde su creación, actualmente múltiples de las actividades cotidianas que realizamos se pueden realizar de forma más rápida y eficaz a través de las redes (reservas de hotel, avión, tren, solicitud de cita previa, transferencias bancarias, compra electrónica, etc.).

Tipo de interacción del usuario. La evolución que ha seguido la web en relación al rol que los usuarios tienen en el acceso a la misma ha ido también evolucionando.

La siguiente información fue recopilada del autor: Pablo E. Lozada, en su artículo denominado “Evolución de la WEB“, en la cual hace referencia a tres etapas en la evolución a Internet:

Web 1.0 Se basa en la Sociedad de la Información, en medios de entretenimiento y consumo pasivo (medios tradicionales, radio, TV, email). Las páginas web son estáticas y con poca interacción con el usuario (web 1.0, páginas para leer).

Web 2.0 Se basa en la Sociedad del Conocimiento mejor conocida como Web Social, la autogeneración de contenido, en medios de entretenimiento y consumo activo. Las páginas web se caracterizan por ser dinámicas e interactivas (web 2.0, páginas para leer y escribir) en donde el usuario comparte información y recursos con otros usuarios, un claro ejemplo son los siguientes:

Comunidades en donde los usuarios pueden incluir sus opiniones, fotografías, y comunicarse con el resto de miembros de su comunidad, como los que conocemos en la actualidad como: MySpace, Facebook, Tuenti, entre otros.

Donde se puede compartir y descargar diferentes tipos de informacion como:

- imágenes: Flick-r
- videos: Youtube
- libros: Google books
- Documentos colaborativos: Wikis
- Páginas personales. Blogs

Web 3.0 Las innovaciones que se están produciendo en estos momentos se basa en sociedades virtuales, realidad virtual, web semántica, búsqueda inteligente, que hasta el momento se encuentran en fases de prueba o en la mayoría de sus casos no han sido culminadas en su totalidad.

En la actualidad ya contamos con un cúmulo de tecnologías sostenibles y razonables que pueden permitirnos realizar diferentes actividades que afiancen nuestras posibilidades comunicativas y expresivas, industriales, culturales, y lúdicas, como hace poco tiempo no nos imaginábamos que pudiera ocurrir.

Por ejemplo, nos permiten: comunicarnos de forma sincrónica y asincrónica, y de manera fiable y rápida y con costos notablemente más reducidos que en las décadas anteriores, con personas situadas en continentes diferentes al nuestro; realizar transacciones comerciales sin entrar en los bancos y cajas de ahorros; efectuar el trabajo desde nuestro propio domicilio; o ofrecer un diagnóstico médico con tanta fiabilidad como si estuviéramos delante del enfermo.

A ellos podemos incorporarle el acceder a bases de datos que hasta hace relativamente poco tiempo estaban limitadas a un círculo reducido de personas, conversar con desconocidos en los círculos IRC, la visita a versiones virtuales de los museos de mayor prestigio y reconocimiento mundial, o la utilización de estas tecnologías para múltiples fines, que van, desde la educación y formación, hasta la industria, la investigación, o la navegación.

1.4 Ventajas y desventajas de las tecnologías de información y comunicación.

Los avances tecnológicos de información y comunicación en los últimos años han traído grandes ventajas para la sociedad, agilizando y movilizando el flujo de la información en los diversos medios tecnológicos sin embargo el uso inadecuado trae desventajas para los usuarios, a continuación, se presentan algunas ventajas y desventajas de las TIC:

Ventajas de las Tecnologías de información y comunicación.

1.- Interacción sin barreras geográficas.

Los usuarios de estas tecnologías se encuentran casi todo el tiempo interactuando entre sí a través de foros o redes sociales. Si se trata de un curso coordinado por un docente, no es necesario que estén todos juntos en un salón para poder interactuar, ya que Internet permite crear foros de discusión y que de esta manera participen todos los integrantes, aunque no estén físicamente cerca.

2.- Diversidad de información.

Mediante el acceso a Internet cualquier persona puede estar informada acerca de las últimas novedades de prácticamente cualquier tema. Esta es una gran ventaja ya que no limita el conocimiento a un libro de texto o un docente dentro del salón, además de que se pueden contrarrestar fuentes y opiniones y llegar a distintos puntos de vista sobre un asunto.

3.- Aprendizaje a ritmo propio.

Con alternativas como los cursos online, cada usuario puede estudiar a su propio ritmo y en el horario que le convenga, ahorrando tiempo y dinero ya que no tienen que trasladarse a una academia.

4.– Desarrollo de habilidades.

Entre ellas, la habilidad de buscar información confiable en la red. Internet es un mar de información donde navegar, pero gran cantidad de los contenidos no son confiables, por lo que utilizando su criterio las personas adquieren habilidades de discernimiento para saber cuándo está frente a información valiosa y cuando está recibiendo información descartable. Además, también se aprende a utilizar las máquinas, lo que resulta de gran utilidad para cualquier persona.

5.– Fortalecimiento de la iniciativa.

En el caso de la educación online cada persona es responsable de su proceso de aprendizaje, por lo que puede resultar una buena manera de reforzar la iniciativa de cada uno para continuar estudiando y aprendiendo.

6.– Corrección inmediata.

El aprendizaje a través de Internet también brinda un sistema de retroalimentación inmediata cuando el usuario se equivoca en una respuesta, permitiendo al estudiante conocer que se está equivocando en el momento que está cometiendo el error.

Desventajas de las tecnologías de información y comunicación.

1 – Distracciones.

Internet, así como una fuente inagotable de conocimiento, lo es en igual medida de distracciones. Es muy fácil que con esta herramienta surjan pérdidas de tiempo a cada rato, por lo que cada persona debe autocensurarse en estas cuestiones y dejar las distracciones de internet para los ratos de ocio, evitándolas al máximo cuando se está trabajando o estudiando.

2 – Aprendizaje superficial.

Como mencionamos más arriba en la web se encuentra información en abundancia, pero muchas veces no es de calidad. Esto puede llevar a aprendizajes incompletos o lo que es peor aún a aprendizajes erróneos.

3 – Proceso educativo poco humano.

El proceso de aprendizaje, al ser a través de una máquina, puede volverse impersonal y frío ya que no se estará en contacto con compañeros y docentes.

4 – No es completamente inclusivo.

El aprendizaje online no es accesible a todo el mundo, ya que gran parte de la población mundial no tiene acceso a esta herramienta. Además, muchas personas se niegan a aprender a utilizar las máquinas, tal es el caso de gran mayoría de los adultos mayores.

5 – Puede anular habilidades y capacidad crítica.

Prácticas como la escritura a mano se ven amenazadas con la masificación de las máquinas. Varios estudios han demostrado que este tipo de escritura beneficia el desarrollo cognitivo, y el uso permanente de las maquinas provocará que muchas

personas “se olviden” cómo es o la dejen de practicar por considerarla poco útil o anticuada.

También el pensamiento crítico puede verse amenazado con Internet, ya que muchos esperarán encontrar en la web todas las respuestas a los dilemas académicos que se presentan dejando de un lado la reflexión personal.

Capítulo II.

Conductas delictivas y su inclusión en la era moderna.

2.1 Factores sociológicos en la producción de conductas delictivas.

> *"La delincuencia entendida como un fenómeno social creado por el conjunto de infracciones contra las normas elementales de convivencia, producidas en un tiempo y lugar determinados, es una problemática que actualmente vive México y que se ha intensificado en los últimos años"* (Herrero, 2007).

Algunos factores sociológicos que influyen en la producción de conductas delictivas como lo son: la desorganización social de la colonia en donde viven, alto índice de marginación, deserción escolar, mala relación con los padres, la interacción con personas que reflejan conductas antisociales y una mala actitud referente a aspectos de la Ley y la Justicia.

Sin embargo, existe una diferencia entre una conducta antisocial o delictiva y un delito, no cualquier conducta es considerada como delito, únicamente aquellas que causen un daño o pongan en peligro lo protegido por el derecho penal. Un acto se convierte en delito cuando infringe la ley y se encuentra anotado en ella.

1.- La conducta antisocial, aunque no se considera como acción delictiva en sí, podría evolucionar hacia la ruta del delito.

2.- Todo comportamiento antisocial que es determinado por una comunidad, sea delito o no, podría tener un impacto negativo para las personas y para la comunidad. Como consecuencia, no se debe pensar que dicho comportamiento no será sancionado simplemente porque no es un delito.

3.- El actuar de forma antisocial es una orientación o tendencia de la conducta, más no una acción delictiva en sí, pero está relacionado con la falta de autocontrol, la

impulsividad y la tendencia a involucrarse en situaciones de riesgo. La falta de autocontrol implica la imposibilidad de vislumbrar acciones alternativas de actuación pro-social.

> *"Desde que se reconoció que la criminalidad no es solamente un hecho individual sino un fenómeno social, la sociología a estado indisolublemente ligada con la explicación de la criminalidad*" (Reyes, 2003).

El estudio integral de la prevención del delito asume que el origen y progreso de la conducta delictiva de un individuo se determina a través de la interacción de tres ámbitos de acción, que configuran los correspondientes niveles de intervención: el primario, que actúa sobre los factores de riesgo individuales, del ámbito familiar y los determinantes sociales; el secundario que interviene en los individuos o grupos en situación de riesgo delictivo y; el terciario, que está orientado a la rehabilitación de quienes han delinquido.

Los factores de riesgo aumentan la probabilidad de que un individuo cometa algún delito o sea más propenso a ser víctima. Dichos factores son modificados por la influencia social expresada en el deseo de tener bienes materiales, de lograr un determinado estatus social o por la presencia de ciertas emociones. Por su parte, los factores protectores ya sea directa o mediante la interacción con otras variables, inhiben o mitigan la aparición de conductas antisociales o delictivas. Comportamientos como el uso y abuso de alcohol y drogas; relaciones sexuales sin protección, fracaso y deserción escolar, entre otros, constituyen factores de riesgo que colocan a las personas en situaciones de mayor vulnerabilidad.

La familia constituye el principal espacio donde se construyen, promueven y fortalecen las actitudes y habilidades que los individuos van adquiriendo para hacer frente a las exigencias de la vida.

Es en este ámbito de convivencia donde se modela el desarrollo de elementos de riesgo que al interactuar con ciertas características inherentes a la personalidad del individuo determinan o no el surgimiento de conductas potencialmente delictivas. Por ejemplo, existe evidencia que vincula la aparición de comportamientos antisociales en infantes y jóvenes con el tamaño y la composición demográfica de la familia, así como la calidad de la interacción intrafamiliar.

El entorno comunitario que los rodea forma parte esencial del desarrollo de los jóvenes quienes a partir de la pubertad pasan más tiempo fuera de su casa y de la escuela. Estas interacciones con los distintos elementos del exterior influyen en la manera cómo los jóvenes van tomando sus propias decisiones. Algunos autores han postulado que la convivencia con sus pares es la principal fuente de influencia en su desarrollo. No obstante, esta interacción suele ser un proceso de elección selectiva, donde los conjuntos de valores del individuo al interrelacionarse con otros reafirman o previenen sus propias conductas antisociales.

Las condiciones de pobreza y marginación, el nivel de exposición a la violencia, el respeto a las reglas sociales, la facilidad de acceso a sustancias adictivas, el capital cultural de la comunidad, o la existencia de acciones para la construcción de valores, son algunos de los elementos que figuran estos incentivos. Las señales físicas y sociales desatendidas del espacio público se han analizado como predictores de la delincuencia en al menos tres formas.

En primer lugar, se encuentra el desorden social como elemento que desincentiva la inversión, merma la cohesión social y estimula el miedo al delito. La segunda propuesta indica que el desorden social y la delincuencia son producto de una misma causa, resultado de una agregación de múltiples factores presentes en los vecindarios. Y la tercera causa advierte que el deterioro de las colonias o barrios dificultan la convivencia entre los vecinos, disminuyen la percepción de seguridad, vuelven más difícil la participación comunitaria y por ende aumenta la percepción de que los delincuentes aprovechan tales áreas para delinquir.

Entre los factores asociados al contexto del lugar en donde viven, los cuales tienden a contribuir al desarrollo del comportamiento desviado incluidas las conductas antisociales que trasgreden a las leyes.

Los lugares en que viven tienden a ser lugares en donde se registran problemáticas como la violencia ya sea dentro de la propia familia, como también en el barrio o colonia, presentando altos índices de delincuencia, demostrando entonces que la comisión de delitos está dentro de las posibilidades de vida de sus habitantes. Así también la existencia de grupos reconocidos como pandillas los cuales generalmente presentan mal comportamiento, conocido como factor asociado al grupo de pares, donde se muestra que el comportamiento antisocial de los jóvenes tiende a realizarse en conjunto o con otros amigos que son también antisociales (Villanueva, 2005).

En el caso de las conductas delictivas enfocadas a los menores de edad se ha probado la continuidad que existe entre el comportamiento antisocial a temprana edad y su persistencia posterior. Este aspecto es de relevancia ya que pone en evidencia el desarrollo de actitudes favorables hacia conductas que trasgreden las leyes. Es en este sentido en donde el involucramiento de actos antisociales en los

menores está asociado a comportamientos más serios y crónicos en su etapa de adultez (Thornberry, 1995).

Por ejemplo existen estudios donde muestran el crecimiento de la gravedad a medida que los niños van creciendo, esto permite tener una sucesión de los actos delictivos cometidos en el tiempo, así como su duración y su coexistencia (Blatier, 2002: citado por Vanderschueren & Lunecke, 2004), más claro lo explica Capdevila, Ferrer & Luque (2005), sobre la persistencia de las conductas antisociales en los jóvenes, permite desarrollar una llamada “carrera delictiva”, que se podrá prolongar más allá de la mayoría de edad.

A continuación, se describen los modelos y teorías que contemplan al delito como un fenómeno social, procediendo a su explicación desde diversos enfoques teóricos. Y trata de encontrar una de sus causas en el contexto social del individuo, desde el punto de vista de cada autor.

Teoría de la Asociación Diferencial.

El autor Sutherland considera que se puede llegar a ser delincuente, según el ambiente en el que uno se haya desarrollado. Las personas al vivir en sociedad se relacionan continuamente con otras personas, pudiendo relacionarse con personas favorables a la ley o, por el contrario, con personas que violan y fomentan la violación a la misma (Marsh, 2006).

Fue uno de un grupo de científicos sociales de la Universidad de Chicago que desafiaron las explicaciones individualistas de la delincuencia. La idea de convertirse en 30 un delincuente fue central en el concepto de asociación diferencial desarrollada por Edwin Sutherland en su teoría de la asociación diferencial, en

donde explica el comportamiento antisocial en cuanto al contacto o asociación con determinados grupos sociales o entornos.

En términos de asociación diferencial, el autor de la teoría se cuestiona cómo surge el comportamiento criminal a lo cual responde: “los individuos tienen asociaciones diferenciales con otras personas que son más o menos dispuestos a la criminalidad”.

La esencia de este enfoque es que el comportamiento antisocial se aprende, el aprendizaje se produce a través de la asociación con otras personas, dicho aprendizaje incluye los medios para llevar a cabo la conducta criminal (Marsh, 2006).

En esta teoría de la Asociación diferencial se destacan las influencias más relevantes que recibió Sutherland, entre ellas, de Shaw y McKay, de los cuales extrajo la idea de la “desorganización social”, como factor que contribuye al delito, al ser precisamente en estas áreas socialmente desorganizadas donde se produce un exceso de definiciones favorables a infringir la ley.

Otra de sus influencias viene de Thorsten Sellin, con la idea del conflicto cultural, el cual es un producto de la progresiva diferenciación de la sociedad y de la inmigración, esta fue incorporada por Sutherland para reforzar el porque la gente aprende valores normativo distintos.

Y por último para elaborar su propia teoría, destaca la influencia de la corriente sociológica del interaccionismo simbólico de Mead. Para dicho autor la gente actúa sobre la base del significado que las situaciones poseen para ellos, esto es el

significado determina el comportamiento; adicionalmente la interacción social consiste en el intercambio de símbolos y significados. Esto lo explica Sutherland en su teoría en el significado que la persona atribuye a una determinada situación objetiva y como este significado se aprende en la interacción que uno desarrolla con sus grupos personales más íntimos (Larrauri y Cid, 2001).

Tomando en cuenta esta teoría, consideramos puesto que toda persona se adecua más o menos a la cultura que la circunda, entonces, el medio sociocultural desempeña un importante papel como factor (Lamnek, 1980).

Teoría de las subculturas.

Su representante más importante es Albert Cohen, alcanzó gran notoriedad y resulta sumamente interesante ya que situó como el eje central de su explicación, el problema de la criminalidad juvenil (David, 1979).

El punto de partida para el desarrollo de su teoría de las subculturas fue la proposición de que “toda acción es el resultado de continuados esfuerzos por solucionar problemas de adaptación”, esto es, su falta de reconocimiento por el grupo de referencia. Según Cohen, la mayoría de los problemas de adaptación se solucionan de forma normal, pero en algunos casos, las personas eligen soluciones desviadas.

Los problemas de adaptación, entonces, son funciones de campos sociales locales y dependen igualmente de la personalidad y los componentes situacionales de tales campos, pues varían con modificaciones en cada uno de estos. Dichos componentes y personalidad son el producto de la estructura y articulación de un sistema más grande, de los subsistemas de reclutamiento, de distribución de papeles, de socialización, de poder, de comunicación, de propiedad, entre otros, los

cuales tienen como efecto conjunto una específica distribución de personalidades y situaciones, y consecuentemente de correspondientes problemas de adaptación.

Pero aun para Cohen, el demostrar los problemas de adaptación no aclara porque la gente actúa como lo hace, y mucho menos explica el comportamiento criminal.

Para la mayoría de estos problemas existe un número concebible de soluciones, algunas de ellas normales y algunas desviadas.

Por qué eligen esas alternativas desviadas hay que buscarlo en “grupos de referencia” que tienen a su alrededor los individuos, ya que las personas seleccionan en un primer momento las soluciones que son compatibles con las expectativas de sus grupos de referencia corrientes, pero cuando estas soluciones no son adecuadas, se buscan otros grupos cuya cultura proporcione respuestas adecuadas.

Finalmente, la subcultura surge cuando hay un número de personas con similares problemas de adaptación para los cuales no existen soluciones institucionalizadas ni tampoco grupos de referencia alternativos que proporcionen otro tipo de respuestas. Entonces, es muy probable que, si las circunstancias los favorecen este grupo de personas desubicado, acabe por encontrarse y unirse, creando una subcultura nueva, en la que solucionen sus problemas de aceptación social (David, 1979).

Teoría de la desorganización social.

Uno de los hechos más reconocidos sobre el crimen es que no se distribuye aleatoriamente entre vecindarios dentro de una ciudad. Esto es, que el crimen no ocurre igualmente en todas las áreas, más bien tiende agruparse en ciertos lugares, y en otros no. La teoría de la desorganización social toma este hecho de la distribución no aleatoria de la delincuencia como punto de partida para la explicación del crimen. Es una de las pocas teorías de la estructura social de la delincuencia que considera ¿Por qué las tasas de delincuencia varían en ciertas áreas o barrios? (Krohn, Lizotte y Penly, 2009).

Las demás cuestiones de interés para la teoría de la desorganización social, ¿Por qué la delincuencia es mayor en algunos barrios, comparándola con otros barrios?, y si más allá de las propias personas que viven en el barrio, ¿existe alguna característica en los barrios que fomenta la delincuencia?

Un elemento central de la teoría es que las comunidades se caracterizan por una dimensión de la organización: en un extremo están las comunidades que se organizan socialmente y en el otro las comunidades socialmente desorganizadas. Esto es un punto clave para la teoría, porque la organización social es la clave para la lucha contra la delincuencia. Las comunidades socialmente organizadas tienen la solidaridad, cohesión y la integración que ayudan colectivamente a mantener los índices de criminalidad más bajos, en cambio, las comunidades socialmente desorganizadas que carecen de estas características tienden a tener mayores tasas de delincuencia.

La conexión entre la organización social y el delito tiene que ser autorregulada. En las comunidades organizadas existe: una vigilancia informal o la observación casual

en las calles del vecindario por parte de las personas que habitan ahí, como parte de sus actividades diarias, existen reglas para tratar de evitar acercarse a ciertas áreas que son consideradas como peligrosas, para la intervención directa en cuestionar a extraños en el vecindario que actúen de manera sospechosa, amonestación a adultos y niños con comportamiento considerado como inaceptable.

En resumen, las comunidades organizadas socialmente, generalmente marcadas por estas características tienen un alto nivel de control social informal y menores tasas de delincuencia.

La desorganización social puede entonces así definirse como la incapacidad de las comunidades locales para tener por parte de los residentes valores comunes y para resolver problemas comunes que experimenten en el lugar.

Algunas características consideradas ecológicas, como la pobreza, el desempleo, la movilidad residencial, y la heterogeneidad racial, pueden influir en el grado de desorganización social, y por consiguiente tener implicaciones de delincuencia.

Por ejemplo, si la gente continuamente entra y salen, se hace más difícil para los residentes conocerse y confiar unos con otros, lo que reduce el control social informal que es necesario para prevenir la delincuencia. Según la teoría, las comunidades caracterizadas por altas tasas de rotación residencial deben experimentar altas tasas de criminalidad, precisamente porque estas comunidades sufren lazos débiles y mantienen un poco control informal. Los estudios demuestran que esto es cierto, incluso resultados similares se registran respecto a los efectos de la pobreza, desempleo y otros factores de las comunidades (Krohn, Lizotte y Penly, 2009).

Teoría del aprendizaje social.

El principal exponente de la teoría del aprendizaje social es Albert Bandura, con la cual explica la conducta humana en los siguientes términos: consiste en “una interacción recíproca y continua entre los determinantes cognoscitivos, los comportamentales y los ambientales”. Haciendo un importante énfasis en el papel que desempeñan las variables sociales para explicar el desarrollo y modificación de la conducta humana, así como la formación de la personalidad (Bandura y Walters, 1988).

El autor Bandura, parte de examinar con cuidado el proceso por el que se alcanza la socialización de la conducta y seleccionar las dimensiones o variables de la conducta infantil que parezcan tener importancia en el proceso de socialización.

Del mismo modo intenta explicar la “conducta desviada” desde los principios de aprendizaje social, incidiendo en tres aspectos sustanciales:

1. Las características de comportamiento de los modelos sociales a los que este expuesto el niño.

2. Las contingencias de refuerzo de su historia de aprendizaje, y

3. Los métodos de instrucciones que se han utilizado para desarrollar y modificar su conducta social (Vázquez, 2003).

Teoría de la desigualdad de oportunidades.

Los autores Cloward y Olhin explican con su teoría de la desigualdad de oportunidades las condiciones para que una persona que experimenta el desajuste entre aspiraciones y oportunidades llegue a desarrollar una respuesta delictiva (Cloward, citado por Larrauri y Cid, 2001).

El punto de partida de estos autores, consiste en señalar que la presión anómica que está en la base de la respuesta delictiva se deriva de la discrepancia entre las aspiraciones culturales inducidas y la posibilidad de lograr tales objetivos por medios lícitos. Una vez que la persona experimenta esta presión que le distancia de los medios lícitos, por advertir que mediante ellos no va a conseguir el anhelado éxito económico entonces ya nada le impide recurrir a los medios ilícitos. En síntesis, para delinquir no solo hay que tener bloqueados los medios lícitos, sino que además se tiene que tener acceso y aprender a utilizar los ilícitos (Cloward, citado por Larrauri & Cid, 2001).

Teoría del Control.

Formulada por Travis Hirschi, consiste en distinguir entre el control ejercido desde fuentes externas al individuo y el control ejercido por el propio individuo. Al primero denominado “control social”, y al segundo “autocontrol”. La sociedad se esfuerza en presionar a sus miembros con modelos de conformidad, en principio, es el control social el que opera de freno para evitar la comisión de delitos. Las que carecen de vínculos sociales estarán más predispuestas a delinquir que aquellas que tienen fuertes vínculos 37 con la sociedad. “la delincuencia se produce cuando los vínculos que nos unen a la sociedad se rompen o se debilitan” (Hirschi, 1969).

Teoría integradora de Farrington.

Integra aportaciones de la teoría de las subculturas, la del aprendizaje social, la de la asociación diferencial, la de la desigualdad de oportunidades y la de control social (Vázquez, 2003).

La delincuencia según Farrington (1992), surgía por un proceso de interacción entre el individuo y el ambiente. El surgimiento de la motivación para delinquir parte de los deseos de bienes materiales para obtener prestigio social o de la búsqueda de sensaciones. Posteriormente, se busca un método legal o ilegal para satisfacer los deseos personales. Obviamente, el pertenecer a una clase baja va a determinar con mayor probabilidad el recurrir a formas ilegales. No obstante, la motivación para cometer actos delictivos no es constante y puede modularse por las creencias o actitudes interiorizadas acerca de la ley (Farrington, Ohlin y Wilson, citado por Farrington, 1992). Las edades en que se llevan a cabo los distintos hechos tiene gran importancia, así como la falta de recursos económicos, un bajo coeficiente intelectual y una crianza de poca calidad, serán factores de riesgo que podrían determinar el comienzo de la delincuencia, los familiares y amigos antisociales tienen una gran influencia en que persista este comportamiento antisocial (Farrington, 1997).

2.1.1 Factores Criminógenos en la producción de conductas delictivas

Los factores criminógenos son los elementos que, en conjunto, favorecen a un determinado resultado antisocial. Lo constituyen factores endógenos y exógenos. Se toman de la generalidad.

Los factores que en los capítulos siguientes veremos son los que se muestran a continuación de acuerdo con el psicólogo Frank Geldard:

1.-Sociales. Pobreza, condiciones de vida estresante, carencia en el hogar, desorganización social, multitud;

2.-Familiares. Padres inmaduros, perturbados mentales, criminales o abusivos, pleitos matrimoniales graves, disciplina infantil deficiente, patrones desordenados de comunicación familiar;

3.-Psicológicos. Estrés, poca inteligencia, falta de control o dominio; y

4.-Biológicos. Defectos genéticos, cuidado prenatal deficiente (drogas, mal alimentación), enfermedad o incapacidad (síndrome Down, retraso mental), etc.

La necesidad obligada de que se estudien los factores en sus orígenes internos y en sus orígenes externos tiene base fundamental para la obtención de resultados completos de lo que da lugar a las conductas antisociales. Así, (DURKHEIM,2003) distingue dos seres inseparables; uno, formado por nuestros estados mentales; y el otro, formado por nuestros grupos sociales.

Factores criminógenos endógenos y exógenos.

En la investigación criminológica deben acercarse elementos relacionados con la conducta del sujeto que nos orienten en el concepto del saber, los motivos que producen la conducta antisocial y así lograr un conocimiento eficaz en esta investigación.

Los factores causales de la antisocialidad comprenden los factores endógenos y exógenos, que se pueden considerar como mecanismos de presión criminógena y tienen las siguientes subdivisiones: los endógenos pueden ser somáticos y psíquicos, y se refieren a las características constitucionales y de personalidad que tienen los individuos; los exógenos pueden ser físicos, familiares y sociales, y se refieren al ambiente por el que se ve rodeado el sujeto.

Los factores endógenos “y” exógenos, y poner la letra “y” entre estos, significa que los términos están estrechamente unidos; y que darán como total, lo que resulte de la suma de ambos. Estos dos factores no se forman por separado, uno es parte de su estructura hereditaria y mental, que lo forma desde adentro y de la estructura de su ambiente, que lo forma desde fuera. Es importante descubrir uno a uno de estos factores que llevan al desorden mental.

Desde la perspectiva de Lombroso, si consideramos al ser humano en su tendencia al delito, observamos que depende de su organización, de la educación que ha recibido y de las circunstancias que lo rodean, y no hay algún problema en admitir la interrelación entre factores ambientales y factores endógenos.

Para hacer una prevención de la antisocialidad es necesario conocer las causas individuales y sociales de ésta, para hacer más fácil la comprensión de este tema, en los capítulos siguiente se hará una explicación de distintos factores causales de ésta, empezando con los endógenos para luego pasar con los exógenos, en base a los estudios de Solís Quiroga y Leija Moreno, que toman como referencia pues es claro que hay estudios que superan a éstos, más amplios y actualizados; además se agregan experiencias observadas (empirismo criminológico).

Factores endógenos.

La relación entre los cambios del cuerpo, las enfermedades corporales y las enfermedades mentales; se basan, en parte a los procesos biológicos entre los que se distinguen ciertos factores que influyen en el desarrollo anormal de una persona, y que éstos pueden llevar a la realización de ciertas conductas antisociales.

Factores somáticos.

Son endógenos los que nacen con el sujeto y actúan hacia el medio exterior produciendo ciertos resultados. Existe relación entre la actividad del organismo con las conductas antisociales.

Para Héctor Solís Quiroga “son causas endógenas somáticas las que se manifiestan en el cuerpo, se refieren a los cambios en la estructura y funcionamiento corporal, así como las anomalías o defectos y enfermedades corporales, hereditarias o adquiridas, también particularidades en su desarrollo”. Estas causas endógenas somáticas que tienen efecto en la antisocialidad, serán estudiadas por la Criminología Biológica.

La determinación de las influencias de los factores hereditarios sobre un niño o un adulto requiere la opinión de un especialista con conocimientos de genética humana. El Criminólogo debe tener conocimiento del valor de sus pruebas como elementos de predicción.

Cambios en la estructura y funcionamiento corporal.

Todas las especies de organismos tienen su origen en un proceso de evolución biológica. Durante este proceso van surgiendo nuevos cambios a causa de una serie de procesos naturales. Para entender lo referente a los factores endógenos, es necesario describir algunos conceptos operacionales que nos servirán para el manejo del tema.

La anatomía es el estudio de la forma y la estructura de los seres vivos. La fisiología es el estudio de cada uno de los órganos de los seres vivos, así como el estudio de sus funciones, pero en conjunto, es el estudio de los procesos físicos y químicos que tienen lugar en los organismos vivos durante la realización de sus funciones necesarias para la vida.

La comprensión adecuada de la estructura implica un conocimiento de la función de los organismos vivos. Por lo tanto, la Anatomía es casi inseparable de la Fisiología, que a veces recibe el nombre de Anatomía Funcional.

La ciencia está descubriendo una de las realidades más sorprendentes de la herencia. Ésta ayuda a explicar los factores endógenos de la antisocialidad. La ciencia tiene un entendimiento más claro del mecanismo, que es tan preciso, que

cumple continuamente con una serie de cambios. Esto tiene que ver con la sustancia llamada ADN, que son las siglas al nombre de ácido desoxirribonucleico. Cada uno de nosotros posee un código genético propio. Este código contiene todas las informaciones indispensables para el desarrollo de nuestro organismo, y claro, lo que determina nuestra tendencia hacia la antisocialidad. El ADN es el portador de la clave de la herencia de todos los seres vivos.

La herencia biológica según Lombroso:

> *"es el estudio de todas aquellas características de un organismo que están determinadas por ciertos elementos biológicamente activos que proceden de sus progenitores"*

Con base a Lombroso, puede existir en determinadas personas que, debido a rasgos hereditarios o genéticos, hay un desarrollo direccional hacia la antisocialidad. Este desarrollo direccional puede disminuirse o aumentarse mediante la acción tanto de circunstancias internas como externas.

En la herencia podemos destacar a los que heredan el alcoholismo, es un tema de preocupación ya que el medio familiar o los padres alcohólicos predisponen a los hijos a desarrollar la actividad de consumir alcohol o en el peor caso, los hijos de alcohólicos nacen con deformidades físicas, el alcoholismo fetal.

La constitución es la estructura peculiar de la conformación biológica y psíquica de un individuo, la cual gobierna sus actitudes, sus actos y sus reacciones. La constitución no quiere decir que una persona reaccione siempre con una constancia mecánica en todas las circunstancias. El término se refiere solamente a las

actividades de reacción que aparecerán probablemente en ciertas circunstancias. La constitución de una persona, es establecida al ser creado durante el desarrollo prenatal o durante la primera infancia, las deformidades aparecen por lesiones, factores nutricios o enfermedades, y predispone a ciertas reacciones y formas de conducta, sin embargo, éstas pueden ser modificadas de tres maneras según el psicólogo americano Werner Wolff:

1.- La predisposición puede permanecer detenida;

2.- Puede ser reprimida; y

3.- Puede ser estimulada y despertada por el ambiente.

El desarrollo de los individuos está expuesto a diversas influencias externas e internas; algunas experiencias tienen mayor impacto que otras, si el entorno se cambia, ellos cambian.

La relación de la herencia con el ambiente es real y es de amplio estudio. El genetista Gregor Mendel demostró que cuando se cruzan dos características contrarias una será dominante y la otra recesiva. De forma análoga en la Criminología, en la herencia y el ambiente, habrá un factor dominante y otro recesivo que desarrolle la antisocialidad.

El estudio de las alteraciones internas ha tenido influencia en la Criminología, las epilepsias, la drogadicción, las anomalías físicas y funcionales, la desnutrición, las anormalidades del desarrollo psicológico, esquizofrenias, nerviosismo, etc. tienen efectos en las personas favoreciendo a la antisocialidad.

El Delito y la herencia.

Las características criminales o antisociales parten del estudio de los elementos constitutivos de la predisposición antisocial: el sexo, la edad, los daños cerebrales, etc. El estudio de estos elementos permite conocer la predisposición antisocial individual, a la que hay que agregar el estudio de las condiciones ambientales como la familia, la situación económica, trabajo, grupos sociales, etc. Todo esto pretende explicar el cómo un ser humano se convierte en antisocial. Los estudios de la herencia tienen conclusión en el área crimino-biológica.

También es importante saber la influencia de las emociones y los vicios de la madre sobre el bebé. Los Médicos, Criminólogos y Psicólogos desarrollistas saben que el ambiente prenatal afecta profundamente al feto. La placenta lo une con la madre, permite que pasen los alimentos y a través de ella se expulsan los desechos; sin embargo, no puede impedir el paso de todas las sustancias nocivas, de modo que la embarazada deberá seguir una dieta sana y no tomar drogas (entre ellas, el alcohol y el cigarro), evitar en lo posible las enfermedades contagiosas y los ambientes que causan estrés. Esto tendrá consecuencias de estrés fetal, causando un desorden psicobiológico; por ejemplo, podemos ver como hay niños que nacen con alcoholismo fetal.

Por otro lado, se define a los enfermos mentales con tendencia a las conductas antisociales a los que desde muy pequeños presentan cierto defecto mental permanente unido a una fuerte tendencia al vicio o al acto antisocial.

Factores exógenos.

Es aquí cuando la Sociología, la Demografía y la Estadística Criminológica trabajan juntas. Se realizan estudios sociológicos de las causas ambientales de la antisocialidad y junto con la Demografía se estudian las características sociales de la población y de su desarrollo a través del tiempo. Se analiza a la población por edades, situación familiar, grupos sociales y actividades económicas. La Estadística sirve para que esos estudios tengan bases científicas y de comprobación numérica, se realizan inventarios de la población, de sus carencias, de sus problemas, etc.

Factores exógenos físicos.

Son factores exógenos los que se refieren al ambiente natural (clima, calor, frío, humedad, etc.) y los ambientes artificiales formados por el ser humano (el barrio, la vivienda, los medios de comunicación, etc.).

El ambiente natural y artificial constituye un estímulo constante al que el sujeto responde continuamente. Hay dos formas principales de respuesta al estímulo en las relaciones del individuo con su ambiente:

1. Puede atacar el ambiente intentando eliminarlo o cambiarlo; o

2. Puede adaptarse a él.

Así entendemos como hay gente que se adapta a las leyes, normas y espacios culturales, mientras otros van en contra de éstos, apartándose o violando las

normas, podrá comenzar desde algo simple como inadaptación familiar pero poco a poco conduce hasta una rebeldía social.

Para el psicólogo Carl Rogers *el ambiente no crea el potencial de crecimiento, pero puede fomentarlo o impedirlo".*

Para otros autores el ambiente es una fuente principal de influencia sobre las personas en desarrollo, lo que a menudo pasa por alto. Una persona en desarrollo está en el centro de varios sistemas ambientales, que incluyen desde la familia hasta la cultura. Se piensa que estos sistemas, interactúan con los individuos e influyen sobre el desarrollo en formas importantes.

El ambiente puede ser definido de la siguiente manera, se refiere a lo que nos rodea: la familia, los amigos, la escuela y muchos otros factores más, incluyendo además el clima. Los seres humanos viven en un medio al cual se adaptan. Si el medio se modifica, se supone que el ser humano debe adaptarse a la nueva situación, pero cuando no se presenta la adaptación, surge un conflicto sin resolver entre el individuo y su medio, y causa una inadaptación psíquica.

La tendencia al dominio del ambiente puede dar lugar a agresividad porque éste en ocasiones frustra al individuo al no poder hacer lo que él desea; por el contrario, el sometimiento, sin que éste implique una sumisión total, puede originar actitudes de compañerismo y cooperación con la colectividad a la que pertenece.

El ambiente es el campo en el que actúa la personalidad, si se pierde, es probable que aparezcan trastornos en ésta; por ejemplo, el desempleo con la falta de dinero, en un comienzo produce sentimientos de inseguridad al desvalorizarse la persona

y después, origina ansiedad y frustración, luego viene el deseo de obtener los bienes por cualquier medio. Si a esto se le agregan las presiones familiares de tener hijos y familia, será una presión fuerte para el sujeto que padezca del desempleo.

"La sociedad, dice Maslow, impide *al individuo satisfacer sus necesidades básicas de amor, comunidad, respeto, realización y pertenencia. El individuo que presenta serias deficiencias en la satisfacción de sus necesidades básicas está enfermo*.

Las actitudes mostradas al ambiente o a la colectividad pueden ser por conflictos internos. La enemistad social, la indiferencia, el mal humor, etc. son la más clara evidencia de problemas internos debidos a la no satisfacción de nuestras necesidades básicas.

El medio físico.

Se han realizado investigaciones de la relación entre las condiciones ambientales y el delito. El factor climático es de importante análisis, se ha comprobado que el acto antisocial se da bajo ciertas circunstancias influidas por el clima. La Criminología Ambiental o Geográfica, demuestra que la antisocialidad se centra en lugares específicos de la ciudad.

Los aspectos a analizar de acuerdo con Leija son los siguientes:

1.- Las diferentes épocas del año; y

2.- Las diferentes regiones en donde el clima actúa en forma muy distinta que otras".

En ambos casos se observan las conductas antisociales favorecidas por el clima. A continuación, se hará una clasificación del tipo de delito que se da de acuerdo a la época del año:

1.- Los delitos sexuales se dan más en época calurosa, las mujeres usan ropa más descubierta y provoca a sujetos enfermos a realizar actos de hostigamiento sexual, abuso sexual, violación, etc.; y

2.- Los delitos patrimoniales se dan más en época de frío, realizando robos, allanamientos, etc., y que en muchas ocasiones dan lugar a la violencia física y/o moral por medio de amagos u otras circunstancias que pongan en peligro a la víctima.

No es exclusivo que los delitos lleven el orden anterior, pues se puede dar cualquiera de ellos en cualquier época del año, pero se hace una clasificación por los más sobresalientes.

Un estudio hecho por Werner Wolf en especial al delito de robo, arrojó los siguientes resultados:

1.- La comparación de los cambios de estación con el delito, indica que los robos aumentan en los meses fríos, debido a que en ellos es mayor la necesidad de alimentos, ropas y abrigo;

2.- Se reveló que el volumen total de delitos es mayor durante las bajas económicas y la elevación de precios en los artículos de primera necesidad, y que existe una relación entre los delitos contra la propiedad;

3.- La proporción de delitos es mayor en las ciudades en las que el contraste entre la riqueza y la miseria es más notorio. La correlación entre la antisocialidad y el desempleo es notable; y

4.- Respecto al estado económico de los antisociales, la mayoría son de clase pobre, pero no hay que olvidar que también abundan los delitos en las clases sociales altas, que son llevados por la avaricia y el poder o posibilidad.

La Política Criminológica ambiental se nota claramente en la opinión del psicólogo conductista Skinner quien sostiene que: *la conducta humana puede ser dirigida, sin tratar de influir en la mente ni de cambiar la personalidad, sino cambiando el medio.*

El barrio o entorno donde se relaciona la persona.

Para Solis Quiroga *el barrio forma parte del medio ambiente social en que se mueve cada persona.*

Comprende sus calles y cualquier vía de acceso; las casas, edificios, los centros de reunión, sean para diversión, vicio, comercio, educación, religión, deportivo, etc., también forman parte de él los diversos tipos de relaciones que desarrollan entre sus habitantes.

Es en el barrio en donde los individuos pasan la mayor parte de su tiempo y éste debe satisfacer las necesidades individuales y sociales. Existen diversos tipos de barrios criminógenos; por ejemplo, aquéllos en que hay pobreza, que carecen de las condiciones mínimas de habitabilidad como agua, drenaje, luz, pavimento o que poseen alguno, pero carecen de otro. Este tipo de barrios, tienen complicaciones de tipo sanitario y educacional.

El barrio tiene importante influencia en el tipo de delito que se comete, su ubicación es importante ya que hay colonias en las que es de difícil acceso para la policía y otros en los que la policía teme ingresar por su alto grado de peligrosidad.

Existen también los barrios ricos en los que de igual manera se da la antisocialidad pero en otra manera, se encuentran actos antisociales relacionados con la avaricia de los sujetos, no se presentan tanto los delitos violentos, sino más bien los delitos que requieren mucha más inteligencia.

De cualquier forma, el barrio, la manera en la que viven y la clase de población que les rodea, influye mucho en la conducta antisocial de las personas.

Los medios de comunicación.

La socialización depende de la transferencia de información por medio de la comunicación. Para entender el proceso social de comunicación y de cómo éste afecta al individuo, debemos entender qué es comunicación. La comunicación se refiere a la transmisión y recibimiento de ideas e información. Entonces los medios de comunicación son los recursos con los que se cuentan para transmitir información de cualquier tipo.

Los medios de comunicación según Ramirez Cavassa pueden ser: *visuales (anuncios, publicaciones), auditivos (radio) y audiovisuales (televisión, filmes por cualquier medio), se emplean según las necesidades, el momento y el impacto buscado; es decir, los diversos medios se aplican con un criterio de oportunidad, eficacia y rentabilidad*.

La comunicación es un proceso natural y necesario. La comunicación es importante porque en ella van las ideas, las costumbres, los hábitos, etc., pero también tiene su lado negativo que es el que se muestra en los siguientes renglones.

El empleo negativo de los medios de comunicación tiene una explicación relacionada con el sistema económico. Empresas fuertes manejan éstos para manipular a los receptores y obtener beneficios. Según Reyes Echandia el *sexo, la violencia y el crimen, son disfrazados con mensajes discretos que son absorbidos por sus destinarios*; por eso los medios de comunicación se han transformado en medios idóneos de enriquecimiento sin importar sus consecuencias negativas y es por eso que invierten grandes cantidades de tiempo y dinero para lograr tener más audiencia.

El comportamiento desarrollado por la influencia de los medios de comunicación tiene base en la imitación de las conductas observadas o escuchadas en éstos. La imitación consiste en copiar las conductas de otra persona real o irreal y que son admiradas por la persona que las imita. Se llaman conductas imitativas a las situaciones que se asemejan al comportamiento de un modelo previamente observado por un sujeto.

Para Eduardo Lozano, *la actividad individual es la fuente y origen de todas las uniformidades sociales, que produce la imitación; por tanto, ésta es una vía por la cual los fenómenos cunden y se extienden socialmente, una vez que una conducta original se ha realizado, y sufre efectos de ejemplo*.

El radio, la televisión, los periódicos, el Internet y otros medios fuertes de comunicación, utilizan en la difusión de sus programas o de su información, diseños especiales que logran obtener la atención de las personas de una manera que se atrapan en éstos.

Para Bryan Key *"en los medios de comunicación se presenta el fenómeno subliminal en el que están incluidas técnicas que tratan de despertar en el individuo una ilusión de realidad para atraer la atención de los emisores y que hacen que millones de seres humanos sean manipulados"*.

El buen diseño y la buena presentación logrará un nivel más alto de audiencia, y son estos medios de comunicación los que en la actualidad constituyen un área importante en la vida diaria; y por esto, deben ser objeto de atención y control por parte de los organismos estatales, pues cada vez más deforman el pensamiento de los que reciben información por medio de éstos.

Cada vez más, se difunde la pornografía, y esto podría parecer no como un problema, porque la pornografía es vista por todos, pero hay que pensar en las consecuencias que puede tener para un menor (me refiero a alguien de 7 a 13 años) ver pornografía.

La pornografía tiene el mensaje subliminal (aunque más que subliminal es muy directo) de que todas las mujeres son de fácil acceso al sexo, entonces el menor crece con la idea de que todas las mujeres son así, y cuando se encuentran con que no todas, puede dar lugar a la violencia física y psicológica y otras veces a la violación; además, en la mayoría de las películas pornográficas no se da el uso de condones, así como el bisexualismo (en su mayoría femenil), el transexualismo (hombres con cuerpo de mujer pero que aún conservan su pene), la zoofilia (sexo o estimulación con cualquier animal, desde serpientes, caballos, peces, burros hasta ratones), la necrofilia (estimulación sexual con muertos: hombres, niños o mujeres), la coprofilia (satisfacción por las heces fecales o la orina, lluvia dorada).

Es con esto con lo que se afecta un menor, reproduciendo todas las actividades anteriores, y causando embarazos no deseados, enfermedades y muchas perversiones, además de lesbianismo y homosexualismo a corta edad, y que pudiera resultar traumante cuando razone de sus actividades en edad más avanzada. La pornografía ha hecho que los niños de diez años ya sepan de lo sexual.

Otro problema es el de la promoción al consumo de alcohol, cigarros y otras drogas, el problema empieza cuando el consumo de éstos es sin medida y motivado por la publicidad que se le da que si eres consumidor gozas de un alto nivel dentro de la sociedad; o, que serás reconocido por los demás por tus actos fuertes o rudos. El consumo del alcohol en exceso ya todos sabemos los efectos que tiene, provoca un estado de inconsciencia que da lugar a cometer conductas antisociales, además de los problemas a la salud que tiene como consecuencia el abuso de este producto; el cigarro, afecta, causa nerviosismo cuando se abstiene de él, además de cáncer y otras dificultades respiratorias.

Uno más es la violencia que se transmite, influye en todos, desde los niños hasta en los adultos, crea una conducta violenta hacia los demás, parecería que las caricaturas en vez de divertir sanamente, lo que hacen es motivar la violencia, utilizando armas, martillos, clavos y otras herramientas que en la caricatura son inofensivas; por ejemplo, se golpea a alguien y no sangra, se dispara a alguien y no se muere, los niños pensarán que lo mismo pasa en la vida real, imagínese a un niño golpeándolo con alguna herramienta o que le quiebre algo en alguna parte del cuerpo, ¿no sería eso peligroso?

Todas las actividades anteriores son reflejadas diariamente por los medios de comunicación, influyendo en niños, adolescentes, jóvenes y adultos, que también se han puesto en contacto persistente con la violencia.

El presenciar actos de violencia influye a que los receptores tomen una conducta violenta, en vez de adoptar una conducta tranquila que requiera meditación.

No debe pasarse la realidad de que se está educando a los menores y a los adolescentes, para matar, destruir, espiar y desconfiar, y que esto ha transformado el sentido de la existencia, que incita a vivir el momento ante la inseguridad posterior, es por eso la importancia de adaptar a los individuos a las normas sociales adecuadas.

La limitación del tiempo que el niño puede ver la televisión y del tipo de programas que pueda ver, en particular durante los primeros años de vida, es muy útil para su desarrollo correcto, también deben considerarse el radio, el Internet, las revistas y otros.

El efecto de los medios de comunicación a nivel de las motivaciones antisociales no parece grave, pero éstos forman una fuente de estímulos criminógenos sobre ciertos sujetos frágiles o fáciles de influenciar; sobre todo, los menores. El estudio de estos efectos será realizado por la Criminología del Arte, viendo a los medios de comunicación como medios de expresión artística-criminógena.

Factores familiares.

Son factores familiares la forma en que está constituida la familia, el número de sus integrantes, su relación de afecto, comprensión, rechazo, etc., su ambiente, su cultura, costumbres, hábitos, el estado económico, etc.

Según John Watson:

> "*los niños son moldeados por sus ambientes; entonces los padres, en gran medida, tienen la responsabilidad de lo que llegarán a ser sus hijos, advirtió que los padres deben enseñar a sus hijos los buenos hábitos*".

El estudio de la familia es importante porque de ella surgen las primeras reglas, conductas, costumbres, etc. y es una educación determinante que influirá en la persona. Los estudios que se realizan a la familia son los siguientes: si es ignorante, débil, no se adapta, con muchos compromisos, siempre ocupada, si presenta posibilidades de divorcio, drogadicción, enfermedades hereditarias, con perversiones, con problemas de relaciones entre sus miembros, egoístas, niños y adolescentes sobreprotegidos, lujos, demasiado rígidos y no adaptados a los cambios, entre muchos otros más.

La economía.

La Economía se estudia en Criminología por la importancia del estado de satisfacción de las necesidades individuales y sociales, la insatisfacción tiene como consecuencia varios de los problemas que veremos más adelante. De manera general, la Economía estudia los procesos de producción, distribución, comercialización y consumo de bienes y servicios.

La importancia de las condiciones económicas en la comisión de hechos antisociales reside en su influencia sobre el desarrollo gradual de personalidades antisociales. La conducta antisocial es en este caso resultado de la inadaptación al ambiente a causa de la inestabilidad económica.

Según Werner Wolff *"los padres agobiados por la pobreza se ven obligados a descuidar la educación de sus hijos. El niño tiene que salir y andar en las calles para encontrar compañía"*. Cuando los padres regresan al hogar, cansados de trabajar, no están en disposición de procurar al niño la debida atención y afecto. Tienen que negar a sus hijos casi todos los juguetes que se exhiben en las tiendas y las diversiones a que los niños con más posibilidades están acostumbrados.

La inestabilidad económica aumenta la inestabilidad emocional de los padres. Si los niños se acostumbran a una conducta anormal y a un bajo nivel moral, tienden a seguir los pasos de sus padres; es decir, los padres se alejan, dejan de dar cariño y atención y los menores comienzan a actuar de la misma manera, es así como se da el alejamiento de los padres con los hijos y que seguramente será muy difícil de tratar.

La falta de dinero y de atención o el exceso de dinero y falta de atención, comúnmente llevan a la familia a ser desorganizada; por ello, la relación familiar debe estar siempre adaptada y estructurada de buena manera.

La conducta antisocial en los ricos también se da, los padres en este caso contrario al anterior, por el exceso de trabajo, desatienden a los hijos, y de igual manera llegan del trabajo cansados y sin ganas de jugar, ni de prestar atención a los menores. Los menores crecen sin atención y al crecer buscan satisfacción en bienes materiales, o se refugian en el consumo de alcohol y otras drogas, en este caso el problema no es la falta de dinero, sino de afectividad, y contando con los recursos necesarios para satisfacer sus gustos, prefieren eso a estar en casa solos.

La cultura.

La cultura se refiere al conjunto de conocimientos que caracterizan a una sociedad o grupo social en un período determinado. El término cultura incluye además modos de vida, creencias, tradiciones, usos, costumbres, sistema de valores, educación, conocimientos, técnicas y leyes.

La cultura ejerce su influencia sobre el individuo desde que éste nace, y aun desde antes. La cultura es la que determina la actitud hacia la anormalidad.

Los trastornos mentales existen en todas las culturas, pero parecen aumentar con el crecimiento de restricciones, por una parte, y con las responsabilidades personales por otra. Para Karen Horney "*la cultura y el crecimiento de la personalidad están relacionados, la cultura impone las situaciones de estrés que entorpecen al crecimiento y, a la vez, proporciona soluciones falsas que son atractivas y fáciles de seguir*".

Subcultura antisocial.

Para el desarrollo de la antisocialidad las circunstancias exteriores tienen una gran importancia para su proceso; sobre todo, en la medida en que esas circunstancias exteriores aportan la ocasión para realizar un acto criminal. Existe el respeto y es considerado por la mayoría, pero dentro de una misma sociedad hay ciertos grupos que se separan de ese respeto, de las normas de la cultura global y entran en conflicto con ella.

2.1.2 Derecho penal y los sujetos del delito.

Sujeto Activo.

Según el derecho penal las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos.

De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes. El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de habilidades no

es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos. Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, estudiosos en la materia los han catalogado como delitos de cuello blanco, término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como delitos de cuello blanco, aun cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros. Asimismo, este criminólogo estadounidense dice que tanto la definición de los delitos informáticos como la de los delitos de cuello blanco no es de acuerdo al interés protegido, como sucede en los delitos convencionales, sino de acuerdo al sujeto activo que los comete.

Entre las características en común que poseen ambos delitos tenemos que el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional. Es difícil elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; no es fácil descubrirlo y sancionarlo en razón del poder económico de quienes los cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los

segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables".

Otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad. Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

Sujeto Pasivo.

Con base al derecho penal tenemos que distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etc., que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los delitos informáticos, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos con objeto de prever las acciones antes mencionadas, debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes

que protejan a las víctimas de estos delitos, la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática, el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantengan bajo la llamada "cifra oculta" o "cifra negra". Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro.

Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración e impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.

2.2 La inclusión de las conductas delictivas en la era tecnológica.

El gran desarrollo tecnológico que se ha producido recientemente han propiciado lo que algunos autores denominan la nueva “revolución” social, con el desarrollo de "la sociedad de la información".

En la cual la “materia prima” es la información y por lo tanto es el motor de esta nueva sociedad, y en torno a ella, surgen profesiones y trabajos nuevos, o se readaptarán las profesiones existentes.

La evolución de los delitos relacionados con la aplicación de las nuevas tecnologías de información y comunicación se orientan en la actualidad a sistematizar normativamente atentados contra los datos personales y la eventual invasión de la intimidad por medios informáticos, es innegable que una nueva forma de entender la intimidad resulta equiparable a la capacidad de disposición sobre las bases de datos automatizadas o convencionales que contienen información respecto de nuestras identidades, sin embargo objetivamente la ampliación punitiva en materia informática en la mayor parte de las legislaciones se limita a castigar el simple acceso a las bases de datos personales , sea cual fuere su contenido , no obstante, se está omitiendo la punibilidad a la capacidad de disposición sobre dichas bases de datos o información que no solamente generan una efectiva lesión sobre nuestra intimidad, sino que adicionalmente su apoderamiento podría producir el robo o suplantación de nuestra identidad con todo y sus catastróficos efectos inherentes.

Es cierto que en la actualidad resulta muy importante en el contexto legislativo, la criminalización del acceso a los datos personajes informatizados cuando se realiza de manera no autorizada, pero resulta trascendental también, criminalizar cuando

se afecta la facultad de disposición o de ejercer la titularidad de nuestra información personal, es decir, del poder de controlar la información sobre uno mismo, lo cual resulta aún más grave.

Existe una relación entre la tecnología y la usurpación o falsificación de la identidad que demuestra que la utilización cada vez más extensa de los dispositivos tecnológicos de información y comunicación generan la ausencia de la presencia de la persona física o directa que suele ser aprovechada para suplantar o falsificar la identidad de una persona en pocas palabras a mayor posibilidades técnicas y distancia entre sujetos se da lugar a una falta de control de su propia identidad y facilita la usurpación de la identidad de la persona.

En consecuencia, ante estas inéditas conductas desarrolladas por la delincuencia de alta tecnología e inclusive realizadas por ladrones convencionales, no resulta un tema menor las graves consecuencias para los ciudadanos que son víctimas del robo de identidad, los efectos directos generados por la suplantación de identidad son en principio daños fundamentalmente económicos, sin embargo la usurpación de identidad suele suceder de forma de perjuicios de distinta naturaleza que podrían incluir ataques a la privacidad o intimidad de las personas, incluso daños de tipo psicológicos.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje; no son los grandes sistemas de información los que afectan la vida privada, sino la manipulación o el consentimiento de ello por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no está frente al peligro de la informática, sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas. La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen por qué ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática, sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

Capítulo III.

Regulación y prevención de los delitos cibernéticos.

3.1 Penalización de los delitos cibernéticos reconocidos por la organización de las naciones unidas.

Tipos de delitos informáticos reconocidos por la organización de las Naciones Unidas:

a) **Fraudes cometidos mediante manipulación de computadoras.**

Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

1.- La manipulación de programas: es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

2.- Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que

se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para decodificar información electrónica en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

3.- Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina técnica del salchichón en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

b) Falsificaciones informáticas.

1.- Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.

2.- Como instrumentos: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

c) Daños o modificaciones de programas o datos computarizados.

1.- Sabotaje informático: es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

Las técnicas que permiten cometer sabotajes informáticos son:

I. **Virus:** es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

II. **Gusanos:** se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno.

Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus. Por ejemplo, un programa gusano que eventualmente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

III. **Bomba lógica o cronológica**: exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son

difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su "detonación" puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

IV. **Acceso no autorizado a servicios y sistemas informáticos**: se produce por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

V. **Piratas informáticos o hackers:** el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a diversos medios de ingreso.

El delincuente aprovecha la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

d) **Reproducción no autorizada de programas informáticos de protección legal:** Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales.

El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual. Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

Acceso no autorizado: uso ilegitimo de contraseñas y la entrada de un sistema informático sin la autorización del propietario.

Destrucción de datos: los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.

Infracción al copyright de bases de datos: uso no autorizado de información almacenada en una base de datos.

Interceptación de correo electrónico: lectura de un mensaje electrónico ajeno

Estafas electrónicas: a través de compras realizadas haciendo uso de la red.

Transferencias de fondos: engaños en la realización de actividades bancarias electrónicas.

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos como lo son:

Espionaje: acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

Terrorismo: mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

Narcotráfico: transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

Otros delitos: las mismas ventajas que encuentran en el Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o viceversa.

El Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos menciona que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada.

De tal manera, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

1.- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.

2.- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

3.- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.

4.- No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

5.- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

6.- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Teniendo presente esa situación, es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. En consecuencia, es necesario que, para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un

régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada.

3.2 Legislación de los delitos cibernéticos en diversos países.

Penalización de los Delitos cibernéticos en México.

A continuación, se habla de la regulación que han tenido los delitos cibernéticos en la legislación mexicana y las conductas ilícitas relacionadas con la informática. Debe aclararse que hasta el momento las leyes regulan los delitos informáticos ya que su competencia es la de sancionar administrativamente conductas ilícitas cuyo bien jurídico a tutelar es la propiedad intelectual.

A nivel internacional se considera que no existe una definición propia del delito informático o delito cibernético, sin embargo, diferentes autores que se han ocupado del tema, y aun cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas, en el caso de México, destaca el autor Julio Téllez Valdés el cual menciona que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de ‘delitos’ en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión ‘delitos informáticos’ esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos, no ha sido objeto de tipificación aún".

Para el autor Carlos Sarzana, en su obra Criminalita e Tecnología, menciona que los crímenes por computadora comprenden "*cualquier comportamiento criminógeno*

en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

Por otro lado, Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "*las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin", y por las segundas, "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin*". Según Téllez Valdés, este tipo de acciones presentan las siguientes características principales:

1.- Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

2.- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

3.- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

4.- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.

5.- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

6.- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

7.- Son muy sofisticados y relativamente frecuentes en el ámbito militar.

8.- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

9.- En su mayoría son imprudenciales y no necesariamente se cometen con intención.

10.- Ofrecen facilidades para su comisión a los menores de edad.

11.- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

12.- Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como delitos informáticos, delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadora, delincuencia relacionada con el ordenador.

Se considera como delitos informáticos todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen uso indebido de

las tecnologías de información y comunicación como medio por el cual se cometen ciertas actividades o conductas ilícitas.

El artículo 217 del Código Penal para el Estado de Sinaloa en México, fue el primer estado de este país en tipificar el Delito Informático; y casualmente es el único que lo denomina así. En dicho artículo, se dispone que al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa. Establece que comete delito informático, la persona que dolosamente y sin derecho, use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información (fracción I); o; Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red (fracción II).

Penalización de los Delitos cibernéticos en Alemania.

Para hacer frente a la delincuencia relacionada con los delitos informáticos Alemania a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Violación al ámbito de la intimidad personal y al ámbito del secreto personal los cuales se contemplan en su código penal los siguientes delitos:

1.- Piratería informática (Articulo 202 a).

Quien sin autorización se procure para sí o para otros datos que no estén destinados para él y que estén especialmente asegurados contra su acceso no autorizado, será castigado con pena privativa de la libertad hasta tres años o con multa.

Datos en el sentido del inciso 1, son solo aquellos que se almacenan o trasmiten en forma electrónica, magnética, o de otra manera en forma no inmediatamente perceptible.

2.- Estafa informática o Estafa por computador (Articulo 263 a).

Quien, con el propósito, de procurarse para sí o para un tercero una ventaja patrimonial antijurídica, en la medida en que él perjudique el patrimonio de otro, por una estructuración incorrecta del programa, por la utilización de datos incorrectos o incompletos, por el empleo no autorizado de datos, o de otra manera por medio de la influencia no autorizada en el desarrollo del proceso, será castigado con pena privativa de la libertad hasta cinco años o con multa.

4.- Alteración de datos (303 a): es ilícito cancelar, inutilizar o alterar datos, inclusive la tentativa es punible.

5.- Sabotaje informático (303 b): destrucción de datos de especial significado por medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.

6.- Utilización abusiva de cheques o tarjetas de crédito (266b). Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causación del error y disposición patrimonial en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del

programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita. Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue también adoptada en los países escandinavos y en Austria.

El legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho Penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos.

Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente

por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician, además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos.

El tipo de daños protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.

Penalización de los Delitos cibernéticos en Francia.

En el caso de Francia La Ley Número 88-19 de 5 de enero de 1988, sobre el fraude informático, menciona lo siguiente:

1.- Acceso fraudulento a un sistema de elaboración de datos (462-2): en este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él, y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

2.- Sabotaje informático (462-3): en este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

3.- Destrucción de datos (462-4): en este artículo se sanciona a quien, intencionadamente y con menosprecio de los derechos de los demás, introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o de transmisión.

4.- Falsificación de documentos informatizados (462-5): en este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

5.- Uso de documentos informatizados falsos (462-6): en este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

Penalización de los Delitos cibernéticos en Gran Bretaña.

Gran Bretaña debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado hasta con cinco años de prisión o multas. Esta ley tiene un apartado que específica la modificación de datos sin autorización. Los virus están incluidos en esa categoría. El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.

Penalización de los Delitos cibernéticos en Holanda.

En Holanda el 1 de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza el hacking, el phreaking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría) y la distribución de virus. La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño. Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

Penalización de los Delitos cibernéticos en España.

En el Nuevo Código Penal de España, el art. 263 señala que se impondrá sanción a quien causare daños en propiedad ajena. En tanto, el artículo 264-2) establece que se aplicará la pena de prisión de uno a tres años y multa a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El Nuevo Código Penal de España sanciona en forma detallada esta categoría delictual (violación de secretos, espionaje, divulgación), aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa, y cuando el hecho es cometido por funcionarios públicos se penaliza con inhabilitación. En materia de estafas electrónicas, el Nuevo Código Penal de España, en su artículo 248, sólo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

Penalización de los Delitos cibernéticos en Chile.

Chile fue el primer país latinoamericano en sancionar una Ley Contra Delitos Informáticos, la cual entró en vigencia el 7 de junio de 1993. Según esta ley, la destrucción o inutilización de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus. Esta ley prevé en el Art. 1 el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta sea tendiente a impedir, obstaculizar o modificar

su funcionamiento. En tanto, el Art. 3 tipifica la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

Los delitos informáticos se encuentran regulados en Chile en tres normas legales: Ley N° 19.2231 , que tipifica figuras penales relativas a la informática; Ley N° 17.3362 , sobre Propiedad Intelectual; y la Ley N° 19.9273 , que modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal en materia de delitos de pornografía infantil.

Ley N° 19.223, que tipifica figuras penales relativas a la informática, cubre adecuadamente las figuras tradicionales de comisión de delitos informáticos, distinguiendo entre sabotaje, espionaje y fraude, informáticos, pero no se adecua a las nuevas formas de comisión, dadas por el avance de la tecnología y la modificación de los conceptos normativos utilizados en la ley, relativos a la tecnología.

De acuerdo a los autores Chilenos Marcelo Huerta y Claudio Líbano, las figuras penales nacionales de la Ley Nº 19.223 pueden clasificarse de la siguiente manera:

1.- Delitos de sabotaje informático: Este delito se tipifica de la siguiente manera en la Ley Nº 19.223:

a. Atentados contra un sistema de tratamiento de la información o de sus partes componentes (artículo 1º, primera parte).

b. Atentados contra el funcionamiento de un sistema de tratamiento de la información (artículo 1º, segunda parte).

c. Atentados contra los datos contenidos en un sistema automatizado de tratamiento de la información (artículo 3º).

2. Delitos de espionaje informático: Se tipifican de la siguiente manera en la Ley Nº 19.223:

a. Delitos de apoderamiento, uso o conocimiento indebido de la información contenida en un sistema automatizado de tratamiento de la información (artículo 2º).

b. Delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información (artículo 4º).

Penalización de los Delitos cibernéticos en Estados Unidos.

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un Caballo de Toya, etc., y en qué difieren de los virus, la nueva ley sanciona la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas (18 U.S.C). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus. El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos.

El Acta define dos niveles para el tratamiento de quienes crean virus, estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta diez años en prisión federal más una multa, y para aquellos que lo transmiten sólo de manera imprudencial, la sanción fluctúa entre una multa y un año en prisión.

El creador de un virus no podrá escudarse en el hecho de que no conocía que con su actuar causaría daño a alguien o que él solo quería enviar un mensaje. Con esta inclusión se elimina la concepción de que el sujeto activo debía poseer conocimientos superiores para la realización de estos actos. En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos al sistema informático en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo. En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos, pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley.

Sin embargo, es importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en las que, entre otras, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de diez mil dólares por cada persona afectada y hasta cincuenta mil dólares el acceso imprudencial a una base de datos.

3.3 Medidas de prevención y recomendaciones ante los delitos cibernéticos.

A continuación, se presentan algunas recomendaciones del país de México con colaboración de su Secretaria de Seguridad Pública del estado de Veracruz, las cuales se dirigen de manera general a niños, jóvenes, adultos, adultos mayores, docentes y padres de familia para que no sean partícipes de este tipo de delitos:

En la 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 en un local que presta el servicio de internet:

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

Recomendaciones para los padres.

1.- La utilización de herramientas de eliminación de software malintencionado para buscar, prevenir, detectar y eliminar este tipo de programas maliciosos como por ejemplo un antivirus y un firewall. Este último es un programa que monitorea la entrada y salida de información entre su computadora e Internet.

2.- Compruebe que el sitio de su banco o donde piensa comprar cuente con las

señales de seguridad.

3.- 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.

4.- Procure usar un seudónimo y evite colocar el nombre, fotos y dirección electrónica de sus hijos en guías y perfiles públicos, a fin de proteger su identidad.

5.- No abra correos electrónicos de remitentes desconocidos ni archivos ejecutables (.exe) porque pueden contener virus que dañen a su computadora y a todos sus archivos.

6.- Establezca, junto con sus hijos, la hora y reglas del uso de Internet y procure que naveguen bajo su supervisión, porque no sabe qué información puedan bajar y corren el riesgo de que abran páginas con pornografía.

Si usted nota las siguientes características en un menor:

1. Se muestra triste y apático.

2. Rehúsa el acercamiento del adulto.

3. Se oculta frecuentemente.

4. Llora y/o se muestra ansioso.

Es una señal de que ha sido maltratado, el maltrato es la agresión física y/o psicológica generada por actos institucionales, familiares o sociales, de acción u omisión por parte de aquellas personas encargadas del cuidado del menor. Por ejemplo: Cuando un niño o niña entra en comunicación con un adulto y cree que está platicando con alguien de su misma edad, y a través de engaños el adulto lo seduce, amenaza e intimida, o manipula sus sueños, ilusiones, emociones y sentimientos.

Recomendaciones para los alumnos:

1.- No todo lo que se ve por Internet o la Web, es real. De hecho, hay servicios y propuestas falsas y peligrosas.

2.- El estar conectados a la red por largas horas todos los días podría generarnos comportamientos antisociales y de aislamiento.

3.- Recuerda que una vez que colocas la información en línea no la puedes retirar tan fácilmente.

4.- Antes de asociarte a un sitio de redes sociales, analiza detenidamente las diferentes opciones que te ofrecen.

5.- Coquetear o seducir en línea con extraños puede tener graves consecuencias.

6.- 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.

7.- 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 "cyberbullying", que es la “ciber-intimidación” realizada por compañeros del entorno escolar o social que intimidan o amenazan por mail anónimos.

8.- Cuando veas o recibas algo en Internet que te haga sentir incómodo/a o amenazado/a, debes hablar inmediatamente con tus padres.

9.- 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.

10.- Si recibes mensajes en los cuales buscan seducirte, te ilusionan, te amenazan, te chantajean o te intimidan, platícalo con un adulto de tu confianza.

11.- 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.

12.- Nunca debes publicar información personal como número telefónico familiar o celular, dirección o nombre de tu escuela.

13.- Comparte tus contraseñas solo con una persona de tu confianza.

14.- Observa siempre un buen comportamiento en línea y no hagas nada que pueda molestar o enojar a otras personas o que sea ilegal.

15.- Nunca hagas nada en Internet que cueste dinero sin que lo sepan tus padres.

16.- Deja que tus padres sepan tu nombre de inicio de sesión en Internet y las direcciones de los chats que visitas.

Te sugerimos cuidarte ante todo de páginas donde:

1.- 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.

2.- Traten de solicitarte información sobre tu condición económica.

3.- No utilices tu nombre ni tu fecha de correo electrónico para nombrar tu dirección de correo electrónico.

4.- Para navegar protegido consulta la página: www.navegaprotegido.org.mx.

Para hacer una denuncia escribe a: delito cibernético_pf@ssp.gob o llama al teléfono: 01800 440 36 90.

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.: # $ % ¿ ¡). 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.

1.- 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.

2.- Cambie las contraseñas con regularidad, al menos cada 90 días. De este modo, es posible limitar el daño causado por alguien que ya haya accedido a su cuenta.

3.- Si observa algo sospechoso con alguna de sus cuentas en línea, lo primero que debe hacer es cambiar su contraseña.

Recomendaciones para los docentes:

1.- Evite bajar software gratuito ya que la mayoría contienen spyware (programas espía) que se instalan automáticamente en su computadora.

2.- Utilice programas que ayuden a filtrar el contenido de sitios de Internet.

3.- Revise su máquina periódicamente y recurra a técnicos especializados para que la limpien de todo tipo software malicioso.

4.- Indague sobre las opciones de privacidad de la información que le brinda su proveedor de servicios de Internet.

5.- Mantenga una supervisión del uso de Internet al interior de la escuela.

6.- Vigile a sus alumnos cuando naveguen en Internet para que no proporcionen sus datos personales o los de su familia.

7.- Durante el recreo esté al pendiente por si observa que alguien toma fotos a sus alumnos.

8.- Si detecta a una víctima de maltrato, canalícela a una institución especializada.

9.- Prohíba el uso de celular al interior de la escuela, ya que puede usarse para comunicarse inadecuadamente con personas adultas que pueden maltratar al menor.

Algunos alumnos capturan fotos con su celular de otros compañeros en situaciones incomodas o lo usan para grabar videos de índole sexual o peleas que posteriormente sube a la red, esto puede causar conflictos personales e implicaciones legales para el autor, por lo que es vital hacer partícipe a los padres de familia en la prevención de un probable delito.

Paginas recomendadas que hablan sobre el maltrato infantil:

Maltrato infantil. Página www.rionet.com.ar

¿Qué es el Maltrato infantil? La violencia contra los niños. www.vidahumana.com

Recomendaciones para los padres:

1.- Cuando usted detecte un caso de abuso sexual de un menor, no intente brindarle ayuda, pues no es el experto y podría causar un daño mayor, mejor canalícelo a una institución especializada.

2.- Ubique dónde están sus hijos en todo momento, procure conocer a sus amigos, gustos y actividades cotidianas.

3.- Enséñeles a confiar en sus instintos y en su cuerpo para reconocer una caricia con malas intenciones de la que no lo es. Dígale que tiene derecho a decir no a lo que sienta que está mal.

4.- Esté alerta de los amigos, familiares o maestros que le prestan atención exagerada o poco usual a sus hijos, pues puede que esté en riesgo su integridad.

5.- Recuerde que los menores no deben ser forzados a mostrar afecto a un adulto o joven si no lo desea. Además, ponga especial atención cuando su hijo(a) esté tratando de evitar a alguien y sobre todo, escuche cuidadosamente SIN ALTERARSE NI PROFERIR AMENAZAS NI INSULTOS cuando le cuente cómo se siente con respecto a otras personas, recuerde que una cabeza fría actúa más eficazmente.

Recomendaciones para los docentes:

Cuando usted detecte un caso de abuso sexual de un menor, no intente brindarle ayuda, pues no es el experto y podría causar un daño mayor, mejor canalícelo a una institución especializada.

Enséñeles a sus alumnos a confiar en sus instintos y en su cuerpo para reconocer una caricia con malas intenciones de la que no lo es. Dígale que tiene derecho a decir no a lo que sienta que esté mal.

Recuerde que, si algún padre de familia, familiar, autoridad escolar, conserje o personal administrativo muestra inclinaciones o preferencias por un alumno, denúncielo al 089 o acuda a una agencia del ministerio público especializada en delitos sexuales y contra la familia.

Recomendaciones para los alumnos:

Los sujetos que traten de seducirte o tocarte a cambio de darte un regalo están cometiendo un delito Recuerda: tu cuerpo es privado y nadie tiene derecho a tocarlo.

Narcomenudeo:

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" para inhibir el apetito, relajarse, activar sus músculos, quitar el estrés, etc., 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. Está tipificado como delito federal contra la salud.

Recomendaciones para los padres:

1.- Platique en familia sobre el tema del consumo, uso y abuso de drogas. Que no le cause pena ni temor, es mejor prevenir que lamentar el silencio.

2.-Si sus hijos van a discotecas, aconséjeles tener cuidado con las personas que pretendan inducirlos al consumo de drogas. Hágales saber que nadie puede obligarlos a consumirlas.

3.- Hable con sus hijos del riesgo de consumir drogas.

4.- Tenga en cuenta que es una realidad que cada día disminuye la edad de inicio de consumo de diferentes sustancias adictivas.

5.- Infórmeles que pueden denunciar la venta de droga, su suministro gratuito o las amenazas para que las consuman al número telefónico 089 de denuncia Anónima, es gratis y funciona los 365 días del año.

6.- Esté consciente de que luchar contra el Narcomenudeo es una labor compartida entre gobierno y sociedad, por ello resulta indispensable comprometer a la ciudadanía con la denuncia, la prevención, y la rehabilitación.

Vender drogas o distribuirlas es un delito, si sabe de alguien que lo hace, denúncielo al 089. (Número Telefónico disponible en todo México)

Recomendaciones para los maestros:

1.- Vender drogas o distribuirla en el exterior o interior de la escuela es un delito, si sabe de alguien que lo hace, denúncielo al 089.

2.- Refuerce el siguiente mensaje a los alumnos: consumir drogas no es atreverse a ser diferente, es autodestruirse.

3.- Identifique y enfatice las fortalezas y cualidades de sus alumnos, acéptelos para que ellos se acepten como son.

Recomendaciones para los alumnos:

1.- Platica con tus amigos y en familia sobre el tema del consumo, uso y abuso de drogas, no te debe causar pena ni temor.

2.- Recuerda que los narcomenudistas siempre innovan la forma de envolverte en el mundo de las drogas, ponte alerta y no te dejes sorprender.

3.- Vender drogas o distribuirla en el exterior o interior de la escuela es un delito federal, si sabes de alguien que lo hace, denúncialo al 089.

Denuncia Anónima.

El 089 es el número telefónico que se debe marcar si se desea realizar una denuncia anónima; atiende llamadas las 24 horas del día los 365 días del año. En el 089 no se identifica el número telefónico de la persona que llama y no se solicitan los datos personales del denunciante.

Conclusión

En los últimos años los delitos cibernéticos han aumentado, y son los que difícilmente son sancionados, dado a la dificultad que estos presentan, puesto que se puede permanecer en el anonimato y solo basta con contar con un computador o un Smartphone y tener acceso a internet para realizar todo este tipo de conductas delictivas, se puede tener acceso a todo tipo de información desde la información personal de un individuo, hasta la base de datos de una institución, incluso existen ciertos delitos más sofisticados como lo es el Hacking que llegan al grado de presentar una amenaza para las naciones, puesto que la mayoría de las instituciones gubernamentales de cada país contienen bases de datos con información de suma importancia y se les puede acceder desde el internet.

De tal forma la delincuencia ha sacado provecho a esta situación, a medida que avanza la tecnología se requieren ciertas habilidades o técnicas para conseguir datos o información, las conductas delictivas se han ido adaptando con los avances tecnológicos por tal motivo es importante tener conocimiento sobre la prevención de la suministración de información a los medios tecnológicos es importante prevenir y disminuir el índice de vulnerabilidad ante los delitos cibernéticos, teniendo en cuenta que todos somos propensos a este tipo de conductas o delitos, se han tomado algunas medidas de seguridad sin embargo aún son muy deficientes e incluso son de difícil comprensión y acceso para la sociedad en general, puesto que la mayoría de las personas omite las medidas de seguridad por su largo contenido de información.

Para concluir con este tema de gran interés y de preocupación, se puede señalar que, dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática.

Asimismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (microprocesadores, inteligencia artificial, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar puesto que se observa el gran potencial de la actividad informática como medio de investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de los ordenadores.

Finalmente, debe destacarse el papel de cada país puesto que son el principal e indelegable regulador de la actividad de control del flujo informativo a través de las redes informáticas.

Bibliografía.

Amoroso Fernández, Yarina. La informática como objeto de derecho. Algunas consideraciones acerca de la protección jurídica en Cuba de los Datos Automatizados en Revista Cubana de Derecho. Unión Nacional de Juristas de Cuba. No. 1. Habana, Cuba. 1991. P.43.

Artega S., Alberto. El delito informático: algunas consideraciones jurídico penales Revista de la Facultad de Ciencias Jurídicas y Políticas. No. 68 Año 33. Universidad Central de Venezuela. 1987. Caracas, Venezuela. P. 125-133.

Bierce, B. William. El Delito De Violencia Tecnológica en la Legislación de Nueva York Derecho de la Alta Tecnología. Año 6 No. 66 Febrero 1994. Estados Unidos. P.20.

Boix Palop,Andres(2002), Libertad de expresión y pluralismo en la red, Revista española de derecho constitucional, Madrid.

Cepal (2003b). Los caminos hacia una sociedad de la información en América Latina y el Caribe. Santiago de Chile. [Versión electrónica]. Fecha de consulta: 02/04/07.

Cabrera, josé (2004). «Navigators and castaways in cyberspace: psychosocial experience and cultural practices in school children's appropriation of the Internet». En: m. bonilla; g. cliché (eds.). Internet and Society in Latin America and the Caribbean (pág. 21-86). [Versión electrónica]

Cabrero, J. (1994): "Nuevas tecnologías, comunicación y educación", Comunicar, 3, 14-25.

Carbonell, Miguel (2002),Notas sobre la regulación constitucional de los medios electrónicos de comunicación, Boletín Mexicano de Derecho comparado, México.

Carpizo, Jorge (coords.), Derecho a la información y derechos humanos. Estudios en homenaje al maestro Mario de la Cueva, México, IIJ, UNAM, 2000.

Castells, Manuel (1997), La era de la información, vol. 1: La sociedad red, Madrid, Alianza.

Del Pont K., Luis Marco y Nadelsticher Mitrania, Abraham.Delitos de Cuello Blanco y Reacción Social. Instituto Nacional de Ciencias Penales. México. 1981.

Cmsi (Cumbre Mundial para la Sociedad de la Información) (2003). Declaración de Principios y Plan de Acción, Ginebra. [Versión electrónica]. Recuperada el 25 de marzo de 2007.

Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal. Contiene las reformas conocidas hasta el 20 de enero de 1997. Greca. Tercera Edición. 1996.

Código Penal y de Procedimientos Penales del Estado de Sinaloa. Anaya 1996. México D.F.

Código Penal y Legislación complementaria española 3 de noviembre del 2016.

Código Penal Alemán del 15 de mayo de 1871, con la última reforma del 31 de enero de 1998.

Código Penal de Chile 18 de marzo del año 2010.

Derechos fundamentales y Estado. Memoria del VII Congreso Ibero-americano de Derecho Constitucional, México, 2002.

Derecho de acceso a la información y organización ciudadana en México", Alegatos, México, núm. 50, enero-abril de 2002.

Durkheim, Émile, Educación y Sociología, Ediciones Península, Barcelona, 2003.

Desantes Guanter, José María, El derecho a la información en el con-texto de los derechos humanos, Revista de Investigaciones Jurídicas de la ELD, México, año 12, núm. 12, 1988.

Escobar, Guillermo y Villanueva, Ernesto (coords.), Nuevas tendencias del derecho de la comunicación. Visiones desde España y México, México, UIA, Lito-fasesa, 2000.

Ferri, E. (1895). Sociologia Criminal.

Hance, Olivier. Leyes y Negocios en Internet. México. De. Mc Gram Hill Sociedad Internet. México. 1996.

Huerta, Marcelo y Líbano, Claudio. Delitos Informáticos, Editorial Jurídica Conosur Ltda., Santiago. 1996, p. 123, Informe Relativo a las Diligencias e Investigación de los Delitos Informáticos contemplados en la Ley N° 19.223 y al Fraude Informático". Disponible en: http://bcn.cl/h3ma (Enero, 2017).

Lima De La Luz, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. No. 1-6. Año L. Enero-Junio 1984.

Los derechos fundamentales en México, 2a. ed., México, UNAM-Porrúa-CNDH, 2005.

Minutti Zanatta, R. (2011) Acceso a la información pública y a la justicia administrativa en México.

Mir Puig,S (Comp.) Delincuencia Informática. Promociones y Publicaciones Universitarias. Barcelona, 1992.

Rodríguez Manzanera, L. (1991) Criminología. México: Porrúa.

Romo Medina, M. (1989) Criminología y derecho. México: Universidad Autónoma de México.

Toniatti, Roberto. Libertad Informática y Derecho a la Protección De Los Datos Personales: Principios de Legislación Comparada. Revista Vasca de Administración Pública. No. 29, Enero-Abril, 1991, España. P.139 -162.

Valenzuela Espinoza, César M., Cultura de la legalidad e información pública: Derecho Comparado de la Información, México, núm. 4, julio-diciembre de 2004

Villatoro, pablo; silva, allison (2005). Estrategias, programas y experiencias de superación de la brecha digital y universalización del acceso a las nuevas tecnologías de la información y comunicación (TIC). Un panorama regional. Santiago (Chile): CEPAL.

Zavala, Antelmo. "El impacto social de la informática jurídica en México". Tesis. México. UNAM. 1996.

Documentos de sitos webs.

Apis, J. E. (s.f.). biblio.juridicas.unam. Recuperado el 01 de 12 de 2015, de biblio.juridicas.unam: http://biblio.juridicas.unam.mx/libros/1/419/20.pdf

Biblioteca del congreso nacional de chile: https://www.leychile.cl/Navegar?idNorma=1984 Codigo Penal Aleman Traducido: https://www.unifr.ch/ddp1/derechopenal/obrasjuridicas/oj_20080609_13.pdf, Claudia López Díaz.

Congresonacionaldechile Recuperado el 05 de 01 de 2016, de https://www.camara.cl/pdf.aspx?prmTIPO=DOCUMENTOCOMUNICACIONCUENTA&prmID=11020

Delitosinformaticos. (2015). Departamento de Peritaje Informático. Recuperado el 01 de 12 de 2015, de Departamento de Peritaje Informático: http://www.delitosinformaticos.info/delitos_informaticos/tipos_delitos.html

Delitosinformaticos. (21 de 08 de 2015). http://www.delitosinformaticos.mx/. Recuperado el 01 de 12 de 2015, de http://www.delitosinformaticos.mx/: http://www.delitosinformaticos.mx/

Granados, M. d. (s.f.). ordenjuridico. Recuperado el 01 de 12 de 2017, de ordenjuridico: http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf

Internetparatodos. (13 de Agosto de 2015). internetparatodos. Recuperado el 01 de 12 de 2015, de internetparatodos: http://internetparatodos.mx/

Jan, E. (12 de Abril de 2015). crimecongress. Recuperado el 01 de 12 de 15, de crimecongress: http://www.un.org/es/events/crimecongress2015/cibercrime.shtml

Peñaloza, P. (2005). criminologiaysociedad. Recuperado el 01 de 12 de 2015, de criminologiaysociedad:http://www.criminologiaysociedad.com/articulos/archivos/SeguridadPublica-LacrisisdeunParadigma.pdf

Salazar, S. A. (1 de Enero de 2013). Revista Digital Universitaria. Recuperado el 01 de 12 de 2015, de Revista Digital Universitaria: http://www.revista.unam.mx/vol.14/num2/art15/art15.pdf

Libien, H. R. (s.f.). ordenjuridico. Recuperado el 01 de 12 de 2015, de ordenjuridico: http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf

Pino, S. A. (s.f.). http://www.oas.org/. Recuperado el 01 de 12 de 2015, de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Ruiz, J. E. (12 de 2015). http://www.ijf.cjf.gob.mx/. Recuperado el 01 de 12 de 2015, de http://www.ijf.cjf.gob.mx/: http://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf