325

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES.

CAMPUS ARAGÓN

CREACIÓN DEL TIPO PENAL DE DELITOS CIBERNÉTICOS EN EL CÓDIGO PENAL FEDERAL MEXICANO.

T E S I S

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN DERECHO

P R E S E N T A :

FRANCISCO MORENO ESCOBAR

ASESOR DE TESIS :
LIC. MARÍA GUADALUPE DURAN ALVARADO

MÉXICO, 2001

Dedicatorias.

A Dios

Por darme la oportunidad de tener esta vida
y compartirla con aquellos que me rodean.

A mis padres

C.P. Francisco Moreno y Sra. Ofelia Escobar a quienes estoy infinitamente agradecido por enseñarme a vivir y por el apoyo que incondicionalmente me han dado en cada una de las metas que me he fijado.

A mi hermana

Alma Delia por su compañía, respaldo y comprensión con que he contado en todo momento.

A mis Tios, primos y sobrinos

quienes me han acompañado a lo largo de
mi vida y han sido un ejemplo a seguir.

A los H. miembros de la Asamblea La Bohemia

a ellas y ellos con quienes compartí lo mejor de mi época de estudiante a quienes agradezco su compañía, consejos y apoyo .

A mis amigos

Miriam, Carlos Ocampo, Eduardo y Benjamin quienes han estado presentes en mis éxitos y fracasos brindándome siempre su amistad.

A mis compañeros y amigos
de la Coordinación de auxiliares

quienes me han ayudado a aprender
y a desarrollarme como profesionista.

A mi alma mater

la Universidad Nacional Autónoma de México por la oportunidad de ser educado en su regazo y desarrollarme como persona.

A mi asesora

Profesora María Guadalupe Durán Alvarado
quien con sus consejos y conocimientos hizo posible que se alcanzara esta meta.

ÍNDICE

ÍNDICE

Página

CAPITULO 3. LEGISLACIONES INTERNACIONALES Y REFERENCIAS NACIONALES ACERCA DE LA INFECCIÓN DE EQUIPOS DE CÓMPUTO POR VIRUS CIBERNÉTICOS.

CAPÍTULO 4. CREACIÓN DEL TIPO PENAL DE DELITOS CIBERNÉTICOS EN EL CÓDIGO PENAL FEDERAL MEXICANO.

INTRODUCCIÓN

INTRODUCCIÓN

El saber computación en nuestros días es de suma importancia , ya que toda nuestra vida gira alrededor de una computadora o en algunos casos de redes de información; esta necesidad ha provocado que el menor de los problemas en los sistemas de cómputo se traduzca en daños, algunas veces irreparables en nuestros negocios, academias o vida común.

Dicho problema se agudiza cuando delincuentes con conocimientos de computación, con toda mala fe, colocan *virus* en nuestros sistemas logrando dañarlos en sus archivos más insignificantes, como en sus unidades físicas, esto es, el daño no solo se limita a la información si no que puede afectar a la memoria de la máquina, a sus componentes físicos como son disco duro, monitores, dispositivos de audio y video etc. y tal vez esto no sea lo más peligroso, si no la posibilidad en redes e Internet de transmitir el virus a una infinidad de usuarios que solo se percatarán de la existencia del virus en sus computadoras una vez que ésta presente los primeros (y en algunos casos, fatales) *síntomas de la infección*

Los autores de libros de estos temas no se ponen de acuerdo respecto del origen de los virus computacionales, sin embargo la mayoría apuntan a dos fuentes. Los primeros señalan que este problema tuvo su origen como un simple juego creado por estudiantes del Instituto de Massachusetts que consistía en bombardear al programa contrincante sin que este se diera cuenta, pudiendo alterar la estructura del programa atacado. Otros señalan que el *boom* de los virus se debió a los esquemas de

protección (que no son otra cosa que virus creados con permiso) que los programadores crearon para proteger su autoría sobre determinados programas.

Ahora bien, sea cual sea el origen de los virus se debe tener en cuenta que en la actualidad muchos sujetos abusan de sus conocimientos y por diversión instalan la más amplia gama de virus en nuestros sistemas de cómputo y redes.

Esta situación ya ha provocado severos problemas en el mundo; cabe mencionar como ejemplo el virus del amor o *I Love You*, que en fecha reciente se distribuyó a través de la Internet y ocasionó pérdidas millonarias.

Pero este problema no solo se restringe a las grandes redes y a las noticias de la televisión; los virus se pueden presentar en las instituciones educativas o de investigación echando a perder años de investigación por la ocurrencia de algunos individuos

Desgraciadamente la actual tecnología no ha podido frenar el avance destructor de los virus cibernéticos, por el contrario lo a acrecentado; por cada nuevo sistema operativo, programa o vacuna, surge un nuevo virus completamente nuevo y por tanto, desconocido, para el cual no existe vacuna.

Pero estos datos son solo la punta de un Iceberg sumamente peligroso; los ataques más comunes de virus cibernéticos van dirigidos a las Instituciones Públicas, mismas

que por lo menos en nuestro país se encuentran completamente indefensas ante la infección generalizada de los equipos de cómputo que guían nuestra vida diaria.

Es por lo antes expresado, que la propuesta a plantear es sancionar a todas aquellas personas físicas que de manera dolosa infecten, destruyan, modifiquen, o alteren por cualquier medio los sistemas de cómputo de terceros, ya que en la actualidad no existe algún tipo penal que prevea y sancione las citadas conductas delictivas quedando los probables responsables totalmente impunes.

La idea va enfocada a sancionar únicamente a personas físicas, ya que como se mencionó antes, algunas empresas de programación utilizan algunos virus para defenderse de la piratería tan en boga, por lo que de sancionarlos podríamos dar solución a parte del problema, pero desataríamos otro de la misma importancia del que se pretende regular.

El ámbito de aplicación de dicha norma se debe restringir al territorio nacional, esto es, que el virus sea creado y difundido dentro del territorio nacional, lo anterior en razón de no entrar en conflictos de leyes, propios del Derecho Internacional Privado.

La sanción propuesta deberá ser en razón a los medios que utilizó el delincuente para infectar; se debe considerar si su actuar fue doloso o culposo y en particular se debe sancionar mayormente a quien abusa de sus conocimientos con el fin de perjudicar a terceros.

En el mismo sentido la acreditación del cuerpo del delito y de la probable responsabilidad se comprobará mediante el auxilio de peritos, quienes deberán ser profesionistas de la informática, esto con el fin de que con sus conocimientos teórico - prácticos auxilien a la Representación Social en la correcta integración de la averiguación previa.

Como requisito de procedibilidad, se estima conveniente recurrir a la denuncia y al seguimiento de oficio por el Ministerio Público, esto en razón de que es un delito que afecta a los intereses de toda la sociedad .

Para el desarrollo del tema propuesto, en el capítulo primero nos remontaremos a los albores de la computación, ya que sería muy complicado intentar abordar el problema planteado sin saber que es una computadora , qué son y cómo funcionan las redes e Internet.

En el capítulo segundo tocaremos el tema medular de la investigación, los virus cibernéticos. Para tal fin indagaremos en las causas que les dieron origen, su clasificación y funcionamiento además de señalar los daños que provocan en redes e Internet.

El capítulo tercero nos servirá para observar como otros países han hecho frente a los multicitados virus, analizaremos sus propuestas y recogeremos lo mejor de ellos para alcanzar una propuesta clara y útil del como sancionar a los *delincuentes cibernéticos*.

Por último y con los datos recopilados en los capítulos anteriores, integraremos el capítulo cuarto que consistirá en la propuesta del tipo penal de Delitos Cibernéticos, abordando el ámbito territorial de aplicación, requisitos de procedibilidad y acreditación del tipo propuesto.

El método empleado para la investigación será el deductivo en los primeros dos capítulos ya que partiremos de la idea general de la idea particular de la computación, enfocándonos primordialmente en los virus cibernéticos y el analítico-comparativo en los dos últimos ya que se realizará el análisis comparativo de varias legislaciones internacionales para poder establecer un tipo penal adecuado a la realidad planteada.

Para documentar la presente indagatoria me auxiliaré de los medios tradicionales, como son los libros y revistas, pero además haré uso de la Internet que hoy en día representa una herramienta amplísima de conocimiento e investigación.

Finalmente, lo que persigue la presente investigación es arrojar un poco de luz sobre este tema, ya que el avance de la tecnología puede, en un momento dado, superar en mucho nuestra legislación penal por no tener una visión amplia del problema que se plantea desde su origen. Debemos tomar en cuenta que las consecuencias de seguir ignorando los posibles problemas ocasionados por un *virus de computadora* en un mundo interconectado son muy serias (tanto económicamente como políticamente), por lo que se requiere tomar conciencia del problema planteado y prever una solución.

CAPÍTULO I

HISTORIA DE LA COMPUTACIÓN

DESARROLLO DE LA COMPUTACIÓN

El hombre para realizar sus labores, ha buscado allegarse aquellas herramientas que faciliten su trabajo; en algunos casos a buscado su comodidad y ha llegado a desear que la máquina trabaje por el.

Éste ánimo impulsó a científicos e investigadores a dedicar sus esfuerzos a crear una máquina que fuera útil para la realización de múltiples trabajos. El matemático inglés Charles Babbage[1], fue el primero en idear una computadora digital real. Lo que buscaba Babbage era crear una *máquina analítica*, pero debido a las limitaciones de su tiempo (1792-1871) nunca la hizo funcionar adecuadamente, pues su diseño era puramente mecánico, sin contar con un *sistema operativo* que le dictara las instrucciones para ejecutar determinada tarea.

No fue sino hasta después de la Segunda Guerra Mundial, cuando investigadores del Instituto de Estudios Avanzados de Princenton y de la Universidad de Pensylvania obtuvieron éxito en la construcción de máquinas de cálculo, pero estos aparatos empleaban grandes tubos de vacio, y era necesario que gente especializada manejara su funcionamiento.

A partir de estos inventos se empieza a desarrollar la idea de programar a un aparato para realizar una determinada actividad, pero el desarrollo tecnológico de esos momentos es muy limitado, por lo que la programación de una máquina requería

[1] Tanenbaum S. Andrew - Sistemas operativos, diseño e implementacion Ed. Prentice Hall Hispanoamericana, Mexico 1988, pag. 5

grandes espacios, ya que se empleaban tablas del tamaño de una pared, enchufes y se dependía de los tubos de vacío los cuales tenían el gran problema de que si se fundían durante la ejecución de algún programa, se tenía que volver a empezar todo el trabajo, desperdiciando mucho tiempo en la solución de este problema. Aunado a las fallas técnicas del aparato se sumaban las fallas humanas en los cálculos e instrucciones que se le daban a la máquina, ya que todas las instrucciones que se le daban partían del principio de cálculos numéricos directos, como la elaboración de tablas de senos y cosenos.

Para el año de 1950 los problemas de programación se empezaron a solucionar con el uso de tarjetas perforadas que eliminaban el uso de tableros enchufables, disminuyendo con estos los errores y desperdicio de tiempo. Las citadas tarjetas eran leídas por la computadora y ejecutaban la instrucción dictada. Pero la verdadera revolución en la construcción de computadoras se dio de 1951 a 1965, gracias a la creación del transistor que eliminó el uso de tubos de vacío, logrando reducir los problemas técnicos,(por lo menos los que el uso de tubos de vacío provocaba).

Si bien es cierto que el transistor representó un avance considerable en el desarrollo de la computación, también lo es que aún se seguía luchando con el problema de espacio, ya que las primeras computadoras requerían de áreas especiales y de personal capacitado para lograr un funcionamiento adecuando.

Para entonces, el uso de las computadoras se encontraba solo al alcance de grandes corporaciones, gobiernos y Universidades, aunado a que su diseño se

encontraba limitado a la realización de una sola función (cálculo o procesamiento de palabras). La necesidad de los usuarios de tener un aparato mas pequeño y versátil impulsó a que IBM creara el Sistema/360 que cubría las expectativas que el público solicitaba. Este sistema fue el primero en usar circuitos integrados, lo cual mejoró su precio y rendimiento sobre los viejos modelos de otras empresas.

Hasta estos momentos las instrucciones que recibía la máquina eran temporales, esto es, si se requería determinada función se dictaban las instrucciones necesarias y se esperaba un tiempo a que se ejecutar el trabajo en particular, sin que se pudiera realizar al mismo tiempo otra tarea en el aparato. Esta limitante dio origen a la creación de la memoria dividida en varias partes, la cual facilitó la realización de varias tareas al mismo tiempo.

Aún así, las computadoras seguían siendo de gran tamaño y la accesibilidad al público en general sumamente limitada; sumado a estos problemas, se contaba con la falta de disponibilidad de la máquina, ya que estas computadoras trabajaban con sistemas *colectivos* por lo que varios usuarios ejecutaban sus instrucciones con la misma computadora al mismo tiempo, lo que retrasaba enormemente el trabajo ya que la computadora tenia que terminar primero con las instrucciones dadas por uno de los usuarios, para luego seguir con el otro. Para hacer frente a este problema Bell Laboratories desarrolló una pequeña computadora que trabajaba con un sistema propio al cual se le denominó UNIX[2] (Por sus siglas en ingles Información

[2]Ibidem p.12

Unicanalizada y Servicio de Computación). Este sistema evolucionó en un lenguaje denominado "C" que se expandió casi gratuitamente entre las Universidades.

La aparición de chips (1980 - 1990) que contienen miles de transistores en un centímetro cuadrado de silicón dejó ver en un futuro cercano la era de la computadora personal (P.C.). Casi al mismo tiempo de la aparición de los chips, se desarrollaron softwares[3] *amables* con el usuario, lo que trajo como consecuencia que las computadoras se acercaran a usuarios que no conocían nada de las computadoras y además no tenían la menor intención de aprender.

En Agosto de 1981 IBM[4] anunció el lanzamiento al mercado de la primera computadora personal, misma que fue recibida por el público usuario con gran aceptación, tanta que la demanda superó a la oferta. En 1982 Compaq desarrolló la PC portátil , continuando su desarrollo la computación sin mayores cambios en su estructura hasta el día de hoy.

IBM se preocupó tanto en desarrollar sus productos, que descuidó sus derechos intelectuales, por lo que miles de empresas en todo el mundo copiaron sin ningún control sus diseños. IBM intentó solucionar este problema cambiando la estructura de sus computadoras, pero todas las empresas que copiaron sus diseños permanecieron fieles a la estructura inicial, aislando a IBM, por lo que esta empresa se vio obligada a regresar a su primer diseño para poder seguir en el mercado.

[3] Son los sistemas operativos y programas con los que la computadora trabaja y el usuario utiliza para relacionarse con la computadora

[4] Norton, Peter. Toda la PC Ed Prentice Hall Hispanoamericana, Mexico 1994 pág 514

Los sistemas de cómputo.

Su definición. Los sistemas de cómputo se integran por la interacción el hombre con la computadora con el fin de obtener datos. Según Leticia Rodríguez dice que "Una computadora es una máquina que procesa datos y las caracteristicas que presenta son alta velocidad en la realización de operaciones y alto grado de precisión"[5]. Por su parte Javier Moreno, profesor del Instituto de Computación y Métodos (ICM) opina que la computación es "el procesamiento lógico y matemático de una serie de datos suministrados para obtener información especifica" y que la computadora es una "aparato electrónico que sirve para procesar datos de manera lógica y matemática con el fin de obtener información"[6].

De los conceptos antes señalados es de hacerse notar las siguientes caracteristicas:
1.- Se requiere primero el procesamiento de una serie de datos con el fin de obtener una información en particular; dicho procesamiento debe ser primero en la mente del hombre el cual deberá idear el método más práctico para la ejecución de una tarea determinada, ya que si no se dan las instrucciones pertinentes, la computadora no sabrá que hacer o realizará la tarea indicada en mucho tiempo y con errores.

Es de hacerse notar que lo más importante en un sistema de cómputo es el soporte humano, el cual se conforma por diversos profesionistas como son los Ingenieros de

[5] Rodriguez Monroy, Leticia et al Computacion basica I Ed Popular, Mexico 1994 pág 39
[6] Moreno, Javier - Apuntes de curso de administracion de sistemas de computo, Mexico 1994

sistemas e Ingenieros en computación además de contar con el personal técnico integrado por los analistas de sistemas, analistas de programas, técnicos en informática, administradores de sistemas y los usuarios comunes.

2.- Una vez establecido el procedimiento a seguir para llevar a cabo determinada tarea, se ingresarán las instrucciones necesarias para que la computadora cumpla con su tarea. La computadora es solo una herramienta que necesita que se le indique la actividad a realizar, ya que sin estas instrucciones solo es un conjunto de cables inútiles.

Las computadoras se encuentran formadas por un Hardware que se integra por todos los componentes físicos del sistema y un Software que son el conjunto de programas que utilizan los componentes físicos para su mejor razonamiento , los cuales desarrollaremos en el siguiente punto.

Para su estudio las computadoras se clasifican en grandes o Mainframe que son capaces de controlar 5 computadoras o más y son utilizadas en sistemas en red; medianas o Minicomputadoras que son capaces de controlar 3 computadoras y pequeñas o Microcomputadoras (P.C.) que son aquellas que más difusión tienen en el público por la diversidad de aplicaciones que se pueden desarrollar en ellas.

Su funcionamiento.- Para comprender como funciona una computadora es necesario saber primero de que elementos se encuentra formada. Toda computadora consta de 5 partes fundamentales:

1.- Procesador o unidad de proceso

2.- Memoria

3.-Dispositivos de entrada y salida

4.- Almacenamiento en discos

5.- Programas.[7]

Procesador.

Es la parte de la computadora diseñada para llevar a cabo o ejecutar los programas. Como características indispensables el procesador debe leer y escribir información en la memoria, además de reconocer y ejecutar una serie de instrucciones proporcionadas por los programas; por último debe instruir a las demás partes de la computadora para una correcta realización de su trabajo .

Toda proporción guardada, podríamos comparar al procesador con nuestro cerebro ya que ambos son los encargados de coordinar el trabajo de una estructura con el fin de obtener resultados óptimos.

Ahora bien, es de suma importancia que el procesador distinga entre programas y datos, siendo los programa la serie de instrucciones que se le dan a la computadora para que realice determinadas tareas y los datos son la información con la que se actúa dentro del programa.

[7] Norton , Peter Op.Cit, pag 2

De no distinguir entre uno y otro la computadora nos sería capaz de realizar ningún trabajo

Memoria.

Es el pizarrón en el que el procesador hace sus notas. Comúnmente entendemos a la memoria de las computadoras como un archivo fijo en el cual se almacenan datos, lo cual es un error, ya que la memoria es temporal (RAM o memoria de acceso aleatorio) o de lectura. (ROM, solo puede ser leído por la computadora y se encuentra formada por rutinas de control de la computadora).

La memoria RAM está diseñada para almacenar datos e instrucciones del sistema operativo y cualquier otra aplicación. Esta memoria es usada como un borrador en el cual se anotan ideas y se borran constantemente. Su característica principal consiste en que es volátil, lo cual significa que al desconectarse la computadora todo lo que se anotó se borra y queda el espacio libre para la próxima sesión. No con esto debemos entender que la información o nuestro trabajo se pierde en definitiva, ya que esto no ocurre. La información se guarda en los discos (que veremos mas adelante) y la memoria solo es el espacio que necesita la máquina para hacer sus cálculos y deducciones para poder hacer funcionar los programas. A mayor memoria, mayor espacio para la computadora para hacer sus cálculos y mayor velocidad en sus respuesta. La memoria RAM se mide en Bits, Bytes, Kilobytes, Megabytes y Gigabytes.

Como ya mencionamos la memoria ROM es usada por la computadora como un instructivo que le señala los caminos que debe seguir para hacer su trabajo; esta memoria solo puede ser leida por la computadora y no puede ser cambiado.

A diferencia del procesador, la memoria mezcla datos y programas, ya que a ésta no le interesa distinguir entre uno y otro toda vez, que esa función ya la realizó el procesador. Es necesario aclarar que la memoria no es de uso exclusivo del procesador, sino que también es usada por los dispositivos de entrada y salida (Teclado, monitor, mouse etc.), siendo esta información volátil, lo cual significa que al apagar nuestra computadora esa información se pierde y se libera espacio para ser empleado en otra ocasión.

Dispositivos de entrada y salida.-

Son el conjunto de accesorios con los que el hombre interactúa con la computadora Los dispositivos de entrada son el teclado, los lectores de discos flexibles, los lectores del disco duro, el mouse, el scanner, el fax, el CD-Romm, las lineas telefónicas y cualquier otro canal de comunicaciones que entre o proporcione información.

Los dispositivos de salida se encuentran formados por la pantalla, la impresora, el disco flexible, las redes y el fax.[8]

[8] Norton, Peter - Toda la P.C., Ed Prentice Hall Hispanoamericana, México 1994, Pag 7

Almacenamiento en discos .

Complementando el círculo de interacción de la computadora con el hombre se encuentran los discos . Los dispositivos de almacenamiento (discos) son unidades lógicas de grabación en medios magnéticos, asignados con las letras A. B, C, D, E, F, donde las dos primeras letras son asignadas a unidades externas (Disquetes, o floppy) y de C a F a unidades internas (Discos duros, o Hard Disk) .[9]

Los discos fueron pensados como solución a la memoria volátil de la computadora, ya que en ellos se guarda la información que puede leer la computadora.

El floppy disk o disco flexible es, hasta el momento, el medio más popular para manejar información de manera portátil. Estos discos están fabricados de un material magnético flexible redondo y están contenidos en un cartucho de plástico.

En un principio los había de dos tamaños 51/4 y 3½, pero debido a su tamaño más reducido y mayor capacidad se hizo más popular entre los usuarios el disco de 3 1/2 .

En la actualidad se pueden utilizar también, como medio de almacenamiento de información los discos compactos (CD,), que cuentan con mayor espacio para la guardar información y su costo es reducido.

[9] Moreno, Javier - Apuntes del curso de administración de sistemas de cómputo Mexico 1994

El disco duro de la computadora es el dispositivo físico que permite almacenar datos y programas en la computadora. Se encuentra formado por platillos giratorios que alcanzan grandes velocidades al momento de buscar determinada información.
Este dispositivo es de mayor capacidad que los antes citados y se encuentra en el interior de la computadora.

Peter Norton señala que la información en el disco no puede ser leída o escrita por los usuarios y no es para ellos. El almacenamiento en disco es la biblioteca de la computadora, su caja de herramientas y su depósito; en este lugar la computadora guarda sus manuales de instrucción (programas), datos y cualquier otra información que necesite tener a la mano.

Programas.

Anteriormente señalamos que el procesador de la computadora es el cerebro que coordina todo su funcionamiento, pero para que este cerebro trabaje es necesario que existan instrucciones que llevar a cabo. Esto son los programas, son todas las directrices que debe seguir la máquina para realizar determinados trabajos

Existen dos clases de programas: de sistema y de aplicación.
Primeramente, los programas de sistema son aquel conjunto de instrucciones que sirven para hacer funcionar a la computadora. Sin un programa de sistema la computadora solo es un conjunto de cables inútiles. (Ej. Windows, MS dos etc)

En segundo lugar están los programas de aplicación (Word, Power Point, Excel, etc.) que son aquellos con los que el usuario trabaja, pudiendo estar diseñados para realizar las más diversas actividades (sumas simples, cálculos científicos, dibujos, procesadores de textos, control de nóminas, actividades administrativas etc.). Es oportuno hacer notar que el usuario no tiene contacto directo con los programas de sistema, ya que como se mencionó son únicamente para el correcto desempeño de la máquina y de sus instrucciones.

En la actualidad el programa de sistema más conocido en todo el mundo es Windows, pero antes de Windows hubo muchos otros programas que poco a poco fueron evolucionando hasta el día de hoy. El mencionarlos a todos sería adentrarnos en una explicación muy técnica del desarrollo de los citados programas, por lo que solo mencionaremos al antecedente inmediato de Windows y base fundamental de la PC., el sistema MS DOS.

El MS DOS (Microsoft Disk Operating System. Sistema Operativo de disco de Microsoft) es un sistema de supervisión u operativo que se encuentra clasificado como de los programas de computadora más complejos, ya que su tarea es básicamente supervisar y dirigir la operación de la computadora, lo que representa un gran reto, ya que al mismo tiempo que la computadora realiza una tarea , también revisa su propia operación, lo cual evita que el usuario se complique la existencia con los problemas que la computadora pueda tener al momento de llevar a cabo sus funciones.

El DOS realiza las siguientes actividades:

1.- Administra dispositivos de entrada y salida de dos maneras: la forma más básica consiste en dar instrucciones a los dispositivos y revisar si estos reportan algún error. En forma más avanzada, además de coordinar a los citados dispositivos, pone especial énfasis en los discos, ya que desarrolla un esquema que le permite a la computadora grabar información, y administrar de la mejor manera posible el espacio del disco, buscando que estas funciones se lleven acabo rápidamente y de la manera más exacta posible.

2.- Controla los programas que se "carguen" en la computadora. Para realizar esta actividad el sistema operativo ajusta el marco de trabajo para la ejecución de un programa a través del establecimiento de límites sobre que partes de la memoria y que partes del almacenamiento en disco pueden ser utilizada por un programa En una PC., esta administración del espacio y recursos no ocurre y se deja al programa *invitado* hacer uso de la totalidad de los recursos.

3.- Procesa comandos. Esta función se refiere a la interacción del usuario con la computadora. En palabras simples podemos decir que lo que el usuario teclea es *traducido* por el DOS para que la computadora entienda la instrucción que se le está dando para la ejecución de un programa.

Pero, ¿Cómo nació el Dos?. En un principio cada fabricante de computadora tenia su propio sistema operativo, diseñado exclusivamente para su computadora y para la ejecución de sus programas, lo que significaba que si Usted tenia una computadora marca "X" , no podía utilizar los programas de las computadoras marca "Y" ni ninguno de sus componentes.

IBM fue el primero en utilizar el DOS creado por Microsoft como sistema operativo en sus computadoras y después de algunos años sacó su propia versión del DOS llamado PC DOS que competía con producto de Microsoft.

Cualquiera que sea la versión del DOS , en su momento unificó a los usuarios al utilizar un solo sistema operativo, el cual era compatible con otros sistemas (UNIX, AIX, XENIX etc.), ya que podía compartir archivos con otros sistemas, lo cual antes del DOS era imposible.

La desventaja que presentaba el multicitado sistema era que su diseño estaba pensado realizar una sola actividad por un solo usuario . Los diseñadores nunca previeron que la PC podía ser usada por 2 o más personas que quisieran realizar más de una actividad al mismo tiempo.

A principios del verano de 1990 apareció en el mercado un producto que habia de cambiar nuestras vidas en todos los sentidos : Microsoft Windows.

Windows en un principio no fue muy aceptado, ya que en el mercado ya existia un producto de Macintosh, llamado GUI el cual superaba en mucho a Windows (ambos utilizan dibujos para hacer mas fáciles de usar su ambiente) y además no habia muchas aplicaciones que utilizaran a Windows, pero este programa contaba con la gran ventaja que era muy fácil de aprender y utilizar, además de que con el tiempo muchos programadores empezaron a utilizar Windows para el desarrollo y ejecución de sus programas.

En otros ambientes distintos a Windows para dar alguna instrucción a la computadora era necesario escribir largas líneas de instrucción como C:\lotus\123 y luego pulsar la tecla enter; en Windows lo único que se necesita es sombrear, ya sea con el teclado o con el mouse el icono del programa y dar doble clic en él para que se ejecute la instrucción deseada.

La accesibilidad que presenta Windows a provocado que sea compatible con varias aplicaciones, lo que hace mas versátil el uso de la PC. (circunstancia que se veia limitada cuando solo existia el MS DOS) además de que es más fácil captar la información a través de imágenes. Aunado a lo anterior, Windows ofrece la posibilidad de compartir datos con otras aplicaciones (Copiar, pegar, editar, etc.), siendo esta característica, la compatibilidad, una de las características más sobresalientes del programa.

En un principio para que Windows se ejecutara, era necesario el soporte del MS DOS, ya que no todos los programas estaban diseñados para ser ejecutados desde Windows y además necesitaba de ciertas características del MS DOS para su correcto funcionamiento. En la actualidad el MS DOS todavía es utilizado por Windows para funcionar, con la diferencia de que ahora Windows absorbió algunas características del DOS y es el programa que administra los recursos y dispone de ellos para ejecutarse a si mismo y a las aplicaciones con las que se cuente.

Las redes de cómputo.

¿Qué es una red?.

La aparición de las PC abrió un mundo desconocido hasta entonces para muchos usuarios y sobre todo para empresarios a los que les facilitaba el desarrollo de su profesión. Pero como señalamos anteriormente las PC estaban diseñadas para ser empleadas por un usuario, ya que en su momento no existia la necesidad de conectar una PC a otra.

Una vez que el desarrollo de la computación logró colocar una PC en cada empresa empezó a surgir la necesidad de comunicar entre sí a las computadoras con el fin de compartir datos y poder obtener mejores resultados en el trabajo. Esta necesidad fue advertida por los productores de computadoras quienes de la noche a la mañana tuvieron como meta el lograr la comunicación de datos y transferencia electrónica de información entre computadoras.

La palabra RED es definida por el diccionario de la lengua española como aparejo de mallas para pescar, cazar, cercar, etc. o sistema de caños y, tuberías, alambres, vías de comunicación agencias o servicios para determinado fin. Aplicando el término a la computación podemos decir que una red es una manera de interconectar computadoras de tal forma que estén conscientes unas de otras y puedan unir sus recursos.

Las computadoras se comunican entre sí a través de un módem y por medio de redes. El módem permite el intercambio de información mediante el uso de líneas telefónicas y las redes conectan directamente a las computadoras , ya sea por medio de cables especiales o por algún medio de comunicación inalámbrica

Las ventajas de utilizar las redes son:

1.- Permiten el acceso simultáneo a programas e información

2.- Permiten a la gente compartir dispositivos periféricos (impresoras etc.)

3.- Se cuenta con un mejor respaldo.

4.- Facilita la comunicación personal por medio del correo electrónico.

Funcionamiento de las redes.

Para saber como funcionan las redes primero hay que saber cuantos tipos de redes existen y en que se diferencian una de otra.

Redes de área local. (LAN).- Este tipo de redes se encuentran conectadas por un solo cable contiguo o algún enlace inalámbrico, pueden estar constituidas desde dos hasta cientos de computadoras, con la particularidad de que este tipo de redes se encuentran físicamente en un solo edificio o en un grupo de edificaciones contiguas. Una red LAN permite que las computadoras interconectadas compartan el hardware (principalmente discos e impresoras), software e información.

Red de área extendida (WAN).- Son dos o más LAN interconectadas generalmente a través de una amplia zona geográfica. Este tipo de redes utilizan sus recursos locales y comparten información con otras computadoras establecidas en otro lugar.
Las redes WAN se conectan por medio de líneas telefónicas o por medio de fibra óptica y en algunos casos por medio de sus enlaces terrestres y aéreos de satélite.

Ahora bien, las redes se organizan de las siguientes formas:

1.- Cliente-servidor. Funciona por medio de una computadora central (Servidor de archivos) que puede almacenar y procesar la información de las computadoras conectadas a la red (Nodos). El servidor de archivos proporciona la información que necesiten los nodos para realizar su trabajo; esta información es de carácter general (base de datos), siendo el nodo el encargado de especificar a la función a realizar. Para dejar esto en claro, pondremos como ejemplo una gran mesa con muchísima comida de la cual cada persona tomará únicamente lo que desee comer y lo demás lo dejará para aquellos a los que se les antoje. Este tipo de conexiones se utiliza usualmente en las redes LAN.

2.- Computación par a par.- Aquí los nodos pueden actuar como clientes y servidores al mismo tiempo, estos es, cada nodo tiene pleno acceso a los recursos de otro nodo, haciendo posible que cada usuario pueda emplear la información, discos, impresoras, etc. de las otras computadoras conectadas a la red.

La Internet.

Su creación

Según José Antonio Carballar Falcón, Internet se podría definir como un red global de redes de ordenadores, cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios; esta definición es de lo más acertada ya que hace mención al instrumento idóneo para el uso de Internet (la computadora y las redes) y al fin que se persigue (el mantener comunicado al todo el mundo entre si a través del uso de una red, permitiendo el libre paso de la información).

Se puede comparar a Internet con una inmensa biblioteca en la cual es posible encontrar la mas variada y amplia información sobre cualquier tema, lo cual la hace una herramienta valiosisima para la investigación, la educación y casi cualquier fin que se le quiera dar, pero debido a su gran tamaño se requiere que el usuario tenga un poco de conocimiento acerca de su funcionamiento para que no se pierda entre tanto material y resulte una herramienta inservible .

Pero, ¿cómo nació esta herramienta?. Cuando el uso de las redes se generalizó, los ingenieros se encontraron con el problema de que cada red WAN tenía sus propias

especificaciones de voltaje, modulación de señal etc., por lo que era sumamente difícil conectarlas entre si o con una red LAN. Esta situación implicaba el aislamiento de ciertos equipos de cómputo, por lo que se hizo necesario unificar todas las redes en una sola.

El departamento de Defensa de E.U. a finales de los 70s. se interesó en el desarrollo de una sola red de cómputo y en sus fines prácticos. Por medio de la Advanced Reserch Projects Agency (ARPA, Agencia de Proyectos de Investigación Avanzados) se inició el proyecto de crear una red única, para lo cual se empezaron a estudiar todos los problemas técnicos que representaba conectar varias redes y a darle solución a los mismos.

La ARPA ofreció recompensas a investigadores, industriales y académicos que presentaran soluciones viables para la conexión de las redes; esta convocatoria abrió el campo para nuevos descubrimientos que darían pié al primer software que soportaría a la red única. El proyecto recibió el nombre de interredes (Internetwork), término que se redujo al nombre de Internet.

Internet tuvo su primera columna vertebral en la red WAN de la ARPA, ya que esta red conectaba a todos los investigadores interesados en el proyecto. Esta base se llamó ARPANET y tenía la característica que además de funcionar como una red WAN común, tenía una conexión adicional en la que los investigadores podían hacer sus experimentos relacionados con el perfeccionamiento de Internet. A medida que fue pasando el tiempo los investigadores perfeccionaron el software de apoyo de

Internet y crearon el protocolo de transmisión de la red, el cual es el idioma común que deben *hablar* las computadoras conectadas en la red para poder comunicarse entre si.

Desde un principio Internet fue pensado en un sistema abierto, lo cual significa que cualquier computadora de cualquier compañía se pudiera comunicar con otras distintas, lo cual no ocurría, ya que cada empresa fabricante de redes tenia sus propias especificaciones de conexión. El sistema abierto facilitaría además que se compartieran datos de los investigadores para perfeccionar el proyecto

El hecho de que cada compañía fabricante de computadoras hiciera sus propios diseños con el fin de emplear únicamente sus redes alentó el desarrollo de Internet, ya que los fabricantes al pretender monopolizar el negocio de las redes, lo que ocasionaron fue que cada compañía se fuera aislando una de otra, por lo que la idea de tener una sola red fue recibida con gusto por los usuarios.

A principios de los 80s., el prototipo de Internet se empezó a probar en algunos centros de investigación académicos e industriales, y al ver el éxito alcanzado, el ejercito de los Estados Unidos decidió utilizar a Internet como su principal sistema de comunicaciones por computadora. Es a partir de este momento que Internet deja de ser un proyecto solo conocido por especialistas y se empieza a convertir en una herramienta útil para fines prácticos.

Los investigadores se percataron que lo que empezó como un proyecto, ya había duplicado su tamaño a solo un año de encontrársele una utilidad práctica. Esta circunstancia ocasionó que el software existente en ese momento fuera insuficiente para soportar a tanto usuarios. Este problema fue solucionado una vez mas con la participación de estudiantes, científicos y militares quienes analizaron la tecnología disponible en ese entonces (Década de los 80s.) y se abocaron a dar una estructura formal a Internet.

El resultado de las investigaciones y estudios realizados desembocaron en el cambio de columna vertebral de Internet, formándose la nueva base a partir de la participación de empresas como IBM (Apoyo en computadoras y software para hacer trabajar a la WAN), MCI (Colaborando con líneas telefónicas para conectar la red) y MERIT (Encargada de operar la red). La nueva columna vertebral recibió el nombre de NSFNET.

En esta época la participación del Gobierno de los Estados Unidos era importante en el financiamiento, pero debido a la creación de la NSFNET el número de usuarios se triplicó, y el costo de mantenimiento también se elevó, por lo que se decidió dar participación a la industria privada, formándose una compañía no lucrativa llamada Advanced Networks Service (ANS, Redes y servicios avanzados).

En 1992 la ANS cambió nuevamente la raíz de Internet construyendo las ANSNET que utiliza líneas de transmisión con mayor capacidad que sus antecesores (30 veces más) y se diferencia de las bases anteriores en que las líneas de transmisión y las

computadoras conectadas son propiedad de una compañía privada. Este hecho da pié a la comercialización y privatización de Internet.

El crecimiento de la red a tenido un doble efecto; por un lado conecta a todo el mundo y cada día que pasa más usuarios se conectan, lo que beneficia a los operadores de la red y por otro lado, su crecimiento descomunal a hecho que los ingenieros se quiebren la cabeza buscando nuevas tecnologías para permitir su correcto funcionamiento y expansión.

¿Como funciona Internet?

Como ya se dijo Internet es un conjunto de redes interconectadas entre si por medio de un ordenador, que utiliza líneas telefónicas, fibra óptica y enlaces por radio.

Para que fluya la información entre computadoras se necesitan de diversos formatos (lo que comúnmente conocemos como direcciones de Internet). Estos formatos son:

1.- El decimal, que utiliza números y puntos, por ejemplo 123.456.789.

2.- De descripción del ordenador destino y otras especificaciones para orientar la información a través de la red, ej. Unam.facultder.edu.mx

Como originalmente Internet surgió de un proyecto estadounidense, los países que se conectan a la red necesitan especificar su origen , Ej. .es. (España), .mx,(México, ar, (Argentina) etc., aunque también se utilizan sufijos para determinar la dirección de

alguna institución educativa (.edu), un centro militar (.mil) o una oficina de Gobierno (.gov)

Ya que se cuenta con la dirección, la información sale de su red de origen y con las instrucciones con que cuenta (dirección de Internet), busca entre las redes conectadas a aquella que se adecue a la dirección.

Anteriormente señalamos que Internet cuenta con un protocolo y lo definimos como el idioma común que deben *hablar* las computadoras entre si para comunicarse. Pues bien, este protocolo es el encargado de guiar la información de la computadora que envía la información hacia la que recibe los datos. Además de realizar esta función el protocolo se encarga de verificar si la información llegó a su destino y en caso de que no sea así hace que se vuelva a enviar.

Actualmente uno de los protocolos más importantes es el de transferencia de hipertexto (http), el cual puede leer e interpretar información de una computadora remota pudiendo transferir texto, imágenes, sonidos, secuencias de video etc. Este protocolo de transferencia forma la base de la colección de información distribuida por la World Wide Web. (WWW).

La World Wide Web, es un conjunto de información acomodada en lugares llamados páginas Web, que incluyen información en forma de textos, gráficos, sonidos y vídeos, y da la facilidad de comunicarse con otras páginas o ficheros

Para poder *navegar* en Internet es necesario contar con un programa *explorador* como Navigator de Netscape, o Internet Explorer, de Microsoft que utilizan el protocolo http para descargar los archivos de la red. En la actualidad se están mejorando los ficheros de la WWW para poder tener acceso a realidad virtual, animación, etc.

Los servicios con los que cuenta Internet son básicamente cuatro:[10] Correo electrónico, servicio de noticias, acceso remoto y transferencia de ficheros.

El correo electrónico sirve para que cada usuario tenga comunicación con cualquier otro a lo largo de todo el mundo e intercambiar información con el. El servicio de noticias es útil para aquellos usuarios que les interese indagar en algún o algunos temas específicos; el acceso remoto facilita la conexión de nuestra computadora con otra computadora o red en cualquier parte del mundo y la transferencia de ficheros sirve para recuperar información de una computadora situada en otra parte del mundo y traerla a la nuestra.

Como hemos visto hoy en dia Internet se ha convertido en el material idóneo para todos los fines (comercio, investigación, comunicaciones etc.), pero como veremos más adelante no todo es maravilloso en este avance tecnológico.

[10] Carballar Falcón Jose Antonio - Internet El mundo en sus manos .De ra-ma, Madrid España 1994 pag. 02

El hecho de ser accesible a cualquiera que tenga la capacidad económica de comprar un equipo de cómputo y el ánimo de investigar en aquello de lo que todos hablan a hecho de Internet una herramienta, pero también a sido el medio para la comisión de diversos ilícitos.

El avance tecnológico tan rápido y la novedad de un producto nuevo y variado no han dado la oportunidad a razonar hasta donde pueden llegar los alcances de esta herramienta ni mucho menos de valorar sus desventajas, por lo que se hace indispensable (desde el punto de vista penal) prever los ilícitos que se puedan cometer en este medio.

CAPÍTULO 2

LOS VIRUS CIBERNÉTICOS

LOS VIRUS CIBERNÉTICOS.

¿Que son los virus cibernéticos?

A principios de la década pasada, pensar que una computadora se podía *enfermar* era una cosa inconcebible y aun más inimaginable era creer que existieran *virus* que atacaran nuestros equipos de cómputo. Pues bien, una vez más la realidad superó a la fantasía y en la actualidad contamos con las más amplia gama de virus y de padecimientos en nuestros equipos de cómputo.

A lo largo del desarrollo del presente capítulo veremos que lo que inició como un juego se a convertido en una pesadilla para todos los usuarios de equipos de cómputo, lo que se traduce en pérdidas millonarias para los usuarios y en grandes ganancias para los productores de programas antivirus, los cuales se deben actualizar constantemente para evitar en la medida de lo posible la pérdida de la información que se tenga.

La palabra virus se encuentra definida por el diccionario de la lengua española como podre, humor maligno, y biológicamente es entendido como el organismo de composición más sencilla capaz de reproducirse en el seno de las células vivas específicas, siendo sus componentes esenciales los ácidos nucléicos y proteínas[11].

[11] Casa Zepol S.A. de C.V .-Acervo Jurídico México 2000.

Esta definición nos sirve de base para comprender lo que es un virus de computadora, ya que su estructura y funcionamiento es muy similar a la de un virus biológico

Existen varias definiciones de los que es un virus, la cual varía desde el punto de vista del autor. Para darnos una idea general citaremos algunas definiciones. El equipo de trabajo de Symantec, opina que los virus son elementos de software diseñados y creados para perjudicar la computadora mediante alteraciones de la forma en que trabaja con su información y permisos[12]

Por su parte Alberto Rojas[13] define a los virus como todo aquel código que al ser ejecutado altera la estructura del software del sistema y destruye programas o datos sin autorización o conocimiento del operador.

En el mismo orden de ideas Ralph Burger [14] aporta una definición que a mi criterio es la más acertada y amplia de lo que es un virus. Señala que "Un programa debe clasificarse como virus si combina los siguientes atributos:

1.- Modificación de códigos del software -que no pertenecen al propio programa virus- a través del enlace de las estructuras del programa virus con las estructuras de otros

[12] http //www symantec it/region/mx/avcenter/vinfodb html - Enciclopedia en linea de virus reales y falsos Pag 01
[13] Citado por Gonzalo Ferreira Cortes - Virus en las computadoras, México 2da Edicion pag MF3-2
[14] Citado por Gonzalo Ferreira Cortes - Ob cit Pag MF 3-3

programas. El virus en sus estructura contiene la instrucción de *adherirse* a determinado programa para así modificarlo y lograr que el programa atacado cumpla con las instrucciones que el virus le dicta.

2.- Facultad de ejecutar la modificación en varios programas, lo que significa que si tenemos varios programas en nuestra computadora, éstos se pueden ver afectados por la acción de un solo virus.

3.- Facultad para reconocer, marcándola, una modificación realizada en otros programas. Cada vez que se enciende la computadora infectada , el virus tendrá la función de cumplir con la orden que su línea de instrucción le dicta, la cual consiste obviamente en infectar al programa y señalar el programa que ya está infectado, esto con el fin de no reinfectar un programa ya dañado y así poder seguir con otros que no lo estén.

4.- Posibilidad de impedir que vuelva a ser modificado el mismo programa, al reconocer que ya está infectado o marcándolo.

5.- El software modificado asimila los atributos anteriores para, a su vez, iniciar el proceso con otros programas en otros discos."

De las definiciones antes citadas es importante hacer resaltar dos aspectos importantes: Los virus de computadoras se diferencian de los virus biológicos en éstos se transmiten por medio de la naturaleza, realizándose el contagio en seres

vivos, cosa que no ocurre con una computadora, ya que para que una computadora pueda ser infectada es necesario introducir en ella algún disco, programa o información que contenga al virus y que éste último se encargue de cumplir con sus órdenes.

Por otra parte, los virus biológicos son estructuras creadas por la naturaleza y los virus de computadora son creados por el hombre con el único fin de destruir y perjudicar a un tercero sin que exista algún motivo aparente. De esta última característica surge la necesidad de perseguir y sancionar a todo aquel delincuente que crea estos programas destructores, ya que no es posible dejar sin castigo a todo aquel sujeto que malintencionadamente coloca estos programas en nuestros sistemas.

¿Como surgen los virus de computadora?.

En párrafos anteriores se hizo mención a que este problema había iniciado como un juego y tal afirmación es cierta ya que si bien, no existen datos precisos de cuando surgió el primer virus (esto en razón de que los primeros ataques fueron a oficinas gubernamentales que decidieron ocultar esa información por no divulgar que sus sistemas de cómputo eran muy frágiles), si existen otros datos que nos pueden servir para indagar en la génesis de este problema.

En los años 60s un grupo de estudiantes del Instituto Tecnológico de Massachusetts desarrolló un programa conocido como *Space War* que consistía en *Bombardear* a

un programa contrincante, el cual no detectaba quien lo estaba atacando. El bombardeo consistía en modificar la información del contrincante el cual se veía afectado de manera inmediata.

Posteriormente los científicos de At&T crearon otro juego llamado *Core War* que era capaz de reproductores cada vez que se ejecutaba. El juego consistía en atacar al adversario destruyendo la memoria de la computadora o impedir su correcto funcionamiento.

Este programa encontró su antídoto (o lo que hoy llamamos antivirus) en otro programa llamado Reeper, ya que este se encargaba de atacar y destruir cada copia del *Core War.* Los científicos de ese entonces advirtieron los problemas que en un futuro no muy lejano podrían causar las estructuras de programas como el *Space War* y el *Core War* por lo que decidieron mantener en secreto sus existencia, pero en 1983 durante un a conferencia en la Association for Computing Machinery en Estados Unidos se dio a conocer la existencia de los citados programas precisando detalles de su estructura.

Para completar la información apareció en la revista Scientific American un artículo denominado *Computer Recreatiosns* que no era mas que una guía detallada de como crear un virus en particular; con esta información los usuarios ya eran capaces de crear y difundir sus propios a otros usuarios.

En 1983, después de mucho investigar, el Dr. Fred Cohen presentó en la Universidad de California el primer virus residente en una PC, lo cual lo hace acreedor al título de Padre de los virus informáticos.

El primer ataque de virus de computadora se difundió ampliamente entre los usuarios y se dio en el año de 1986 por el virus Paquistán. Este virus fue desarrollado por dos hermanos paquistanies que se dedicaban al comercio de computadoras y software. Dentro de sus actividades estaban la de crear sus propios programas y piratear con programas conocidos, ya que se dedicaban a vender copias ilegales de programas famosos a los que les agregaban un virus benigno (solo mandaba un mensaje), pero que tenia la cualidad de poder ser modificado por otros usuarios.

Esta característica se convirtió en su principal defecto ya que al vender muchisimas copias de sus programas piratas, el virus pudo ser modificado y *perfeccionado* por otros programadores, logrando crear uno de los virus más nocivos que se conocen.

En 1987 IBM fue atacada por un virus benigno que se llamaba *Christmas* el cual mandaba un mensaje navideño que al repetirse en múltiples ocasiones logró paralizar las actividades de la citada empresa por 72 horas.

Durante los años siguientes se repitieron varios ataques con virus *benignos* siendo dos casos los más importantes a nuestro criterio: El primero no fue propiamente un ataque por virus, sino una amenaza. En Octubre de 1989 un sujeto autodenominado tecnoterrorista dijo que habia infectado una gran cantidad de computadoras y que el

viernes 13 se destruirían toda clase de archivos guardados en el disco duro y en disquetes.

Esta situación causó pánico entre los usuarios y puso en evidencia la fragilidad de las defensas de los usuarios en contra de actos como los de este loco. El hecho fue que la terrible profecía no se cumplió, pero si se convirtió en una señal de alarma que todos los usuarios debían considerar.

El otro asunto relevante fue dado a conocer a la opinión pública por el New York Times en el que se informaba que las computadoras de la NASA habían sido infectadas por virus durante el lanzamiento del transbordador Atlantis. El virus se difundió por la red de la NASA e infectó a los particulares a través de la conexión comercial que tiene la NASA.

El funcionamiento de los virus

Como veremos en el siguiente punto el funcionamiento de un virus puede ser muy variado, dependiendo del tipo de instrucción que siga. Sin embargo la mayoría de los virus siguen un mismo principio (parecido al modo en que trabaja un programa común) que a continuación describiremos.

Un programa común se ejecuta en nuestra PC cuando se teclea su nombre o se hace click en el icono que le corresponda. Una vez hechos esto, el programa ocupa parte

de la memoria RAM de la computadora y permanece ahí mientras no se desconecte el aparato o se le de la instrucción de terminar.

Para que un equipo de cómputo se infecte es necesario que algún programa contaminado se ejecute o simplemente se visualice el contenido ¿Como sucede esto? Pueden ser diversas las fuentes de infección, como ejemplo podemos citar el uso de programas piratas, que generalmente contienen algún tipo de virus (benigno o maligno), por *bajar* o recibir algún programa que contenga a virus ya sea por medio de redes o de Internet, etc. Estas acciones permiten que el virus se introduzca a la computadora y busque colocarse en la memoria RAM, en el sector 0 o de arranque del disco duro de la computadora o en alguna otra área que sea útil para infectar los archivos.

Dependiendo del tipo de virus que se trate la infección se puede dar en el mismo momento o se puede esperar alguna instrucción (detección del llenado del disco duro, una fecha u hora etc.). Una vez infectada la computadora, desde el momento en que se enciende el virus estará presente infectando o esperando el momento preciso para su labor, pudiendo ser esta el controlar los accesos de lectura y grabación en los discos, atacar programas con extensiones .COM o .EXE (siendo estas extensiones características fundamentales de cualquier programa), etc.

Ya instalado en funciones, el virus se encargará de verificar los programas que se ejecuten en la computadora para ver si ya está infectado. Al realizar la infección el virus deja una marca, por lo que al no detectar la marca procede a la modificación de

la estructura del programa ejecutado, logrando con esto infectar a todos los programas que se ejecuten.

La infección consiste básicamente en almacenar una copia del programa virus en el programa infectado; esta acción provoca que se pierda parte de la información del programa infectado, ya que ese lugar está siendo empleado por el virus.

¿Como se percata el usuario de que la computadora está infectada?, dependiendo del tipo de virus serán los síntomas que se presentan; puede llevarse más tiempo de lo normal la carga del programa, se puede tardar mucho en realizar una tarea simple, envía mensajes de error poco usuales, se enciende luces de los dispositivos aunque no se estén utilizando (floppy disk, CD room, etc.), se puede observar una disminución considerable en la memoria del equipo, desaparecen archivos, aparecen sectores dañados en el disco duro, se reduce el espacio utilizable del disco duro de manera súbita, los programas *crecen* o reducen su tamaño, al final de la ejecución del programa aparecen signos y letras *raros* o en casos muy trágicos la computadora no arrancará y enviará una serie de mensajes incomprensibles.[15]

Ahora bien, no todos los mensajes de error se deben a que la computadora está infectada, algunas veces existen fallas en el equipo físico (hardware) o en los programas (software), que pueden deberse a otras circunstancias (como una

[15] Monroy Rodriguez Leticia et.al, Computación básica 1, Ed. Popular , primera de, México 1994 pág 115 y 116

variación en el flujo eléctrico), por lo que es recomendable agotar todas las posibilidades antes de pensar en un virus.

Tipos de virus existentes

Señalar a cada uno de los virus por su nombre, creador y forma de ataque, más que una investigación sería una transcripción literal de lo que se conoce y además sería casi imposible ya que cada día surge un nuevo virus con sus características propias.

Los estudiosos del tema no se ponen de acuerdo en la clasificación de los virus, por lo que solo mencionaremos las clasificaciones más comunes de estos.

Caballos de Troya.- Se introducen al sistema bajo una apariencia distinta a la de un virus. Pueden presentarse como basura o información perdida sin alguna causa aparente. Este tipo de virus esperan alguna indicación para que llegado el momento se activen y comiencen sus actos destructivos, atacando principalmente la información guardaba en discos.

2.- *Bombas de tiempo*.- Son programas que se alojan en la memoria del sistema o en archivos de programas ejecutables (.com ó .exe). Este de tipo de virus esperan un fecha y hora especifica para realizar su función. En esta clase de virus no todos son destructivos , si no que existen algunos que solo envían un mensaje.

3.- *Autorreplicables.*- Son los más parecidos a los biológicos, ya que una vez que infectan los programas ejecutables se autorreproducen. Al igual que las bombas de tiempo esperan una fecha y hora programada o un determinado plazo para ejecutarse. Un ejemplo de este virus es el llamado *viernes trece* que se ejecuta en esta fecha y se borra junto con el programa infectado, evitando así ser detectado.

4.- *Esquemas de protección.*- No se consideran estrictamente un virus, pero son igual de dañinos porque se activan cuando se ha copiado o se intenta copiar un programa que está protegido contra copia. El esquema de protección bloquea el programa, altera sus estructura original o altera sus archivos, haciendo muy difícil la recuperación.

5.- *Virus promocionales.*- Este tipo de virus permiten la copia ilegal de un programa y su funcionamiento normal, pero al paso del tiempo y una vez que el usuario ya cuenta con varios archivos importantes el virus se encarga de modificar su estructura y no permite que la computadora siga funcionando correctamente. Este tipo de virus es empleado por productores legales de programas con el fin de que se obligue al usuario a comprar el programa original para poder usar la información bloqueada o alterada.

6.- *Infectores del área de carga inicial.*- Su función es infectar el área de carga de los disquetes o del disco duro, logrando con esto tomar el control de la computadora cuando esta se enciende, impidiendo cualquier actividad en la computadora.

7.- *Infectores del sistema.*- Este tipo de virus se alojan en programas que se encuentran en la memoria y funciona cuando el virus toma el control de la computadora e infecta a cualquier disco que sea introducido a la unidad con la finalidad de copiarlo o simplemente para ver su directorio.

8.- *Infectores de programas ejecutables.*- Son las más peligrosos ya que infectan cualquier programa. Generalmente los programas en su nombre cuentan con una extensión la cual puede ser .com o .exe y el virus busca estas extensiones para que en cuanto el programa se ejecute el virus ataca y se copia dentro de la estructura del programa. Estos virus pueden marcar las zonas que ya infectaron para no seguirse auterreplicando, pero existen otros que no lo hacen y pueden duplicarse tantas veces que logran saturar la capacidad de almacenamiento de la computadora

9.- *Gusanos.*- Este tipo de virus se reproducen a si mismos y no requieren de un programa anfitrión , sino que se aloja en la memoria de la computadora y se posiciona en una determinada dirección, logrando con esto infectarla y una vez hecho esto se copia en otra dirección y se borra del ya infectado. Al momento de borrarse el virus borra también el programa en el que se ubicó

10.- *Virus lógicos.*- Son programas normales que si no se manejan con cuidado pueden producir daños en la información, modificándola y tomando su lugar

Por otra parte, el Centro de Cálculo de la facultad de Ingeniería de la UNAM, presentó la siguiente clasificación de virus:

1.- Virus benignos.- Este tipo de virus no provocan un daño específico, solo se concretan a enviar mensajes durante el tiempo en el que el usuario está trabajando, lo que resulta muy molesto ya que distrae al usuario de su actividad.

2.- Virus burlones.- Una vez que realizó su labor destructiva envían un mensaje burlándose de su *travesura*.

3.- *Virus caóticos.-* Se abstienen de destruir los archivos, pero causan daños al sistema, logrando que éste se *caiga*.

4.- Virus crecidos.- Su labor es la de marcar sectores dañados en el disco duro, con lo que se reduce considerablemente la capacidad de almacenamiento del disco duro

5.- Virus descarados.- Este tipo de virus se parece a los virus burlones, ya que además de mandar mensajes burlones, mandan el nombre del autor, dirección y su teléfono.

6.- Virus físicos - Se encargan de dañar al monitor y a las cabezas de lectura - grabación de las unidades de disco, haciéndolas trabajar constantemente hasta que se queman.

7.- Virus juguetones.- Son aquellos que se transmiten por medio de la copia de programas de juego.

8.- Virus malditos.- Antes de realizar la infección verifican la cantidad de información guardada, y si es poca espera hasta que se llena para destruirla toda.

9.- *Virus misteriosos.*- Este tipo de virus se asemeja a una falla del equipo en su software, por lo que el usuario puede pensar que no se trata de el ataque de un virus.

10- Virus mutantes.- Su caracteristica principal consiste en que una vez que infectaron un programa alteran su estructura para infectar a otro y evitar asi ser detectados.

11- Virus resentidos.- Son aquellos que fueron creados por programadores despedidos de las empresas o degradados a un puesto menor

12- Virus simples .- Se caracterizan por no *presentarse* si no que borran los programas y la información de manera inmediata.

13- Virus supervisores - Son elaborados por las mismas empresas para detectar a los empleado que realizan copias de programas sin autorización.

14- *Virus temporales.-* Este tipo de virus esperan una fecha u hora especifica para activarse.

15- *Virus vengadores.-* Algunas empresas con el fin de evitar que se utilicen copias ilegales de sus productos insertan una instrucción que destruye parte de la información del programa al intentar copiarlo.

16- *Virus viajeros.-* *Se transportan* a través de cualquier medio de comunicación, como por ejemplo los sistemas de telecomunicación, el módem, microondas, redes y más recientemente , por Internet.

Las clasificaciones antes enunciadas son las que a mi criterio son las más importantes y completas, ya que engloban las caracteristicas especificas de los virus que hasta ahora se conocen y dan una idea clara de los daños que pueden causar. Es necesario decir que cada quien da la clasificación que mejor le convenga, siendo un claro ejemplo de esto las distinciones que existen entre las clasificaciones que manejan los creadores de los programas antivirus más comunes (Norton los clasifica en reales y falsos y Mac Afee toma más en cuenta la primera lista citada). Esta distinción de clasificaciones en nada afecta a la creación de los programas antivirus por una sencilla razón : en la actualidad son pocos los virus que cuentan con una sola característica de las citadas, ya que normalmente reúnen varias de ellas, lo que hace más difícil su detección y destrucción

Hasta estos momentos lo único que podemos hacer para defendernos del ataque de un virus es seguir las siguientes recomendaciones:

1.- No utilizar softwares de dudosa procedencia , ya que estos representan un riesgo latente en contra de nuestros equipos de cómputo.

2.- Se deberán tener respaldos de los programas con los que cuente nuestro equipo, para que en el caso de que se de la infección no perdamos toda nuestra información.

3.- Tener un programa antivirus actualizado constantemente . Es mejor prevenir que lamentar.

4.- Controlar y limitar el uso del equipo de cómputo a las personas que sean de toda nuestra confianza.

5.- Verificar ***todos*** los discos que utilicemos en nuestros equipos.

Estas medidas de prevención son útiles para disminuir en la medida de lo posible el ataque de un virus.

Su difusión en redes e internet.

La gran novedad que resultó ser el uso de las redes y sobretodo de Internet ocasionó que los usuarios dejaran de lado las reflexiones pertinentes respecto de las medidas de seguridad que se debian seguir para evitar sufrir algún daño en los equipos de cómputo o en la información guardada en ellos; esta circunstancia se dio muy probablemente a que al momento de la creación de los citados sistemas de

comunicación a nadie se le ocurrió que alguien quisiera o pudiera entrar a los sistemas de cómputo.

Sin embargo, fue muy poco el tiempo que se tuvo que esperar a que algunos sujetos echaran a andar su intelecto con el fin primero de introducirse al las computadoras conectadas en redes e Internet, para ver su contenido y más adelante con el propósito de enviar un virus.

Pero ¿Como se da este problema?. Como lo mencionamos en anteriores capítulos, para que una computadora esté conectada en una red o a Internet es necesario contar con un nodo (en el caso de la red) o con un módem (en el caso de Internet) o con ambos. Esta conexión da acceso a la gran mayoría de los recursos que ambos medios de comunicación suministran; el caso de Internet es casi ilimitado, ya que basta con tener un poco de ingenio y tiempo para *navegar* en Internet y entrar a donde sea. El funcionamiento de la red es un poco más limitado ya que solo abarca tanto como interconexiones se tengan, pudiendo limitar los recursos a un área especifica.

Esta circunstancia da la pauta para que terceros ajenos a nuestro trabajo puedan entrar a nuestra computadora desde una computadora remota conectada ya sea a Internet o una red pudiendo ver y modificar el contenido de nuestros archivos. Se debe aclarar que la persona que entre a un sistema de cómputo no es cualquier individuo, ya que debe contar con conocimientos aunque sea empíricos para saber como y por donde puede entrar.

Este riesgo , en sistemas basado en Windows, puede tener limitantes , ya que las computadoras no siempre están conectadas a la red, y lógicamente al no estar conectado el tercero no puede entrar a los archivos de la computadora desde un sitio remoto. Pero si consideramos que existen otros sistemas como el UNIX[16] que está diseñado para trabajar constantemente veremos que el riesgo es mayor, ya que este sistema al conectarse a Internet deja al descubierto sus archivos ocasionado que casi cualquier usuario pueda entrar al sistema.

La principal ventaja de Internet se puede convertir en su principal defecto si no se toman las medidas de seguridad necesarias, ya que el tráfico sin control de información pone al descubierto a la mayoría de las computadoras conectadas. Ahora bien, no se debe entender lo anterior como algo tremendista, ya que la mayoría de los usuarios son inexpertos o neófitos cuando se trata de entrar a otro sistema de cómputo sin permiso. El peligro real lo representan aquellas personas que tienen el tiempo, conocimiento e intención de entrar a un sistema. Por medio de las redes e Internet un Hacker puede entrar a nuestros sistemas y modificar, borrar, alterar o introducir algún tipo de virus en nuestros archivos y lograr su destrucción.

Pero no todo se limita a la intromisión de un Hacker en nuestros sistemas; al utilizar el intercambio de información que se da en Internet y las redes se puede transmitir algún virus, esto al *bajar* algún juego de computadora de la red, música, videos, o al

[16] Data Becker edition, traducido por Natalia Cervera et al Todo sobre Internet Ed Macrocombo S A , España 1996, pag. 387

no tener cuidado con los E-mail que se reciben. Actualmente la mayoría de los servicio de Internet proporcionan ciertos mecanismos de seguridad que solicitan autorización al usuario para bajar determinado programa, siendo esto útil de alguna manera para tener precaución con lo que se está obteniendo.

El caso del E-mail es de mencionarse en particular: el hecho de recibir un mail no implica que por la recepción la computadora ya esté infectada. Como hemos mencionado anteriormente, los virus son programas y como tales necesitan ser ejecutados. Cuando se recibe un mail contaminado puede ser que adjunto al mensaje se anexe un programa, por lo que el peligro real lo representa el programa adjunto y no el texto enviado (esto hasta el momento en que se redacta esta tesis, ya que no descartamos que en un futuro se pueda enviar un virus y que este destruya con el simple hecho de ser enviado).

Existen métodos técnicos mediante los cuales los programadores pueden intentar bloquear el acceso de terceros a los sistemas de cómputo, tanto en redes como en Internet (cortafuegos o firewalls), pero estas medidas de seguridad son costosas y no son del todo eficaces, ya que pueden llegar a limitar el flujo de la información y las rutas de acceso al sistema *protegido* pueden volverse de fácil falsificación.

Modos de Infección.

En los puntos anteriores hemos hecho mención a que son los virus, su historia, funcionamiento y tipos que a la fecha se conocen, pero ¿Como se transmiten?

Vayamos al principio del problema. Cuando se dio el boom de la computación los programas para computadora resultaron ser de altos precios, por lo que algunas personas se dedicaron a comprar el programa original y a vender copias ilegal del mismo por todos lados, haciendo así accesible al publico usuario el programa, pero los programadores vieron mermadas sus ganancias, por lo que se decidió usar esquemas de protección para proteger el producto original y evitar la piratería. Los esquemas de protección pueden dañar seriamente la computadora, afectando generalmente al disco duro.

Estos hechos hicieron que algunos programadores se empeñaran en diseñar un programa que fuera igual de destructor que un esquema de protección, teniendo como único fin el de perjudicar a los usuarios.

En un principio la copia ilegal de programas originales era la principal fuente de *contagio*, pero debido al auge de Internet, los medios de contagio se han ampliado siendo los medios más comunes de infección los siguientes.

1.- Software introducido o usado en los sistemas por un extraño, quien tuvo acceso a las computadoras

2.- Software traido de su casa de un empleado que tiene un sistema infectado sin él saberlo.

3.- Software recibido (regalado o comprado) de alguna persona que tiene su computadora infectada.

4.- Software intencionalmente infectado por un empleado descontento o malicioso.

5.- Cualquier otro tipo de software (incluyendo Sistemas Operativos, Programas de aplicación, juegos, utilidades, etc.) que se traen de cualquier fuente externa[17]

Los daños que ocasionan.

En este punto daremos una vista general a los daños que pueden causar los virus cibernéticos, ya que como hemos señalado en párrafos anteriores, no todos los virus realizan la misma actividad, ni están diseñados para causar los mismos daños, además se debe estar consciente que la mayoría de los virus conocidos contienen más de una de las características que se señalaron en la clasificación antes señalada.

Daños en archivos.

Normalmente el daño ocasionado consiste en la alteración o destrucción total o parcial de sus contenidos. Con el fin de no alargar inútilmente esta Tesis señalaremos como archivos a los programas de aplicación, sistemas operativos y el contenido de los mismos.

Conforme a la clasificación de los virus dada con anterioridad, podemos señalar como virus de programas a los virus de Macros, ya que estos se adjuntan al programa, siendo atacados generalmente los procesadores de palabras como Word, Works, Word Perfect y las hojas de cálculo como Excel, Quattro y Lotus, pudiendo este tipo

de virus entorpecer el correcto funcionamiento de los citados programas con mensajes de error I ejecutarlos o al destruir parte o el total de la información de los trabajos realizados en los citados programas de aplicación; virus autorreplicables, ya que estos se autorreproducen en los programas con el fin de infectar a otros programas ejecutables (que son aquellos que en su nombre o extensión contienen los atributos .com o .exe). Este tipo de virus al infectar el programa o detectar se está intentando eliminarlo, se borra a si mismo y al programa infectado, pudiendo afectarlo en sus funciones esenciales; infectores de programas ejecutables, cuya función es la de atacar cualquier programa, ya sean hojas de cálculo, juegos, procesadores de palabras, etc., resultando este uno de los más peligrosos.

Daños en memoria.

Siguiendo con el criterio anterior , podemos señalar como virus de memoria a los gusanos, ya que estos se alojan en la memoria para desde ahí arrastrarse de programa en programa borrándose después de la infección. Este hecho provoca que al borrarse del lugar que infectó, también borra parte o todo el archivo afectado; los caballos de Troya, que esperan el momento adecuado para ejecutarse y realizar la tarea que el programador le haya señalado; bombas de tiempo, los cuales se guardan en la memoria del sistema o en los discos o en los archivos ejecutables en espera de que se cumpla una fecha u hora determinada para destruir. No siempre este tipo de virus será destructor, si no que algunas veces solo mandará un mensaje sin ningún daño; Infectores del área de carga inicial, cuya función es infectar los disquetes o el disco duro en su sector de arranque, logrando con esta acción tomar el control de la

[17] http //usuarios tripod es/janny/ *Introduccion a los virus* Pag 03

computadora desde que se enciende, pudiendo infectar todo lo que pase por su camino; infectores del sistema que tienen como misión la de introducirse en los programas de sistema o en otros programas que se alojen en la memoria. Como infectan a los archivos del sistema operativo, estos virus tomarán el control de la computadora desde el inicio ya que lo primero que hace la computadora al encenderse es buscar el sistema operativo y al estar infectado este , todo lo demás también lo estará; aunado a lo anterior, todo disco que se introduzca en la computadora será infectado .

Daños en equipo físico.

No existe en la actualidad un virus que directamente destruya o altere el equipo físico, como son monitores, teclados, mouse, módem etc., pero lo que si existe son una gran variedad de virus que al atacar el software hacen trabajar constantemente a los diversos dispositivos antes señalados pudiendo quemarlos, pero esto no se debe a que el virus esté diseñado para realizar esa labor, si no que al destruir parte del o los programas que dan soporte a los multicitados dispositivos, los programas enviarán instrucciones erróneas que pueden traducirse en la destrucción física de nuestra computadora.

Clasificación de daños causados por virus según su gravedad

Daños Triviales.

Utilizaremos para ejemplificar este tipo de daños al virus FORM cuya tarea consiste en que el día 18 de cada mes cualquier tecla que presionemos hace sonar el beep.

Deshacerse del virus implica, generalmente, segundos o minutos y lo único que ocasiona son molestias.

Daños menores.

El virus JERUSALEM se encarga de borrar, los viernes 13, todos los programas que uno trate de usar después de que el virus haya infectado la memoria residente. En el peor de los casos, tendremos que reinstalar los programas perdidos.

Daños moderados.

Existen virus capaces de formatear el disco duro, y de mezclar la información en él contenida o dañar los archivos que le son útiles para ubicar los archivos y programas, o sobreescribe el disco duro. En este caso, es necesario reinstalar el sistema operativo y corremos el riesgo de perder el toda nuestra información.

Daños mayores.

Algunos virus, dada su lenta velocidad de infección y su alta capacidad de pasar desapercibidos, pueden lograr que se pierda la información capturada recientemente en la computadora, pudiendo además obstaculizar su recuperación. Un ejemplo de esto es el virus DARK AVENGER, que infecta archivos y acumula la cantidad de infecciones que realizó. Cuando este contador llega a 16, elige un sector del disco al azar y en él escribe la frase: *Eddie lives ... somewhere in time* (Eddie vive ... en algún lugar del tiempo).

Esto puede haber estado pasando por un largo tiempo sin que lo notemos, y para este entonces el intentar recuperar la información contenida en el disco duro puede resultar una misión imposible, ya que el virus puede haber infectado gran cantidad de la información de nuestra computadora.

Daños severos.

Los daños severos son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No sabemos cuándo los datos son correctos o han cambiado, pues no hay pistas obvias como en el caso del DARK AVENGER (es decir, no podemos buscar la frase Eddie lives ...).

Daños ilimitados.

Algunos programas dan facilidad a los hackers par obtener la clave del administrador del sistema y la pasan a un tercero (esto en redes) Con esta facilidad el hacker puede crear su propio usuario con los privilegios máximos, fijando el nombre del usuario y la clave. El daño es entonces realizado por la tercera persona, quien ingresará al sistema y haria lo que quisiera

Una infección se soluciona con las llamadas *vacunas* (que impiden la infección) o con los remedios que desactivan y eliminan, (o tratan de hacerlo) a los virus de los archivos infectados pero hay cierto tipo de virus que no son desactivables ni removibles, por lo que se debe destruir el archivo infectado y si no se tiene el respaldo pertinente se pierde en definitiva la información.

CAPÍTULO 3

LEGISLACIONES INTERNACIONALES Y REFERENCIAS NACIONALES ACERCA DE LA INFECCIÓN DE EQUIPOS DE CÓMPUTO POR VIRUS CIBERNÉTICOS

PAÍSES EN QUE SE ENCUENTRA REGULADA LA INFECCIÓN DE EQUIPOS DE CÓMPUTO POR VIRUS CIBERNÉTICOS.

En el desarrollo de éste capitulo daremos una ráplda revisión a las legislaciones penales de otros países con el fin de estudiar como han enfrentado el problema de los virus de las computadoras, como han definido el delito y como lo están sancionando. Del estudio practicado, tomaremos los datos más importantes para poder entrar al desarrollo del cuarto capitulo, que consistirá en la formulación de nuestra propuesta al tipo penal de Delitos Cibernéticos.

El antecedente principal de estos temas lo encontramos en el estudio realizado por la Organización de la Cooperación y Desarrollo Económico (OCDE)[18], el cual se llevó a cabo en el año de 1983, teniendo como finalidad el armonizar en el plano internacional las leyes penales a efecto de luchar contra el problema del uso indebido de los programas computacionales, que en ese entonces se encontraba en sus inicios.

Desde estos momentos se empezó a advertir 2 tipos de problemas a los que habia que hacerles frente: el económico, que consiste en afectar diversos intereses por medio del robo de información entre empresas, la destrucción de programas y/o datos trascendentes que pudieran perjudicar las finanzas de una empresa o país y alguna otra variante de delitos cometidos con equipos de cómputo por delincuentes

[18] http://www.stj-sin.gob.mx/Delitos_Informaticos2 htm

informáticos; y el Jurídico-Penal, que consideraba la posibilidad de que la protección jurídico penal nacional pudiera perjudicar el flujo internacional de la información, esto a causa de las restricciones o medidas de seguridad empleados por los Estados con el fin de evitar la infección viral. Después de deliberar se resolvió elaborar una lista con recomendaciones a los Estados miembros de la OCDE. Podemos decir que como inicio de reflexión sobre el problema de los virus fue un buen intento, pero desgraciadamente solo se quedó en eso, ya que la recomendación no era obligatoria y se restringía a los Estados que eran socios de la OCDE, quienes podían o no aplicar el criterio establecido.

En 1986, nuevamente la OCDE publicó un informe titulado *Delitos de informática: Análisis de la normativa jurídica* en donde se reseñaban las normas legislativas vigentes y las propuestas de reformas en diversos Estados miembros, pero nuevamente se concretaba a señalar una lista mínima de ejemplos de uso indebido de la computadora los cuales podrían ser prohibidos y sancionados por las leyes penales de cada Estado miembro. Las conductas que se señalaban como delictivas eran el fraude, la falsificación informática, la alteración de datos y programas de computadora, sabotaje Informático, acceso no autorizado, interceptación no autorizados y la reproducción no autorizada de un programa de computación protegido.

En 1990, durante el Octavo Congreso sobre prevención del Delito y Justicia Penal, organizada por la ONU y llevado a cabo en Cuba, se tocó nuevamente el tema de los delitos informáticos, pero solo se limitó al estudio de la reproducción y difusión no

autorizadas de programas informáticos y el uso indebido de los cajeros automáticos, por lo que solo se emitieron recomendaciones tendientes a solucionar estos temas, dejando de lado el estudio de los virus cibernéticos.

La asociación Internacional de Derecho Penal, realizó un coloquio en 1992, durante el cual se emitieron más recomendaciones a los Estados para hacerle frente a los delitos informáticos. Estas recomendaciones contemplaban que en la medida en que el Derecho Penal tradicional fuera insuficiente para hacerle frente a la nueva realidad, deberá promoverse la modificación, la redefinición de delitos o la creación de otros nuevos. Las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación, además, deberá tenerse en cuenta hasta que punto el Derecho Penal se extiende a esferas afines con un criterio importante para ello, como es el de limitar la responsabilidad penal con objeto de que éstas queden circunscritas primordialmente a los actos deliberados.

Hasta esta fecha predominan únicamente sugerencias que hacen las organizaciones multinacionales a los Estados miembros. Son pocos los paises que toman en cuenta el problema y se esfuerzan en buscar una solución viable aunado a que topamos con el problema de la diversidad de códigos penales y maneras de perseguir el delito La hipotética idea de unificar el criterio de todos los Derechos Penales de todos los países del mundo sería una solución efectiva en el plano de lo ideal, pero en nuestra actualidad esto sería poco menos que imposible.

Todas las recomendaciones se enfocan a que los Estados revisen sus legislaciones y tomen medidas que consideren pertinentes para ***prever*** el daño que se puede sufrir. Desgraciadamente en nuestro país sufrimos una rara enfermedad que nos obliga a tener que padecer algún malestar para entonces empezar a pensar como solucionar el problema y poner parches en todos lados, que lejos de solucionar aunque sea en parte el problema, termina por agravarlo más.

Países en que se encuentra regulado este problema.

En México el avance de la computación (o aún más de Internet) se encuentra en pañales, (muchos profesionistas siguen desconociendo como usar una computadora para su trabajo), siendo ésta la causa probable por la cual nuestras autoridades no han prestado la atención debida al problema que en un futuro no muy lejano deberemos enfrentar.

La literatura existente en este rubro se enfoca más al aspecto de la protección de Derechos de autor , y los pocos que llegan a tocar el tema de esta tesis se concretan a señalar ejemplos de infección sin que se proponga algún a solución (ya no soñar en una probable previsión del problema en los códigos penales locales).

En este caso en particular ha sido la sociedad y algunas escuelas las que se ha preocupado por estudiar el fenómeno de los virus y de publicar el resultado de sus investigaciones en Internet.

Por lo anterior considero que nos puede ser de gran utilidad para el fin que perseguimos el estudiar como otros paises han regulado la delincuencia informática, y en forma especifica a los delitos cometidos mediante el uso de virus cibernéticos.

Alemania.

La segunda Ley contra la criminalidad económica del 15 de Mayo de 1986[19] contempla las siguientes conductas como delitos: a) Alteración de datos, que señala como ilícitos el cancelar, inutilizar o alterar datos; de esta circunstancia la tentativa es punible; b) Sabotaje informático, que comprende la destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos de especial significado, siendo en este caso la tentativa punible.

Cabe hacer la observación que por lo que hace al sabotaje informático, solo se atiende a la *destrucción de datos especiales*, sin que se defina que es un dato especial y aún existiendo dicha definición, se está limitando el bien jurídico tutelado, haciendo particular una ley que deberia ser general, logrando con esto dejar en estado de indefensión a aquellos a que no se encuadran en el supuesto de *dato especial*. Como dato rescatable de esta definición es que la tentativa es punible

Austria.

En este pais la Ley de reforma del Código Penal del 22 de Diciembre de 1987 contempla lo siguiente:

[19] http://www stj_sin gob mx/Delitos_Informaticos2 htm

a) Destrucción de datos. El artículo 148 de la citada ley sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero, influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión de especialistas en sistemas.

A diferencia del legislador alemán, la ley es amplia con relación al bien jurídico tutelado por la norma, pero a nuestro criterio es una definición bastante técnica, que en la práctica requeriría de muchas aclaraciones, además no precisa por que medios se va a introducir, cancelar o alterar el procesamiento de datos y señala que el perjuicio debe ser patrimonial, lo cual significa que debe ser estimado en dinero, debiendo tomar en cuenta que hasta este momento es muy difícil estimar en pecuniario un conjunto de datos intangibles y que en ocasiones puede ser imposible estimar un monto debido al valor intelectual o estimativo que el usuario le otorgue a sus archivos.

Atinadamente el legislador austriaco prevé una sanción especial para aquellos que abusan de sus conocimientos técnicos (especialistas en sistemas), lo cual será retomado por nosotros en el capitulo 4.

Francia.

En Francia la ley número 88-19 del 05 de Enero de 1988[20] sobre fraude informático establece en su artículo 462-3 una conducta intencional definiendo la misma como al que a sabiendas de estar vulnerando los derechos de terceros haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos. El artículo 462-4 también describe como conducta típica al que de manera intencional y a sabiendas de estar vulnerando los derechos de terceros, en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste contiene, o sus modos de procesamiento o de transmisión.

La pena prevista para estas actividades es de diez mil a cien mil francos y de dos a dos años de prisión.

Al igual que la legislación austriaca, la definición del tipo penal francés es técnica, olvidándose de definir que es un *sistema de procesamiento automatizado*, y contempla la sanción para aquellos que hayan actuado intencionalmente, extendiéndose la pena a la infección hecha de manera directa o indirecta.

Ahora bien, el tipo penal padece del mismo vicio que el Austriaco: se sustenta en una valoración de datos intangibles para la aplicación de la norma jurídica, y a nuestro criterio la pena privativa de libertad es ridícula si consideramos el daño tan severo que puede provocar un delincuente de esta especie.

[20] http://www.megazona.com/ZONAVirus/Informes/legislacion_03.htm.

Estados Unidos.

En 1994 los legisladores Estadounidenses se dieron a la tarea de crear una ley simple y eficaz para hacerle frente a los delincuentes informáticos y poner un freno a los ataques de virus, que para ese entonces ya eran constantes en aquélla nación.

De este compromiso surgió el Acta Federal de Abuso Computacional (18 U.S.C. sec. 1030)[21], que evita hacer definiciones plagadas de tecnicismos y sobretodo no entra en la distinción de las diversas clases de virus que existen.

Las conductas penalizadas son la transmisión de programas, información, códigos o comandos que causen daños a la computadora, a sistemas informáticos, a las redes, información, datos o programas. Las penas se prevén según dos criterios: 1. - A los que intencionalmente cáusenle daño por un virus se les aplicará una pena de hasta 10 años en prisión federal, mas una multa, y 2. - En el caso de que la transmisión sea imprudencial, la pena va de la multa a un año de prisión. Otra gran virtud de la legislación norteamericana es que se preocupó por definir al virus, (computer contaminant) entendiendo como tal no solo al grupo de instrucciones informáticas comúnmente llamados virus o gusanos, sino todas aquellas instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o redes.

[21] http://www.megazona.com/ZONA Virus//Informes/Legislacion_03.htm

Otra manera de penalizar a los delincuentes cibernéticos, es mediante el pago de diez mil dólares por persona infectada y hasta cincuenta mil dólares para el caso de acceso imprudencial a una base de datos

La ventaja de la descripción de la conducta típica y antijurídica que hace el legislador norteamericano, es que se abstiene de utilizar términos técnicos y se concreta a enunciar como se va a acusar el daño a la computadora, sin entrar tampoco en el problema de otras legislaciones de intentar valuar el monto al que haciende la pérdida de datos o información.

Otra situación relevante es la manera en que penaliza la conducta antijurídica. La mayoría de las legislaciones de los otros países que hemos revisado se concretan a sancionar la conducta dolosa con penas ridículas, pareciendo que los legisladores de esos países carecen de sensibilidad respecto del problema planteado. El hecho de sancionar tanto al creador como al difusor imprudencial del virus es, a nuestro punto de vista una medida acertada ya que al sancionar al difusor imprudencial, se obliga a todos los usuarios a verificar el contenido, legalidad y seguridad de los archivos que reciben y los que envían (esto mediante el uso de un buen programa antivirus), pudiendo con esto reducir en gran medida los estragos que causan los virus.

En el mismo orden de ideas, consideramos que es válido fijar una multa por la infección a cada usuario afectado, ya que con esto se logra salvar el obstáculo de dar un valor determinado a un conjunto de datos intangibles, los cuales pudieran llegar a tener un valor meramente estimativo.

España.

El artículo 263 del Código Penal Español, referente al Daño en propiedad ajena refiere 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 medio dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soporte o sistemas informáticos.

Este tipo penal parece haber tomado muchos de los elementos del tipo Estadounidense ya que mención únicamente al resultado y no al medio para causar algún daño a una computadora, pero se concreta a sancionar la conducta dolosa.

En Gran Bretaña y Holanda también se encuentra regulada la infección por virus de computadoras, sin que aporten algún dato relevante para el estudio que practicamos. En América latina, la infección viral a computadoras se encuentra regulada en Chile y Argentina, resaltando ésta última, por la diferenciación que hace entre los daños causados al software y a las bases de datos, pero incurre en el error de la mayoría de las legislaciones de considerarlo como Daño en propiedad ajena y no como un tipo distinto que puede contar con sus propias características.

Tratados Internacionales en esta materia.

No existen tratados que se enfoquen en particular a combatir los daños ocasionados por el ataque de virus de computadoras. La gran mayoría de los

tratados hablan exclusivamente de la piratería y de derechos de autor, sin que se pueda tomar dato alguno para considerarlo dentro del estudio que practicamos.

La Organización de las Naciones Unidas señala como tipos de delitos informáticos los fraudes cometidos mediante manipulación de computadoras, los daños o modificaciones de programas o datos computarizados y las falsificaciones informáticas. Dentro de los daños o modificaciones encontramos:

1. - El sabotaje informático, consistente en el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadoras con la intención de obstaculizar el funcionamiento normal del sistema. El modo de cometer el sabotaje es mediante:

a) Virus, que se encuentran definidos como una serie de claves programáticas que pueden adherirse a los programas legítimos, y propagarse a otros programas informáticos.

b) Gusanos, los cuales se fabrican de forma parecida a los virus y tienen como fin modificar y destruir datos, logrando cumplir con su cometido mediante la infiltración del gusano en un programa legítimo. A diferencia del virus, el gusano no se puede regenerar.

c) Bomba cronológica.- Es un programa que cuenta con la instrucción precisa de en una fecha y hora determinada iniciar su acción destructiva; son difíciles de detectar, por lo que es posible pedir un *rescate* para evitar que la *bomba* detone.

El problema del tipo penal de Daño en propiedad ajena.

Como hemos visto, la mayoría de los países cometen el error de considerar el ataque de un virus cibernético, como un daño en propiedad ajena, esto en atención a que a simple vista lo que se distingue es una conducta dolosa mediante la cual el sujeto activo causa un detrimento patrimonial a un sujeto pasivo. Esta consideración errónea nos lleva al callejón sin salida de valuar el monto de lo dañado, y como lo mencionamos con antelación, esto es muy difícil.

Nuestra actual legislación penal federal contempla en sus artículos 397, 398 y 399 al Daño en propiedad ajena. Los artículos 397 y 398 señalan diversas circunstancias que son consideradas como daño en propiedad ajena, pero no son relevantes para el fin de esta tesis. Sin embargo, el artículo 399 señala *Cuando por cualquier medio se causen daño, destrucción o deterioro de cosa ajena, o de cosa propia en perjuicio de tercero, se aplicarán las sanciones del robo simple*; esta descripción de una conducta típica y antijurídica podría considerarse suficiente para resolver una querella presentada por el daño sufrido por el ataque de un virus, pero como explicaremos más adelante, este precepto legal es sumamente insuficiente y presenta diversos obstáculos insalvables en la práctica.

Como hemos descrito en capítulos anteriores la función de un virus es atacar el software, logrando en la mayoría de los casos la destrucción o inutilización de la información guardada en el equipo de cómputo. Esta inutilización parcial o total puede

traducirse en un detrimento patrimonial en agravio del infectado por la falta de datos para la realización de alguna actividad; esto significa que la simple infección ***NO*** representa un detrimento en el patrimonio del infectado, sino que el detrimento se puede observar cuando la falta de información interrumpe o dificulta alguna actividad económica.

Teniendo esto en cuenta estamos en posibilidad de explicar porque nuestra actual legislación no es suficiente para el caso planteado: La primera parte del artículo 399 podría ser útil, ya que no limita los objetos que pueden ser afectados, si no que es un concepto amplio al mencionar que el daño se cause por *cualquier medio* a *cosa ajena o propia en perjuicio de tercero*.

El párrafo antes citado podría ser utilizado para el fin que perseguimos, con sus debidas modificaciones, ya que la esencia de la infección viral es que un sujeto infecte a varios usuarios (terceros) causándoles pérdidas. La hipótesis de destruir una cosa propia con el fin de causar un perjuicio a un tercero también es aplicable y para que quede clara la idea pondremos un ejemplo: El ejecutivo Pedro Pérez trabaja para la empresa *Patito S.A. de C.V.* y para la realización de su trabajo cuenta con información vital para la empresa y la guarda en su PC que se encuentra en su domicilio. Por azares del destino se entera que próximamente va a ser despedido y con el fin de perjudicar a la empresa deliberadamente infecta su computadora con alguno de los virus existentes, destruyendo su información y la información de la empresa. En este ejemplo se observa la intención (dolo) de perjudicar al tercero al deteriorar o destruir un bien propio.

Por otro lado, está la infección accidental que pude sufrir un equipo, sistema o redes de cómputo: El mismo empleado, Pedro Pérez consiguió en el mercado negro un *simulador de vuelo* (juego para computadora) y como no tiene tiempo para jugarlo en su casa, lo instala en la PC que le dan en la empresa para trabajar y que está conectada en red; desconoce que el producto está infectado con el virus *Natas* y sigue todas las instrucciones de la instalación. Al momento de querer jugar la pantalla se pone negra y aparece un mensaje que dice *su computadora está siendo infectada por el virus natas*, desesperado apaga la computadora y la vuelve a encender, se da cuenta que la computadora no arranca y manda mensajes de error: la infección está terminada y corre el riesgo de infectar a la red de toda la empresa, pudiendo destruir la información de todos. ¿Porqué pasó esto?, primeramente por comprar programas piratas y luego por no tener la precaución de verificar el contenido del disco con un programa antivirus actualizado. En este caso no existe la intención deliberada de perjudicar a un tercero, pero por negligencia se hace, pudiendo tener resultados desastrosos.

Hasta este punto el artículo en comento resulta útil, ya que la descripción hecha por el legislador nos da campo para poder adecuar la conducta al tipo penal de una manera muy general. El siguiente punto es la pena, que según señala el artículo 399 del multictado código, será conforme a las reglas aplicables al robo simple. Esta consideración nos lleva a pretender valuar el detrimento patrimonial sufrido, ya que el artículo 370 del código penal federal fija sus penas en relación a la cuantía de lo afectado.

Esta situación nos complica la existencia ya que hasta el momento no existe medio alguno por el cual estimar el valor de un conjunto de datos intangibles; solo en algunos casos se podría estimar el valor de la consecuencia, pero no se sanciona el acto de colocar un virus en una PC. , redes o sistemas de cómputo.

Al hablar de consecuencia nos referimos a que la falta de información se traduzca en algún detrimento económico, por ejemplo, la empresa que no cuenta con la información suficiente para cerrar un trato de una suma considerable de dinero, por lo que ve perdidas sus expectativas de llevar a cabo el trato y obtener ganancias.

En los casos de atacar Instituciones de investigación, la información solo interesa a esos centros, por lo que años de trabajo se pueden echar a la basura, sin que se le pueda sancionar al responsable por el hecho de no poder estimar el monto de lo afectado.

Actualmente nos encontramos con el obstáculo de no contar con el personal adecuado para el estudio de este tipo de problemas (con problemas en las Procuraduría contamos con peritos valuadores), por lo que es necesario reunir a un equipo especializado en búsqueda, detección y detención de los creadores de los virus y de sus difusores.

Por otro lado el artículo 371 del citado ordenamiento penal señala en sus párrafo primero y segundo que *para estimar la cuantía del robo se atenderá únicamente al*

valor intrinseco del objeto del apoderamiento, ***pero si por alguna circunstancia no fuere estimable en dinero o si por su naturaleza no fuere posible fijar su valor*** *, se aplicará prisión de* ***tres días hasta cinco años****. En los casos de tentativa de robo,* ***cuando no fuere posible determinar su monto,*** *se aplicará de* ***tres días a dos años de prisión***

Este artículo parece salvar el obstáculo de valuar el detrimento patrimonial que resulta de la infección viral, y aparte sanciona la tentativa (que aplicándolo al caso particular que propondremos resultaría muy útil para sancionar al creador del virus que todavía no ha afectado a nadie por no haber sido utilizado el programa), pero las penas que estable a nuestro criterio son muy benévolas con el responsable del ilícito si consideramos la magnitud de los problemas que se pueden ocasionar

Finalmente es de hacerse notar que el delito de Daño en propiedad ajena se persigue a petición de ofendida (querella), lo que implica que el Ministerio Público no puede realizar su función investigadora hasta que el ofendido no presente su querella por el ilícito y cabe la posibilidad de otorgar el perdón al delincuente.

Nuestra opinión en el caso del tipo penal de delitos cibernéticos que proponemos es que éste se debe de hacer del conocimiento del Ministerio Público a través de la denuncia y no la querella como ocurre en el Daño en propiedad ajena, lo anterior en razón a que en el Daño en propiedad ajena el Estado deja la potestad a los ciudadanos de querellarse por el ilícito sufrido, ya que la sociedad en general no ve

afectados sus intereses, pero en el caso de la infección por medio de virus de computadora no solo se puede afectar a los particulares, sino que también se puede atacar a Instituciones públicas y con esto se vería afectada la vida de los gobernados a no poder realizar sus funciones y labores

Consideramos que para el caso especifico de esta tesis es necesario señalar parámetros en la norma jurídica que sean útiles para sancionar debidamente a los responsables de infecciones virales, debiendo establecer una pena fija por la infección hecha dolosa o culposamente, y además señalar una multa para los casos en los que como resultado de la infección se provoque un detrimento patrimonial.

Antecedentes en nuestro país.

En la actualidad en Estado de Sinaloa regula en su Código Penal al Delito Informático, el cual se encuentra en el Título décimo Delitos contra el patrimonio, Capítulo V, artículo 217 que a la letra dice:

Artículo 217. Comete delito informático, la persona que dolosamente y sin derecho:
I.- Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar a o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o

II.- Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en base, sistema o red.

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.

El citado artículo representa un avance importante en la toma de conciencia del problema que planteamos, ya que si bien es cierto en México aún no sufrimos graves problemas por el uso de virus de computadoras, también lo es que no debemos ser ajenos dicha situación y que es mejor prever que lamentar. Sin embargo es necesario hacer las siguientes precisiones:

El artículo que comentamos habla de dos circunstancias: el fraude informático y la infección de virus cibernéticos. Consideramos que por sus propias y especiales características dichas conductas deben preverse y sancionarse por separado, esto con el fin de tener una tipo penal que sea útil para cada uno de los casos, aunado que se pueden delimitar y describir mejor las circunstancias que se pretendan regir

La fracción II señala una serie de conductas y un resultado al que se sanciona con pena de seis meses a dos años y multa. Consideramos que al señalar conductas específicas se está limitando el rango de aplicación de la norma jurídica, además de que se omite el medio por el cual se intercepte, interfiera, reciba, use, altere, dañe o

destruya un soporte lógico (siendo que no se define que es un *soporte lógico*) o programa de computadora.

Se debe tomar en cuenta que se sanciona únicamente al que actúa de manera dolosa, descuidando a los que de manera accidental o negligente infectan un equipo o sistema de cómputo, tal y como ya lo explicamos en párrafos anteriores.

Otro problema que observamos, es que no se sanciona al creador del virus, sino que solo menciona circunstancias consumadas, siendo que el virus puede ser colocado en Internet esperando que alguien lo abra e inicie la infección. Esta circunstancia puede ser sancionada como tentativa, ya que la resolución de cometer el ilícito se está exteriorizando en parte o totalmente con el fin de obtener un resultado.

Desde nuestro punto de vista el inconveniente mas serio de este artículo es su ámbito de aplicación territorial ya que el mismo se limita al territorio del Estado de Sinaloa, lo cual significa que el virus sea difundido y los daños causados dentro de esos límites. Esta situación nulifica el beneficio que pudiera tener la norma, ya que generalmente el creador del virus se encuentra en un lugar y los infectados en distintas zonas geográficas del país o en el extranjero.

Finalmente merece comentario la pena que prevé el citado artículo. El legislador del Estado de Sinaloa acierta al fijar una pena y una multa, ya que con esto salva el problema antes mencionado del Daño en propiedad ajena, pero la pena privativa de libertad, (como en el caso de las legislaciones de otros países) es benévola con el

delincuente, esto si consideramos que el creador del virus no es un delincuente común y corriente, ya que éste debe tener cierto status social para poder contar con un equipo de cómputo actualizado para poder difundir su creación, que debe ser una persona inteligente para idear al virus, además debe tener estudios en programación de sistemas de cómputo y debe contar con un acceso a Internet.

Este conjunto de características nos dan a un delincuente profesional que merece una pena privativa de libertad más alta que la que el multicitado ordenamiento penal prevé. Es también de considerarse que el daño que se puede ocasionar puede ser muy grave (Ejemplo: se puede paralizar la actividad de una empresa privada o de los órganos gubernamentales), por lo que no sería exagerado considerar esta conducta como delito grave por la Ley penal.

CAPÍTULO 4

CREACIÓN DEL TIPO PENAL DE DELITOS CIBERNÉTICOS EN EL CÓDIGO PENAL FEDERAL MEXICANO

CREACIÓN DEL TIPO PENAL DE "DELITOS CIBERNÉTICOS" EN EL CÓDIGO PENAL FEDERAL MEXICANO.

Después de que en capítulos anteriores hemos visto la problemática que representan los virus cibernéticos, sus creadores y el riesgo que significa seguirlos ignorando desde el punto de vista del Derecho, entraremos al estudio de nuestra propuesta, desglosando cada uno de sus puntos.

Para comprender en su totalidad nuestra propuesta es necesario saber qué es un delito y como se integra el mismo, por lo que acudiremos a la doctrina y principalmente a la teoría del delito para contestar estas interrogantes.

A través del tiempo los diversos estudiosos de la ciencia penal han proporcionado sus definiciones de lo que es un delito, pero por su importancia y su uso práctico sobresalen dos: la primera, la de Carrara[22] que señala que el delito no es un hecho sino un *ente jurídico*, esto es, una infracción a la Ley, una contradicción entre la conducta y la Ley, y la segunda , la que nos proporciona nuestro Código Penal Federal en su artículo 7, el cual señala que *delito es el acto u omisión que sancionan las leyes penales.*

[22] **Cortes Ibarra,** Miguel Ángel.- Derecho Penal Parte general, Ed. Cárdenas editor y distribuidor, 4ta ed Mexico 1992, pág. 125

Para los efecto de esta tesis tomaremos como punto de partida la definición que nuestro Código Penal Federal proporciona, ya que no pretendemos elaborar un tratado acerca de la teoría del delito, sino hacer una propuesta de tipo penal.

El delito consta de las siguientes características:

a) Conducta.

b) Tipicidad.

c) Antijuridicidad,

d) Imputabilidad.

e) Culpabilidad

f) Punibilidad,

La ausencia de cualquiera de estos elementos implica necesariamente que la conducta desplegada por el sujeto no sea considerada por la ley penal como delito

La conducta es el elemento esencial del delito, que en materia penal debemos entender como el comportamiento activo u omisivo que, complementado con los otros elementos constituyen al delito. La acción se forma por actuar voluntariamente, con una violación a una norma penal; la omisión la doctrina la divide en dos: la omisión simple que consiste en no realizar voluntariamente aquello que la ley penal obliga a hacer y la comisión por omisión u omisión impropia que se da cuando culposa o dolosamente se omite realizar la conducta que evitaría la producción del resultado dañoso.

Según Miguel Ángel Cortes Ibarra, la conducta se integra por dos elementos: el psíquico o interno y el material o externo. El elemento psíquico es el ánimo del sujeto activo del delito de hacer o dejar de hacer algo con el fin de alcanzar un propósito; por su parte, el elemento externo o material de la conducta se encuentra formado por la exteriorización del elemento psíquico, esto es, después de haber reflexionado en lo que se va a hacer o dejar de hacer se lleva a cabo lo pensado.

Dentro del estudio de lo que es la conducta encontramos que existen dos sujetos: el activo, que será aquella persona física que actúa o deja de actuar, generando un delito y el pasivo que es la persona física o moral sobre quien recae el daño o perjuicio causado por la conducta del delincuente. Ahora bien, se distinguen dos tipos de sujetos pasivos a los que la doctrina denomina como sujeto pasivo de la conducta, quien es el que reciente directamente la acción de sujeto activo, pero puede no ser el titular del bien jurídico que la norma protege y sujeto pasivo del delito, quien es el titular del bien jurídico tutelado por la norma mismo que resulta afectado por el actuar del sujeto activo.

Para dejar en claro lo antenor expondremos el siguiente ejemplo: El ciberpunk a puesto en Internet un juego para computadora que puede ser copiado de manera gratuita y el empleado José (que tiene acceso a Internet desde la computadora de su trabajo) lo *baja*, ignorando que el juego no es mas que una cubierta para un virus. En el momento que terminó de *bajarlo* el virus empieza a trabajar y se esparce por toda la compañía, causándole pérdidas económicas.

Suponiendo que existiera el tipo penal que propondremos más adelante, el ciberpunk es el sujeto activo del delito ya que éste ideó el modo de perjudicar a los demás mediante la infección del virus y lo coloca en la red en espera que algún incauto lo copie; el empleado José estaría cometiendo un delito de comisión por omisión ya que al *bajar* el programa debe tener la precaución de verificar, con un programa antivirus, si el juego no está infectado o es un virus, por lo que está dejando de realizar una conducta que evitaría un resultado dañoso para la empresa en la que trabaja, siendo ésta última el sujeto pasivo del delito, ya que es la empresa la que va a ser la que resulte afectada por el daño que la norma jurídica debería proteger (la computadora, sus programas, redes, etc.) .

Para poder entrar al estudio del siguiente elemento del delito, es necesario saber que es un tipo penal. Según el maestro Eduardo López Betancourt, "el tipo penal es la descripción hecha por el legislador, de una conducta antijurídica, plasmada en la ley"[23].

Según el mismo autor los elementos del tipo son la acción, los sujetos y el objeto; de la acción ya hablamos anteriormente y de los sujetos cabe hacer la precisión que el citado maestro refiere que el Estado es considerado como un sujeto ya que éste espera que con la amenaza de la pena, que el sujeto activo se abstenga de realizar su conducta antijurídica; por su parte el sujeto activo está consiente de la actitud del

[23] **López Betancourt**, Eduardo - Teoría del delito Ed Porrua, 7 ed Mexico 1999, pag 126

Estado, quien lo perseguirá y lo castigará, y el sujeto pasivo confía en que el castigo al delincuente haga desistir a otros de la ejecución de un hecho delictivo[24]

El objeto se distingue en material y jurídico, entendiendo el primero como la persona o cosa donde recae materialmente la acción; en este caso pueden coincidir el objeto material y el jurídico aunque esto no siempre suceda así. El objeto jurídico es el bien protegido por la ley penal, mismo que puede no ser el objeto material.

El delito se integra por elementos objetivos, subjetivos y normativos. Los elementos objetivos son la descripción de la conducta antijurídica desde el punto de vista externo, esto es, son la manifestación de la voluntad en el mundo material. Los elementos subjetivos atienden al ánimo que tuvo el sujeto activo para la realización de una conducta penalmente sancionada; los elementos subjetivos se crean en la psique del autor del acto.

El maestro Jiménez Huerta señala que "la importancia de los elementos típicos subjetivos es extraordinaria, pues aparte de condicionar la posible aplicación de la figura típica, sirven para excluir apriorísticamente las configuraciones basadas en los contornos y perfiles del actuar culposo"[25].

[24] **López Betancourt**, Eduardo - Ob cit pág 128
[25] **Jiménez Huerta**, Mariano, citado por **Eduardo López Betancourt**.- Ob cit pag 136

En nuestro caso atenderemos a los elementos subjetivos del delito con el fin de poder distinguir a aquellas personas que premeditadamente busquen causar un perjuicio a terceros en sus equipos de cómputo de quien por *accidente* introduzcan un virus a cualquier equipo de cómputo.

Los elementos normativos hacen referencia a lo antijurídico y generalmente va vinculado a la conducta y medios de ejecución; se puede reconocer por frases como *sin derecho y sin consentimiento, indebidamente, sin justificación*, etc. Los elementos normativos, señala López Betancourt, son una llamada de atención al juez, en los que se trata de advertir debe confirmar la antijuridicidad de la conducta, ya que con estos elementos, un hecho aparentemente lícito puede pasar a ser un hecho ilícito; asimismo puede ocurrir lo contrario, es decir que un hecho aparentemente ilicito no lo sea.

Una vez explicado que es un tipo penal y como se conforma entraremos al estudio de lo que es la Tipicidad. Conforme a lo expuesto por el maestro Luis Jiménez de Asúa[26], la tipicidad es la exigida correspondencia entre el hecho real y la imagen rectora expresada en la ley en cada especie de infracción, esto significa que la conducta exteriorizada por un sujeto, para que sea considerada como delito debe ubicarse dentro de alguna de las descripciones señaladas en la Ley penal.

[26] **Jiménez de Asúa**, Luis - Tratado de Derecho Penal, III, 2da ed. Ed. Losada, S.A., Buenos Aires, 1958, pag 744.

Ahora bien, es necesario distinguir los términos tipicidad y tipo, como ya mencionamos la tipicidad *es el adecuamiento de la conducta* a la descripción del delito establecido en la ley penal y el tipo es únicamente *la descripción de la conducta que se considera como un delito* .

Doctrinariamente se dice que la tipicidad se rige por los siguientes principios:

a) *Nullum crimen sine lege* - No hay delito sin ley.

b) *Nullum crimen sine tipo - No hay delito sin tipo.*

c) *Nulla poena sine tipo* - No hay pena sin tipo.

d) *Nulla poena sine crimen* - No hay pena sin delito.

e) *Nulla poena sine lege* - No hay pena sin ley.

En la actualidad la ley penal que nos rige se ve superada, ya que como vimos en capítulos anteriores existe la conducta dañosa (la destrucción o alteración de los equipos de cómputo), existen sujetos activos (aquellos que crean el virus y/o lo distribuyen) y sujetos pasivos (todo aquel que reciente el daño causado por los virus) y no existe ley que persiga y sancione a los autores de la citada conducta, y al no estar tipificada esta conducta no puede ser considerada como delito y carece de sanción (atipicidad). Este punto es la médula de la presente tesis, ya que como lo hemos explicado en capítulos anteriores los actos realizados por profesionales de la computación con el fin de perjudicar a terceros no se encuentran previstos en nuestro Código Penal Federal (si bien es cierto que el tipo penal existe en el estado de Sinaloa, también lo es que su ámbito de aplicación territorial es sumamente limitado)

por lo que consideramos que es urgente establecer los parámetros que sirvan de base para crear un tipo penal adecuado y eficaz que pueda hacer frente a la realidad que nos podemos enfrentar.

La antijuridicidad es lo contrario a derecho y la doctrina distingue dos tipos: La material que es propiamente lo contrario a derecho, por cuanto hace a la afectación genérica hacia la colectividad y la formal que es la violación de una norma emanada del Estado.

La imputabilidad es la capacidad de entender y querer para realizar determinado acto La imputabilidad implica salud mental y aptitud psíquica de actuar El sujeto primero deberá ser imputable para luego ser culpable.

La culpabilidad según el maestro López Betancourt, puede tener diversas definiciones dependiendo del punto de vista que el autor tenga al momento de emitir su opinión pero en términos generales podemos entender a la culpabilidad como "el nexo que se da entre dos entes; en la culpabilidad es la relación entre el sujeto y el delito, esto es, el nexo intelectual y emocional entre el sujeto y el delito"[27]

Según el citado maestro la culpabilidad consta de los siguientes elementos

a) La exigibilidad de una conducta conforme a la ley;

b) La imputabilidad y

[27] **López Betancourt** Eduardo - Teoría del delito 7a. ed. Ed. Porrua México 1999 pag 214

c) La posibilidad concreta de reconocer el carácter ilícito del hecho realizado.

Existen dos tipos de culpabilidad que son el dolo y la culpa. El dolo consiste en el conocimiento de la realización de circunstancias que pertenecen al tipo, y voluntad o aceptación de realización del mismo. La culpa, según lo establecido por la Suprema Corte de Justicia de la Nación "radica en obrar sin poner en juego las cautelas y precauciones exigidas por el Estado para evitar que se cause daño de cualquier especie. Comete un delito imprudente, quien en los casos previstos en la ley, cause un resultado típicamente antijurídico, sin dolo, pero como consecuencia de un descuido evitable"[28]

Para probar la existencia de la culpa es necesario reunir los siguientes elementos

1.- La ausencia de la intención delictiva.

2.- La presencia de un daño igual al que pudiera resultar de un delito intencional

3.- La relación de causalidad entre el daño resultante y la actividad realizada

4.- Que el daño sea producto de una omisión de voluntad, necesaria, para preservar de un deber de cuidado, indispensable para evitar un mal Esta omisión de la voluntad exige que el hecho sea previsible.

Finalmente la punibilidad es la amenaza de una pena que contempla la ley para aplicarse cuando se viola la norma . En cuanto a este elemento hay autores que no lo

[28] **Semanario Judicial de la Federación**, tomo LVIII, sexta época, segunda parte, pag 24-25 y Vol 83, segunda parte, septima época pag. 30-31, citado por **López Betancourt**, Eduardo Ob Cit Pag 234

consideran como un elemento del delito si no una consecuencia, pero si atendemos a la definición del articulo 7 del Código Penal federal, el cual señala que *delito es toda acción u omisión que sancionan las leyes penales*, veremos que este elemento es indispensable en la constitución del delito (o por lo menos para ser considerado como tal en nuestro sistema jurídico), ya que el citado artículo atiende a la pena a la que se hará acreedor cualquier sujeto que incurra en alguna de las conductas que la ley penal prevé, siendo que si no se encuentra sancionada determinada conducta no se podrá considerar la misma como delito por no encuadrar en la definición del artículo 7 del Código Penal Federal.

Definición del tipo penal propuesto

Una vez que hemos revisado brevemente la teoria del delito y que en los capítulos anteriores hemos analizado la problemática que representa el diseño, transmisión e infección por virus cibernéticos, entraremos a nuestra propuesta del tipo penal, describiendo y justificando cada uno de sus elementos

El tipo penal propuesto es el siguiente:

Comete delito cibernético aquel que diseñe o transmita intencional o accidentalmente y por cualquier medio, un programa, instrucciones , información, códigos o comandos de una computadora propia o ajena a otra causando daños a la misma, a sus sistemas informáticos, redes, información, datos y/o programas.

La palabra cibernético (a), según el diccionario de la lengua España tiene diversos significados de los que sobresalen:

I. Ciencia que estudia comparativamente los sistemas de comunicación y regulación automática de los seres vivos con sistemas electrónicos y mecánicos semejantes a aquellos. Entre sus aplicaciones está el arte de construir y manejar aparatos y máquinas que mediante procedimientos electrónicos efectúan cálculos complicados y otras operaciones similares.

II. Arte de gobernar, estudio de la dirección, regulación y comunicaciones en máquinas, calculadoras, organismos y actividades económicas.

III. Ciencia que estudia los mecanismos automáticos de las máquinas.

Como se puede advertir desde el título de la presente Tesis, nuestra definición atiende a *delitos cibernéticos* y no a *delitos informáticos* como lo hace la mayoría de los autores y algunos tipos penales de las legislaciones que hemos revisado.

Esta circunstancia se ve sustentada en que la palabra *informático* significa *ciencia del tratamiento automático y racional de la información considerada como soporte de los conocimientos y las comunicaciones. El tratamiento de la información se hace con*

el ordenador o la computadora...[29]. De la anterior definición se desprende que la palabra *informático* únicamente hace referencia a la información considerada como *soporte de los conocimientos y las comunicaciones* pudiendo entender como tales a los programas de computadora y a sus archivos de programa, pero nunca a los programas que están diseñados únicamente para diversión o entretenimiento ni a los archivos o programas que el usuario haya creado y que tenga almacenados en su computadora.

Es de considerar también que la definición antes citada hace referencia a que la información recibe un trato *automático y racional* tarea que se le adjudica al ordenador o computadora, por lo que la citada definición solo atiende a la manera de trabajar de la computadora y descuida la interacción del usuario con la computadora

La palabra *cibernético* desde nuestro punto de vista describe mejor la interacción del usuario al señalar que *estudia comparativamente los sistemas de comunicación y regulación automática de los seres vivos con sistemas electrónicos*, aunado a que no limita el alcance de la definición a la manera de trabajar de la computadora (como sucede en la definición de la palabra *informático)* si no que abarca lo concerniente a la construcción y manejo de aparatos electrónicos que efectúan cálculos complicados y otras funcionas automáticamente.

[29] **García-Pelayo y Gross** Ramon - Larousse diccionario básico escolar Editorial Larousse S A de C V , Mexico 1987, pág. 158

Siguiendo con el análisis de nuestra propuesta de tipo penal vemos que el delito puede ser cometido de manera dolosa (Diseño y/o transmisión del virus por cualquier medio con el fin de perjudicar a un tercero) o culposa (la transmisión del virus por no seguir medida previas de *vacunación* o revisión del contenido del disco o archivos que se ejecuten en la computadora).

Como se pudo observar en el desarrollo del capítulo tercero la mayoría de los tipos penales hablan únicamente de perseguir a aquellos que dolosamente diseñen o distribuyan un virus, sin que se considere a los que accidentalmente distribuyan el virus ya sea en redes, Internet o cualquier otro medio. Consideramos que es grave esta omisión ya que si una persona dolosamente distribuye el virus causando daños y perjuicios a terceros se puede excusar diciendo que el no sabia que el programa o archivos que transmitía eran un virus, por lo que al no estar penado se deja a un delincuente sin sanción.

Ahora bien, la pena no puede ser la misma que en el caso de la infección dolosa, ya que puede suceder que el sujeto efectivamente *contagie* a otros de manera accidental (como sucedió con el virus I Love You, que una vez que infectaba una computadora se autorreplicaba por medio del correo electrónico e infectaba a otras personas). Consideramos necesario sancionar a estos *infectores accidentales* ya que todo usuario tiene la obligación de mantener sus computadoras limpias de virus mediante el uso de programas antivirus actualizados y abstenerse de instalar en sus computadoras programas *piratas*.

Al referirnos al modo de infección decidimos no utilizar tecnicismos informáticos que podrían dificultar el entendimiento del tipo penal a personas que desconocen del tema y peor aún, limitar el alcance del tipo penal a medios que en la actualidad son usuales o novedosos y que en un futuro podrían estar en desuso.

El tipo penal propuesto está enfocado a sancionar a los creadores y distribuidores de virus cibernéticos, pero en un tipo penal no podemos decir que se sancionará al creador o distribuidor de un virus, primeramente porque sería necesario definirlo y especificar las características del mismo, tarea que como ya explicamos en capítulos anteriores es muy complicada, ya que dependiendo del creador del virus serán las características y funciones que este tenga y segundo porque lo que ahora conocemos como *virus* puede ser que en algunos años ya no sea considerado como tal o que el concepto quede corto para afrontar las nuevas realidades.

Es por lo anterior que dentro de tipo penal propuesto se señalan las características más comunes en las estructura de un virus (ser un programa, estar oculto en información o datos e integrarse por códigos o comandos de computadora) las cuales juntas o separadas pueden ser perjudiciales a terceros si se manejan con el fin de afectar a terceros.

Por último hacemos referencia a los daños que se causa al *infectar* una computadora con un virus, el cual se puede percibir desde la pérdida de datos por alteraciones a

los programas o destrucción de archivos hasta el daño físico a algunos de sus componentes.

Su ámbito de aplicación

En el ámbito nacional.

Al señalar que el tipo penal propuesto debería ser ingresado al Código Penal Federal, debemos entender que la norma jurídica se aplicará a nivel federal, esto es, se sancionaría al que diseñe o distribuya el virus en el territorio nacional, esto sin importar la nacionalidad del que distribuya o diseñe el virus con la única condición de que la distribución se haya originado en el territorio nacional, ya que no podemos pretender que nuestra ley penal se extraterritorialice y se sancione al diseñador y distribuidores que se encuentran en otro país

El problema del Derecho Internacional Privado

Lo ideal es que existiera un acuerdo entre la mayoría de los Países con el fin de llegar a un común denominador y poder perseguir a los diseñadores y distribuidores de los virus cibernéticos a nivel internacional, ya que el fenómeno de infección viral se ha dado a ese nivel debido en gran parte a el desarrollo de Internet

Podemos ver que el diseñador es Inglés, el diseño se realizó en Alemania y la infección ya afectó a Latinoamérica, Rusia, y Estados Unidos . Cada uno de los

países quiere aplicar su propia legislación al respecto y pretende imponer su sanción a otros países.

En este asunto nos vemos ante un conflicto de Leyes al querer un Estado imponer su legislación a otro u otros países.

La tarea del Derecho Internacional Privado es elegir la ley competente para una situación jurídica concreta, cuando cabe la posibilidad de aplicación de normas jurídicas provenientes de Estados diversos[30]. Si contáramos con algún acuerdo internacional el problema de los creadores y distribuidores de los virus cibernéticos a nivel Internacional se vería resuelto en gran medida, ya que sin importar el origen del virus y el lugar de los daños se podría perseguir al delincuente. Sin embargo esto resulta muy complicado, ya que hasta el momento lo único que han logrado algunas organizaciones internacionales es emitir recomendaciones que pueden o no tomar en cuenta los Estados afiliados a dichas organizaciones internacionales que estudian la problemática los virus.

Pero no solo se debe atender al problema Internacional; también se debe ver al interior del país, que es finalmente lo que persigue la presente tesis.

Para poder suscribir cualquier tratado se debe tener el mínimo conocimiento del problema y conocer los efectos que éste produce en el país. Si bien es cierto que un Tratado Internacional solucionaría en gran medida el problema a nivel multinacional,

---

[30] **Arellano García** Carlos - Derecho Internacional Privado Mexico 1998, Ed Porrua , decimo segunda ed Pág. 3

también lo es que el tratado no podría sancionar a los delincuentes que hayan actuado en su país de origen y los efectos del virus se hayan producido en el mismo. Es por esta razón que es necesario contar con una legislación nacional que sancione el hecho delictivo y no dejar solo al Tratado Internacional como única solución al problema que se plantea.

Los requisitos de procedibilidad.

Para que se pueda seguir un proceso penal en contra de persona alguna es necesario que se cumplan los supuestos que señala el artículo 16 párrafo segundo de nuestra Constitución Política que señala *No podrá librarse orden de aprensión sino por la autoridad judicial y sin que preceda* ***denuncia o querella*** *de un hecho que la ley señale como delito, sancionado, cuando menos con pena privativa de libertad y existan datos que acrediten el cuerpo del delito y que hagan probable la responsabilidad del indiciado.*

Según el maestro Cesar Agusto Osorio y Nieto los requisitos de procedibilidad son las condiciones legales que deben cumplirse para iniciar una averiguación previa y en su caso ejercitar la acción penal contra el responsable de la conducta típica.[31] Son la denuncia y a la querella los requisitos de procedibilidad que exige la Constitución Mexicana en su artículo 16 para girar una orden de aprehensión, y son el medio por el cual se informa al Ministerio Público de la comisión de un delito.

[31] **Osorio y Nieto** Cesar Augusto - La averiguación previa Ed Porrua, 11a ed Mexico 1998, pág 09

Según Colin Sánchez[32]la palabra denuncia o el verbo denunciar desde un punto de vista gramatical, significa: aviso, poner en conocimiento de la autoridad competente, verbalmente o por escrito, lo que se sabe respecto a la comisión de hechos que son o pueden ser delictivos. Por su parte Osorio Nieto señala que la denuncia es la comunicación que hace cualquier persona al Ministerio Público de la posible comisión de un delito perseguible de oficio[33].

Como se desprende de las definiciones antes citadas, la denuncia puede ser hecha por cualquier persona que tenga conocimiento de los hechos delictivos, aún si ser ésta la directamente ofendida; en estos casos, el agente del Ministerio Público tiene la obligación de investigar de oficio los hechos, esto significa que se deberán realizar todas y cada una de las diligencias pertinentes para acreditar el cuerpo del delito y la probable responsabilidad, sin que el denunciante pueda otorgar el perdón en favor del indiciado.

Por otro lado, la querella[34]puede definirse como una manifestación de voluntad, de ejercicio potestativo, formulada por el sujeto pasivo o el ofendido con el fin de que el Ministerio Público tome conocimiento de un delito no perseguible e oficio, para que se inicie y se integre la averiguación previa correspondiente y en su caso se ejercite la acción penal.

---

[32] **Procuraduría General de Justicia del Distrito Federa.**- Apuntes del programa de formacion practico-teorico para oficiales secretarios Mexico 1999, Pag. 21

[33] **Osorio y Nieto, Cesar Augusto** - Idem

[34] **Procuraduría General de Justicia del Distrito Federal** - Ob.cit., Pag 23

A diferencia de la denuncia, la querella debe ser formulada por el directamente ofendido (aún cuando el agraviado sea menor de edad) o por su representante legal (esto puede ocurrir en el caso de personas morales o personas físicas que cuentan con apoderados legales), además en este caso el agraviado puede otorgar el perdón al probable responsable, lo cual implica la extinción de la acción penal, por lo que el Ministerio público deja de investigar y da por concluido el asunto.

La querella da libertad al agraviado de ejercitar o no su derecho, esto en razón de que la querella tiene como fundamentación política la ausencia de interés jurídico por parte del Estado en perseguir determinados ilícitos, por la naturaleza misma de éstos, o que pudiendo tener interés directo se da prioridad a la voluntad de la víctima u ofendido.

La denuncia y el seguimiento de oficio por parte del Ministerio Público

Como ya se mencionó la denuncia es el medio por el cual cualquier persona (aún sin ser la agraviada directamente) informa al Ministerio Público de la posible comisión de un delito y que no se puede otorgar el perdón al responsable del ilícito, por perseguirse el ilícito de oficio.

Consideramos que en el caso de los delitos cibernéticos la denuncia es el medio idóneo para informar al Ministerio Público de la comisión del ilícito, ya que si se persiguiera por querella los únicos facultados para formular la misma serían el directamente agraviado o su representante legal sobre de los daños y perjuicios que éste sufriera, pero debemos tomar en cuenta que el problema planteado en esta

Tesis contempla a una gran cantidad de usuarios que pueden verse afectados por el virus de manera indirecta, esto significa que el mismo virus puede dañar al equipo de cómputo y sus archivos de programa (afectando al dueño de la computadora), y también puede afectar, dañar o destruir el trabajo que se esté realizando en la computadora (que puede ser información de cualquier usuario).

De seguirse a petición de parte cada uno de los agraviados tendría que formular su querella por el mismo hecho y cualquiera de los agraviados estarían en posibilidad de otorgar el perdón al probable responsable, lo que extingue la acción penal de manera definitiva de cada variante del ilicito.

Por el contrario, con la denuncia de cualquier persona se persigue el mismo hecho con sus diversos efectos como una unidad y no es posible otorgar el perdón al probable responsable, lo que obliga al agente del Ministerio Público a realizar cuanta diligencia estime pertinente para la correcta integración de la averiguación previa

El Estado debería tener particular interés en la previsión y sanción del ilícito materia de la presente Tesis, ya que si bien es cierto que hasta el momento en México no se ha presentado algún problema considerable por el uso de virus cibernéticos, también lo es que se podría dar el problema afectando no solo a particulares, si no también a organismos Estatales, afectando con esto a terceros , es por este motivo que considerando la obligación del Estado de proteger a sus gobernados, se debe perseguir de oficio el ilícito causado por virus y no dejar la potestad a los afectados de querellarse por el daño que llegasen a sufrir.

La acreditación del tipo penal.

Para acreditar un tipo penal es necesario que el agente del Ministerio Público cumpla con los requisitos que le exige el artículo 16 párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos el cual exige que para iniciar un proceso penal debe existir denuncia o querella (de los cuales ya hablamos) y que existan datos que acrediten el cuerpo del delito y que hagan probable la responsabilidad del indiciado.

El Ministerio Público tiene la obligación de reunir todos los medios de convicción suficientes para integrar el cuerpo del delito que se trate y buscar los indicios necesarios para que la conducta realizada por algún sujeto sea considerada como un ilícito por la ley penal.

La probable responsabilidad

El artículo 168 párrafo tercero del Código federal de procedimientos penales señala que la probable responsabilidad del indiciado se tendrá por acreditada cuando, de los medios de prueba existentes, se deduzca su participación en el delito, la comisión dolosa o culposa del mismo y no exista acreditada a favor del indiciado alguna causa de licitud o alguna excluyente de culpabilidad.

Por su parte Osorio y Nieto[35] opina que por probable responsabilidad se entiende la posibilidad razonable de que una persona determinada haya cometido un delito y existirá cuando del cuadro procedimental se deriven elementos fundados para considerar que un individuo es probable sujeto activo de alguna forma de autoría; concepción, preparación o ejecución o inducir o compeler a otro a ejecutarlos. Se requiere, para la existencia de la probable responsabilidad, indicios de responsabilidad, no la prueba plena de ella, pues, tal certeza es materia de la sentencia.

Para el caso particular del tipo penal que se propone es necesario tomar en cuenta que debido al carácter técnico del ilícito es necesario recurrir a personal especializado con el conocimiento técnico y científico que auxilie al Ministerio Público en la realización de su labor.

El Ministerio Público deberá reunir todos aquellos indicios que puedan servir para probar que determinada persona deliberadamente introdujo un virus en una computadora propia o ajena o lo colocó en Internet a la espera de que alguien lo *baje* o accidentalmente se causó la infección de algún equipo de cómputo.

La intervención de peritos en computación es fundamental ya que solo estos estarán en posibilidad de determinar el origen y daño causado a las computadoras afectadas pudiendo aportar indicios que lleven a acreditar la responsabilidad de algún sujeto.

---

[35] **Osorio y Nieto, Cesar Augusto** Ob cit pag 30

Dicha la labor debe consistir en *seguirle la pista* al delincuente a través de los medios que utilizó para lograr la infección. La determinación del procedimiento a seguir para alcanzar dicho fin corresponde exclusivamente a los peritos, quienes son los que tienen el conocimiento técnico y científico necesario para poder resolver esta interrogante.

El cuerpo del delito.

El código federal de Procedimientos penales en su artículo 168 párrafo segundo señala que *por cuerpo del delito se entiende el conjunto de los elementos objetivos o externos que constituyen la materialidad del hecho que la ley señala como delito, así como los normativos, en el caso de que la descripción típica lo requiera.*

La ley procedimental penal federal exige únicamente que se reúnan los elementos objetivos o externos del hecho y los elementos normativos si lo exige el tipo penal, lo cual constituye la materialidad del delito; esto se diferencia de otras legislaciones locales que exigen también la acreditación de los elementos subjetivos que el tipo exija. Consideramos que para una adecuada integración del delito se deben reunir todos y cada uno de los elementos que lo conforman y no restringirlos solo a una parte.

El tipo penal que proponemos consta de elementos objetivos, que describen la conducta realizada por el delincuente y su consecuencia *(Comete delito cibernético aquel que diseñe o transmita ..... por cualquier medio, un programa , información,*

códigos o comandos de una computadora propia o ajena a otra causando daños a la misma, a sus sistemas informáticos, redes, información, datos y/o programas) y elementos subjetivos, consistente en la motivación del delincunte para actuar (*dolosa o culposamente*). El hecho de determinar si el proceder del sujeto activo fue con dolo o culposamente es con el fin de individualizar la pena, la cual no podrá ser igual para el que maquinó la forma de perjudicar a terceros y para el que por negligencia afectó a otros.

La sanción aplicable.

Como lo hemos señalado en a lo largo del presente trabajo, la intención es sancionar tanto a quien crea el virus como a quienes de menera dolosa o imprudencial lo transmiten, pero también es conveniente considear la tentativa del ilícito ; para tal fin se deben tomar en cuenta los tipos penales que han aplicado otros países en esta materia y los antecedentes del tema en nuestro país.

Parámetros de la sanción.

El tipo penal que proponemos contiene dos hipótesis la creación del virus y la trasmisión por cualquier medio del mismo La mayoría de las legislaciones penales de otros países se enfocan a sancionar únicamente el daño causado por el uso de virus cibernéticos, sin que tomen en cuenta que el virus existe y es nocivo aún antes de ser usado.

Desde que el diseñador del virus está ideando la manera de hacer funcionar su virus se denota el interés de perjudicar a terceros (debemos recordar que un virus no tiene otra función mas que la de afectar o destruir los equipos de cómputos, sus programas y datos), por lo que resulta importante sancionar al creador del virus aunque éste no haya causado aún daño alguno, lo cual podemos configurar como tentativa del delito, ya que se exterioriza la resolución de cometer el ilícito al crear el virus con el fin de perjudicar a terceros, realizando en parte (el diseño del virus exclusivamente) o totalmente (el diseño y distribución por cualquier medio sin afectación de terceros) los actos ejecutivos que deberían producir el resultado.

Las reglas para la aplicación de sanciónes en caso de tentativa se encuentran previstas en el artículo 63 del Código Penal Federal, el cual señala que se aplicará a jucio del Juez hasta las dos terceras partes de la sanción que se le debiera imponer de haberse consumado el delito; que en el caso de que no fuere posible determinar el daño que se prendió causar, cuando éste fuera determinante para la correcta adecuación tipica se aplicará hasta la mitad de la sanción señalada en el parrafo anterior, y que en el caso de la tentativa punible de delito grave así calificado por al ley , la autoridad judicial impondrá una pena de prisión que no será menor a la pena mínima y podrá llegar hasta las dos terceras partes de la sanción máxima prevista para el delito consumado.

Aunado a lo anterior consideramos que el delito en comento debería considerarse como un delito grave y por tanto adicionarse a la lista de delitos graves que establece el artículo 194 del Código de pocedimientos penales federal, ya que como lo hemos

mencionado con antelación, el ilícito en comento no solo afecta a los particulares, si no que también se puede ver afectada la vida de la población en general al atacarse el sistema de cómputo de algunas dependencias gubernamentales o financieras

Ahora bien, el tipo penal prevee que el ilícito se puede cometer de manera dolosa, esto es, que se lleven a cabo todas las maquinaciones pertinentes para causar un daño o perjuicio a terceros mediante el uso de los virus cibernéticos o de manera culposa, lo cual significa que se produzca el daño y/o perjuicio sin tener el ánimo de que éste se produzca.

Tomando en consideración lo anterior, podremos ver que no sería justo sancionar de la misma manera a quien utilizó todos los medios a su alcance para infectar a terceros que a quien por falta de cuidado en los programas y datos que utiliza infecta a terceros.

Para el primer caso consideramos que lo adecuado es fijar una pena privativa de libertad mas una multa por persona resulte infectada y para el segundo caso fijar una multa por no haber tenido la precaución de verificar la licitud del contenido de la información que recibia, enviaba o comercializaba.

También debemos considerar en la pena la gravante del ilicito que puede ser que el delito sea cometido por aquellas personas que abusan de sus conocimientos técnicos y científicos o de la información a que tienen acceso para distribuitr o crear un virus.

La pena pecuniaria.

Consideramos que la pena pecuniaria se debe fijar tanto en el caso de la infección dolosa o culposa. Pocas son las legislaciones penales en el mundo que contemplan la sanción a la infección culposa y consideramos que esta omisión puede ser grave , ya que se le da escape al delincuente con la excusa de que el ilicito se cometió sin intención de perjudicar a otras personas.

La legislación penal norteamericana es la que mejor a tratado el tema de los virus cibernéticos, por lo que nos apoyaremos en ella para proponer la sanción pecuaniaria a nuestro tipo penal.

Primero abordaremos la pena en el caso del actuar doloso. Se impondra una multa de hasta quinientas veces el salario mínimo vigente por persona infectada por el virus. Esta situación obedece a la obligación del Estado de procurar justicia y reparar el daño a los sujetos pasivos del ilícito que no ven en nada reparado su daño teniendo a una persona en la carcel. El ilícito cometido culposamente debe constar únicamente de una multa suficiente para reparar el daño ocasionado a terceros, por lo que se deberá fijar una multa de hasta 300 veces el salario mínimo vigente.

La pena privativa de libertad

Como lo mencionamos antes, la pena privativa de libertad la consideramos solo para el caso de que el delito se cometa dolosamente. Considerando la gravedad del problema que puede causar un virus , estimamos que la pena adecuada al tipo básico

doloso es de 5 a 15 años de prisión, más la multa de la que ya hablamos anteriormente.

En párrafos anteriores mencionamos que el ilicito podia ser agravado por alguna circunstancia. El hecho que que un profesional de la computación utilice sus conocimientos o los instrumentos a su alcance para pejudicar a terceros debe ser considerada como agravante, ya que estas personas conocen perfectamente el alcance de sus inventos y están actualizados en cuanto a los avances que hay sobre el tema., por lo que estimamos que esta circunstancia en particular debe ser sancionada aumentando hasta una mitad en su minimo y máximo de la pena correspendiente al tipo penal básico.

Tomando en consideración los razonamientos y opiniones antes explicados la redacción final del tipo que se propone queda de la siguiente manera:

Comete delito cibernético aquel que diseñe y/o transmita intencional o accidentalmente y por cualquier medio, un programa, instrucciones , información, códigos o comandos de una computadora propia o ajena a otra causando daños a la misma, a sus sistemas informáticos, redes, información, datos y/o programas.

Al que cree y/o transmita de manera intencional un programa, instrucciones, información códigos o comandos de computadora cuasando daños y/o perjuicios a

terceros, se le impondrán de 5 a 15 años de prisión y multa de hasta quinientas veces el salario mínimo vigente por persona afectada .

En los casos en que la transmisión del programa, instrucciones, información, codigos o comandos de computadora hayan causado un daño o perjuicio de manera involuntaria, se impondrá una multa de hasta 300 veces el salrio mínimo vigente.

Cuandc el delito sea cometido por personas que por su trabajo, ocupación o educación tengan conocimienos especializados en el uso de programas, instrucciones, información códigos y comandos de computadora, se le aumentará la pena hasta en una mitad en su mínimo y máximo de la pena correspondiente al tipo penal básico.

Cabe hacer la presisión que el tipo penal propuesto se encuentra integrado por los elementos que a nuestra consideración son los más relevantes y las penas propuestas son en razón a la gravedad del problema que puede generar una infección por virus en nuestro país.

Finalmente, es de hacerse notar que corresponde al Poder Legislativo Federal hacer el estudio del tema que se plantea en la presente tesis y en su caso el establecimiento de los parámetros necesarios para la creación de un tipo penal útil para la previsión y sanción de las conductas que se enunciaron en el desarrollo de la presente investigación.

CONCLUSIONES

CONCLUSIONES.

Primera.- El avance de la computación en nuestros días a obligado al hombre a depender en gran medida de la computadora y de los servicios que ésta presta para la realización de su trabajo y para su vida diaria. En los últimos tiempos, el desarrollo de la Internet ha provocado la unificación del mundo al facilitar las comunicaciones y negocios.

Segunda.- Al mismo tiempo que la computación se ha desarrollado para facilitarle la vida al hombre, también se han desarrollado diversos fenómenos tendientes a perjudicar el trabajo del hombre con la computadora.

Tercera.- El avance de Internet a permitido que se cometan diversos ilícitos, de los que destacan las *infecciones* causadas por los *virus de computadoras*, los cuales tienen como función alterar, modificar o destruir los archivos, programas y equipos de cómputo de terceros.

Cuarta.- Los virus no tienen otra función que no sea la de perjudicar a terceros; la infección se puede realizar por medio del uso de programas *piratas*, por la copia de programas infectados desde Internet o por la distribución del virus por este mismo medio

Quinta.- El hecho de que un virus se aloje en la computadora de un tercero puede provocar daños a los programas y datos, lo cual no es posible valuar. La pérdida de

información puede causar perjuicios al usuario si la información que contenía su computadora era importante para la realización de alguna otra actividad.

Sexta.- Algunos países del mundo se han percatado del problema que representan los virus de computadoras y han incluido en sus legislaciones tipos penales que prevén y sancionan dicha conducta, destacando la legislación penal norteamericana por su estudio del tema y por las sanciones que prevé.

Séptima.- En México, el tema de los virus de computadora se encuentran contemplados en la Ley penal del Estado de Sinaloa; sin embargo el tipo penal que lo menciona contiene también otras hipótesis, lo que ocasiona que el citado problema sea tratado superficialmente y con una penalidad baja, aunado a que por estar contemplado en una ley local su ámbito de aplicación no puede extenderse a otras regiones del país.

Octava.- En el Código Penal Federal no se contempla algún tipo que prevea y sancione la infección por virus de computadora; el tipo penal que se podría utilizar para el caso de la infección por virus de computadora es el de Daño en propiedad ajena, pero este tipo penal prevé sanciones mínimas para el caso de que el detrimento no pueda ser estimando en dinero.

Novena.- Existe la necesidad de crear un tipo penal que prevea y sancione las infecciones por virus de computadora y sus consecuencias en México con el fin de afrontar los ilícitos que se ocasionen por el uso de los virus de computadora

Décima.- Nuestra propuesta del tipo penal de Delitos cibernéticos, prevé que tanto la creación como la distribución del virus por cualquier medio, ya sea intencional o culposamente sea sancionada, en el primer caso con pena privativa de libertad y en el segundo caso con una multa, esto en razón a la gravedad del problema que puede ocasionarse por el uso de virus de computadoras.

Décima primera.- Opinamos que es necesario sancionar más severamente a aquellos que abusan de sus conocimientos técnicos y científicos para crear y distribuir un virus , ya que ese tipo de personas conocen los alcances del virus y los problemas que éste puede ocasionar.

Décima segunda.- El poder Legislativo Federal debe tomar conciencia de que si no se estudia el problema de los virus de computadoras en este momento, en un futuro cercano puede representar un problema serio para el país, esto en razón al avance de la computación que cada vez más nos hace dependientes de los servicios que se obtienen de ella.

GLOSARIO

GLOSARIO

Bit.- Unidad de medida de la memoria que en lenguaje binario puede significar 1 ó 0.

Byte.- 8 bits.

Chip. Circuito integrado de una superficie de 2 a 12mm de lado y aproximadamente 1mm de espesor, que puede contener varios cientos de componentes eléctricos (transistores, resistencias etc.)

CPU.- Unidad central de proceso. Contiene aquellos circuitos y chips de memoria que controlan la interpretación y ejecución de instrucciones de la computadora.

Disquete.- Medio magnético y portátil de almacenamiento de datos

Gigabite.- Mil millones de bites.

Hardware.- Término que indica todas las partes físicas, eléctricas y mecánicas de una computadora como son la fuente de poder, procesador, pantalla, teclado, monitor, Mouse, módem etc.

Kilobyte.- Un millar de bites.

Megabyte.- Un millón de bites.

Memoria RAM.- Memoria de acceso aleatorio, almacena temporalmente la información; si se desconecta la energía eléctrica la información se pierde.

Memoria ROM.- Memoria de lectura. Almacena en forma permanente instrucciones y datos.

Mouse.- Dispositivo de entrada de información a la computadora

Software.- Son las instrucciones que ordenan a la computadora realizar una tarea en particular.

Sistema Operativo.- Programa de controla a la computadora y maneja los dispositivos con los que cuenta.

Transistor.- Amplificador y rectificador de impulsos eléctricos.

BIBLIOGRAFÍA

BIBLIOGRAFIA.

DOCTRINA

ARELLANO GARCÍA, Carlos. Derecho Internacional privado. Ed. Porrua, México 1998, *12a ed. 986 páginas*

AZPILCUETA, Hermilo Tomás. Derecho Informático. Ed. Abeledo-Perrot, Argentina 1987, 89 páginas

CARBALLAR FALCON, José Antonio. Internet: Como descubrir el mundo. Ed. RA-MA, Madrid España 1997, 197 páginas

CARBALLAR FALCON, José Antonio. Internet: El mundo en sus manos. Ed RA-MA, Madrid España 1994, 102 páginas

COLIN SÁNCHEZ Guillermo. Derecho Mexicano de Procedimientos Penales. Ed. Porrua, México 1990 12 ed. 631 páginas

COMER E. Douglas. Traducción de Hugo Alberto Acuña Soto El libro de Internet. Ed. Prentice Hall Hispanoamericana S.A., México 1995, 312 páginas

CORTES IBARRA, Miguel Angel. Derecho Penal Parte general. Ed. Cárdenas editores y distribuidores, México 1992, 4ta ed. 491 páginas

CORREA M. Carlos, et.al. Derecho Informático. Ed. De Palma, Argentina 1987 , 341 páginas

LÓPEZ BETANCOURT, Eduardo. Teoria del delito. Ed. Porrua, México 1999, 7a ed. 313 páginas

FERREYRA CORTES, Gonzalo. Virus en las computadoras. Ed. Macrobit, México 1991, 2da ed. 136 páginas

GONZALEZ BUSTAMANTE, Juan José. Principios de Derecho Procesal Penal Mexicano. Ed. Porrua México 1959, 3ª.ed. 419 páginas

MALO CAMACHO, Gustavo. Derecho Penal Mexicano Ed. Porrua México 1996 2da. ed., 714 páginas

MIAJA DE LA MUELA Adolfo. Derecho Internacional Privado, Tomo Segundo. Ed. Atlas, Madrid 1987, 10 ed. revisada., 773 páginas

NORTON Peter, traducción de Sergio Luis Ma. Ruiz Faudón et.al. Toda la PC. Ed. Prentice Hall Hispanoamericana, México 1994, 596 páginas

NORTON Peter, traducción de Sérgio Luis Ma. Ruiz Faudón et al. INTRODUCCIÓN A LA COMPUTACIÓN. Ed. Prentice Hall Hispanoamericana México 1994, 5ta. ed. 567 páginas.

OSORIO Y NIETO Cesar Augusto. La averiguación previa. Ed. Porrua, México 2000, 11a de. 679 páginas

PEREZNIETO CASTRO Leonel. Derecho Internacional Privado. Ed. Harla, México 1991, 5ta ed., 511 páginas

RODRIGUEZ MONROY, Leticia, et.al. Computación básica I Ed. Popular México 1994, 100 páginas

TANENBAUM S Andrew. Traducción de Juan Carlos Vega Fagoaga Sistemas Operativos, diseño e implementación Ed. Prentice Hall Hispanoamericana S A. México 1988, 741 páginas.

TELLEZ VALDEZ, Julio. Derecho Informático. Ed. Mac Graw Hill, México 1996 2da ed., 283 páginas

TEXTEIRO VALLADARES, Haroldo. Derecho Internacional Privado. Introducción y parte general. Ed. Trillas, México 1987 624 páginas.

LEGISLACIÓN

Constitución Política de los Estado Unidos Mexicanos. Ed Mc Graw Hill México 1999, 7ª ed. 184 páginas

Código Penal Federal Ed. Sista México 2000, 170 páginas

Código Federal de Procedimientos Penales Ed Sista, México 2000, 115 páginas

Código Penal para el Distrito Federal Editonal Sista, México 1999 ,155 páginas

Código de Procedimientos Penales para el Distrito Federal, Ed. Delma, , México 1999, 2ª ed. , 295 páginas

ECONOGRAFIA

CZEPOL.- Acervo Jurídico Czepol , México 2000

SOFTWARE VISUAL.- Compila 2000.- Compilación de Leyes del Distrito Federal .Software Visual S.A. de C.V. , México 2000.

http://www.guiahappy.com/assen/lvh.hmt.- LÓPEZ, José Luis.- Los Virus Hoy. México,2000

http://usuarios.tripod.es/janny/- Introducción a los virus, México 2000

http://www.symantec.it/region/mx/avcenter/vinfodb.html.- Enciclopedia en línea de virus reales y falsos. México 2000.

http://tiny.uasnet.mx/prof/cln/der/silvia/leyint.htm Delitos informáticos. México 2000

http://www.megazona.com/ZONAVirus//Informes/legislacion_03.htm.

Procuraduría General de Justicia del Distrito Federal. Apuntes del programa de formación práctico teórico para oficiales secretanos. México 1999