UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
CAMPUS ARAGÓN

"NECESIDAD DE ADICIONAR EN EL CÓDIGO PENAL PARA EL DISTRITO FEDERALUN TIPO PENAL RELATIVO A LA CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMATICOS"

T E S I S

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN DERECHO

P R E S E N T A :

JULIO CHINCOYA ZAMBRANO

ASESOR: **LIC. ABUNDIO ESTRADA GARDUÑO**

FES Aragón

NEZAHUALCOYOTL, EDO. DE MEXICO
2010

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

ÍNDICE

Pág

CAPÍTULO 2.

EL CÓDIGO PENAL VIGENTE PARA EL DISTRITO FEDERAL Y LOS DELITOS INFORMÁTICOS.

CAPÍTULO 3.

NECESIDAD DE ADICIONAR UN TIPO PENAL EN EL CÓDIGO PENAL DEL DISTRITO FEDERAL EN MATERIA DE CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICOS.

D E D I C A T O R I A S

A DIOS, creador de todo lo existente, por enseñarme y acompañarme en mi camino.

A MIS PADRES: JUANA ZAMBRANO RODRÍGUEZ Y MIGUEL CHINCOYA CANCINO, gracias por darme el don maravilloso de la vida; por enseñarme el camino del bien y por ser el soporte de mi vida... Los amo¡

A MIS HERMANOS: MIGUEL KAERY, RICARDO Y VERÓNICA, por su amor y su apoyo en todos los momentos de mi vida.

A MIS TÍOS Y PRIMOS, ESPECIALMENTE A NAYELI Y DANIEL, por su apoyo y comprensión incondicionales.

A MI PAREJA, PAMELA GONSEN, gracias por tu apoyo incondicional en esos momentos tan difíciles te amo.

A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO Y EN ESPECIAL A LA FACULTAD DE ESTUDIOS PROFESIONALES CAMPUS ARAGÓN, por formarme como abogado y persona de bien, al servicio de las causas justas.

A MI APRECIABLE JURADO: gracias por su tiempo, consejos y apoyo.

A MI ASESOR, EL LIC. ABUNDIO ESTRADA GARDUÑO, por sus consejos y sabia asesoría en mi trabajo de tesis.

A TODOS MIS AMIGOS Y COMPAÑEROS: mi agradecimiento por sus comentarios y confianza depositada.

INTRODUCCIÓN.

El siglo pasado marcó sin lugar a dudas, uno de los más prolíferos en materia de cambios y adelantos tecnológicos en todos los campos, siendo el de la informática uno de los que mayor grado de desarrollo alcanzó.

Las computadoras han venido a simplificar la mayor parte de las tareas en el hogar, la oficina y en el desarrollo del país. Asimismo, los distintos programas informáticos o “software”, han facilitado aún más todo lo que el ser humano requiere para sus labores diarias.

Sin embargo, no todos los que conocen de computadoras y de software lo utilizan para bien, sino que hay personas que en el idioma inglés reciben el nombre de “hackers”, cuya tarea es penetrar a través de Internet, a lugares o webs no autorizadas, destinadas a los gobiernos o inclusive a estados financieros de ellos y de personas, cuyas fortunas pueden ser materialmente sustraídas en sólo cuestión de minutos a través de la red. Hay otras personas que con el simple ánimo de causar severos daños a los equipos de cómputo de particulares, de gobiernos o de instituciones logran desarrollar archivos llamados comúnmente: “virus informáticos”, los cuales han causado ya serios daños patrimoniales en el mundo, ya que Internet es una excelente vía para propagar este tipo de archivos malignos que tienen diferentes funciones, pero, en general, se utilizan para causar daños en el disco duro de las computadoras, para borrar los archivos existentes en las mismas, para alentarlas o para poder penetrar a información contenida en los diferentes archivos de una persona o institución pública o privada, violando con ello, la intimidad personal, derecho fundamental de los gobernados.

De esta manera, han surgido varios virus informáticos como el *“I love you”, “sircam*”, “*virus Kurnikova*”, “*VBS*”, “*SST*” y otros más, ya que diariamente son creados uno o varios tipos de virus con fines diferentes y que se propagan a través

de Internet, llegando a millones de posibles navegadores que resultarán seguramente infectados en el mundo.

Posiblemente la creación y propagación de virus informáticos no constituiría un objeto de interés para el Derecho penal si no fuera porque con tales conductas se daña o afecta el patrimonio de las personas a través de sus estados financieros o inclusive, los de una nación y con ello, se puede producir un serio colapso a nivel mundial, ya que todas las economías están interconectadas por lo que llamamos globalización. Diariamente se realizan muchas operaciones multimillonarias a través de Internet, por lo que si se introduce un virus informático en un equipo, se podrá causar un daño patrimonial de grandes dimensiones.

En este tenor de ideas, se debe aceptar que México un país que crecimiento en materia de informática, por lo que el hablar de virus en este campo puede resultar casi inadvertido en cuanto a sus serias consecuencias jurído-penales; sin embargo, en naciones como los Estados Unidos, Alemania, Francia o España, ya hay legislaciones que regulan y sancionan la creación y propagación de virus informáticos. Cabe decir y reconocer con toda justicia que el Código Penal Federal contempla ya de una manera muy sencilla la destrucción, modificación o pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo en sus artículos 211bis-1, 211bis-2, 211bis-3, 211bis-4, 211bis-5, 211bis-6 y 211bis-7, sin embargo, estimamos que este es sólo un principio en materia del combate jurídico-penal a los delitos informáticos cuyos daños pueden ser irreparables.

En la presente investigación de tesis, se pretende hacer una explicación inductiva-deductiva sobre la importancia de los delitos informáticos en su modalidad de creación y propagación de virus informáticos, haciendo especial referencia en la forma en que estos archivos pueden causar daños patrimoniales en ocasiones irreparables. Se desea también advertir que el actual Código Penal para el Distrito

Federal es omiso en cuanto a este tipo de delitos considerados como limpios, ya que requieren de amplios conocimientos de informática y de contar con un equipo computacional para perpetrar la conducta, por lo que resulta de gran interés y de preocupación que el Código Penal para el Distrito Federal cuente con un tipo penal que regule ye sancione la creación y propagación de virus informáticos como delito, por lo que en su momento se hará un proyecto de la posible redacción que llevaría ese tipo penal que es improrrogable ya en esta ciudad en la que no hay control de los Cafés Internet, en los que se pueden fraguar y llevar a cabo muchos delitos informáticos, entre ellos, la creación y propagación de virus informáticos.

No se entienden cuál fue el motivo de la omisión legislativa de este tipo de ilícitos en el Código Penal para el Distrito Federal, sin embargo, en la presente investigación se demostrará de demostrar la real necesidad de llenar esa laguna jurídica penal con la creación de un tipo penal justo a las necesidades de la sociedad en materia de protección informática, por lo que esta investigación se justifica plenamente.

El presente trabajo de investigación documental está estructurada en tres Capítulos en los que abordamos estos contenidos temáticos:

En el Capítulo Primero, se explicará lo que son los virus informáticos y su trascendencia en el campo de la informática.

En el Capítulo Segundo, se hablará sobre los aspectos generales del nuevo Código Penal para el Distrito Federal, tendiente a manifestar y demostrar que el mismo no alude a los delitos informáticos como sí lo hacen el Código Penal y el de Procedimientos Penales de Sinaloa.

En el Capítulo Tercero, se abundará en la necesidad de que el Código Penal para el Distrito Federal cuente con un tipo penal que regule y sancione la creación y propagación de virus informáticos, proponiendo la redacción del mismo, así como otras acciones jurídicas y administrativas para evitar que a través de la creación y propagación de archivos malignos se causen daños patrimoniales considerables a los demás.

CAPÍTULO 1.
LA INFORMÁTICA. ASPECTOS GENERALES.

1.1. LA INFORMÁTICA.

Actualmente, el término *informática* resulta ampliamente conocido y usado por gran parte de los habitantes de este planeta. Sin embargo, engloba a muchos adelantos en materia de computadoras y programas,. La informática se ha convertido en una ciencia que sufre adelantos día a día.

Sobre la informática, dice el autor Padilla Segura: *"Es casi por todos sabido que el término informática tiene su origen en Francia. Quienes lo gestaron como neologismo uniendo a las dos primeras sílabas del término information, las tres últimas sílabas de automatique con lo que este vocablo de nuevo cuño, en su momento, daba a entender claramente la intención de referirse a un proceso de información automatizada. En forma más explícita quiso significar el tratamiento automático de los datos que constituyen la información".*[1]

De este concepto se destaca que el término *informática* deriva de las dos voces francesas citadas, por lo que engloba entonces las acepciones de información y automático. Posiblemente, mucho se desconoce ese hecho.

La Enciclopedia Encarta Microsoft 2004 dice de la informática lo siguiente: "Informática o Computación, conjunto de conocimientos científicos y de técnicas que hacen posible el tratamiento automático de la información por medio de computadoras. La informática combina los aspectos teóricos y

[1] PADILLA SEGURA, José Antonio. Informática Jurídica. I.P.N. México, 1991, p. 5

prácticos de la ingeniería, electrónica, teoría de la información, matemáticas, lógica y comportamiento humano. Los aspectos de la informática cubren desde la programación y la arquitectura informática hasta la inteligencia artificial y la robótica".[2]

Julio Téllez Valdez dice por su parte que: *"La palabra informática es un neologismo derivado de los vocablos información y automatización, sugerido por Philipe Dreyfus en el año de 1962".*[3] Posteriormente, el mismo autor nos ofrece el siguiente concepto de la informática en general: "En el sentido general, la informática es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una toma de decisiones".

José Antonio Padilla Segura dice por su parte que*: "Desde mediados de los años sesenta se vienen sucediendo los intentos más o menos felices de encontrar una definición o hacer una buena descripción de lo que es la informática. La realidad es que a medida que el tiempo ha transcurrido, esto que fue una disciplina o una rama de la ciencia y de la técnica, se ha convertido en un complejo campo de conocimientos, de experiencias y de aplicaciones, en todas las tareas del quehacer humano. Es por ello que no es fácil aplicarle una definición legal".*[4]

De lo anterior debemos puntualizar que el hecho de intentar llevar a cabo una definición o un concepto representa una labor ardua, más si se trata de una nueva disciplina que aplica y conjuga la información y la automatización, es decir, el uso de las computadoras para la correcta toma de decisiones y la solución de problemas diarios.

---

[2] Enciclopedia Encarta Microsoft 2010. Microsoft Corporation, 2010.
[3] TÉLLEZ VALDEZ, Julio. Derecho Informático. Editorial McGraw Hill, 2ª edición, México, 1996, p. 5.
[4] PADILLA SEGURA, José Antonio. Op. Cit. P. 1.

Así, es dable hablar de una informática en general y de una informática jurídica que es el conjunto de técnicas o procedimientos destinados a la sistematización de la información jurídica para simplificar las labores propias de esta importante área del conocimiento humano.
Es importante señalar que existe una parte de la informática que está íntimamente relacionada con la ciencia jurídica, recibe el nombre de informática jurídica. Sobre ella podemos señalar lo siguiente.

Todas las ramas del conocimiento humano, al igual que las artes se han visto enriquecidas con la informática, dado el hecho de que se ha convertido en un instrumento imprescindible en la difusión, intercambio, sistematización y avance de cualquier tipo de conocimiento. El Derecho no ha sido la excepción ya que rápidamente ha aprovechado las ventajas que nos da la misma.

"Desde su nacimiento de la informática jurídica (aproximadamente en 1959), se le ha denominado de diversas formas: El juez estadounidense Lee Loevinger le llamó "jurimetrics"; el Italiano Mario G. Lozano la llamó "Giuscibernética" señalando que la cibernética aplicada al Derecho produce una depuración cuantitativa y cualitativa. En América Latina se le conoce como "Jurismática", en Alemania se le conoce con el nombre de "Elektronische Datenverabeitung und Recht", en Francia "Informatique Juridique", en los países sajones *"computers and law*". [5]

La incorporación de la informática dentro del ámbito jurídico ha sido de manera rápida y rotunda. A pesar de que ya en la década de los ochentas, se empezaban a usar las computadoras, es hasta la década de los noventas cuando su uso se generaliza y el ámbito jurídico empieza a hacer aprovechamiento de estos recursos.
Para el autor Segura Padilla es necesario regular la informática debido a "la influencia que la ciencia y sus aplicaciones tecnológicas han llegado a cobrar

[5] Ibid. p. 1.

en las sociedades modernas", "... unánimemente se reconoce que tales recursos son determinantes en los campos político, económico y social, y consecuentemente, resulta imprescindible para los Estados y sus gobiernos, asumir posiciones y definir criterios sobre tales materias, que sean congruentes con los grandes objetivos nacionales". "La materia informática es de tal complejidad y trascendencia, que lagunas de sus aplicaciones constituyen renglones estratégicos o prioritarios en las sociedades modernas. Tiene el carácter de instrumento insustituible en el campo de la política, ya que no es concebible él legitimo y cabal de ejercicio del poder si no se cuenta con medios de comunicación permanentes y eficaces que hagan posible él dialogo entre gobernados y gobernantes".[6]

Es por esto que el Senado de la República propuso la reforma al articulo 73 fracción X de la Constitución Política para agregarle el termino "informática" de así, el Congreso General tendría facultad para legislar sobre esta materia, considerando impostergable la regulación de todos los procesos informáticos que a diario tienen lugar. Disponen algunos numerales del Anteproyecto de decreto por el que se adiciona la fracción X del artículo 73 de la Constitución Política:

> PRIMERO. Que el Senado de la República está plenamente consciente de la necesidad de actualizar, enriquecer y consolidad la infraestructura jurídica que permita diseñar nuevas estrategias que conduzcan a nuestro país su desarrollo integral, el cual está estrechamente ligado al proceso que se logre en el campo de la informática.
>
> SEGUNDO. Que la informática se ha convertido en factor primordial de la moderna organización social – cuyas modalidades debe adoptar oportunamente – a la cual nuestro país debe integrarse cada

[6] Ibíd. p. 2

vez mas estrechamente y que tal organización requiere del apoyo, del estímulo y de la orientación de todos sus miembros y, especialmente, del Estado.

TERCERO. Que cada día resultan mas evidentes, importantes y trascendentes las repercusiones de la informática en la configuración cultural de nuestro pueblo, por lo que es necesario adoptar las medidas pertinentes, entre ellas las de orden jurídico, para defender y preservar ese patrimonio nacional que es base y componente indispensable para perdurará como nación independiente cuyos valores y manifestaciones puedan trascender históricamente.

CUARTO. Que la complejidad de la informática y el hecho de que constituye un fenómeno de convergencia tecnológica hacen que influya en gran número de procesos técnicos, lo cual conduce a considerarla como una actividad de importancia nacional y prioritaria ya que de lo contrario otras importantes áreas de actividad se verían seriamente afectadas.

QUINTO. Que hasta hoy, el marco jurídico de la informática en nuestro país no ha logrado alcanzar una cabal unidad y coherencia ya que esta formada por disposiciones que se encuentran dispersas en distintos ordenamientos jurídicos y administrativos de donde se desprende la necesidad de expedir una legislación federal unificadora de las políticas y de los criterios relativos".[7]

Por alguna causa, la reforma planteada a la fracción X del articulo 73 constitucional no se pudo llevar a cabo, sin embargo, consideramos que queda de manifiesto la importancia que ha adquirido la informática en nuestro país en el aspecto jurídico.

[7] Idem.

1.2. IMPORTANCIA DE LAS COMPUTADORAS EN LA VIDA DIARIA.

En términos generales, el “ordenador” o Computadora, es un dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

El mundo de la alta tecnología nunca hubiera existido de no ser por el desarrollo del ordenador o computadora. Toda la sociedad utiliza estas máquinas, en distintos tipos y tamaños, para el almacenamiento y manipulación de datos. Los equipos informáticos han abierto una nueva era en la fabricación gracias a las técnicas de automatización y han permitido mejorar los sistemas modernos de comunicación. Son herramientas esenciales prácticamente en todos los campos de investigación y en tecnología aplicada, incluyendo, obviamente al Derecho.

A raíz de los grandes avances en materia de informática en general, la sociedad ha podido avanzar a pasos seguros y agigantados, ya que las computadoras han venido a hacer las tareas más simples. Los trabajos más sofisticados como son ecuaciones y fórmulas matemáticas complejas son realizadas en sólo cuestión de minutos por las computadoras, las cuales están también presentes en los hogares, en las oficinas públicas y privadas, en las escuelas, en los organismos internacionales, etc.

Posiblemente, hace unos quince o veinte años, quien poseía una computadora en su casa era considerado como alguien con grandes recursos económicos, sin embargo, en la actualidad, los precios de estos aparatos han bajado considerablemente, por ejemplo, actualmente es posible comprar una PC o

Laptop a precios baratos gracias a los paquetes que ofrece TELMEX (Teléfonos de México), empresa mexicana que cuenta con varios planes de venta a plazos, con cargo al recibo telefónico mensual, incluyendo el servicio de Internet por una año.

Por otra parte, es dable señalar que los gobiernos, economías y sistemas mundiales dependen mucho de sus redes de computadoras; las comunicaciones y transferencias de grandes sumas de dinero son realizadas gracias a estos aparatos que han venido a revolucionar la vida del ser humano, simplificándola enormemente. Las computadoras han traído grandes beneficios, sin embargo, también es justo reconocer que han causado el despido de muchas personas, ya que sus servicios han sido asimilados también por las computadoras, como el caso de las secretarias. Por otra parte, la automatización que se vive ha hecho una sociedad virtual que se comunica a través de la red, que tiene amigos y hasta parejas gracias a Internet. Hoy, ya no es necesario comprar un libro, ya que en Internet se puede encontrar. En materia de comunicaciones, el correo normal o común y corriente ha dejado de ser la vía ideal, ya que la mayoría de las personas se comunican a través del chat, se envían e mails o correos electrónicos que, si bien son una gran ventaja por la reducción de tiempo y de inversión, también lo es que nuestra vida se ha vuelto muy automática o “robotizada”. Tal pareciera que las computadoras han controlado nuestra vida y no al revés, por lo que se debe ponderar las ventajas y desventajas que trae el uso de las computadoras en la actualidad.

En materia de los Derechos de Autor es también importante decir que a través de la red, es posible que uno puede bajar una canción o video sin necesidad de pagarlo, es decir, de manera ilegal, dañando los derechos de autor y los derechos conexos y si de ilicitud se trata, aunque también hay webs en los que tal acción es totalmente legal y permitida, por lo que se debe considerar que Internet sigue siendo una red anárquica, es decir, que no cuenta con una regulación jurídica, nacional ni internacional, por lo que la misma se presta para

muchas situaciones ilegales como la venta de drogas, de armas, de personas; el tráfico de menores, el terrorismo, entre otros más.

1.3. PARTES DE QUE INTEGRAN LAS COMPUTADORAS:

En la actualidad se utilizan dos tipos principales de ordenadores (nombre con el que también se le conoce a las computadoras): Analógicos y digitales. Sin embargo, el término ordenador o computadora suele utilizarse para referirse exclusivamente al tipo digital. Los ordenadores analógicos aprovechan la similitud matemática entre las interrelaciones físicas de determinados problemas y emplean circuitos electrónicos o hidráulicos para simular el problema físico. Los ordenadores digitales resuelven los problemas realizando cálculos y tratando cada número dígito por dígito.

Las instalaciones que contienen elementos de ordenadores digitales y analógicos se denominan ordenadores híbridos. Por lo general se utilizan para problemas en los que hay que calcular grandes cantidades de ecuaciones complejas, conocidas como integrales de tiempo. En un ordenador digital también pueden introducirse datos en forma analógica mediante un convertidor analógico digital y viceversa (convertidor digital a analógico).

El ordenador analógico es un dispositivo electrónico o hidráulico diseñado para manipular la entrada de datos en términos de, por ejemplo, niveles de tensión o presiones hidráulicas, en lugar de hacerlo como datos numéricos. El dispositivo de cálculo analógico más sencillo es la regla de cálculo, que utiliza longitudes de escalas especialmente calibradas para facilitar la multiplicación, la división y otras funciones. En el típico ordenador analógico electrónico, las entradas se convierten en tensiones que pueden sumarse o multiplicarse empleando elementos de circuito de diseño especial. Las respuestas se generan

continuamente para su visualización o para su conversión en otra forma deseada.

Las computadoras se componen básicamente de dos grandes partes: El hardware y el software. A continuación hablaremos de ambos.

1.3.1. EL HARDWARE.

La palabra *Hardware,* proviene del inglés y se aplica a la parte de las computadoras que tienen que ver con su estructura, es decir, su apariencia física y todo lo que contiene. Es por ende el equipo utilizado para el funcionamiento de una computadora. El hardware se refiere a los componentes materiales de un sistema informático. La función de estos componentes suele dividirse en tres categorías principales: entrada, salida y almacenamiento. Los componentes de esas categorías están conectados a través de un conjunto de cables o circuitos llamado bus con la unidad central de proceso (CPU) del ordenador, el microprocesador que controla la computadora y le proporciona capacidad de cálculo.

"El soporte lógico o software, en cambio, es el conjunto de instrucciones que un ordenador emplea para manipular datos: Por ejemplo, un procesador de textos o un videojuego. Estos programas suelen almacenarse y transferirse a la CPU a través del hardware de la computadora. El software también rige la forma en que se utiliza el hardware, como por ejemplo la forma de recuperar información de un dispositivo de almacenamiento. La interacción entre el hardware de entrada y de salida es controlada por un software llamado BIOS (siglas en inglés de 'sistema básico de entrada/salida')". [8]

[8] Ibid. P. 80.

Aunque, técnicamente, los microprocesadores todavía se consideran hardware, partes de su función también están asociadas con el software. Este hecho de que los microprocesadores presenten tanto aspectos de hardware como de software, hace que a veces se les aplique el término intermedio de microprogramación, o firmware.

El hardware de entrada consta de dispositivos externos —esto es, componentes situados fuera de la CPU de la computadora— que proporcionan información e instrucciones. Un lápiz óptico es un puntero con un extremo fotosensible que se emplea para dibujar directamente sobre la pantalla, o para seleccionar información en la pantalla pulsando un botón en el lápiz óptico o presionando el lápiz contra la superficie de la pantalla. El lápiz contiene sensores ópticos que identifican la parte de la pantalla por la que se está pasando. Un mouse, o ratón, es un dispositivo apuntador diseñado para ser agarrado con una mano. Cuenta en su parte inferior con un dispositivo detector (generalmente una bola) que permite al usuario controlar el movimiento de un cursor en la pantalla deslizando el mouse por una superficie plana. Para seleccionar objetos o elegir instrucciones en la pantalla, el usuario pulsa un botón del mouse. Un joystick es un dispositivo formado por una palanca que se mueve en varias direcciones y dirige un cursor u otro objeto gráfico por la pantalla de la computadora. Un teclado es un dispositivo parecido a una máquina de escribir, que permite al usuario introducir textos e instrucciones. Algunos teclados tienen teclas de función especiales o dispositivos apuntadores integrados, como trackballs (bolas para mover el cursor) o zonas sensibles al tacto que permiten que los movimientos de los dedos del usuario dirijan un cursor en la pantalla.

“Un digitalizador óptico (o escáner óptico) emplea dispositivos fotosensibles para convertir imágenes (por ejemplo, una fotografía o un texto) en señales electrónicas que puedan ser manipuladas por la máquina. Por ejemplo, es posible digitalizar una fotografía, introducirla en una computadora e integrarla en un documento de texto creado en dicha computadora. Los dos

digitalizadores más comunes son el digitalizador de campo plano (similar a una fotocopiadora de oficina) y el digitalizador manual, que se pasa manualmente sobre la imagen que se quiere procesar. Existen cámaras digitales que permiten tomar imágenes que pueden ser tratadas directamente por el ordenador". [9]

Un micrófono es un dispositivo para convertir sonidos en señales que puedan ser almacenadas, manipuladas y reproducidas por el ordenador. Un módulo de reconocimiento de voz es un dispositivo que convierte palabras habladas en información que el ordenador puede reconocer y procesar.
Un módem es un dispositivo que conecta una computadora con una línea telefónica y permite intercambiar información con otro ordenador a través de dicha línea. Todos los ordenadores que envían o reciben información deben estar conectados a un módem. El módem del aparato emisor convierte la información enviada en una señal analógica que se transmite por las líneas telefónicas hasta el módem receptor, que a su vez convierte esta señal en información electrónica para el ordenador receptor.

El hardware de salida consta de dispositivos externos que transfieren información de la CPU de la computadora al usuario informático. La pantalla convierte la información generada por el ordenador en información visual. Las pantallas suelen adoptar una de las siguientes formas: un monitor de rayos catódicos o una pantalla de cristal líquido (LCD, siglas en inglés). En el monitor de rayos catódicos, semejante a un televisor, la información procedente de la CPU se representa empleando un haz de electrones que barre una superficie fosforescente que emite luz y genera imágenes. Las pantallas LCD son más planas y más pequeñas que los monitores de rayos catódicos, y se emplean frecuentemente en ordenadores portátiles.

[9] Ibid. P. 81.

Las impresoras reciben textos e imágenes de la computadora y los imprimen en papel. Las impresoras matriciales emplean minúsculos alambres que golpean una cinta entintada formando caracteres. Las impresoras láser emplean haces de luz para trazar imágenes en un tambor que posteriormente recoge pequeñas partículas de un pigmento negro denominado tóner. El tóner se aplica sobre la hoja de papel para producir una imagen. Las impresoras de chorro de tinta lanzan gotitas de tinta sobre el papel para formar caracteres e imágenes.

El hardware de almacenamiento sirve para almacenar permanentemente información y programas que el ordenador deba recuperar en algún momento. Los dos tipos principales de dispositivos de almacenamiento son las unidades de disco y la memoria. Existen varios tipos de discos: duros, flexibles o disquetes, magneto-ópticos y compactos. Las unidades de disco duro almacenan información en partículas magnéticas integradas en un disco; estas unidades, que suelen ser una parte permanente de la computadora, pueden almacenar grandes cantidades de información y recuperarla muy rápidamente. Las unidades de disquete también almacenan información en partículas magnéticas integradas en discos intercambiables, que de hecho pueden ser flexibles o rígidos. Los disquetes almacenan menos información que un disco duro, y la recuperación de la misma es muchísimo más lenta. Las unidades de disco magneto-óptico almacenan la información en discos intercambiables, sensibles a la luz láser y a los campos magnéticos; pueden almacenar tanta información como un disco duro, pero la velocidad de recuperación de la misma es algo menor. Las unidades de disco compacto, o CD-ROM, almacenan información en las cavidades grabadas en la superficie de un disco de material reflectante. *“La información almacenada en un CD-ROM no puede borrarse ni sustituirse por otra. Los CD-ROM pueden almacenar aproximadamente la misma información que un disco duro, pero la velocidad de recuperación de información es menor. Hay unidades que permiten escribir discos compactos y, si el soporte lo permite, reescribir la información hasta más de 1.000 veces*

sobre el mismo disco; son las unidades CD-RW (del inglés CD-ReWritable) que además de leer y reescribir discos CD-RW, también pueden leer y escribir discos compactos CD-R (que sólo permiten grabar la información una vez) y leer CD-ROM. En la actualidad también es frecuente encontrar en los ordenadores unidades DVD, que permiten leer, y algunas también escribir, unidades del mismo tamaño que los CD pero con una capacidad de almacenamiento muy superior". [10]

La memoria está formada por chips que almacenan información que la CPU necesita recuperar rápidamente. La memoria de acceso aleatorio (RAM, siglas en inglés) se emplea para almacenar la información e instrucciones que hacen funcionar los programas de la computadora. Generalmente, los programas se transfieren desde una unidad de disco a la RAM. Esta memoria también se conoce como memoria volátil porque la información contenida en los chips de memoria se pierde cuando se desconecta el ordenador. La memoria de sólo lectura (ROM, siglas en inglés) contiene información y software cruciales que deben estar permanentemente disponibles para el funcionamiento de la computadora, por ejemplo el sistema operativo, que dirige las acciones de la máquina desde el arranque hasta la desconexión. La ROM se denomina memoria no volátil porque los chips de memoria ROM no pierden su información cuando se desconecta el ordenador.

Algunos dispositivos se utilizan para varios fines diferentes. Por ejemplo, los disquetes también pueden emplearse como dispositivos de entrada si contienen información que el usuario informático desea utilizar y procesar. También se pueden utilizar como dispositivos de salida si el usuario quiere almacenar en ellos los resultados de su computadora.

Para funcionar, el hardware necesita conexiones materiales que permitan a los componentes comunicarse entre sí e interaccionar. Un bus constituye un

[10] Ibid. p. 82.

sistema común interconectado, compuesto por un grupo de cables o circuitos que coordina y transporta información entre las partes internas de la computadora. El bus de una computadora consta de dos canales: uno que la CPU emplea para localizar datos, llamado bus de direcciones, y otro que se utiliza para enviar datos a una dirección determinada, llamado bus de datos. Un bus se caracteriza por dos propiedades: la cantidad de información que puede manipular simultáneamente (la llamada “anchura de bus”) y la rapidez con que puede transferir dichos datos.

Una conexión en serie es un cable o grupo de cables utilizado para transferir información entre la CPU y un dispositivo externo como un mouse, un teclado, un módem, un digitalizador y algunos tipos de impresora. Este tipo de conexión sólo transfiere un dato de cada vez, por lo que resulta lento. La ventaja de una conexión en serie es que resulta eficaz a distancias largas.

Una conexión en paralelo utiliza varios grupos de cables para transferir simultáneamente más de un bloque de información. La mayoría de los digitalizadores e impresoras emplean este tipo de conexión. Las conexiones en paralelo son mucho más rápidas que las conexiones en serie, pero están limitadas a distancias menores de 3 m entre la CPU y el dispositivo externo.

1.3.2. EL SOFTWARE.

La segunda parte de las computadoras es el *Software*, un conjunto de programas de computadoras. Son las instrucciones responsables de que el hardware (la máquina) realice su tarea. Como concepto general, el software puede dividirse en varias categorías basadas en el tipo de trabajo realizado. Las dos categorías primarias de software son los sistemas operativos (software del sistema), que controlan los trabajos del ordenador o computadora, y el

software de aplicación, que dirige las distintas tareas para las que se utilizan las computadoras. Por lo tanto, el software del sistema procesa tareas tan esenciales, aunque a menudo invisibles, como el mantenimiento de los archivos del disco y la administración de la pantalla, mientras que el software de aplicación lleva a cabo tareas de tratamiento de textos, gestión de bases de datos y similares. Constituyen dos categorías separadas el software de red, que permite comunicarse a grupos de usuarios, y el software de lenguaje utilizado para escribir programas (ver Lenguaje de programación).

Además de estas categorías basadas en tareas, varios tipos de software se describen basándose en su método de distribución. Entre estos se encuentran los así llamados programas enlatados, el software desarrollado por compañías y vendido principalmente por distribuidores, el freeware y software de dominio público, que se ofrece sin costo alguno, el shareware, que es similar al freeware, pero suele conllevar una pequeña tasa a pagar por los usuarios que lo utilicen profesionalmente y, por último, el infame vapourware, que es software que no llega a presentarse o que aparece mucho después de lo prometido.

“El software es de suma importancia en cualquier equipo de computadora ya que permite al mismo realizar diversas y complicadas tareas que facilitan las labores del hombre, por ejemplo, estadísticas, gráficas, recuentos, capturas, transferencias, pero también existen programas que se han creado con fines ilegales o de espionaje o destrucción. En este caso, nos referimos a los virus informáticos, que dicho sea, son programas, pero, que su finalidad es la anteriormente señalada, causar un daño en la información o el equipo de las personas. Así, a través de un virus informático es dable robar información, modificarla o destruirla, posiblemente ante la inexperiencia de la persona la

cual sólo recibió un correo electrónico y decidió abrirlo, con ello permitió que el virus salga y haga su trabajo destructivo". [11]

1.3.3. LOS PROGRAMAS INFORMÁTICOS:

Como lo hemos señalado, las computadoras constan de dos grandes partes que son: el hardware y el software. El primero de ellos es el equipo duro o material de que consta una computadora, mientras que el segundo de ellos se integra por el conjunto de programas que tienen una vital importancia para el equipo, ya que se crean para dar las ordenes necesarias para que el mismo funcione y ejecute adecuadamente las tareas para las que fue creado. Así, un programa computacional es un conjunto de ordenes estructuradas y elaboradas con minuciosidad que sirven para que la computadora pueda cumplir con los objetivos para los cueles fue creada, por ejemplo, el programa denominado "WINDOWS", es un conjunto de patrones u ordenes que sirven para que la computadora opere o funcione perfectamente, sin él, no sería posible el realizar escritos, gráficas o consultar el correo electrónico. Otro programa similar, aunque no muy conocido es LINUX, un sistema operativo de calidad con el que operan algunas computadoras como las de la firma MCINTOSH, la competencia de MICROSOFT.

Existen miles de programas que pueden ser instalados en una computadora, desde los que ya vienen incluidos en el equipo, hasta aquellos que se pueden conseguir de manera legal o ilegal en el comercio informal sobre diferentes tópicos como ciencias, artes, cálculo, lectores de documentos, juegos, ocio y multimedia o para hachear, es decir, poder entrar ilegalmente en los equipos de otras personas conectadas a Internet.

[11] STAIR, Ralph M., et al. Principles of Information Systems, Thomson Learning, Inc., 6a edición, Boston, 2003, pp. 132

"Los programas son la parte inteligente de las computadoras por que resultan imprescindibles para que una persona pueda trabajar correctamente. Cada día se crean varios programas cuya finalidad es facilitar aún más las labores de estos fieles equipos que han venido a simplificar la vida del ser humano". [12]

Se conoce como software al equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos del sistema, llamados hardware.

"Tales componentes lógicos incluyen, entre muchos otros, aplicaciones informáticas, como el procesador de textos, que permite al usuario realizar todas las tareas concernientes a la edición de textos— o el software de sistema, tal como el sistema operativo, que, básicamente, permite al resto de los programas funcionar adecuadamente, facilitando la interacción con los componentes físicos y el resto de las aplicaciones, proporcionando también una interfaz para el usuario".[13]

Software es una palabra proveniente del inglés (literalmente: partes blandas o suaves), que en español no posee una traducción adecuada al contexto, por lo cual se la utiliza asiduamente sin traducir y así fue admitida por la Real Academia Española (RAE)."[14] Aunque no es estrictamente lo mismo, suele sustituirse por expresiones tales como *programas (informáticos)* o *aplicaciones (informáticas)*.

Software es lo que se denomina *producto* en Ingeniería de Software. Probablemente la definición más formal de software sea la siguiente: Es el

---

[12] SILBERSCHATZ, Abraham. Operating System Concepts, Editorial Addison-Wesley, 4a edición, New York, 1994, p.p. 58.
[13] Ibid. p. 59.
[14] KNUTH, Donald E. The Art of Computer Programming, Volume 1, Editorial Addison-Wesley, 3a edición, Boston, 1997, p. 37.

conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación.

Considerando esta definición, el concepto de software va más allá de los programas de cómputo en sus distintos estados: código fuente, binario o ejecutable; también su documentación, datos a procesar e información de usuario forman parte del software: es decir, abarca todo lo intangible, todo lo "no físico" relacionado.

"El término «software» fue usado por primera vez en este sentido por John W. Tukey en 1957. En las ciencias de la computación y la ingeniería de software, el software es toda la información procesada por los sistemas informáticos: programas y datos. El concepto de leer diferentes secuencias de instrucciones desde la memoria de un dispositivo para controlar los cálculos fue introducido por Charles Babbage como parte de su máquina diferencial. La teoría que forma la base de la mayor parte del software moderno fue propuesta por vez primera por Alan Turing en su ensayo de 1936"[15], "Los números computables", con una aplicación al problema de decisión.

"Un programa informático es un conjunto de instrucciones que una vez ejecutadas realizarán una o varias tareas en una computadora. Sin programas, estas máquinas no pueden funcionar correctamente. Al conjunto general de programas, se le denomina software y así, se refiere al equipamiento lógico o soporte lógico de una computadora digital" [16].

En informática, se los denomina comúnmente *binarios*, (propio en sistemas unix, donde debido a la estructura de este último, los ficheros no necesitan hacer uso de extensiones. Posteriormente, los presentaron como ficheros

[15] Ibid. p. 38.
[16] Idem.

ejecutables, con extensión *.exe*, en los sistemas operativos de la familia Windows) debido a que una vez que han pasado por el proceso de compilación y han sido creados, las instrucciones que se escribieron en un lenguaje de programación que los humanos usan para escribirlos con mayor facilidad, se han traducido al único idioma que la máquina comprende, combinaciones de ceros y unos llamada código máquina. El mismo término, puede referirse tanto a un programa ejecutable, como a su código fuente, el cual es transformado en un binario cuando es compilado.

Generalmente el código fuente lo escriben profesionales conocidos como programadores. Se escribe en un lenguaje que sigue uno de los siguientes dos paradigmas: imperativo o declarativo y que posteriormente puede ser convertido en una imagen ejecutable por un compilador. Cuando se pide que el programa sea ejecutado, el procesador ejecuta instrucción por instrucción.

De acuerdo a sus funciones, se clasifican en software de sistema y software de aplicación. En los computadores actuales, al hecho de ejecutar varios programas de forma simultánea y eficiente, se le conoce como multitarea.

Una vez escritos, pueden ser ejecutados de diversas formas:

- “Mediante un programa que va adaptando las instrucciones conforme son encontradas. A este proceso se lo llama *interpretar* y a los programas que lo hacen se los conoce como intérpretes. Ejemplos de esto son bash, clásico en estaciones Unix y que fue escrito para el proyecto GNU o Python, cuya peculiaridad además de ser multipropósito, está en su facilidad de uso y productividad y de hecho, es usado en parte de los proyectos Google y Youtube.
- Traduciendo el código escrito del programa (lo que se denomina código fuente), a su equivalente en lenguaje máquina. A este proceso se le llama *compilar* y al programa traductor se le denomina compilador.

Ejemplos de esto son: El lenguaje C, que combina en su sintaxis características de medio y bajo nivel y el compilador gcc usado en el proyecto GNU."[17]

1.3.3.1. CLASES DE PROGRAMAS INFORMÁTICOS.

Antes de hablar de los tipos o clases de programas informáticos, es menester decir que el término programa tiene los siguientes significados: "PROGRAMA n. m. (gr. programma). Exposición general de las intenciones o proyectos de una persona, partido, etc.

2. Proyecto, plan.

3. Lista de las distintas partes o detalles de un trabajo, espectáculo, ceremonia, etc.

4. Folleto o impreso que contiene dicha lista.

5. Sesión de cine, teatro, etc., o emisión de televisión, radio, etc.

6. Conjunto de instrucciones, datos o expresiones registrados en un soporte, que permite ejecutar una serie de operaciones determinadas, solicitadas a un ordenador, a un aparato automático o a una máquina-herramienta.

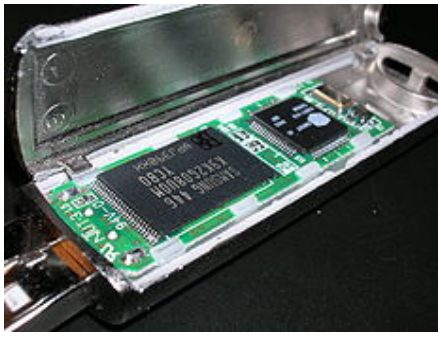
7. Argent. y Urug. Amorío que no se toma en serio.

8. Argent. y Urug. Amante ocasional."[18]

Típicamente, los programas se almacenan en una memoria no volátil (por ejemplo un disco), para que luego el usuario de la computadora, directa o indirectamente, solicite su ejecución. Al momento de dicha solicitud, el programa es cargado en la memoria de acceso aleatorio o RAM del equipo, bajo el control del software llamado sistema operativo, el cual puede acceder directamente al procesador. El procesador ejecuta (corre) el programa, instrucción por instrucción hasta que termina. A un programa en ejecución se le

[17] Ibid. p. 40.
[18] Diccionario Enciclopédico El Pequeño Larousse Interactivo. Larousse Multimedia, México, 2008.

suele llamar también proceso. Un programa puede terminar su ejecución en forma normal o por causa de un error, dicho error puede ser de software o de hardware.



El microcontrolador a la derecha de la Memoria USB está controlada por un firmware empotrado.

Algunos programas están empotrados en el hardware. Una computadora con arquitectura de programas almacenados requiere un programa inicial almacenado en su ROM para arrancar. El proceso de arranque es para identificar e inicializar todos los aspectos del sistema, desde los registros del procesador, mecanismos de control conocidos como controladores de dispositivos hasta el contenido de la memoria.

Seguido del proceso de inicialización, este programa inicial carga al sistema operativo e inicializa al contador de programa para empezar las operaciones normales. Independiente de la computadora, un dispositivo de hardware podría tener firmware empotrado para el control de sus operaciones. El firmware se utiliza cuando se espera que el programa cambie en raras ocasiones o nunca, o cuando el programa no debe perderse cuando haya ausencia de energía.

Los programas históricamente se cargaron manualmente al procesador central mediante interruptores. Una instrucción era representada por una configuración de estado abierto o cerrado de los interruptores. Después de establecer la

configuración, se ejecutaba un botón de ejecución. Este proceso era repetitivo. También, históricamente los programas se cargaban manualmente mediante una cinta de papel o tarjetas perforadas. Después de que el programa se cargaba, la dirección de inicio se establecía mediante interruptores y el botón de ejecución se presionaba.

La programación automática es un estilo de programación que crea código fuente mediante clases genéricas, prototipos, plantillas, aspectos, y generadores de código para aumentar la productividad del programador. El código fuente se genera con herramientas de programación tal como un procesador de plantilla o un IDE. La forma más simple de un generador de código fuente es un procesador macro, tal como el preprocesador de C, que reemplaza patrones de código fuente de acuerdo a reglas relativamente simples.

Un motor de software da salida, un código fuente o lenguaje de marcado que simultáneamente se vuelve la entrada de otro proceso informático. Podemos pensar como analogía un proceso manejando a otro siendo el código máquina quemado como combustible. Los servidores de aplicaciones son motores de software que entregan aplicaciones a computadoras cliente. Por ejemplo, un software para wikis es un sevidor de aplicaciones que permite a los usuarios desarrollar contenido dinámico ensamblado a partir de artículos. Las Wikis generan HTML, CSS, Java, y Javascript los cuales son interpretados por un navegador web.

“Los programas se pueden categorizar según líneas funcionales. Estas categorías funcionales son software de sistema y software de aplicación. El software de sistema incluye al sistema operativo el cual acopla el hardware con el software de aplicación”. “El propósito del sistema operativo es proveer un ambiente en el cual el software de aplicación se ejecuta de una manera

conveniente y eficiente". [19] Además del sistema operativo, el software de sistema incluye programas utilitarios que ayudan a manejar y configurar la computadora. Si un programa no es software de sistema entonces es software de aplicación. El middleware también es un software de aplicación que acopla el software de sistema con la interfaz de usuario. También son software de aplicación los programas utilitarios que ayudan a los usuarios a resolver problemas de aplicaciones, como por ejemplo la necesidad de ordenamiento.

A los fines prácticos se puede clasificar al software en tres grandes tipos:

- Software de sistema: Su objetivo es desvincular adecuadamente al usuario y al programador de los detalles de la computadora en particular que se use, aislándolo especialmente del procesamiento referido a las características internas de: memoria, discos, puertos y dispositivos de comunicaciones, impresoras, pantallas, teclados, etc. El software de sistema le procura al usuario y programador adecuadas interfaces de alto nivel, herramientas y utilidades de apoyo que permiten su mantenimiento. Incluye entre otros:

    - Sistemas operativos.
    - Controladores de dispositivos.
    - Herramientas de diagnóstico.
    - Herramientas de Corrección y Optimización.
    - Servidores.
    - Utilidades.
    -

- Software de programación: Es el conjunto de herramientas que permiten al programador desarrollar programas informáticos, usando diferentes alternativas y lenguajes de programación, de una manera práctica. Incluye entre otros:

[19] Idem.

- Editores de texto.
- Compiladores.
- Intérpretes.
- Enlazadores.
- Depuradores.
- Entornos de Desarrollo Integrados (IDE): Agrupan las anteriores herramientas, usualmente en un entorno visual, de forma tal que el programador no necesite introducir múltiples comandos para compilar, interpretar, depurar, etc. Habitualmente cuentan con una avanzada interfaz gráfica de usuario (GUI).

- Software de aplicación: Es aquel que permite a los usuarios llevar a cabo una o varias tareas específicas, en cualquier campo de actividad susceptible de ser automatizado o asistido, con especial énfasis en los negocios. Incluye entre otros:
  - Aplicaciones para Control de sistemas y automatización industrial.
  - Aplicaciones ofimáticas.
  - Software educativo.
  - Software empresarial.
  - Bases de datos.
  - Telecomunicaciones (p.ej. internet y toda su estructura lógica).
  - Videojuegos.
  - Software médico.
  - Software de Cálculo Numérico y simbólico.
  - Software de Diseño Asistido (CAD).
  - Software de Control Numérico (CAM).[20]

[20] PRESSMAN, Roger S. (2003). Ingeniería del Software, un enfoque Práctico, Editorial Mc Graw Hill, 5ª edición, México, 2008, p. 49.

1.3.3.2. OBJETIVO DE LOS PROGRAMAS INFORMÁTICOS.

La computadora no puede realizar ninguna función por sí misma, sino que requiere de alguna instrucción que le dirija y organice las operaciones a cumplir. Dichas instrucciones están agrupadas en forma de programas que son depositados en la memoria del ordenador y conforman lo que se conoce como software.

Así, el objetivo de los programas es precisamente dar instrucciones al equipo para efecto de que éste realice determinadas tareas de acuerdo a las necesidades del usuario.

Como se ha señalado, existe cierto software que requiere el equipo para efecto de funcionar correctamente y satisfacer las necesidades mínimas que espera el usuario. En caso de que el ordenador no cuente con esos programas o bien, que sufran algún daño, por ejemplo debido a una descarga eléctrica excesiva, el equipo seguramente no podrá funcionar correctamente.
Tenemos también el software adicional que el usuario adquiere e instala en su equipo para diversos fines: diversión, trabajo, etc., los cuales se conocen como utilidades y que varías de acuerdo a las necesidades del usuario y al potencial o memoria que tenga el equipo, ya que dichos programas ocupan generalmente mucho espacio.

En el caso de los virus informáticos, podemos advertir que se trata de programas cuya finalidad es alterar o destruir los que ya se encuentran en el ordenador, por ello, resultan muy peligrosos para los equipos y la información almacenada en ellos.

1.4. LOS VIRUS INFORMÁTICOS.

En las últimas tres décadas, la informática y todos sus contenidos han experimentado un notable avance, inclusive, podemos considerarlo como vertiginoso, creándose computadoras cada vez más potentes, de respuesta más rápida y que satisfacen las necesidades de trabajo imperante en empresas, instituciones oficiales y de las personas en general. De la misma manera, se han creado programas computacionales o "software" que enriquecen las capacidades de las computadoras y facilitan la vida diaria del hombre. Sin embargo, dicho avance ha traído consigo la creación de mecanismos o programas tendientes a causar daño a los usuarios de la red de Internet, lo que constituye uno de los principales inconvenientes y peligros de la súper carretera de la información llamada Internet. A este tipo de programas destinados a dañar los archivos que obran en la computadora de otras personas se les conoce con el nombre de "Virus Informáticos".

Los virus informáticos se han multiplicado rápidamente, al igual que otros programas cuya utilidad es manifiesta. Muchos de ellos han cobrado fama debido a que su propagación es fácil y rápida, por lo que en cuestiones de minutos llegan a infiltrarse en las computadoras de otros países.

A continuación intentaremos explicar qué es un virus informático y como se crea.

Un virus informático es un programa o código, en ocasiones complejo y la mayoría de las ocasiones es realmente muy simple. Su único objetivo es entrar en el sistema del ordenador (Computadora), duplicarse y propagarse a todos los archivos que sea posible, sin que el usuario tenga conocimiento de ello, hasta que es muy tarde y el virus haya conseguido infectar: dañar los archivos informáticos que obran en el equipo, lo cual puede causar un severo daño en el mismo.

Otra definición de virus informático es: *"Un virus informático es un programa creado con el fin de realizar una función en particular, generalmente perjudicial para una computadora, un sistema o una red. El perjuicio puede ser en contra de la información o la seguridad de las máquinas infectadas. Una de las características más importante de un virus es que se puede auto-duplicar las veces que quiera; de la misma forma puede programarse para pasar inadvertido, incluso disfrazarse de un archivo inofensivo hasta que llega el momento de ejecutarse y armar el relajo….."*.[21]

Como podemos advertir, este concepto es mucho más completo, pues nos ofrece otra clase de información que debemos analizarla a efecto de poder comprender en toda su magnitud los alcances de los virus informáticos. Así, encontramos en la revista citada que un virus es un programa de cómputo creado con el fin de causar daño a una o varias computadoras, a los sistemas o a las redes de ella. El perjuicio que puede causar un virus puede ir contra los archivos de información que están dentro de una o varias computadoras o contra la seguridad de los equipos infectados. Un virus es capaz de auto duplicarse muchas veces; puede a su vez alojarse durante algún tiempo en una o varias computadoras y permanecer en estado de latencia hasta que ql usuario abra el archivo, momento en el cual el virus saldrá e infectará los demás archivos, hasta dañarlos e inclusive, afectar la seguridad de la máquina misma u ordenador (como se le nombre en España).

El virus informático puede adoptar la forma de un archivo totalmente inofensivo y así confundir al usuario quien fácilmente le permitirá salir y cumplir sus propósitos. El término virus informático tiene un sentido metafórico o virtual, como si se tratase de un conjunto de microorganismos unicelulares o pluricelulares que se alojan en el cuerpo humano y que causan alguna enfermedad. Se ha considerado que gracias al enorme parecido con los

[21] Revista "www.vivir en internet" Publicación mensual, 09/2001. Editorial Planeta, México. p. 59.

programas informáticos creados para causar daño en los archivos y en la seguridad de los equipos de cómputo, a su desarrollo, etc., son virus, en términos virtuales.

1.5. PRINCIPALES ANTECEDENTES DE LOS VIRUS INFORMÁTICOS.

La creación de los virus informáticos es muy reciente al igual que las computadoras mismas. Según algunos datos su nacimiento se remonta a fines de los años sesentas, cuando los norteamericanos Douglas Mcllory, Víctor Vysottsky y Robert Morris idearon un juego llamado: Core War", el cual se convirtió rápidamente en el pasatiempo favorito de algunos programadazos de los laboratorios Bell de la industria AT&T. Como se desprende de su nombre, "Core War" era una batalla en el core o memoria organismo, cuyo hábitat era precisamente la memoria del ordenador. A partir de una señal, cada programa intentaba forzar al otro efectuar una instrucción inválida. El primero que lo consiguiera ganaría el juego. Una vez terminado el juego, se borraría todo rastro de la batalla de la memoria de la máquina. Se cuenta que este tipo de entrenamientos se sancionaban por los superiores de esa compañía por considerar que era muy peligroso que se dejara un organismo suelto (programa computacional), que pudiera terminar con las informaciones que habrían de aplicarse al día siguiente. Esto ocasionó que el juego se efectuara de forma clandestina.

"Core War" es casi desconocido para la mayoría de las personas que se encontraban relacionadas con la informática, lo cual significa que no tuvo mucha difusión como un juego. Se cuenta que en el año de 1987 un periodista de los Estados Unidos perdió la información de seis meses de trabajo que tenía guardada en un disco, al intentar recuperarla pudo darse cuenta de que se

trataba de un acto de sabotaje. Casualmente, en el disco se encontraba un número telefónico de una tienda de computación de Pakistán y el mensaje decía lo siguiente:

"Bienvenidos al calabozo…..llámenos para la vacuna".

La información del periodista había sido víctima de un virus maligno.
Se hicieron algunas investigaciones al respecto y se pudo concluir que la tienda a la que hacía referencia era "Brain Computer Services", la cual de dedicaba entre otras cosas a vender copias ilegales de algunos programas muy caros con un precio de $ 1. 50 cada uno, lo cual ya nos muestra que desde entonces se realizaban actos de piratería que no son originarios de nuestro país, los cuales tuvieron bastante éxito debido al considerable ahorro que representaba para el consumidor el comprarlos de forma ilegal. Durante los años de 1986 y 1987, algunos de los clientes de esta tienda fueron algunos estudiantes de los Estados Unidos, quienes eran atraídos por el bajo costo de los programas. No obstante, escondido en el disco se encontraba un virus, por lo que cada vez que el programa era abierto y ejecutado, el virus infectaba a la computadora y ésta a su vez a los discos de otros usuarios. Cabe resaltar que los diseñadores de virus fueron los hermanos Amjad y Basit Farooq Alvi, quienes eran los dueños de la tienda de computación referida de nacionalidad pakistaní.

En el año de 1985 los hermanos Amjad Alvi, decidieron hacer un software, sin embargo, de manera sorpresiva el software fue copiado y usado sin permiso. De esta forma se cuenta que Amjad ideó un programa que pudiera duplicarse y cuya función fuera la de infectar la computadora de un usuario que no contara con autorización de los creadores del programa, con lo que el mismo se vería en la necesidad de llamarles para reparar los daños.

Tiempo después, los hermanos Farooq Alvi tenían en su poder un virus que incluían en sus copias ilegales, y sucedía que cuando un pakistaní deseaba

una copia del programa se le vendía libre de virus, pero cuando se trataba de un extranjero, se le vendía una copia contaminada.

De acuerdo con las declaraciones de los hermanos Alvi, en su país las leyes del Derecho de Autor no incluyen el software, por lo que vender copias piratas no constituye un delito, contrariamente con la mayoría de las legislaciones del mundo, como la de los Estados Unidos y la de México, donde se prohíbe este tipo de prácticas, al menos teórica y jurídicamente, puesto que en la realidad constituye un modo de vida para muchas personas el realizar copias piratas de casi todos los programas de moda o que representan alguna utilidad para los usuarios y cuyo costo normal es muy alto.

Con respecto a la Ley Federal del Derecho de Autor y la Protección de los programas de cómputo en nuestro país tenemos lo siguiente:

> “Artículo 101. Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica”.
>
> “Artículo 102. Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos”.

Finalmente, el artículo 106 nos hable de los derechos que la Ley le concede al autor del programa de cómputo.

"Artículo 106. El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:
I. La traducción permanente o provisional del programa en todo o parte, por cualquier medio y forma;
ll. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;
III.- Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y
IV. La descompilación y el desensamblaje".

Los programas de computación deberán ser inscritos en el Registro Federal del Derecho de Autor para que surtan efectos contra terceros "erga omnes".

Finalmente se cuenta que los hermanos Alvi dejaron de vender copias en el año de 1987, advirtiendo que había sido una lección para los piratas.[22]
Resulta importante imaginar que aquél juego de entretenimiento se habría de convertir en una poderosa arma capaz de colapsar y dañar los archivos de millones de usuarios en todo el mundo, ya que a través de Internet es posible que lleguen a su destino en sólo cuestión de minutos o segundos, cundiendo el pánico entre los usuarios y causando un detrimento patrimonial que puede llegar a estimarse en millones de dólares.

Actualmente existen muchos virus informáticos, pues su propagación es relativamente fácil. Posiblemente estamos ante una nueva forma de terrorismo mundial que en cualquier momento pone en jaque a las instituciones económicas, financieras y políticas del mundo.

[22] LÓPEZ ORTÍZ, Alex y Daniel M. Germán, en América on line México. www.americaonline.com.mx. Lunes 02 de julio de 2001.

1.6. ALGUNOS CASOS DE VIRUS INFORMÁTICOS.

En nuestros días existen algunos estudios sobre virus informáticos, gracias a ellos es que podemos advertir la existencia de diferentes tipos o clases de ellos.

Hemos citado, que un virus informático es un programa para replicarse y distribuirse por sí mismo, sin que el usuario del equipo contaminado se de cuenta. Estos virus se distribuyen adhiriéndose a otros programas (como sus programas de procesamiento de palabras u hoja de cálculos: Word, Excel o Outlook, entre otros) o en el sector de arranque de un disquete. Cuando un archivo que ha sido previamente infectado es ejecutado, o la computadora es arrancada desde el disquete infectado, el virus es automáticamente también ejecutado. Es normal que el virus se esconda en la memoria del ordenador, esperando infectar al próximo programa que corra, o el próximo accesado.

Gran parte de los virus pueden mostrar un mensaje en cierta fecha, borrar archivos después de que el programa infectado ha corrido un cierto número de veces. En estos casos, nos enfrentamos ante efectos benignos, pero existen otros en los que los efectos son detrimentales y molestos, reduciendo así, la velocidad del sistema, causando cambios menores en la pantalla de la computadora. Algunos virus más, son amenazadores, al causar la caída del sistema, archivos dañados e inclusive, la pérdida de información. Otro ejemplo de virus es el famoso “SirCam”, mejor conocido como: “hola como estás”, del cual encontramos que: *“Recientemente el mundo fue infectado por un famoso virus: “SirCam”. Por si acaso no tienen computadora (o se fueron de vacaciones y no se enteraron), le diré que este virus es tan práctico y de tan veloz propagación, que antes de ser noticia mundial ya se había encargado de*

dar de baja (temporalmente) servidores de mails de compañías transnacionales para ser desinfectados".[23]

Si observamos de cerca al SirCam, podemos encontrar algo interesante: este virus es bilingüe, y se basa en la terminación de la dirección de correo para enviar mensajes en inglés en los casos de dominio.com, o en español en los casos de dominio.com.mx. el mensaje dice lo mismo, en ambos idiomas, y al parecer, el original podría ser el escrito en español. Súmenle a esto el curioso dato de que este virus fue programado para usar un servidor del mail".com.mx" en caso de que la víctima no tuviera uno válido, y podemos crear el rumor de que el "SirCam" es un virus mexicano…." [24]

Algunos datos estadísticos que podemos mencionar, arrojan datos asombrosos, por ejemplo en el año de 1986 sólo se conocía la existencia de un virus informático en todo el mundo. En la actualidad, se estima que existen casi 48000 virus en todo el mundo, con nuevos ejemplos y variantes, entre 70 y 100 de ellas que aparecen cada semana. Un dato alentador es que de los 48000 virus muy pocos están en libertad.

A continuación citaremos algunos de los tipos de virus informáticos en la actualidad:

Infectores de archivos:
Son virus que se pegan o reemplazan archivos .Com y .EXE, aunque en algunos casos infectan archivos con extensiones .SYS, DRV, DLL, BIN, OVL, y OVY. Con estos virus, los programas sanos usualmente se infectan cuando son ejecutados con el virus en la memoria. En otros casos, son infectados al ser abiertos o el virus simplemente infecta a todos los archivos desde el que fue corrido.

[23] Idem..
[24] Ibid. p.61.

Dentro de esta categoría de virus también encontramos a los infectores del Sector de Arranque: cada drive lógico, tanto en discos duros como floppies, contiene un sector de Arranque, el cual contiene información específica acerca del formato del disco y los datos almacenados en él, y contiene un pequeño programa llamado precisamente “Programa de Arranque” (que carga los archivos de sistema del MS-DOS). El programa de Arranque muestra el mensaje “Non-sytem disk or Disk Error”, si los archivos del MS-DOS no están presentes.

Una computadora se puede llegar a infectar con un virus del Sector de Arranque, dejando un diskette infectado en el drive de arranque y encendiéndola. Cuando el programa de arranque es leído y ejecutado, el virus entra en la memoria e infecta al disco duro de la computadora. Hay que tomar en cuenta que cada disco contiene un Sector de Arranque, por lo que es fácil infectar una máquina con un disco de datos.

Infectores del récord Maestro de Arranque:
El primer sector físico de cada disco duro (Lado O, Track 0, Sector 1) contiene el récord Maestro de Arranque (Master Boot Récord) y la tabla de partición. El citado Récord Maestro de Arranque (MBR) contiene un pequeño programa llamado “Programa Maestro de Arranque”, el cual busca en la Tabla de Partición lo valores para la localidad inicial de la Partición de Arranque, y ordenándole al sistema ir allí y ejecutar cualquier código que encuentre a su paso.
En los floppies, los mismos virus infectan los Sectores de Arranque.

Una computadora se puede llegar a infectar con un virus del Récord Maestro de Arranque de la misma manera que se infecta con un virus del Sector de Arranque, es decir, dejando un diskette infectado en el drive de arranque y

encendiéndola. Así, cuando el Programa del Sector de arranque sea leído y ejecutado, el virus entra en la memoria e infecta el MBR del disco duro.

Infector Directo:
Un virus estará activo sólo cuando un archivo infectado está siendo ejecutado.

Infector Residente en Memoria:
Un virus Infector Residente en Memoria a un programa convencional que termina y permanece residente en memoria (TSR), toma el control del sistema y continúa infectando cada vez que se use la computadora, incluso si se cierra el programa infectado. El virus mantiene el control hasta que la memoria de la computadora sea limpiada, re-iniciándola “en frío” o con un “Reset”.

Virus Polimórfico:
Es un virus que deliberadamente cambia de propio código de programación para impedir que sea detectado. Cada archivo infectado por este virus contendrá un conjunto diferente de instrucciones, aún en el caso de que todos ellos se encuentren infectados por este mismo virus.

Virus Escondido (Stealth):
Es un virus programado para que activamente busque ocultarse contra su detección, o bien, que es capaz de defenderse contra los intentos de analizarlo o removerlo. Estos virus contienen una ingeniería especial que les permite eludir la detección con herramientas antivirus tradicionales. Esto lo logra quedándose en la memoria después de ejecutarse. Desde allí monitorea i intercepta las llamadas del sistema operativo. Cuando el sistema intenta abrir un archivo infectado, el virus escondido le muestra la versión no infectada, escondiéndose de esta manera.

Incluso, algunos detectores de virus, usando las técnicas tradicionales, pueden propagar el virus. Esto se da porque abren y cierran los archivos para

revisarlos, lo que da al virus oportunidades adicionales para propagarse. Los detectores también fallan al encontrar al virus, porque en el momento de abrir el archivo para la detección, se causa que el antivirus temporalmente desinfecte el archivo, haciéndolo aparecer como normal.

Gusano.

Los "gusanos" de computadoras son programas que pasan de computadora a computadora por medio de una red (como el Internet, por ejemplo). A diferencia de los virus citados, no infectan programas, diskettes o archivos con capacidad para macros. En su lugar, hacen copias de si mismos y las envían a través de la red a otras máquinas. Los "gusanos" provienen al igual que los virus de fuentes anónimas o no localizables,

"Se encuentran frecuentemente equipados con descifradores de passwords basados en diccionarios y otras herramientas tipo "craker" que les permiten penetrar en otros sistemas. Se dice que los "gusanos" con frecuencia roban los datos que se encuentran en una computadora".[25]

1.7. LA CREACIÓN DE LOS VIRUS INFORMÁTICOS Y SU REPERCUSIÓN.

El uso de Internet y de los programas que se han ido creando para hacer de esta súper carretera, un mejor vehículo de comunicación ha sido también empleado, por desgracia por delincuentes, quienes han encontrado formas relativamente exitosas aunque no fáciles para causar daño en los equipos informáticos de millones de usuarios en el mundo, a través de la creación y propagación de los virus informáticos, que no son sino programas que se crean ex profeso para causar daños, algunos de carácter irreversible.

[25] Vid. LÓPEZ-ORTÍZ, Alex y Daniel M. Germán en América on Line México. www.aol.com.mx.Lunes 02 de julio de 2008.

Si bien es cierto, este tipo de programas se crearon de forma accidental, como un juego, lo cierto es que con el paso del tiempo, los virus informáticos se han convertido en una amenaza a los millones de usuarios de Internet quienes reciben muchos e mails o correos electrónicos, algunos de desconocidos, por lo que al abrirlos, activan el mecanismo de desarrollo destructivo del virus.

Se trata de un tema apasionante, sobre todo desde el punto de vista jurídico, materia en la que falta mucho por hacer, sobre todo en nuestra legislación, por lo que en los puntos siguientes de esta investigación abundaremos sobre el particular.

1.8. LA PROPAGACIÓN DE VIRUS INFORMÁTICOS Y SU REPERCUSIÓN.

Desde su creación los virus informáticos delimitaron perfectamente su objetivo, causar daño leve o grave a otros equipos de computación, aunque si recordamos, en sus inicios surgen principalmente como un juego y con el paso del tiempo se han ido desarrollando como una forma de perjudicar a los demás en el aparente anonimato.

Actualmente la creación y propagación de los virus informáticos ocasiona serios y devastadores daños, no sólo en lo que respecta a los usuarios particulares, sino que también a las economías del mundo, logrando con ello poner en peligro la misma seguridad y paz mundial.

A continuación citaremos los efectos y la propagación de los virus informático, para tal efecto hemos tratado de abarcar los campos más sobresalientes en los que consideramos que provocan mayores trastornos.

1.9. LOS VIRUS INFORMÁTICOS DESDE DIFERENTES ÁNGULOS.

Los virus informáticos pueden ser apreciados desde diversos ángulos como son los siguientes:

ECONÓMICOS. En actualidad la creación y propagación de virus informáticos ha logrado generar serios daños en la economía, no sólo de las personas físicas quienes realizan diversas operaciones bancarias o bursátiles a través del Internet, realizando a su vez diferente contratos nacionales o transaccionales. También es muy común que las personas utilicen esta red para comprar algún objeto utilizando su tarjeta de crédito, o para pagar algún servicio. Los virus informáticos también pueden dañar a los sistemas económicos del mundo, los cuales dependen totalmente del uso de computadoras, por lo que de introducirse uno o varios virus podrían causar un colapso económico de gran intensidad y repercusión mundial, lo cual podríamos traducirlo en la pérdida de millones de dólares. Afortunadamente, los Estados han podido tomar sus precauciones, pero sin lugar a dudas viven bajo el temor fundado de que un virus se introduzca en los equipos de cómputo y cause daños. Debemos recordar que los “hackers” o piratas se encuentran en constante actualización, por lo que los virus sufren constantes adelantos y se sofistican en poco tiempo, lo cual significa que es más difícil el detectarlos e impedir que logren su objetivo. Pensemos que un virus se active en las principales bolsas de valores del mundo, los resultados serían catastróficos, en cuestiones de minutos se perderían millones de dólares, y las economías de algunos países se vendrían abajo.

Sin poner en tela de juicio el aspecto económico es el de mayor importancia para los países; de hecho, el mundo actual gira en torno a la economía, por lo

cual, los virus informáticos se convierten en una seria y constante amenaza contra todas las naciones, ya sea del primer mundo o en vías de desarrollo.

POLÍTICOS. La creación y propagación de virus informáticos tiene a su vez una trascendencia política, puesto que los daños que pueden causar frecuentemente son considerados como actos de los cuales debe responder un país independientemente del autor de los mismos. La comunidad internacional espera que se combata a todo acto que tenga como finalidad crear y propagar algún tipo de virus informático, sancionando a su autor o autores. Por eso es que en algunos países ya existe una policía científica encargada de investigar este tipo de ilícitos y de llevarlos ante los tribunales correspondientes.

Con estos postulados no queremos decir que existe una responsabilidad de los Estados cuando uno de sus nacionales crea y propaga un virus informático, al menos desde el punto de vista del Derecho Internacional, aunque si existe una responsabilidad de tipo moral, puesto que hemos señalado que los daños que puede llegar a causar con la propagación de virus informáticos pueden ser verdaderamente siniestros, sobretodo económicamente para los países. Por esto mismo, hoy es factible saber dónde ha sido creado un virus informático y aunque no constituya aún un delito internacional, el país en el que ha sido creado este microprograma debe encontrar al responsable y sancionarlo tan rápido como le sea posible, dándolo a conocer al mundo.

Por otra parte, la creación y propagación de virus informáticos puede tener una connotación política internacional de suma importancia, como un clima de inestabilidad internacional. Por esto, consideramos que los Estados deben crear caminos de colaboración permanente y de lucha constante contra este perjuicio moderno que constantemente amenaza a nuestro mundi moderno virtual de globalización, en donde las economías, las culturas e inclusive los sistemas políticos se encuentran entrelazados.

En lo que respecta a lo interno, la creación y propagación de virus informáticos también podemos considerarlo como un asunto de seguridad nacional, puesto que todo país guarda información confidencial en sus archivos, y un virus puede dañar dicha información en cualquier momento, dando por resultado serios daños en el aspecto político y económico. De esta manera, es importante que consideremos que la creación y propagación de virus informáticos puede llegar a convertirse en un asunto de seguridad nacional.

INTERNACIONALES. Algunos años antes, los virus informáticos eran hechos que se consideraban aislados porque no representaban un serio problema económico y de seguridad nacional, y es que como ya lo mencionamos, nos encontramos inmersos en un mundo globalizado, interconectado en virtud a la economía, las comunicaciones, la cultura y el comercio. La globalización es un fenómeno que tiene muchas ventajas y desventajas, entre ellas, podemos encontrar que los países basan sus relaciones comerciales, económicas, culturales, tecnológicas y políticas en el uso de las computadoras, las cuales les permiten hacer transacciones de cantidades grandes de dinero en cuestión de minutos. Los adelantos cibernéticos como el Internet ha acortado las fronteras entre los países. Por este motivo, México ha llevado a cabo numerosos tratados de libre comercio con muchos países o bloques económicos como la Unión Europea.

Insistimos que el exacto cumplimiento a los compromisos adquiridos por nuestro país depende en gran medida del uso de las computadoras y del Internet como instrumentos de logística indispensables.

Desafortunadamente, la falta de regulación internacional sobre la creación y propagación de virus coadyuva con aquellos quienes pretenden obtener algún tipo de beneficio económico al realizar los programas computacionales cuya finalidad es causar daño a los servidores de millones de usuarios en todo el mundo.

Por último, consideramos importante citar que un virus recién creado en un país lejano del nuestro, puede llegar en sólo cuestión de minutos, es decir, laceración y propagación de virus informáticos representa un problema de índole mundial, puesto que involucra a todos los países y cuya solución debe ser tomada por la comunidad internacional a través de tratados que implementen mecanismos de combate y de colaboración entre ellos para que así logren ubicar a los creadores de virus, sancionando estas conductas duramente mediante las reformas legales internas correspondientes y así irlos aniquilando paulatinamente.

SOCIALES. Nuestra sociedad se ha informatizado, es decir: las computadoras han entrado en nuestra vida tomando así un lugar mucho muy especial.
Como gobernados, tenemos derecho a expresarnos oralmente o por escrito, de conformidad con los artículos 6º y 7º de la Constitución Política de los Estados Unidos Mexicanos. Esa libertad de expresión debe incluir necesariamente el uso de la computadora y de Internet, por lo tanto, cuando alguien crea y propaga un virus informático, estará causando severos daños a una gran cantidad de usuarios, daños que se pueden traducir en pérdidas económicas casi invaluables. Por desgracia, la falta de una regulación jurídica adecuada, en muchos países entre ellos México, hace posible que personas sin escrúpulos y muy ambiciosas, busquen obtener beneficios económicos substanciosos, sembrando el pánico entre los usuarios que utilizan la red llamada Internet.

Sin lugar a dudas nuestra sociedad necesita tener la seguridad de que podrá usar sus equipos de cómputo y la red de Internet sin que al abrir un archivo se encuentre con la desagradable sorpresa de que un virus ha infectado sus archivos.

Es bien cierto que México está aún rezagado en el campo de la investigación y la regulación de los virus informáticos, por eso hace falta que los legisladores

tomen conciencia y sobretodo conozcan todo lo referente a los virus informáticos, para que con ello estén posibilidad de crear tipo penales que puedan sancionar dichas conductas. A su vez es indispensable que nuestro país cuente con una política científica especializada en virus informáticos, que pueda fácilmente encontrar a los autores de virus informáticos y ponerlos a disposición del Ministerio Público, pero también puedan auxiliar al órgano jurisdiccional que conozca de este tipo de causas penales.

CAPÍTULO 2.
EL CÓDIGO PENAL VIGENTE PARA EL DISTRITO FEDERAL Y LOS DELITOS INFORMÁTICOS.

2.1. EL CÓDIGO PENAL VIGENTE PARA EL DISTRITO FEDERAL.

Después de algunos meses de investigación en diversos medios y foros, se decidió que era impostergable ya que el Distrito Federal contara con un nuevo Código Penal que estuviera más acorde a las necesidades de la población en materia de combate y prevención de la criminalidad.

En la elaboración del actual Código Penal para el Distrito Federal participaron académicos, abogados litigantes, sociedad, jueces y magistrados, los cuales dieron sus opiniones enriqueciendo el modelo del actual Código Sustantivo Penal para el Distrito Federal.

Este Código fue publicado en la Gaceta Oficial del Distrito Federal el 16 de julio del 2002, mediante el Decreto del señor Andrés Manuel López Obrador, entonces Jefe de Gobierno de esta ciudad.

El Código Penal vigente para el Distrito Federal obedece a una ratio legis justificada plenamente, lo que se debe traducir en un verdadero combate a la criminalidad, a través de penas actualizadas y de nuevos tipos penales.

En el ámbito de la procuración de la justicia (ante el Ministerio Público), el Código Penal representa nuevas opciones para que la representación social

pueda iniciar averiguaciones previas en conductas u omisiones que antes no constituían delito alguno, pero que ahora, sí son materia de investigación. Así, el Ministerio Público ve ampliada su esfera de competencias a nivel averiguación previa con nuevos tipos penales que, sin embargo, representan también nuevos retos ya que no resulta fácil su correcta integración, por lo que la Procuraduría General de Justicia deberá implementar las instrucciones a través de los acuerdos necesarios para que los Ministerio Públicos puedan integrar correctamente sus indagatorias.

A nivel administración de justicia (ante el juez penal), sucede lo mismo. El Código Penal implica mayores retos, algunos de ellos complejos, como ocurre en tipos novedosos como sería el de creación y propagación de virus informáticos que proponemos y objetivo de este trabajo de investigación.

2.2. LA EXPOSICIÓN DE MOTIVOS DEL CÓDIGO PENAL VIGENTE PARA EL DISTRITO FEDERAL.

En los antecedentes del Proyecto de Decreto que contiene el Código Penal para el Distrito Federal se destaca la justificación de dicho cuerpo normativo:

> *"Partido de la Revolución Democrática: El Código Penal vigente es reflejo de muchas tendencias y doctrinas a veces coincidentes, pero en otras confrontadas, por eso vemos necesario entrar a una revisión integral y es en ese marco, que presentamos esta iniciativa de Código Penal para el Distrito Federal, sin dejar de insistir en que estamos abiertos a otros puntos de vista y que buscamos, con todas y todos los diputados que conforman este órgano de gobierno, dar respuesta a la sociedad capitalina. En este orden de ideas, surgen algunas cuestiones fundamentales*

que tendríamos que reflexionar: Por qué un nuevo Código penal para el Distrito Federal? ¿Qué tipo de Código Penal es el que requiere esta gran ciudad?....".

Posteriormente, la misma exposición de motivos agrega:

"En atención a ello, el Código debe precisar con nitidez los presupuestos de la pena, las medidas de seguridad y los criterios político-criminales para la individualización judicial de las penas. Asimismo, resulta imperativo revisar el catálogo de delitos, para determinar por una parte, qué nuevas conductas habrá de penalizar y cuáles se deben excluir del Código Penal, partiendo de la base de que sólo deben regularse aquellas conductas que revisten gravedad y buscando una mayor racionalización de las penas".

El Código Penal para el Distrito Federal se justifica plenamente en la necesidad cada día más creciente de que la sociedad cuente con un ordenamiento penal sustantivo más acorde a sus necesidades, castigándose con más severidad los delitos considerados graves y, por otra parte, se incorporan nuevos tipos penales que en el Código de 1931 no estaban tipificados y que obedecen a la necesidad mencionada de la sociedad del Distrito Federal de tener leyes que castiguen con mayor severidad los ilícitos penales.

Por otra parte, el Código Penal para el Distrito Federal contiene una serie de principios o garantías penales que sustentan la acción penal del Estado contra los infractores de dichas normas. A este respecto, el artículo 1º de Código en comento establece que:

"A nadie se le impondrá pena o medida de seguridad, sino por la realización de una acción u omisión expresamente prevista como delito en una ley vigente al

tiempo de su realización, siempre y cuando concurran los presupuestos que para cada una de ellas señale la ley y la pena o la medida de seguridad se encuentren igualmente establecidas en ésta".

De esta manera, no se podrá imponer una pena a una persona, sino por la realización de una acción u omisión que se encuentre expresamente señalada por la ley como delito. Sobre esto, el artículo 2 del mismo Código dispone que:

"No podrá imponerse pena o medida de seguridad, si no se acredita la existencia de los elementos de la descripción legal del delito de que se trate. Queda prohibida la aplicación retroactiva, analógica o por mayoría de razón, de la ley penal en perjuicio de persona alguna.
La ley penal sólo tendrá efecto retroactivo si favorece al inculpado, cualquiera que sea la etapa del procedimiento, incluyendo la ejecución de la sanción. En caso de duda, se aplicará la ley más favorable".

El artículo 3 del Código Penal para el Distrito Federal señala que, para que la acción o la omisión sean penalmente relevantes, deben realizarse de manera dolosa o culposa:

"Para que la acción o la omisión sean penalmente relevantes, deben realizarse dolosa o culposamente".

De la misma manera, para que la acción u omisión sean consideradas como delictivas y se puedan sancionar, es menester que lesionen o pongan en peligro, sin justa causa, el bien jurídico tutelado por la ley penal:

"Para que la acción o la omisión sean consideradas delictivas, se requiere que lesionen o pongan en peligro, sin causa justa, al bien jurídico tutelado por la ley penal".

Es así que esta serie de principios penales que contiene el Código Sustantivo en comento, dan certeza jurídica a toda persona de que sólo se podrá sancionar a alguien si se comprueba que efectivamente ha cometido un delito establecido en la ley como tal.

2.3. CLASIFICACIÓN DE LOS DELITOS QUE HACE EL CÓDIGO PENAL PARA EL DISTRITO FEDERAL.

Así como hay varios conceptos y definiciones del delito, los autores se han dado a la tarea de clasificar estas figuras antijurídicas. El hecho de clasificar algo implica una tarea difícil y que obedece esencialmente a objetivos didácticos determinados. Para efectos de esta investigación, hablaremos brevemente sobre la clasificación que hace el Código Penal vigente para el Distrito Federal.

Como lo hemos señalado con antelación, el Código Penal para el Distrito Federal establece nuevos delitos de acuerdo con algunos reclamos de la sociedad del Distrito Federal, aunque en esencia conserva los lineamientos de los Códigos Penales anteriores.

El Código Penal para el Distrito Federal contiene la siguiente clasificación de delitos en el Libro Segundo, Parte Especial:

1) Delitos contra la vida y la integridad corporal: homicidio, lesiones, ayuda o inducción al suicidio y aborto.
2) Procreación asistida, inseminación artificial y manipulación genética.
3) Delitos de peligro para la vida o la salud de las personas: omisión de auxilio o de cuidado y peligro de contagio.
4) Delitos contra la libertad personal: Privación de la libertad personal; privación de la libertad con fines sexuales; secuestro; desaparición forzada de personas; tráfico de menores y retención y sustracción de menores o incapaces.

5) Delitos contra la libertad y la seguridad sexuales y el normal desarrollo psicosexual: Violación, abuso sexual; hostigamiento sexual; estupro; incesto.

6) Delitos contra la moral pública: Corrupción de menores e incapaces; pornografía infantil; lenocinio.

7) Delitos contra la seguridad de la subsistencia familiar.

8) Delitos contra la integridad familiar: violencia familiar.

9) Delitos contra la filiación y la institución del matrimonio: estado civil y bigamia.

10) Delitos contra la dignidad de las personas: Discriminación.

11) Delitos contra las normas de inhumación y exhumación y contra el respeto a los cadáveres o restos humanos: inhumación, exhumación y respeto a los cadáveres o restos humanos.

12) Delitos contra la paz, la seguridad de las personas y la inviolabilidad del domicilio: amenazas; allanamiento de morada, despacho, oficina o establecimiento mercantil.

13) Delitos contra la intimidad personal y la inviolabilidad del secreto: violación de la intimidad personal y revelación de secretos.

14) Delitos contra el honor: difamación y calumnia.

15) Delitos contra el patrimonio: Robo; abuso de confianza; fraude; administración fraudulenta; insolvencia fraudulenta en perjuicio de acreedores; extorsión; despojo; daño en propiedad; encubrimiento por receptación.

16) Operaciones con recursos de procedencia ilícita: operaciones con recursos de procedencia ilícita.

17) Delitos contra la seguridad colectiva: Portación, fabricación e importación de objetos aptos para agredir y pandilla, asociación delictuosa y delincuencia organizada.

18) Delitos contra el servicio público cometidos por servidores públicos: Disposiciones generales sobre servidores públicos; ejercicio indebido y abandono del servicio público; abuso de autoridad y uso ilegal de la fuerza pública; coalición de servidores públicos; uso indebido de atribuciones y facultades; intimidación; negación del servicio público; tráfico de influencia;

cohecho; peculado; concusión; enriquecimiento ilícito; usurpación de funciones públicas.

19) Delitos cometidos contra el servicio público cometidos por particulares: Promoción de conductas ilícitas; cohecho y distracción de recursos públicos; desobediencia y resistencia de particulares; oposición a que se ejecute alguna obra o trabajo públicos; quebrantamiento de sellos; ultrajes a la autoridad; ejercicio indebido del propio derecho.

20) Delitos en contra del adecuado desarrollo de la justicia cometidos por servidores públicos: Denegación o retardo de justicia y prevaricación; delitos en el ámbito de la procuración de justicia; tortura; delitos cometidos en le ámbito de la administración de justicia; omisión de informes médico forenses; delitos cometidos en el ámbito de la ejecución penal; evasión de presos.

21) Delitos contra la procuración y administración de justicia cometidos por particulares: Fraude procesal; falsedad ante autoridades; variación del nombre o domicilio; simulación de pruebas; delitos de abogados, patronos y litigantes; encubrimiento por favorecimiento.

22) Delitos cometidos en el ejercicio de la profesión: responsabilidad profesional y técnica: Usurpación de profesión; abandono, negación y práctica indebida del servio médico; responsabilidad de directores, encargados, administradores o empleados de centros de salud y agencias funerarias, por requerimiento arbitrario de la contraprestación; suministro de medicinas nocivas o inapropiadas.

23) Delitos contra la seguridad y el normal funcionamiento de las vías de comunicación y de los medios de transporte: Ataques a las vías de comunicación y los medios de transporte: delitos contra la seguridad del tránsito de vehículos; violación de correspondencia y violación de la comunicación privada.

24) Delitos contra la fe pública: Falsificación de títulos al portador y documentos de crédito público; falsificación de sellos, marcas, llaves cuños, troqueles, contraseñas y otros; elaboración o alteración y uso indebido de placas,

engomados y documentos de identificación de vehículos automotores; falsificación o alteración y uso indebido de documentos.
25) Delitos ambientales: Alteración y daños al ambiente.
26) Delitos contra la democracia electoral: Delitos electorales.
27) Delitos contra la seguridad de las instituciones del Distrito Federal: rebelión: Ataques a la paz pública, sabotaje; motín y sedición.
Se puede apreciar de la simple lectura que hay nuevos delitos que obedecen a las actuales condiciones y reclamos de la sociedad del Distrito Federal, puesto que uno de los objetivos del Código Penal vigente es precisamente contar con una normatividad sustantiva más moderna y adecuada a los tiempos de cambio de esta ciudad que garantice la seguridad de las personas en su vida, su libertad, papeles y posesiones.

Es de observarse que la clasificación que establece el Código Penal para el Distrito Federal obedece al criterio del bien jurídico tutelado, es decir, el derecho jurídicamente protegido de las personas, por ejemplo, en el delito de homicidio es la vida; en el de secuestro es la libertad deambulatoria de las mismas, en los delitos patrimoniales es la propiedad o posesión de bienes muebles o inmuebles, etc.

2.4. SU ESTRUCTURA.

Algunos autores se han dado a la tarea de clasificar estas figuras antijurídicas. El hecho de clasificar algo implica una tarea difícil y que obedece esencialmente a objetivos didácticos determinados. Para efectos de nuestra investigación, hablaremos brevemente sobre este aparatado.

Primeramente hablaremos de las clasificaciones que hace la doctrina penal. El autor argentino Francisco Torrejón clasifica los delitos en:

A) "Delitos contra las personas (homicidio y lesiones).

B) Delitos contra la honestidad y el honor.

C) Delitos contra la libertad (amenazas, etc.).

D) Delitos contra la propiedad (robo).

E) Delitos contra el Estado y la comunidad (delitos contra la seguridad pública, el orden público, contra la seguridad de la nación, contra los poderes públicos y el orden constitucional, la administración pública, contra la fe pública, etc.

F) Delitos contra el estado civil.

G) Según su requisito de procedencia: denuncia o querella".[26]

Otras clasificaciones de los delitos nos indican que hay delitos de comisión o acción, en los que se prohíbe llevar a cabo una conducta, por ejemplo: *matar, violar, robar, privar de la vida*, etc. hay también delitos de omisión, en los que la ley ordena una conducta determinada y el agente no la realiza. El autor César augusto Osorio y Nieto apunta que: *"De acuerdo con este criterio los delitos pueden ser de acción y de omisión. La acción es el movimiento corporal, la actividad, la conducta activa, con la cual se viola la ley prohibitiva, por ejemplo, el homicidio, el robo, la violación, etc".*[27] En cuanto a la omisión, el autor la define así: *"…es el no hacer, la actitud pasiva; por lo tanto, en los delitos de omisión encontramos ausencia, abstención de conducta activa".*[28] En los delitos de omisión podemos ubicar dos clases, los de simple omisión y los de comisión por omisión. Los primeros son aquellos en los que el agente se abstiene de realizar una conducta jurídicamente ordenada por la norma penal, como sucede en los delitos de omisión de auxilio. También se les conoce como delitos de omisión propia. En los delitos de comisión por omisión u omisión impropia, el agente decide no actuar para efecto de que se produzca el

[26] Vid. www.cels.org.ar/estadisticascom. 19 de junio de 2010, a las 19:34 horas.
[27] OSORIO Y NIETO, César Augusto. Síntesis de Derecho Penal. Parte General. 2ª edición, México, 1998, p. 47.
[28] Idem.

resultado delictivo, como sucede en el caso de quien debe cuidar de un enferme y el sujeto activo resuelve no proporcionarle los medicamentos prescritos a fin de causarle la muerte.

Atendiendo al resultado que producen, los delitos son formales y materiales. “A los primeros se les denomina también de simple actividad o de acción y a los segundos delitos de resultado. Los delitos formales son aquellos en los que se agota el tipo penal en con el actuar o movimiento corporal del agente y no es necesario que se produzca un resultado externo. En los delitos materiales, para su integración, se requiere la producción de un resultado objetivo o material, como en el homicidio, el robo y otros más”.[29]

En relación con el daño que se causa a la víctima o, al bien jurídico, los delitos pueden ser de lesión y de peligro. *“Los primeros causan daños directos y efectivos en los intereses jurídicamente protegidos por la norma violada. Los segundos, no causan daño a los intereses, pero sí los ponen en peligro, como el abandono de personas o la omisión de auxilio”.*[30]

Por su duración, los delitos pueden ser instantáneos, continuos o continuados. El Código Penal vigente en su artículo 17º dice:

> ***ARTÍCULO*** *17 (Delito instantáneo, continuo y continuado). El delito, atendiendo a su momento de consumación, puede ser:*
> *I. Instantáneo: cuando la consumación se agota en el mismo momento en que se han realizado todos los elementos de la descripción legal;*
> *II. Permanente o continuo: cuando se viola el mismo precepto legal, y la consumación se prolonga en el tiempo; y*

[29] Idem.
[30] Ibid. p. 48.

III. Continuado: cuando con unidad de propósito delictivo, pluralidad de conductas e identidad de sujeto pasivo, se concretan los elementos de un mismo tipo penal".

De conformidad con lo anterior, el tiempo en el que el agente activo actúa determina el tipo de delito de que se trata.

De acuerdo a la culpabilidad, los delitos pueden ser dolosos y culposos. Recordemos que la preterintencionalidad ya no existe en el Código Penal para el Distrito Federal.

De acuerdo a su estructura o composición, los delitos se clasifican en simples y complejos. *"Son simples aquellos en los cuales la lesión jurídica es única, como el homicidio. Son complejos aquello en los cuales el tipo consta de dos infracciones, cuya fusión da nacimiento a una figura delictiva nueva, superior en gravedad como el robo en casa habitación".*[31]

De acuerdo al número de actos integrantes de la acción típica, los delitos pueden ser unisubsistentes y plurisubsistentes. *"Los primeros se forman por un solo acto, mientras que los segundos constan de varios actos".*[32]

De acuerdo al número de sujetos que participan, pueden ser unisubjetivos y plurisubjetivos. *"Los primeros son aquellos en los que sólo participa una persona, mientras que en los segundos participan varias personas".*[33]

De acuerdo a la materia, los delitos pueden ser federales, comunes, militares y políticos (los cuales siguen siendo materia de polémicas doctrinales).

[31] Ibid. p. 49.
[32] Idem.
[33] Ibid. p. 50.

2.5. LOS NUEVOS TIPOS PENALES QUE ESTABLECE.

Una de las principales características del Código Penal para el Distrito Federal es que incorpora nuevas descripciones legales de delitos, los cuales obedecen a una ratio legis y social que resultaba ya insoslayable e impostergable.

Por mucho tiempo, la sociedad del Distrito Federal ha reclamado que se sancionara de manera más efectiva y con penas más duras ciertas conductas que han lesionado seriamente a la misma, como el secuestro y su variante el secuestro expres. De esta manera, si bien, el Código Penal para el Distrito Federal está basado en su homólogo anterior de 1931, también lo es que incorpora nuevos tipos penales que de acuerdo a las opiniones de la sociedad civil eran necesarios. Así, en el Libro segundo que contiene los delitos y sus penas, se incorporaron delitos interesantes por su alcance y contenidos, tales como el de simulación de pruebas, el de discriminación, turismo sexual, entre otros, cuya incorporación constituye un gran paso contra la lucha contra la delincuencia la cual se ha diversificado notablemente. Consideramos un poco contradictoriamente que el hecho de sancionar penalmente una conducta u omisión, es decir, convertirla en delito, no es propiamente la solución más adecuada, lo que parece ser la política del Gobierno del Distrito Federal, no obstante ello, la inserción de los nuevos delitos en el Código Penal merece el derecho de la duda, es decir, que se requiere de algunos años para poder determinar si la medida legislativa fue adecuada o no. De esta suerte, será la historia la que premie al Gobierno del Distrito Federal o le reclame sobre la incorporación de tales delitos. En caso de que los mismos no resulten viables en la práctica, estarán condenados indudablemente a convertirse en letra muerta, como ha sucedido en la mayoría de los Códigos Penales anteriores.

2.6. LA AUSENCIA DE TIPOS PENALES EN MATERIA DE VIRUS INFORMÁTICOS EN SU MODALIDAD DE CREACIÓN Y PROPAGACIÓN.

De la lectura de los diferentes delitos y sus respectivos numerales que contiene el Código Penal vigente para el Distrito Federal, se puede observar que no hay ninguno que se refiera a los informáticos, y mucho menos, a los virus informáticos en específico, tema esencial de esta investigación. Esta omisión legislativa resulta francamente incomprensible, ya que los delitos que se cometen a través de la informática, por ejemplo, mediante el uso de la red, causan daños patrimoniales que pueden ser incuantificables y que incluso, pueden poner en peligro la seguridad de la nación y del mundo. Por ejemplo, hace dos años, la página de Internet de la Presidencia de la República estaba infectada por un virus que no permitía su funcionamiento normal, lo que significa que fue relativamente fácil que un “hacker” o persona dedicada a usar la red para fines ilícitos entrara a la página de la Presidencia de la República y propagara un virus que inutilizó por algunas horas el funcionamiento de la misma.

La omisión mencionada por parte del Legislativo del Distrito Federal se debe a la falta de conocimiento de la informática en general y de la jurídica en particular, lo que significa que los diputados no están actualizados en cuanto a los principales adelantos en este importante campo, hecho que bajo ninguna manera se puede justificar, toda vez que la época en que se vive la globalización implica que haya más y mejores conocimientos de los principales adelantos tecnológicos.

Con esto se quiere decir, con todo respeto que la mayoría de nuestros legisladores, al menos del Distrito Federal, se han quedado rezagados en materia de informática, no así, en otras entidades como el Estado de Sinaloa

que ya cuenta con un apartado especial dedicado a los delitos informáticos en el artículo 217 del Código Penal, el cual constituye un excelente inicio y precedente para que los demás Estados de la República actualicen su legislación sustantiva y adjetiva penal en materia de delitos informáticos. Dicho numeral establece de manera literal lo siguiente:

CAPÍTULO V
DELITO INFORMÁTICO
"ARTÍCULO 217. *Comete delito informático, la persona que dolosamente y sin derecho:*
I. Use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; 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 la 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".

Es innegable el valor que posee este numeral ya que constituye un paso legislativo importante en materia de los delitos informáticos, por lo que no dudamos que en algún tiempo pueda ser el modelo para que muchas otras entidades de la Federación resuelvan incorporarlo en sus leyes sustantivas penales.

2.7. EL CÓDIGO PENAL DE 1931 Y LOS DELITOS INFORMÁTICOS.

El Código Penal anterior para el Distrito Federal fue publicado en el diario Oficial de la Federación en fecha viernes 14 de agosto de 1931. Cabe decir que su aplicación era dual, es decir, que fungía tanto para el distrito Federal como para toda la República en materia de fuero federal.

Este Código que fue abrogado por el actual, estaba dividido en dos Libros, el primero que se refería a la parte dogmática y el Libro segundo, que versa sobre los delitos en particular.

De la lectura de los delitos que integran el anterior Código Penal para el Distrito Federal no se observa que haya contado con algún tipo de regulación jurídica de los delitos informáticos. Los únicos tipos penales que podemos comparar con el tema que se expone son los siguientes:

> *Artículo 210.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto".*
>
> *"Artículo 211.-La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial".*

"Artículo 211-bis.- A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Estos tres artículos hablan del delito de revelación de secretos, sin embargo, no hacen mención del uso de recursos informáticos, ni de los daños causados a través de ese medio.

El mismo Código contenía en sus artículos del 367 al 381 el delito de robo; del 382 al 385, el delito de abuso de confianza y del 386 al 389, al delito de fraude. El delito de daño en propiedad ajena se tutelaba en los artículos 397 a 399. Estos delitos son clasificados como ilícitos contra las personas en su patrimonio y tampoco hacen alusión a la utilización de medios informáticos para su comisión.

El artículo 400-bis habla del delito de operaciones con recursos de procedencia ilícita, en el que tampoco se habla de la utilización de medios informáticos.

Por lo anterior, podemos afirmar categóricamente que el Código Penal de 1931 no regulaba los delitos informáticos de manera alguna. Resulta incomprensible que no se haya visto influenciado por el Código Penal de Sinaloa en su artículo 217, ya trascrito.

Este artículo resulta, por demás, novedoso y visionario, ya que regula y sanciona de manera penal, la utilización de los sistemas de datos, computadoras o cualquier parte de ellas, con el propósito de diseñar, ejecutar o para alterar un esquema o artificio, es decir programas o la información existente en los equipos de cómputo de una o varias personas físicas o morales, con la finalidad de causar un daño o de defraudar, para obtener dinero, bienes o información ajena.

El Código Penal anterior e incluso el actual debieron importar este tipo penal e incorporarlo, ya que la creación y propagación de virus informáticos constituyen un verdadero problema de alcance mundial que puede ocasionar daños en el patrimonio de una persona de grandes magnitudes, ya que toda la información financiera se encuentre guardada y soportada en los equipos de cómputo y generalmente se hacen operaciones millonarias a través de Internet. A lo anterior hay que agregar que es muy común que las personas suelan hacer compras a través de Internet, utilizando un tarjeta de crédito internacional para pagar dichas compras, la cual puede ser utilizada ilegalmente por un hacker y despojar de los fondos a su titular, gracias a los virus informáticos, es decir, programas especializados que tienen por objetivo permitir a su creador monitorear permanentemente los movimientos e información que intercambia el sujeto pasivo, por lo que resulta fácil tener acceso a los números de tarjetas de crédito ya así, realizar diversas compras en la red. Pasarán algunos días antes de que el titular se de cuenta de que su tarjeta fue utilizada en la red y que se hicieron compras sin su autorización. Recordemos que Internet es una gran red de redes que no se encuentra todavía regulada ni internacional ni nacionalmente, por lo que es fácil que se cometan varios delitos informáticos.

Finalmente, se puede agregar que el Código Penal para el Distrito Federal siguió el modelo del Código de 1931 en materia de delitos informáticos, sin realizar regulación jurídica alguna, dejando una enorme laguna jurídica en materia de los delitos que se cometen utilizando los recursos informáticos.

Creemos que esta laguna jurídica debe llenarse a la brevedad, ya que los delitos informáticos son un mal de nuestro tiempo y si no los detenemos legislativamente, podrán cobrar magnitudes insospechadas.

2.8. EL CÓDIGO PENAL FEDERAL Y LOS DELITOS INFORMÁTICOS.

El actual Código Penal Federal es también el Código Penal de 1931 para el Distrito Federal, por lo cual, fungía simultáneamente para el fuero local y para el fuero federal. Con la abrogación de ese Código para el Distrito Federal, se convirtió en ley única en materia penal sustantiva federal.

Es importante señalar que este Código contiene en su Libro Segundo, Título Noveno, capítulo Segundo el delito de acceso ilícito a sistemas y equipos de informática en sus artículos 211-bis-1 al 211-bis-7, con lo que a diferencia de los Códigos Penales (el anterior) y el Nuevo, sí contiene una regulación de los delitos informáticos en los siguientes términos:
(D.O.F. 17 DE MAYO DE 1999).

> *Artículo 211-bis-1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.*
>
> *Artículo 211-bis-2. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.*
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún*

mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa

Artículo 211-bis-3. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.
Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211-bis-4. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

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

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero,

indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa".

Artículo 211-bis-6. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211-bis-7. Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211-bis-8. Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

De la lectura de los artículos anteriores se observa que los mismos son tipos penales generales que aluden solamente a la destrucción o robo de información en los equipos de cómputo a través de mecanismos informáticos, los cuales no son aclarados; pero que se debe reconocer que es un gran paso en materia del combate a los delitos informáticos, pero, consideramos que por tratarse de conductas que constantemente evolucionan (casi diariamente sala a la luz un virus diferente), es menester que los legisladores profundicen más en el problema y creen tipos penales relativos a delitos informáticos, por ejemplo, la creación y propagación de virus informáticos, la destrucción o el robo de información a través de ellos, etc.

Por otra parte, es importante que los legisladores se modernicen en el ámbito de la informática, primeramente y después, en el campo basto de los delitos mencionados, para efecto de que la legislación tanto federal como local cuente con tipos penales más específicos o exactos y que logren sancionar esta clase de conductas que ya no son producto de la fantasía o de la ciencia ficción, sino

que son una realidad producto de la gran evolución tecnológica que estamos viviendo y que sin duda, habrá de incrementarse en los próximos años.

Cabe mencionar que en otros países, ya existen desde hace algunos años, leyes que combaten los delitos informáticos, por lo que nos aventajan considerablemente en el tratamiento del tema que nos ocupa.

CAPÍTULO 3.
NECESIDAD DE ADICIONAR UN TIPO PENAL EN EL CÓDIGO PENAL DEL DISTRITO FEDERAL EN MATERIA DE CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICOS.

3.1. CONCEPTO DE DELITO.

En términos generales, el ser humano debe respetar las normas jurídicas elaboradas y que garantizan la paz y armonía social. Si el sujeto obligado al cumplimiento de las mismas no lo hace cabalmente, será objeto de una sanción de acuerdo a la naturaleza de la norma jurídica que haya incumplido, esto es, si se incumple una norma civil, la consecuencia jurídica será diferente a la que corresponde si se trata de una norma penal.

Aunque el derecho, como sistema normativo prevea que se sancionará a quienes cometan conductas consideradas como delitos, con penas diversas, siendo la más ejemplificativa la de cárcel, lo cierto es que la incidencia delictiva en México ha aumentado en las últimas décadas.

Por otra parte, desde hace siglos, los autores o juristas se han dado a la tarea de analizar o estudiar al delito, como una figura prohibida y que causa variados daños a la víctima u ofendido y a la sociedad misma.

El delito ha sido objeto de muchas opiniones doctrinales que tratan de explicarlo y razonarlo, sin embargo, se trata de una figura que se ha

transformado rápidamente a la par que el hombre lo ha hecho. El delito ha merecido un tratamiento diverso a través de los años. Se han elaborado teorías y doctrinas sobre su naturaleza y esencia, sin embargo, no se ha podido llegar a un punto de acuerdo entre los autores, ni siquiera en cuanto a un concepto o definición que sea universalmente válida.

Es innegable que el delito en la actualidad no es igual al delito de hace diez o veinte años; algunos bienes jurídicos tutelados han cambiado, mientras que otros son relativamente nuevos; además, el modus operandi también ha cambiado gracias a los adelantos tecnológicos.

Esta conducta u omisión, que el Estado sigue tratando de reprimir, castigar y prevenir mediante nuevas y más duras penas. Por ejemplo, hoy existen más figuras delictivas, debido a la necesidad de tipificar y sancionar conductas que han causado daños patrimoniales o morales a los sujetos pasivos e inclusive a la sociedad misma.

Gramaticalmente, el término “delito”, viene del latín: *delictum, delinquo, delinquere*, que significa desviarse, resbalar, abandono de una ley.

Roberto Reynoso Dávila citando a Carrara señala sobre el orígen del vocablo: *“Cometer una falta, y crimen, del griego cerno, iudio en latín, que a pesar de ser en su origen término que significa las acciones menos reprensibles, llegan finalmente a designar los más graves delitos.*
Elemento es aquello que concurre para la formación de algo complejo, como las letras que forman una palabra, los átomos que forman una molécula, los cuerpos simples que se combinan para formar una sal, el género próximo y la diferencia específica de toda definición esencial, o el acto humano y sus

calificativas de antijuricidad y culpabilidad que integran el delito y en materia de cualquiera de los cuales desaparece tal delito".[34]

Para el autor Eduardo Massari: *"…el delito no es éste, ni aquél, ni el otro elemento; está en el conjunto de todos sus presupuestos, de todos sus elementos constitutivos, de todas sus condiciones; está antes que en la inmanencia, en la confluencia de todos ellos".*[35]

Roberto Reynoso Dávila cita en su obra a los siguientes doctrinarios:
Pellegrino Rossi dice: *"Delito es la infracción de un deber exigible en daño de la sociedad o de los individuos".*
Reinhart Frank: *"El delito es la violación de un derecho fundado sobre la ley moral".*
Gian Domenico Romagnosi: *"El delito es le acto de una persona libre e inteligente, perjudicial a los demás e injusto".*
Rafael Garófalo fue más allá y habló del "delito natural" diciendo que éste es: *"… la violación de los sentimientos altruistas de piedad y de probidad en la medida media indispensable para la adaptación del individuo a la sociedad".*
Enrico Ferri dice: *"…los delitos son las acciones punibles determinadas por móviles individuales y antisociales que perturban las condiciones de vida y contravienen la moralidad media de un pueblo en un tiempo y lugar determinado".*[36]

Fernando Castellanos Tena, autoridad en la materia, retoma al autor italiano Carrara quien dice del delito: *"… es la infracción de la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo moralmente imputable y*

[34] REYNOSO DÁVILA, Roberto. Teoría General del Delito. Editorial Porrúa, 3ª edición, México, 1998, p. 13.
[35] Citado por CREUS, Carlos. Derecho Penal. Parte General. Editorial Astrea, Buenos Aires, 1988, p. 26.
[36] REYNOSO DÁVILA, Roberto. Op. Cit. pp. 17 y 18.

políticamente dañoso".[30] Posteriormente cita a Edmundo Mezger quien dice del delito que: *"… es una acción punible; esto es el conjunto de los presupuestos de la pena".*[37]

De lo expuesto por los autores obtenemos que el delito es un elemento toral para el Derecho Penal y que ha sido estudiado por la doctrina desde hace mucho tiempo, por lo que no existe a la fecha una definición que sea universalmente aceptada, dado que el delito es una figura que se transforma. Sin embargo, podemos decir que se trata de un acto u omisión que contraviene las leyes penales sustantivas y que causa un daño al sujeto pasivo y lesiona moralmente la sociedad, por lo que es castigado seriamente de acuerdo sea el bien jurídico lesionado y el daño causado.

3.2. LOS DELITOS INFORMÁTICOS:

En países, como los Estados Unidos, España, Alemania o Argentina existen ya desde hace algunos años los llamados "delitos informáticos o delitos cibernéticos", los cuales no deben ser vistos como una fantasía o el producto de Internet, sino como una nueva realidad que amenaza a todos países inmersos en la globalización y México no es la excepción, ya que el uso de computadoras, se ha extendido rápidamente a todos los círculos del país. Así, amas de casa, estudiantes, profesores, profesionistas, servidores públicos, deportistas, etc., dependen totalmente del uso de las computadoras y de los programas más comunes.

En México existen conductas que pueden ser ubicadas como delitos informáticos desde hace muchos años, sin embargo, el tratamiento que se ha

[30] CASTELLANOS TENA, Fernando. Lineamientos Elementales de Derecho Penal. Editorial Porrúa, 43a edición, México, 2002, pp. 127 y 128.
[37] Idem.

dado a tales ilícitos es actualmente incipiente, como lo hemos visto con los artículos 211-bis1 al 211-bis-8 del Código Penal Federal, así como el artículo 217 del Código Penal para el Estado de Sinaloa, a pesar que se trata de conductas que pueden causar serios daños en el patrimonio de los sujetos pasivos. Esto significa que estamos ante la presencia de un nuevo tipo de delincuencia llamada de “cuello blanco”, que persigue causar daño a los equipos de cómputo ajenos, interviniendo en sus contenidos o información, destruyéndola, robándola e inclusive, llevado a cabo actos de transferencia de fondos de una cuenta a otra de manera ilegal.

El ritmo vertiginoso que ha marcado la globalización, aunado a los sistemas neo liberales han beneficiado la creación y propagación de los delitos informáticos, los cuales, sin embargo, requieren de excelentes y amplios conocimientos en materia computacional o informática, por lo que no cualquiera puede llevarlos a cabo, como sí sucede con ilícitos como el robo, el fraude, el homicidio o la violación.

Los delitos informáticos son el resultado del avance en materia tecnológica y cultural al servicio del hombre, ya sea para bien o para causar un daño o perjuicio a los demás.

3.3.1. CONCEPTO.

Antes de proceder a dar algunos conceptos de los delitos informáticos es conveniente partir de las siguientes premisas.

1. En la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación, y condiciona su desarrollo de la informática; tecnología

cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

2. La informática esta hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de Información para ejecutar tareas que en otros tiempos realizaban manualmente.

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporados a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee, un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en las que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados. En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos.

Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Este es el panorama de este nuevo fenómeno científico-tecnológico en las sociedades modernas. Por ello, ha llegado a sostenerse que la Informática es hoy una forma de Poder Social. Las facultades que el fenómeno pone a

disposición de Gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información".

Esta marcha de las aplicaciones de la informática no sólo tiene un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.

Debido a esta vinculación, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la OCDE a PARIS en MAY83, el término ***delitos relacionados con las computadoras*** se define como:

> *“Cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos. La amplitud de este concepto es ventajosa, puesto que permite el*

uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminológicos, económicos, preventivos o legales".[38]

La informatización se ha implantado en casi todos los países. Tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta, comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como "criminalidad informática".

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

[38] www.delitosinformaticos.com.es día 17 de enero de 2011 a las 13:36 horas.

La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos. A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

El estudio de los distintos métodos de destrucción y/o violación del hardware y el software es necesario en orden a determinar cuál será la dirección que deberá seguir la protección jurídica de los sistemas informáticos, ya que sólo conociendo el mecanismo de estos métodos es posible encontrar las similitudes y diferencias que existen entre ellos. De este modo se pueden conocer los problemas que es necesario soslayar para conseguir una protección jurídica eficaz sin caer en el casuismo.

En consecuencia, la legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, de acuerdo a las peculiaridades del objeto de protección, sea imprescindible.

La humanidad no esta frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen porque

ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

Otras opiniones sobre los delitos informáticos señalan lo siguiente:
"Dar un concepto sobre delitos informáticos no es labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de delitos en el sentido de acciones típicas; es decir, tipificadas o contempladas en textos jurídico-penales, se requiere que la expresión delitos informáticos esté consignada en los Códigos penales, lo cual en nuestro país al igual que en otros muchos, no ha sido aún objeto de tipificación sin embargo y habida cuenta de la urgente necesidad de esto, emplearemos dicha alusión; aunque para efectos de una conceptuación, hagamos el distingo pertinente entre lo típico y lo atípico.
De esta manera tenemos que, dependiendo del caso, los delitos informáticos son actitudes en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".[39]

El mismo autor cita a continuación a otro doctrinario quién dice de los delitos informáticos lo siguiente. Carlos Sarzana: *"Cualquier Comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo".* Nidia Callegari dice: *"aquél que se da con la ayuda de la informática o de las técnicas anexas".*[40]

Rafael Fernández Calvo señala: *"...la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo*

[39] TÉLLEZ VALDEZ, Julio. Op. Cit. pp. 103 y 104.
[40] www.tiny.uasnet.mx/prof/cin/der/silvis/INDEX.htm. Del 15 de julio del 2010 a las 20:45 horas.

utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1º de la Constitución Española".[41]

María de la Luz Lima Malvido apunta: *"...en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que en su sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel, ya sea como método, medio o fin".*[42]

Alejandro Bertelli dice sobre los delitos informáticos que: *"Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por La Ley, que se realiza en el entorno informático y está sancionado con una pena".*[43]

De acuerdo con las anteriores opiniones de los doctrinarios, podemos concluir que los delitos informáticos son aquellas conductas realizadas por personas con conocimientos profundos de computación y de programas computacionales y que tienen por objetivo causar daños patrimoniales a los equipos de otros usuarios o de obtener ingresos o ganancias ilícitas a través de operaciones fraudulentas, utilizando a la computadora y a sus programas como medio o instrumento de comisión.

[41] www.ctv.es/users/mqp/delitos.html. Del 15 de julio del 2010 a las 20:53.
[42] www.colosus.rhon.itam.mx/-sriosma. Del 15 de julio del 210 a las 21:03 horas.
[43] Idem.

3.3.2. CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS.

De acuerdo con el doctrinario Julio Téllez Valdez, los delitos informáticos presentan las siguientes características principales: - *"Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.*

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

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

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

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

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

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

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

- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley".[44]

Coincidimos con el autor en que los delitos informáticos son esencialmente calificados como "de cuello blanco", en relación con otros ilícitos que requieren de un nivel de preparación y de conocimientos técnicos como el fraude, puesto que la informática es una ciencia que necesita de mucho tiempo de estudio y

[44] TÉLLEZ VALDEZ, Julio. Op. Cit. Pp. 103 y 104.

de práctica para su adecuado manejo y dominio, por lo que no cualquier delincuente común y corriente puede cometer un delito informático.

3.3.3. OBJETO.

El objeto de los delitos informáticos es la salvaguarda de la información o bienes informáticos contenidos en el disco duro de los equipos e inclusive el que conste en memorias USB adicionales o correos electrónicos.

3.3.4. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS.

El autor Julio Téllez Valdez clasifica a los delitos informáticos en atención a dos criterios, ya sea como instrumentos o medio y como fin u objetivo.

En el primer caso o supuesto, están englobadas las conductas que utilizan las computadoras como un medio o símbolo en la comisión de ilícitos, como la falsificación de documentos con el uso del scanner. Ejemplo de esto es la falsificación de títulos y cédulas profesionales, tarjetas de crédito, actas de nacimiento, matrimonio y defunción; la variación de los activos y los pasivos en la situación financiera de una empresa, la planeación o simulación de los delitos convencionales como el homicidio, el robo, el fraude, el terrorismo, etc; el robo de tiempo de la computadora; la lectura, sustracción o copiado de información confidencial; la modificación de datos tanto de entrada como de salida; el aprovechamiento indebido o la violación de un código para entrar a un sistema introduciendo instrucciones inapropiadas; la variación del destino de cantidades de dinero hacia una cuenta bancaria apócrifa o técnica del salami; el uso no autorizado de programas de computo; la introducción de instrucciones que provocan interrupciones en la lógica interna de los programas

para obtener beneficios económicos o de otro tipo; la alteración en el funcionamiento de los sistemas a través de virus informáticos, etc.

1. "Como instrumento o medio.

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)

b. Variación de los activos y pasivos en la situación contable de las empresas.

c. Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)

d. Lectura, sustracción o copiado de información confidencial.

e. Modificación de datos tanto en la entrada como en la salida.

f. Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

g. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

h. Uso no autorizado de programas de computo.

i. Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.

j. Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

k. Obtención de información residual impresa en papel luego de la ejecución de trabajos.

l. Acceso a áreas informatizadas en forma no autorizada.

m. Intervención en las líneas de comunicación de datos o teleproceso". [45]

[45] PADIILA SEGURA, José Antonio. Op. Cit. p. 56.

En el segundo caso, el autor se refiere a las conductas criminógenas que se dirigen contra las computadoras, sus accesorios o programas, como la programación de instrucciones para producir un bloqueo total en el sistema de uno o varios ordenadores o computadoras; la destrucción de programas por cualquier método; daño a la memoria de la computadora; daño físico a la computadora o a sus accesorios; sabotaje político o terrorismo en el que se pueda destruir o apoderarse de los centros neurálgicos computarizados con fines de chantaje, etc.

2. Como fin o como objeto.

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

a. "Programación de instrucciones que producen un bloqueo total al sistema.
b. Destrucción de programas por cualquier método.
c. Daño a la memoria.
d. Atentado físico contra la máquina o sus accesorios.
e. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
f. Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.)". [46]

Por otra parte, existen diversos tipos de delitos que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

[46] Ibid. p. 57.

- **"Acceso no autorizado:** Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
- **Destrucción de datos:** Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- **Infracción al copyright de bases de datos:** Uso no autorizado de información almacenada en una base de datos.
- **Interceptación de e-mail:** : Lectura de un mensaje electrónico ajeno.
- **Estafas electrónicas:** A través de compras realizadas haciendo uso de la red.
- **Transferencias de fondos:** Engaños en la realización de este tipo de transacciones.

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

- **Espionaje:** Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- **Terrorismo:** Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
- **Narcotráfico:** Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- **Otros delitos:** Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés". [49]

La Organización de las Naciones Unidas ha realizado la siguiente clasificación de los delitos informáticos:

[49] Ibid. p. 58.

a) Fraudes cometidos mediante la utilización o manipulación de las computadoras.

b) Los daños o modificaciones de programas o datos computarizados.

En España se conoce un verdadero catálogo de delitos informáticos , por lo que hay webs que se dedican a referir casos delictivos de esa magnitud:

Sofisticación de los fraudes en la Red

Detenido un hombre en Valencia por estafas de lotería (con imágenes)

Estafa de envío de fax a números de tarificación especial 803

Lotería de navidad como gancho para estafa

Uso fraudulento de tarjetas bancarias

Nueva ciberestafa relacionada con una loteíia

Estadísticas de estafas y delitos en España durante 2002

Principales fraudes denunciados por consumidores estadounidenses y consejos para su prevención

Detenciones por manipulación de tragaperras, cuya información se obtenía de Internet

Delincuentes utilizaban sofisticados métodos para duplicar tarjetas de crédito

Datos sobre estafas en subastas en Internet

Fraudes y estafas utilizando servicios de contactos a través de 906 y mensajes a móviles SMS

Sitio fraudulento simula ser un servicio de eBay para recoger tarjetas de crédito

Denuncia contra un cliente por piratear la señal de televisión de pago

Solución al timo del 906

Tarifa plana, recibo de infarto

Estafa en reventa de billetes de avión comprados por Internet

El uso del spam para realizar fraudes

Los nueve fraudes y abusos más frecuentes a través de las líneas 906

Detectados robos en Uruguay a través de contactos por Internet

Reino Unido multa a empresa española por fraude en conexiones a Internet para acceder a contenido sexual

Descubierto fraude utilizando banco en Internet falso

Desarticulada red internacional de estafadores por chat y correo electrónico
Desarticulada red de fraude de tonos y lógos para móviles que utilizaba un 906
Alerta sobre el posible fraude en registro de dominios con terminación '.eu'
Estafa por venta de propiedad por Internet en el Amazonas
Utilización de mensajes SMS de forma fraudulenta
La Policía detiene a tres nigerianos por supuesta estafa a un magnate saudí a través de Internet
Fraude los correos sobre inversiones en Nigeria: ejemplos de las correos electrónicos remetidos (inglés)
El fraude de los correos sobre inversiones en Nigeria
Fraude en sitios de contactos con mujeres Rusas
La firma electónica y los delitos en la Red (Venezuela)
Resumen de la ley de Delitos Informáticos en Venezuela
Todo lo que quiso saber de los 906 pero nunca se atrevió a preguntar
Estafas en teletrabajo: Reflexiones sobre la búsqueda de teletrabajo
Delito de estafa informática (art. 248.2 c.p.español)
Estafas en la red, a la caza del ciberincauto
Regalo de WebCam a cambio de un correo
Manuales de hackeo de cuentas de correo hotmail
El fraude de las subastas online, líder de los cibercrímenes.
Los 10 fraudes más comunes.
Sexo Gratis.
Reclamaciones de pedidos.[50]

3.3.4. CONSECUENCIAS DE LOS DELITOS INFORMÁTICOS.

Los delitos informáticos producen esencialmente daños de tipo patrimonial en los equipos de cómputo de los usuarios, pudiendo afectar tanto el software

[50] www.delitosinformáticos.com.-estafas. 11 de marzo del 2011, a las 21:34 horas.

(programas e información o bienes informacionales que gozan de derecho a la privacidad) como el hardware, es decir, el equipo de computo mismo.

De esta forma, un delito informático va dirigido esencialmente contra los equipos de cómputo de otras personas, lo cual se puede lograr a partir de la creación de un virus informático el cual se propaga a través de Internet o de un disquette de un tercio. Sin embargo, es la red de redes o Internet la vía más idónea para hacer llegar a los demás equipos de usuarios un virus que pueda causar serios daños a los mismos, siempre y cuando estén conectados a la red.

Son los hackers o personas que se dedican a hacer o crear virus informáticos los que deciden o determinan la misión del virus, la cual puede ser variada: destruir información o equipo, sustraerla, etc.

Los delitos informáticos pueden también dirigirse hacia el patrimonio financiero de una persona, por ejemplo, los famosos fraudes bancarios en los que el sujeto activo mediante el conocimiento y uso de programas computacionales y de Internet, puede hacer una transferencia de los fondos de una persona en otra cuenta recientemente abierta, con lo que el daño patrimonial causado al pasivo será definitivo y las ganancias pueden ser millonarias.

En casos menos dramáticos, cuando un usuario utiliza su tarjeta de crédito para comprar algún bien o servicio en Internet, su crédito puede ser robado y utilizado por hackers que están al acecho y que inmediatamente captan el número de tarjeta de crédito y sustraen todo el crédito, a pesar de que los bancos estén en constante modernización y sofisticación de las tarjetas de crédito que ya son blindadas o con chip, pero, el riesgo está siempre latente en el red.

3.3.5. LOS DELITOS INFORMÁTICOS EN OTROS PAÍSES.

Los delitos informáticos ya son parte de las conductas prohibidas penalmente por gran parte de los países en el mundo. Así, naciones como los Estados Unidos, Canadá, Alemania, Francia, España, Argentina, etc., ya constituyen motivo de causas penales, lo que indica un notable adelanto en materia jurídica, al igual que lo hay en el campo informático. Estos países llevan la delantera en esos campos y hay que reconocer que en México estamos en una etapa de desarrollo y lejos de los demás Estados.

El tema de los delitos informáticos constituye una preocupación de la Organización de las Naciones Unidas, lo que indica que los demás países deben incorporarse rápidamente al adelanto en el combate contra los mismos. Incluso, en esos países ya hay una policía cibernética, misma que existe afortunadamente en México.

Alemania.

Este país sancionó en 1986 la **Ley contra la Criminalidad Económica**, que contempla los siguientes delitos:

- Espionaje de datos.
- Estafa informática.
- Alteración de datos.
- Sabotaje informático.

Austria.

La **Ley de reforma del Código Penal**, sancionada el 22DIC87, en el artículo 148, 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 comenten este hecho utilizando su profesión de especialistas en sistemas.

Gran Bretaña.

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

Holanda.

El 1º de Marzo de 1993 entró en vigencia la **Ley de Delitos Informáticos**, en la cual se penaliza el hacking, el preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.

Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

Francia.

En enero de 1988, este país dictó la **Ley relativa al fraude informático**, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

Asimismo, esta ley establece en su artículo 462-3 una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos. Por su parte el artículo 462-4 también incluye en su tipo penal una conducta 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.

También la legislación francesa establece un tipo doloso y pena el mero acceso, agravando la pena cuando resultare la supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

Por último, esta ley en su artículo 462-2, sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la pena correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

España.

En el ***Nuevo Código Penal de España***, el art. 263 establece que el que causare daños en propiedad ajena. En tanto, el artículo 264-2) establece que se aplicará la pena de prisión de uno a tres años y multa... a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los

datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

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

Chile.

Chile fue el primer país latinoamericano en sancionar una **Ley contra delitos informáticos**, la cual entró en vigencia el 7 de junio de 1993.

Según esta ley, la destrucción o inutilización de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus. Esta ley prevé en el Art. 1º, el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento. En tanto, el Art. 3º tipifica la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

3.3.6. LA CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICOS COMO DELITO:

A continuación se hablará sobre la creación y propagación de virus informáticos como delito, en el entendido que en la legislación penal del Distrito Federal no hay tipos al respecto.

3.3.5.1. SUS EFECTOS.

Los efectos principales de los virus informáticos como delitos a través de su propagación son causar daño que esencialmente es de índole patrimonial, afectando ya sea a sus equipos de cómputo, su información guardada en archivos o carpetas o inclusive, sus inversiones o dinero guardado en alguna cuenta bancaria, por lo que este tipo de delitos constituyen una seria amenaza para quienes dependen de las computadoras y realizan operaciones a través de Internet.

En este sentido, los efectos de la creación y propagación de virus informáticos se asemejan a delitos como el robo de información o el daño en propiedad privada.

3.3.5.2. EL BIEN JURÍDICO TUTELADO.

En todos los delitos existe un bien jurídico tutelado, es decir, el bien que se trata de proteger jurídicamente al crear el tipo penal y establecerle una sanción. En el caso de los delitos patrimoniales como los que se han citado: robo, daño en propiedad privada e inclusive los delitos informáticos en su modalidad de

creación y propagación de virus, el bien jurídicamente tutelado o protegido es el patrimonio del sujeto pasivo, entendiendo por tal, desde el equipo de cómputo, como su software o programas, así como su información contenida en archivos o carpetas, la cual puede ser muy valiosa en dinero o estimativamente para el sujeto.

3.3.5.3. LA CALIDAD DE LOS SUJETOS QUE INTERVIENEN.

En el delito que se propone, de creación y propagación de virus informáticos, el sujeto activo requiere de un perfil específico, ya que debe tratarse de una persona que cuente con amplios conocimientos en informática, debe manejar los principales programas computacionales y saber cómo hacer un virus informático y establecer sus funciones destructivas o de espionaje para que se introduzca en el equipo de otros usuarios y lleve a cabo su misión, por ejemplo, un hacker es el perfil de una persona que puede crear y propagar fácilmente un virus informático, el cual no es otra cosa que un programa que se crea y se hace llegar a través de Internet y una vez que el usuario y destinatario lo abre, el programa mismo se ejecuta y consuma sus funciones ante la indiferencia e ignorancia del sujeto pasivo.

Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "ingresa" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.
Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos (Nros. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada. Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", los estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las

empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros".

Asimismo, este criminólogo estadounidense dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Es difícil elaborar estadísticas sobre ambos tipos de delitos. Sin embargo, la cifra es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables" otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

En lo que se refiere a delitos informáticos, Olivier HANCE en su libro "Leyes y Negocios en Internet", considera tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:

a. "Acceso no autorizado: Es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente pero decide voluntariamente mantenerse conectado.

b. Actos dañinos o circulación de material dañino: Una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento casi siempre se es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).

c. Interceptación no autorizada: En este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él".[51]

Las leyes estadounidense y canadiense, lo mismo que los sistemas legales de la mayoría de los países europeos, han tipificado y penalizado estos tres tipos de comportamiento ilícito cometidos a través de las computadoras.

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

[51] Cfr. HANCE, Oliver. Leyes y Negocios en Internet. Editorial McGraw Hill, México, 1997, p. 67.

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

a. "Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.
b. Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
c. Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
d. No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
e. Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
f. Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional". [52]

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente aún en países como la Argentina, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

[52] Ibid. p. 68.

De esta forma, la sociedad se enfrenta a un nuevo tipo de delincuentes, más capacitados y altamente sofisticados, por lo que también suelen ser denominados como de cuello blanco.

En cuanto al sujeto pasivo, puede ser cualquier persona, basta con que cuente con un equipo de cómputo y tenga un correo electrónico, el cual es obtenido fácilmente en empresas como **hotmail**, **esmas**, **altavista, yahoo,** etc. El sujeto pasivo regularmente revisa su correo electrónico, pudiendo ser un estudiante, ama de casa, profesionista, autoridad, etc., por lo que se puede decir que sólo se requiere que cuente con el equipo de cómputo y tenga además de su correo electrónico, conocimientos básicos sobre computación y los principales programas. Adicionalmente puede suceder que el sujeto posea una o varias cuentas bancarias y realice constantemente transacciones financieras en Internet, para qué puede ser una víctima potencial de este tipo de delitos.

Puede ser sujeto pasivo una autoridad estatal o dependencia de éste, ya que las mismas dependen ciento por ciento de Internet, por lo que de crearse y propagarse un virus informático, se puede afectar a intereses y actividades estatales.

3.3.5.4. EL RESULTADO.

El delito de creación y propagación de virus informáticos es un ilícito penal de resultado eminentemente material, ya que el sujeto pasivo puede resultar dañado en su equipo, en el hardware o en el software, donde se incluye su información guardada en archivos o carpetas, pudiendo ser este el principal daño al abrir un correo que contiene un virus informático. Es por esto que resulta muy aconsejable que el sujeto realice varias copias soportadas de su información para efecto de que puede salvarla de destrucción parcial o total en caso de abrir un e mail que contiene un virus informático.

3.3.5.5. LA FORMA DE COMISIÓN.

Se trata de un delito de acción en cuanto a su forma comisiva, por lo que para llevarse a cabo se requiere de una preparación previa del delito, esto es, que se trata de un ilícito que esencialmente admite el dolo como forma, aunque puede ser que una persona cree un virus informático, sin el ánimo de causar daño a los demás, como sucedió en su origen, cuando estos programas fueron creados como una forma de juego, sin embargo, por accidente es posible que lo haga llegar a otros usuarios vía Internet o como una simple broma. Hay que recordar que los virus informáticos nacieron como accidentes y como bromas producto de la ociosidad, por lo que esencialmente son dolosos, pero, pueden admitir el grado de culpa.

3.3.5.6. LA TENTATIVA.

En el caso del delito en cita, la tentativa tiene lugar ya que una persona puede haber diseñado uno o varios virus informáticos e intentar enviarlos a varios usuarios de la red con el ánimo de causar daño, pero, los destinatarios de correos electrónicos al ver que se trata de un mensaje desconocido y dado que saben de la existencia constante de virus informáticos, decide no abrirlo y eliminarlo, impidiendo que otros correos de ese destinatario lleguen a su computadora, con lo que el delito sólo queda en grado de tentativa, ya que uno de los mecanismos para prevenir ser infectado por un virus es ser muy cuidadoso con los e-mails que se reciben. Se aconseja que si se reciben correos de desconocidos, lo mejor es nunca abrirlos y eliminarlos inmediatamente. Puede resultar abrirlos en un café Internet para evitar causar daño al equipo propio.

Por otra parte, es común que se cuente con sistemas antivirus que inmediatamente se actualizan y empiezan a trabajar, anulando la gran mayoría de los virus. Estos programas son tan exactos que logran advertir al usuario que hay un virus en el equipo y que ya se desactivó, pudiendo restablecer el archivo o sanearlo.

Es posible que el autor de un virus informático cree un poderoso programa para la destrucción parcial o total de la información de los receptores del mismo, sin embargo, al enviarlos, el servidor que utiliza no trabaja y por ello, los receptores del virus no podrán abrir un correo que no recibieron y con ello, salvarán su equipo. En este caso estamos ante un caso del delito en su grado de tentativa acabada, ya que por causas ajenas, el autor del ilícito no logró el resultado.

3.4. LA CREACIÓN Y ADICIÓN DE UN TIPO PENAL EN EL DISTRITO FEDERAL QUE REGULE Y SANCIONE LA CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICOS.

Es sabido que la sociedad avanza a pasos agigantados, por lo que sus necesidades en materia legislativa también, hecho que resulta más notorio ante el aumento de población en el Distrito Federal y con ello, de los problemas principales que ello trae consigo, como la falta de empleos bien remunerados, la carestía y las crisis económicas, las constantes devaluaciones, el bajo poder adquisitivo de la moneda e indudablemente, el aumento exagerado de la criminalidad que es el principal problema al que se enfrentan diariamente los habitantes de esta ciudad.

3.4.1. SU JUSTIFICACIÓN LEGAL.

En consecuencia, ante el aumento exagerado de conductas delictivas de cuello blanco en las que se utiliza a las computadoras como medio comisivo, y el enorme hueco legal o laguna jurídica, es más que necesario que el Distrito Federal cuente con una regulación jurídica adecuada en materia de delitos informáticos.

Es innegable que la informática ha ido cobrando mucha importancia en la vida diaria de las personas en el mundo y en el caso de México, esta importancia hoy es más palpable que nunca. Gran parte de las actividades en el país giran en relación a las computadoras y los programas informáticos. Sin embargo, todo avance tecnológico representa también la posibilidad de que sea utilizado como un instrumento para bien o para mal. En el último de los casos, los delitos informáticos son una realidad que amenaza a gran parte de la sociedad que utiliza los equipos de cómputo, puesto que al acceder a Internet o abrir un correo electrónico se corre el riesgo de abrir también un virus y con ello, permitir que un programa cause daño al equipo o a la información guardada.

En muchos países, los delitos informáticos constituyen objeto de tutela jurídica, por lo que ya cuentan con una regulación adecuada que busca combatir y sancionar este tipo de ilícitos producto de la modernidad. Nuevamente citamos el caso de nuestro país donde un avance significativo es el caso del Código Penal de Sinaloa que ya contempla este tipo de delitos, así como el Código Penal Federal en sus numerales invocados, sin embargo, es menester que el Distrito Federal cuente con una regulación adecuada a la par de las necesidades de la sociedad en materia de delitos informáticos.

3.4.2. SU JUSTIFICACIÓN SOCIAL.

De acuerdo con lo expuesto, consideramos que es necesario que se reforme a efecto de adicionar el Código Penal para el Distrito Federal para que contenga un tipo penal que sancione la creación y propagación de virus informáticos, toda vez que el uso de los equipos de informática se encuentran en serio riesgo al entrar a la red, ya que fácilmente pueden recibir uno o varios correos electrónicos que contengan virus, mismos que pueden causar serios daños en sus equipos o en su información.

Es necesario que todo usuario de la red tenga la certeza de que al entrar a Internet no será objeto del ataque de un virus que causará daños casi irreparables al mismo.

Por otra parte, se podrá garantizar también que los cafés Internet que tanto han proliferado en el Distrito Federal, cuenten con mayor regulación y vigilancia ya que son el lugar adecuado para crear y propagar los virus informáticos e incluso, para realizar otro tipo de delitos como los fraudes electrónicos o incluso, la pornografía y prostitución infantil.

3.4.3. SU JUSTIFICACIÓN INFORMÁTICA.

Desde el punto de vista informático, el hecho de que el equipo de cómputo comience a dar problemas que concluyan en la pérdida o destrucción parcial o total tanto de la información como del equipo mismo, constituye necesariamente un serio perjuicio para el usuario, puesto que tendrá que acudir a un profesional especializado para que revise el equipo y trate de salvar la información si no tiene el respaldo adecuado. El técnico tendrá que formatear el

equipo y analizar todos sus contenidos, causando una erogación considerable que incluso puede requerir que se tenga que adquirir una nueva máquina.

Los daños que puede causar un virus informáticos son considerables y pueden traducirse en un serio detrimento económico y de información privada del usuario.

En el momento en que el Distrito Federal cuente con una regulación adecuada en materia de delitos informáticos, se podrá brindar la seguridad necesaria a los mismos usuarios de equipos de cómputo, muchos de los cuales han invertido gran parte de su capital para comprar su equipo y guardar su información, por lo que es menester que la ley penal respalde su inversión y su información.

3.4.4. PROYECTO DE REDACCIÓN DEL TIPO PENAL EN MATERIA DE CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICOS.

Derivado del desarrollo del presente trabajo de investigación documental, proponemos que la impostergable creación de un nuevo tipo penal para el Código Penal para el Distrito Federal en materia de creación y propagación de virus informáticos, por todas y cada una de las razones ya explicadas.

Así, el texto que proponemos estaría contenido en el Título Décimo Tercero: Delitos contra la Intimidad Personal y la Inviolabilidad del Secreto, adicionándole un Capítulo, que sería el Tercero que se denominaría: delitos informáticos. El texto del delito de creación y propagación de virus informáticos quedaría contenido en dos artículos adicionales que serían el 213-bis y el 213-ter, en los siguientes términos:

“Artículo 213-bis.-Se entiende por delito informático la utilización de equipos de cómputo para ocasionar ya sea culposa o dolosamente, daños o perjuicios a otros equipos, para la obtención de un beneficio o lucro o simplemente para dañarlos en su software o hardware”.

“Artículo 213-ter.- Comete el delito de creación y propagación de virus informático el que a sabiendas invente un programa computacional destinado a llegar a otros equipos para causarles un daño total o parcial y hacerlo llegar a otras personas por medio de Internet. A quien cometa el delito de creación y propagación de virus informáticos se le aplicará una pena de uno a cinco años de prisión y una multa de mil a cinco mil días de salario mínimo general vigente para el Distrito Federal”.

Estamos convencidos que la incorporación de este tipo penal podrá cubrir las necesidades jurídicas en materia de informática jurídica en el Distrito Federal. Se propone una pena de uno a cinco años de prisión y una multa de mil a cinco mil días, por tratarse de un ilícito que afecta el patrimonio y la información del usuario de un equipo de cómputo.

Adicionalmente, consideramos importante que se adopten otras medidas legales suplementarias como es la revisión constante de las páginas o webs que se visitan en los Cafés Internet que se han proliferado en el Distrito Federal y cuyos propietarios no tienen el menor cuidado de verificar la información o actividades que los clientes llevan a cabo, por lo que pueden crear varios virus informáticos afectando con su propagación a millones de usuarios de la red. Es por esto que estimamos que sería oportuno que la Policía Federal Preventiva en su sección de policía informática visitara constantemente estos lugares para efecto de verificar que no se creen virus que puedan causar daño a otros.

Es también necesario que nuestra sociedad cuente con una verdadera cultura en materia informática, ya que si bien, muchos de nosotros estamos inmersos en este fenómeno, hay todavía, quienes no conocen las ventajas de las computadoras, por lo que debe fomentarse su estudio a todos niveles a efecto de hacer segura la navegación en la red.

CONCLUSIONES.

PRIMERA.- Conjuntamente al desarrollo y sofisticación que han observado las computadoras en los últimos diez años, los programas o *software* utilizado, también ha evolucionado notablemente, siendo Internet, uno de los más importantes en materia de comunicación e información.

SEGUNDA.- El dominio de la ciencia informática ha traído grandes ventajas para el ser humano en todos los campos, sin embargo, también se le ha dado un uso negativo o perjudicial, a través de la creación de programas cuya finalidad es causar un daño a los usuarios de los equipos computacionales o de la red. Se trata de personas con amplios conocimientos de esta disciplina que se han convertido en delincuentes de cuello blanco, capaces de robar una cuantiosa cuenta bancaria a través de una simple transacción a través de Internet en cuestión de minutos, o bien, quienes pueden sustraer o dañar información de otras personas mediante la creación y propagación de los virus informáticos. A este tipo de personas que realizan estas actividades se les conoce como: *hackers* y curiosamente, al encontrarlos son comúnmente contratados para trabajar en firmas poderosas como Microsoft u otras compañías, en lugar de seguirles alguna causa penal.

TERCERA.- Un delito informático es toda conducta culposa o dolosa realizada por personas que cuentan con amplios conocimientos de informática y que utilizan como instrumento delictivo a la computadora y a uno o varios programas computacionales, tendiente a causar un daño o perjuicio en el equipo de uno o varios usuarios, por lo que se trata de un delito eminentemente patrimonial, ya que la información que se posee en un ordenador constituye parte del patrimonio de una persona.

CUARTA.- Existen varios tipos de delitos informáticos como son: El robo o *hackeo* de información a través un programa; el fraude informático (transferencia de una cuenta bancaria a otra en cuestión de minutos); la pornografía y prostitución infantil; la apología de un delito como el terrorismo, la sedición, el motín; y la creación y propagación de un virus informático tendiente a causar daño en la información o en el equipo de cómputo de una o varias personas, ya sea para la obtención de un beneficio económico, como revancha o simplemente por la ociosidad.

QUINTA.- Los virus informáticos son programas de cómputo creados con la finalidad de causar daño en los archivos, programas o en el equipo o hardware del usuario por personas que cuentan con amplios conocimientos computacionales. En sus orígenes, los virus informáticos se crearon como una forma de diversión, pero, con el paso del tiempo, se han convertido en una amenaza para los usuarios de Internet.

SEXTA.- Los virus informáticos pueden multiplicarse rápidamente e incluso, pasar desapercibidos por el usuario, hasta el momento en que abra un archivo nuevo y permita que el virus se ejecute y logre su cometido perjudicando la información, los programas o el equipo del usuario.

SÉPTIMA.- Los virus informáticos producen una merma o daño en el patrimonio del usuario, mismo que puede ascender a millones de dólares, si se trata de empresas o de Gobiernos, los cuales manejan información financiera, hacen transferencias o compras a través de Internet.

OCTAVA.- Existen varios tipos de virus informáticos como son: Las bombas, los camaleones, los reproductores, los gusanos y los caballos de Troya, entre otros. Cada uno de estos virus tiene una misión específica, pero la característica común

es la de causar un daño en la información o archivos, programas o en el equipo de los usuarios.

NOVENA.- Los virus informáticos se han convertido en pocos años en verdaderas amenazas contra la información y los equipos de los usuarios que navegan en la red, siendo ésta la principal vía de propagación de dichos programas perjudiciales.

DÉCIMA.- Casi diariamente se crea y propaga un virus informático en el mundo, por lo que podemos decir que estamos ante una especie de terrorismo informático que atenta contra la seguridad de la información y de las operaciones que se hacen en la red.

DÉCIMA PRIMERA.- Ante este clima de incertidumbre informática, la mayoría de los Estados han elaborado una legislación propia que pueda sancionar a los creadores y propagadores de virus informáticos como son los Estados Unidos, Alemania, Francia, Inglaterra, Argentina, Chile, Canadá, etc.

DÉCIMA SEGUNDA.- En México, desgraciadamente no se ha dimensionado el problema de los virus informáticos, por lo que apenas en el Código Penal Federal en sus artículos 211-bis del 1 al 7 se establecen algunos lineamientos al respecto. Mención aparta merece el Código Penal del Estado de Sinaloa cuya legislación penal incluye un tipo penal adecuado a la creación y propagación de virus informáticos en su artículo 217, una verdadera innovación que debe ser seguida por otras entidades de la Federación, mientras que el Código Penal para el Distrito Federal es omiso en cuanto a este tema importante.

DÉCIMA TERCERA.- Los delitos informáticos y especialmente la creación y propagación de virus informáticos deben ser considerados también como delitos de cuello blanco, una nueva forma de delincuencia, por lo que México requiere de

un marco legal más adecuado en este campo, producto de la globalización y de los avances tecnológicos.

DÉCIMA CUARTA.- Ante la falta de una marco jurídico adecuado en el Código Penal para el Distrito Federal, se estima conveniente que se haga una reforma y adición que llene la laguna jurídica existente, por tanto, se propone la redacción de dos nuevos artículos insertos en el Título Decimotercero Delitos contra la Intimidad Personal y la Inviolabilidad del Secreto, adicionándole un Capítulo, el Tercero que se denominaría: Delitos informáticos, conteniendo dos artículos cuya redacción puede ser la siguiente:

"Artículo 213-bis.-Se entiende por delito informático la utilización de equipos de cómputo para ocasionar ya sea culposa o dolosamente, daños o perjuicios a otros equipos, para la obtención de un beneficio o lucro o simplemente para dañarlos en su software o hardware".

"Artículo 213-ter.- Comete el delito de creación y propagación de virus informático el que a sabiendas invente un programa computacional destinado a llegar a otros equipos para causarles un daño total o parcial y hacerlo llegar a otras personas por medio de Internet. A quien cometa el delito de creación y propagación de virus informáticos se le aplicará una pena de uno a cinco años de prisión y una multa de mil a cinco mil días de salario mínimo general vigente para el Distrito Federal".

Creemos que estos tipos penales podrán cubrir las necesidades jurídicas en materia de informática jurídica en el Distrito Federal. Proponemos una pena de uno a cinco años de prisión y una multa de mil a cinco mil días, por tratarse de un ilícito que afecta el patrimonio y la información del usuario de un equipo de cómputo.

Por otro lado, se considera también importante que se tomen otras medidas legales suplementarias como es la revisión constante de las páginas o webs que se visitan en los Cafés Internet que se han proliferado y cuyos propietarios no tienen el menor cuidado de verificar la información o actividades que los clientes trabajan, pudiendo fácilmente crear un virus informático, por lo que se piensa que sería oportuno que la Policía Federal Preventiva en su sección de policía informática visitara constantemente estos lugares para efecto de verificar que no se creen virus que puedan causar daño a otros.

Es también necesario que la sociedad cuente con una verdadera cultura en materia informática, ya que si bien, muchos están ya inmersos en este fenómeno, hay todavía quienes no conocen las ventajas de las computadoras, por lo que debe fomentarse su estudio a todos niveles

BIBLIOGRAFÍA.

AMUCHATEGUI REQUENA, I. Griselda. Derecho Penal. Editorial Oxford, 2ª edición, México, 2004.

ARELLANO GARCÍA, Carlos. Métodos y Técnicas de la Investigación Jurídica. Editorial Porrúa, México, 1999.

AZÚA REYES, Sergio T. Metodología y Técnicas de la Investigación Jurídica. Editorial Porrúa, 2ª edición, México, 1998.

CASTELLANOS TENA, Fernando. Lineamientos Elementales de Derecho Penal. Editorial Porrúa, 43a edición, México, 2002.

CREUS, Carlos. Derecho Penal. Parte General. Editorial Astrea, Buenos Aires, 1988

GONZÁLEZ DE LA VEGA, Francisco. El Código Penal Comentado. Editorial Porrúa, 12ª edición, México, 1996.

GONZÁLEZ QUINTANILLA, José. Derecho Penal Mexicano. Editorial Porrúa, 4ª edición, México, 1997.

GONZÁLEZ VEGA, Rogelio. Informática General. Editorial Tecnológica Iberoamericana, 2ª edición, Madrid, 1998.

HANCE, Oliver. Leyes y Negocios en Internet. Editorial McGraw Hill, México, 1997.

JIMÉNEZ DE ASÚA, Luís. Lecciones de Derecho Penal. Editorial Pedagógica Iberoamericana, México, 1995.

LÓPEZ BETANCOURT, Eduardo. Introducción al Derecho Penal. Editorial Porrúa, 7ª edición, México, 1999.

MALO CAMACHO, Gustavo. Derecho Penal Mexicano. Editorial Porrúa, 2ª edición, México, 1998.

MENDEL, Lawrence. Historia de las Computadoras. Editorial Progreso, Barcelona, 1999.

MOTO SALAZAR, Efraín. Introducción al Estudio del Derecho. Editorial Porrúa, 40ª edición, México, 1994.

OSORIO Y NIETO, César Augusto. La Averiguación Previa. Editorial Porrúa, 9ª edición, México, 1998.

_____ Síntesis de Derecho Penal. Editorial Trillas, 3ª edición, México, 1990.

PADILLA SEGURA, José Antonio. Informática Jurídica. I.P.N. México, 1991.

PAVÓN VASCONCELOS, Francisco. Manual de Derecho Penal Mexicano. Editorial Porrúa, 14ª edición, México, 1999.

PORTE PETIT CANDAUDAP, Celestino. Apuntamientos de la Parte General de Derecho Penal I. Editorial Porrúa, 17ª edición, México, 1998.

REYNOSO DÁVILA, Roberto. Teoría General del Delito. Editorial Porrúa, 3ª edición, México, 1998.

ROJAS AMANDI, Víctor Manuel. El uso de Internet en el Derecho. Editorial Oxford, México, 1991.

TÉLLEZ VALDEZ, Julio. Derecho Informático. Editorial McGraw Hill, 2ª edición, México, 1996.

TORREJÓN, Francisco. Derecho Penal, tomo I.. Editorial Depalma, 2ª edición, Buenos Aires, 2001.

LEGISLACIÓN.

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. Editorial SISTA S.A. México, 2011.

CÓDIGO PENAL FEDERAL. Editorial SISTA S.A. México, 2011.

CÓDIGO FEDERAL DE PROCEDIMIENTOS PENALES. Editorial SISTA S.A. México, 2011.

CÓDIGO PENAL PARA EL DISTRITO FEDERAL. Editorial SISTA S.A. México, 2011.

CÓDIGO DE PROCEDIMIENTOS PENALES PARA EL DISTRITO FEDERAL. Editorial SISTA S.A. México, 2011.

CÓDIGO PENAL PARA EL ESTADO DE SONORA. Editorial SISTA S.A., México, 2011.

CÓDIGO DE PROCEDIMIENTOS PENALES PARA EL ESTADO DE SINALOA. Editorial SISTA S.A., México, 2011.