UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES "ARAGÓN"

"NECESIDAD DE CONTAR CON UN TIPO PENAL EN EL DISTRITO FEDERAL RELATIVO A LA CREACIÓN Y PROPAGACIÓN DE LOS VIRUS INFORMÁTICOS".

T E S I S

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN DERECHO

P R E S E N T A :

EDGAR ISRAEL RAMÍREZ ÁLVAREZ

ASESOR:
LIC. ENRIQUE M. CABRERA CORTES.

NEZAHUALCOYOTL, EDO. DE MÉXICO **2006**

A DIOS:

GRACIAS A DIOS POR HABERME DADO LA VIDA Y POR QUE YO SE QUE EL ES EL CULPABLE DE HABERME PUESTO EN ESTE CAMINO TAN MARAVILLOSO QUE ES EL DERECHO

A MI MADRE:

GRACIAS MAMA PRINCIPALMENTE POR HABERME DADO LA VIDA, POR EDUCARME DE LA MANERA QUE LO HICISTE Y POR GUIARME TODA MI VIDA, POR ENSEÑARME EL VALOR DE LA VIDA Y DE LA HONRADEZ Y SOBRE TODO POR SER MI MADRE, YA QUE TU ERES LO MAS PRECIADO QUE DIOS ME PUDO DAR.

TU SABES, QUE ESTE GRAN LOGRO TE LO DEBO EN GRAN PARTE A TI Y QUE TAMBIÉN ES TUYO.

¡GRACIAS MAMÁ! POR ESTAR SIEMPRE CONMIGO YA SEA EN LAS BUENAS COMO EN LAS MALAS, TE QUIERO MUCHO MAMY.

A MI PADRE:

GRACIAS PAPA POR TODO LO QUE ME DISTE Y ME SIGUES DANDO, YA QUE TU ME GUIASTE EN MIS PRIMEROS PASOS TODA VEZ QUE TU ME ENSEÑASTE A LEER, SUMAR, RESTAR Y TANTAS COSAS QUE AHORA EN VERDAD NO SE COMO PAGARTE, PERO CREME QUE CON EL TIEMPO LO VOY A IR ASIENDO.

MUCHAS GRACIAS POR TU APOYO, COMPRENSIÓN CARIÑO Y SOBRE TODO, POR SER MI PAPA.

TU AL IGUAL QUE MI MADRE SIENTETE ORGULLOSO DE ESTE GRAN LOGRO, POR QUE SABEMOS QUE ESTE GRAN SUEÑO TE LO DEBO EN GRAN PARTE A TI.

GRACIAS PAPA POR ESTAR SIEMPRE CONMIGO Y POR APOYARME EN TODAS MIS DECISIONES, AUNQUE YO SE QUE A VECES SON MUY MALAS, PERO SE QUE VAN A CAMBIAR MUY PRONTO. TE QUIERO MUCHO PAPI, POR FAVOR NUNCA LO OLVIDES.

A MIS HERMANOS
ALFONSO, JOSE JUAN Y
PAMELA:

QUIERO DARLES LAS GRACIAS POR TENERLOS A USTEDES Y POR HABER COMPARTIDO TANTAS COSAS A SU LADO, POR BRINDARME TODO SU APOYO Y POR ALENTARME Y OTRAS VECES REGAÑARME PARA PODER ALCANZAR MIS METAS, POR CONFIAR EN MI, CON EL SIMPLE HECHO DE TENERLOS A MI LADO.

QUIERO DEDICARLES ESTE GRAN LOGRO, Y DARLES LAS GRACIAS POR ESTAR SIEMPRE A MI LADO Y POR SUS CONSEJOS, QUE ME HAN SERVIDO DE MUCHO. LOS QUIERO MUCHO.

BESOS MIL.

A MI UNIVERSIDAD:

QUIERO DARLE LAS GRACIAS CON TODA MI ALMA A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, POR HABERME ABIERTO LAS PUERTAS EN EL AÑO DE 1994 Y POR HABERME COBIJADO DURANTE MI DESARROLLO ACADÉMICO Y EN ESPECIAL QUIERO AGRADECER A LA ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES "ARAGÓN" HOY FACULTAD DE ESTUDIOS SUPERIORES "ARAGÓN" EL HABERME PERMITIDO CONCLUIR MIS ESTUDIOS Y HABERME HECHO LA PERSONA QUE HOY SOY.

A MIS PROFESORES:

GRACIAS POR HABERME COMPARTIDO UN POCO DE SU GRAN SABIDURÍA Y EXPERIENCIA, YA QUE SIN ESTA NO HUBIERA PODIDO LLEGAR A DONDE ESTOY AHORA.

GRACIAS POR TODO EL TIEMPO QUE ME DEDICARON, EN VERDAD LO APRECIO MUCHO.

A MIS AMIGOS:

GRACIAS A TODOS USTEDES QUE HAN ESTADO A LO LARGO DE MI VIDA, POR HABERME APOYADO, ALENTADO Y SOBRE TODO POR HABERME BRINDADO SU AMISTAD, TANTO EN LOS MOMENTOS DE DICHA COMO EN LOS MOMENTOS DIFÍCILES, POR HABERME EXPLICADO COSAS QUE NO ENTENDÍ Y QUE CON SUS PALABRAS SE HICIERON MAS FÁCILES DE DIGERIR Y SOBRE TODO QUIERO DARLES LAS GRACIAS POR QUE SIGUEN CONMIGO.

GRACIAS: ALICIA, MIGUEL ÁNGEL, ISRAEL, ALLAN, OMAR, RODRIGO, TANIA, MARTHA GABRIELA, MARIANA, JESÚS, JESICA, ADRIANA, LUCIA, LAURA, MARIBEL, ADÁN, AÍDA, CARLOS, CITLALLY, EDWIN, ELIZABETH, IXBALANQUE, LILY, JOSÉ LUIS, MARGARITA, MIRIAM, NADIA, NOEMÍ, OLGA LIDIA, PAOLA, GABRIELA XOCHIQUETZAL, ERIC, HÉCTOR, JOSÉ RAMÓN, MANUEL, VÍCTOR, ROSS, SONIA, SUSANA, RAFAEL, ERIKA, JUANA, AURORA, ROGELIO, FERNANDO, JORGE, OMAR, HÉCTOR L., ALBERTO, ADRIÁN, NAYELLI, BERENICE, SANDRA, VANESA, Y A TODOS AQUELLOS QUE SE QUEDARON EN MIS PENSAMIENTOS.

Í n d i c e.

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 facilitada 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 casi diario se puede decir que se crea uno o varios tipos de virus con tareas 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, 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 es un país que apenas está creciendo en materia de informática, por lo que el hablar de virus en este campo puede resultar casi inadvertido en cuanto a sus serias consecuencias jurídico-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 Nuevo Código Sustantivo Penal para el Distrito Federal cuente con un tipo penal que regule y 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 Nuevo 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 ad hoc a las necesidades de la sociedad en materia de protección informática, por lo que esta investigación se justifica plenamente.

Nuestra investigación 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 Nuevo 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.

La metodología empleada para la elaboración de la presente investigación fueron los métodos: comparativo, inductivo-deductivo, jurídico y la técnica de investigación documental.

CAPÍTULO 1.
LOS VIRUS INFORMÁTICOS Y SU TRASCENDENCIA EN LA VIDA DIARIA.

1.1. CONCEPTO DE INFORMÁTICA.

En la actualidad, el término *informática* es muy conocido y usado por gran parte de los habitantes de este planeta. Sin embargo, hay que decir que encierra un conjunto de adelantos en materia de computadoras y programas que el término mismo no alcanza a describir, por lo que a continuación se procederá a explicarlo.

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]

Definitivamente 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

[2] Enciclopedia Encarta Microsoft 2004. Microsoft Corporation, 2004.
[3] Téllez Valdez, Julio. Derecho Informático. Editorial McGraw Hill, 2ª edición, México, 1996, p. 5.
[4] Padilla Segura, José Antonio. Op. Cit. P.

decir, el uso de las computadoras para la correcta toma de decisiones y la solución de problemas diarios.

Se puede 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.

1.2. LAS COMPUTADORAS EN LA VIDA DIARIA.

El llamado “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 tenía 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, la página y buscador de Internet “es más”, ha lanzado a la venta computadoras desde 2,500 pesos, mientras que TELMEX tiene varios planes de venta a plazos, con cargo al recibo telefónico mensual, incluyendo el servicio de Internet por una año.

Los gobiernos y la economía del mundo dependen mucho de sus redes de computadoras; las comunicaciones y transferencias de grandes sumas 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.

El caso de los Derechos de Autor también es muy importante, ya que a través de la red, 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, se debe considerar que el Internet sigue siendo una red anárquica, es decir, que no cuenta con una regulación jurídica ni 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, etc.

1.3. PARTES DE QUE CONSTA UNA COMPUTADORA:

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.

Todo lo que hace un ordenador digital se basa en una operación: la capacidad de determinar si un conmutador, o 'puerta', está abierto o cerrado. Es decir, el ordenador puede reconocer sólo dos estados en cualquiera de sus circuitos microscópicos: Abierto o cerrado, alta o baja tensión o en el caso de números, 0 o 1. Sin embargo, es la velocidad con la cual el ordenador realiza este acto tan sencillo lo que lo convierte en una maravilla de la tecnología moderna. Las velocidades del ordenador se miden en megahercios (millones de ciclos por segundo), aunque en la actualidad se alcanzan velocidades del orden de los gigahercios (miles de millones de ciclo por segundo). Un ordenador con una velocidad de reloj de 1 gigahercio (GHz), velocidad bastante representativa de un microordenador o microcomputadora, es capaz de ejecutar 1.000 millones de operaciones discretas por segundo, mientras que las supercomputadoras utilizadas en aplicaciones de investigación y de defensa alcanzan velocidades de billones de ciclos por segundo.[5]

La velocidad y la potencia de cálculo de los ordenadores digitales se incrementan aún más por la cantidad de datos manipulados durante cada ciclo. Si un ordenador verifica sólo un conmutador cada vez, dicho conmutador puede representar solamente dos comandos o números. Así, ON simbolizaría una operación o un número, mientras que OFF simbolizará otra u otro. Sin embargo, al verificar grupos de conmutadores enlazados como una sola unidad, el ordenador aumenta el número de operaciones que puede reconocer en cada ciclo. Por ejemplo, un ordenador que verifica dos conmutadores cada vez,

[5] González Vega, Rogelio. Informática General. Editorial Tecnológica Iberoamericana, 2ª edición, Madrid, 1998, p, 78.

puede representar cuatro números (del 0 al 3), o bien ejecutar en cada ciclo una de las cuatro operaciones, una para cada uno de los siguientes modelos de conmutador: OFF-OFF (0), OFF-ON (1), ON-OFF (2) u ON-ON (3). En general, los ordenadores de la década de 1970 eran capaces de verificar 8 conmutadores simultáneamente; es decir, podían verificar ocho dígitos binarios, de ahí el término bit de datos en cada ciclo. Un grupo de ocho bits se denomina byte y cada uno contiene 256 configuraciones posibles de ON y OFF (o 1 y 0). Cada configuración equivale a una instrucción, a una parte de una instrucción o a un determinado tipo de dato; estos últimos pueden ser un número, un carácter o un símbolo gráfico. Por ejemplo, la configuración 11010010 puede representar datos binarios, en este caso el número decimal 210 (ver Sistemas numéricos), o bien estar indicando al ordenador que compare los datos almacenados en estos conmutadores con los datos almacenados en determinada ubicación del chip de memoria. El desarrollo de procesadores capaces de manejar simultáneamente 16, 32 y 64 bits de datos permitió incrementar la velocidad de los ordenadores. La colección completa de configuraciones reconocibles, es decir, la lista total de operaciones que una computadora es capaz de procesar, se denomina conjunto, o repertorio, de instrucciones. Ambos factores, el número de bits simultáneos y el tamaño de los conjuntos de instrucciones, continúa incrementándose a medida que avanza el desarrollo de los ordenadores digitales modernos.[6]

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

1.3.1. EL HARDWARE.

El término *Hardware,* viene del inglés y se aplica al a parte de las computadoras que tienen que ver con la estructura de la misma, es decir, su apariencia física y todo lo que contiene. Es por ende el equipo utilizado para el

[6] Ibid. P. 79.

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').[7]

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

[7] Ibid. P. 80.

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.[8]

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.

[8] Ibid. P. 81.

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.

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.[9]

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

[9] Ibid. P. 82.

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 unas conexiones materiales que permitan a los componentes comunicarse entre sí e interaccionar. Un bus constituye un 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.

1.4. CONCEPTO DE VIRUS INFORMÁTICO.

El virus informático es un programa de ordenador que se reproduce a sí mismo e interfiere con el hardware de una computadora o con su sistema operativo (el software básico que controla la computadora). Los virus están diseñados para reproducirse y evitar su detección. Como cualquier otro programa informático, un virus debe ser ejecutado para que funcione: Es decir, el ordenador debe cargar el virus desde la memoria del ordenador y seguir sus instrucciones. Estas instrucciones se conocen como carga activa del virus. La carga activa puede trastornar o modificar archivos de datos, presentar un determinado mensaje o provocar fallos en el sistema operativo.

Un virus informático es antes que nada, un programa o código que suele ser complejo por lo general, aunque también puede ser simple.

El objetivo o finalidad de un virus informático es entrar en el sistema de la computadora, duplicarse y propagarse a todos y cada uno de los archivos que sea posible, sin que el usuario del equipo se pueda percatar, hasta que el virus haya cumplido su misión es que aquel se dará cuenta de la magnitud de los daños.

A manera de concepto de virus informático tenemos lo siguiente:

“Un virus 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 importantes 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".[10]

Los virus informáticos son programas generalmente destructivos, que se introducen en el ordenador (al leer un disco o acceder a una red informática) y pueden provocar pérdida de la información (programas y datos) almacenada en el disco duro. Existen programas antivirus que los reconocen y son capaces de "inmunizar" o eliminar el virus del ordenador. La continua aparición de nuevos tipos de virus hace necesario mantener en el ordenador la versión más actualizada posible del programa antivirus.

Así, el virus informático 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 estas.

El daño que puede ocasionar el virus es contra los archivos de información que se encuentran dentro de una o varias computadoras o contra la seguridad de los equipos que resulten infectados.

Un virus informático puede autoduplicarse muchas veces: Igualmente puede auto ajustarse durante algún tiempo en una o varias computadoras y permanecer en estado de latencia (dormido), hasta que el usuario abra el archivo, en cuyo preciso momento el virus saldrá e infectará los archivos existentes poco a poco, pudiendo dañarlos y hasta afectar la seguridad de la computadora misma.

[10] Revista: Vivir en Internet. Publicación mensual. Septiembre de 2001, México, p. 59.

Puede ser que el virus informático adquiera el tipo de un archivo normal que llega a través de un e mail, por lo que a primera vista parece inofensivo y se puede confundir al usuario el cual no se dará cuenta del tipo de archivo que está abriendo y liberando, ni mucho menos de sus terribles efectos devastadores para su información.

Falta decir que en su mayoría, los virus informáticos son programas que se crean y propagan en forma de archivos cuya tarea esencial es la de causar daños a los equipos de cómputo que reciben los mismos y los liberan. Los daños son, como ya se ha manifestado muy variables: Desde alentar el sistema del equipo, hasta la pérdida de archivo de información o inclusive, un daño serio en el disco duro, lo que propiciará que el equipo no funcione.

1.5. ANTECEDENTES DE LOS VIRUS INFORMÁTICOS.

En 1949, el matemático estadounidense de origen húngaro John von Neumann, en el Instituto de Estudios Avanzados de Princeton (Nueva Jersey), planteó la posibilidad teórica de que un programa informático se reprodujera. Esta teoría se comprobó experimentalmente en la década de 1950 en los Bell Laboratories, donde se desarrolló un juego llamado Core Wars en el que los jugadores creaban minúsculos programas informáticos que atacaban y borraban el sistema del oponente e intentaban propagarse a través de él. En 1983, el ingeniero eléctrico estadounidense Fred Cohen, que entonces era estudiante universitario, acuñó el término "virus" para describir un programa informático que se reproduce a sí mismo. En 1985 aparecieron los primeros caballos de Troya, disfrazados como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUKE-LA. Pronto les siguió un sinnúmero de virus cada vez más complejos. El virus llamado Brain apareció en 1986, y en 1987 se había extendido por todo el mundo. En 1988 aparecieron dos nuevos

virus: Stone, el primer virus de sector de arranque inicial, y el gusano de Internet, que cruzó Estados Unidos de un día para otro a través de una red informática. El virus Dark Avenger, el primer infector rápido, apareció en 1989, seguido por el primer virus polimórfico en 1990. En 1995 se creó el primer virus de lenguaje de macros, WinWord Concept.[11]

Actualmente el medio de propagación de virus más extendido es Internet, en concreto mediante archivos adjuntos al correo electrónico, que se activan una vez que se abre el mensaje o se ejecutan aplicaciones o se cargan documentos que lo acompañan.

El origen de los virus informáticos es reciente, se dice que, en la década de los sesentas los norteamericamnos Douglas Mallory, Victor Vysottsky y Robert Morris, crearon un juego al que denominaron “Core War”, el cual llegó a ser un pasatiempo muy divertido en los laboratorios Bell de la industria AT&T, como ya se expuso renglones arriba.

Core War era una batalla en la core o memoria de la computadora, donde dos jugadores escribían cada una un programa organismo, cuyo hábitat era la memoria del ordenador o computadora. Después de una señal, cada programa intentaba forzar al otro a efectuar una instrucción inválida. El primero que lo lograra, ganaba el juego.

Una vez terminado el juego, se borraba todo vestigio de la batalla de la memoria de la máquina.

Estos juegos habían sido prohibidos y sancionados por los ejecutivos de esa empresa, por señalarse que con ello se liberaba un organismo que quedaba suelto en el juego, por lo que el mismo podría llegar

[11] Mendel, Lawrence. Historia de las Computadoras. Editorial Progreso, Barcelona, 1999, p. 67.

hasta otras informaciones que serían aplicadas al día siguiente, lo cual produjo que el juego se realizara de forma clandestina.

Este juego permaneció casi desconocido por la gran mayoría, sin embargo, se dice que en el año de 1987, un periodista de los Estados Unidos llegó a perder la información de seis meses de trabajo por virtud a un virus que había adquirido. El periodista había introducido un disquete en el que se encontraba un número telefónico de una tienda de computación de Pakistán. El mensaje decía lo siguiente:

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

Estas personas habían creado un virus informático con la finalidad de vender las vacunas y hacer grandes negocios. Después de algunas investigaciones se pudo determinar que la tienda era "Brain Computer Services". Su giro era entre muchos otros, vender algunos programas informáticos de manera ilegal, que eran muy caros a un precio accesible: un dólar y medio, siendo los primeros casos de piratería de programas computacionales que a la postre serían un gran negocio como hoy lo vemos.

Durante las décadas de los sesentas y setentas, los consumidores potenciales eran los estudiantes de Estados Unidos.

A medida que se introducía el disco y se abría, se liberaba el virus e infectaba la computadora, hecho que se repitió muchas veces.

Hoy se sabe que los diseñadores de los virus eran: Amjad y Basit Farooq Alvi, de nacionalidad pakistaní.

Años más tarde, estas mismas personas crearon un virus que integraron a las copias de programas que vendían, por lo que cuando un extranjero adquiría una copia, también encontraba un virus que se liberaba

cuando se abría el programa. En Pakistán, los derechos de autor no constituyen un objeto de tutela jurídica, por lo que no era sancionado el delito de piratería intelectual.

Desde entonces, los virus informáticos se han venido utilizando como armas perfectas para causar daños inclusive a nivel mundial. Tal es el caso de virus famosos como el *"Anna Kournikova",* que incluía fotos de la famosa tenista rusa o el caso del virus *"I love you",* que también causó un colapso mundial.

Los virus informáticos son creados casi a diario, por lo que los usuarios de Internet deben ser muy cuidadosos al visitar lugares que no se conozcan y al abrir correos electrónicos desconocidos, ya que es probable que se encuentren incluidos algunos virus informáticos con resultados insospechados.

1.6. LA CREACIÓN DE LOS VIRUS INFORMÁTICOS.

Los virus informáticos se difunden cuando las instrucciones —o código ejecutable— que hacen funcionar los programas pasan de un ordenador a otro. Una vez que un virus está activado, puede reproducirse copiándose en discos flexibles, en el disco duro, en programas informáticos legítimos o a través de redes informáticas. Estas infecciones son mucho más frecuentes en los PC que en sistemas profesionales de grandes computadoras, porque los programas de los PC se intercambian fundamentalmente a través de discos flexibles o de redes informáticas no reguladas.

Los virus funcionan, se reproducen y liberan sus cargas activas sólo cuando se ejecutan. Por eso, si un ordenador está simplemente conectado a una red informática infectada o se limita a cargar un programa infectado, no se infectará necesariamente. Normalmente, un usuario no ejecuta

conscientemente un código informático potencialmente nocivo; sin embargo, los virus engañan frecuentemente al sistema operativo de la computadora o al usuario informático para que ejecute el programa viral.

Algunos virus tienen la capacidad de adherirse a programas legítimos. Esta adhesión puede producirse cuando se crea, abre o modifica el programa legítimo. Cuando se ejecuta dicho programa, ocurre lo mismo con el virus. Los virus también pueden residir en las partes del disco duro o flexible que cargan y ejecutan el sistema operativo cuando se arranca el ordenador, por lo que dichos virus se ejecutan automáticamente. En las redes informáticas, algunos virus se ocultan en el software que permite al usuario conectarse al sistema

Existen seis categorías de virus: Parásitos, del sector de arranque inicial, multipartitos, acompañantes, de vínculo y de fichero de datos. Los virus parásitos infectan ficheros ejecutables o programas de la computadora. No modifican el contenido del programa huésped, pero se adhieren al huésped de tal forma que el código del virus se ejecuta en primer lugar. Estos virus pueden ser de acción directa o residentes. Un virus de acción directa selecciona uno o más programas para infectar cada vez que se ejecuta. Un virus residente se oculta en la memoria del ordenador e infecta un programa determinado cuando se ejecuta dicho programa. Los virus del sector de arranque inicial residen en la primera parte del disco duro o flexible, conocida como sector de arranque inicial, y sustituyen los programas que almacenan información sobre el contenido del disco o los programas que arrancan el ordenador. Estos virus suelen difundirse mediante el intercambio físico de discos flexibles. Los virus multipartitos combinan las capacidades de los virus parásitos y de sector de arranque inicial, y pueden infectar tanto ficheros como sectores de arranque inicial.

Los virus acompañantes no modifican los ficheros, sino que crean un nuevo programa con el mismo nombre que un programa legítimo y engañan al sistema operativo para que lo ejecute. Los virus de vínculo modifican la forma en que el sistema operativo encuentra los programas, y lo engañan para que ejecute primero el virus y luego el programa deseado. Un virus de vínculo puede infectar todo un directorio (sección) de una computadora, y cualquier programa ejecutable al que se acceda en dicho directorio desencadena el virus. Otros virus infectan programas que contienen lenguajes de macros potentes (lenguajes de programación que permiten al usuario crear nuevas características y herramientas) que pueden abrir, manipular y cerrar ficheros de datos. Estos virus, llamados virus de ficheros de datos, están escritos en lenguajes de macros y se ejecutan automáticamente cuando se abre el programa legítimo. Son independientes de la máquina y del sistema operativo.

Cabe decir que los usuarios pueden prepararse frente a una infección viral creando regularmente copias de seguridad del software original legítimo y de los ficheros de datos, para poder recuperar el sistema informático en caso necesario. Puede copiarse en un disco flexible el software del sistema operativo y proteger el disco contra escritura, para que ningún virus pueda sobrescribir el disco. Las infecciones virales se pueden prevenir obteniendo los programas de fuentes legítimas, empleando una computadora en cuarentena para probar los nuevos programas y protegiendo contra escritura los discos flexibles siempre que sea posible.

Para detectar la presencia de un virus informático se pueden emplear varios tipos de programas antivíricos. Los programas de rastreo pueden reconocer las características del código informático de un virus y buscar estas características en los ficheros del ordenador. Como los nuevos virus tienen que ser analizados cuando aparecen, los programas de rastreo deben ser actualizados periódicamente para resultar eficaces. Algunos programas de

rastreo buscan características habituales de los programas virales; suelen ser menos fiables.

Los únicos programas que detectan todos los virus son los de comprobación de suma, que emplean cálculos matemáticos para comparar el estado de los programas ejecutables antes y después de ejecutarse. Si la suma de comprobación no cambia, el sistema no está infectado. Los programas de comprobación de suma, sin embargo, sólo pueden detectar una infección después de que se produzca.

Los programas de vigilancia detectan actividades potencialmente nocivas, como la sobre escritura de ficheros informáticos o el formateo del disco duro de la computadora. Los programas caparazones de integridad establecen capas por las que debe pasar cualquier orden de ejecución de un programa. Dentro del caparazón de integridad se efectúa automáticamente una comprobación de suma, y si se detectan programas infectados no se permite que se ejecuten.

Hay varios sistemas de protección del equipo de cómputo que los usuarios pueden adquirir y que dan cierto grado de seguridad, entre ellos están: *panda antivirus, Mccafee,* etc. Estos sistemas pueden bajarse directamente de Internet, así como sus actualizaciones. Su costo es gratuito.[12]

Una vez detectada una infección viral, ésta puede contenerse aislando inmediatamente los ordenadores de la red, deteniendo el intercambio de ficheros y empleando sólo discos protegidos contra escritura. Para que un sistema informático se recupere de una infección viral, primero hay que eliminar el virus. Algunos programas antivirus intentan eliminar los virus detectados, pero a veces los resultados no son satisfactorios. Se obtienen resultados más fiables desconectando la computadora infectada, arrancándola de nuevo desde

[12] Vid. www.pandaantivirus.com.

un disco flexible protegido contra escritura, borrando los ficheros infectados y sustituyéndolos por copias de seguridad de ficheros legítimos y borrando los virus que pueda haber en el sector de arranque inicial.

En la actualidad, los autores de un virus cuentan con varias estrategias para escapar de los programas antivirus y propagar sus creaciones con más eficacia. Los llamados virus polimórficos efectúan variaciones en las copias de sí mismos para evitar su detección por los programas de rastreo. Los virus sigilosos se ocultan del sistema operativo cuando éste comprueba el lugar en que reside el virus, simulando los resultados que proporcionaría un sistema no infectado. Los virus llamados infectores rápidos no sólo infectan los programas que se ejecutan sino también los que simplemente se abren. Esto hace que la ejecución de programas de rastreo antivírico en un ordenador infectado por este tipo de virus pueda llevar a la infección de todos los programas del ordenador. Los virus llamados infectores lentos infectan los archivos sólo cuando se modifican, por lo que los programas de comprobación de suma interpretan que el cambio de suma es legítimo. Los llamados infectores escasos sólo infectan en algunas ocasiones: por ejemplo, pueden infectar un programa de cada 10 que se ejecutan. Esta estrategia hace más difícil detectar el virus.

Es importante también agregar que existen otros programas informáticos nocivos similares a los virus, pero que no cumplen ambos requisitos de reproducirse y eludir su detección. Estos programas se dividen en tres categorías: caballos de Troya, bombas lógicas y gusanos. Un caballo de Troya aparenta ser algo interesante e inocuo, por ejemplo un juego, pero cuando se ejecuta puede tener efectos dañinos. Una bomba lógica libera su carga activa cuando se cumple una condición determinada, como cuando se alcanza una fecha u hora determinada o cuando se teclea una combinación de letras. Un gusano se limita a reproducirse, pero puede ocupar memoria de la computadora y hacer que sus procesos vayan más lentos.

1.7. LA PROPAGACIÓN DE VIRUS INFORMÁTICOS.

Por propagar se entiende la acción y efecto de distribuir o hacer llegar a algún lugar el virus informático creado con anterioridad.

La propagación de los virus informáticos puede ser por varios mecanismos, principalmente por medio de Internet. Se crea el virus y se envía conjuntamente con un e mail, por lo que al abrirlo se libera el virus y este empezará su labor destructiva. Así, si se envían muchos e mails o simplemente, la persona que lo recibe primeramente, lo abre y a su vez lo reenvía a sus conocidos, habrá contaminado a varios usuarios y ellos a su vez a otro tanto, inclusive, el virus puede correr de un país a otro, de un continente a otro en sólo cuestión de minutos, llegando a constituir una verdadera epidemia mundial.

El correo electrónico es la vía más idónea para propagar el virus informático.

Puede ser que se cree una página en Internet o web y se adjunte un virus en ella, por lo que los navegantes que lleguen ahí, resultarán contaminados y posiblemente no se den cuenta hasta dentro de algunos días, cuando empiecen a notar los daños causados.

Un virus informático puede estar también contenido en un diskete, por lo que al abrirlo, se libera el mismo y así empezará su labor. No sucede así con los cds, los cuales difícilmente pueden tener un virus informático debido a su tecnología.

1.8. EFECTOS DE LA CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICOS:

La creación y propagación de virus informáticos constituye un acto que puede poner en peligro no sólo los equipos de los usuarios comunes y corrientes, sino que inclusive puede ir más allá, causando serios percances en los sistemas computacionales de gobiernos u organismos internacionales. A continuación se abundará en este punto.

1.8.1. SOCIALES.

En la actualidad, la sociedad mundial (y en ella la mexicana) depende totalmente de las computadoras y de los programas creados ex profeso para que estos equipos puedan resolver cada día situaciones y problemáticas más complicadas. Los alumnos de escuelas primarias, secundarias y de preparatoria ya utilizan las computadoras para sus tareas. En muchos hogares, las computadoras cumplen con tareas importantes: La organización de las actividades, el registro de los gastos, etc.

Si un virus informático entra a una computadora en el hogar, la oficina, la clínica, el banco, etc., las actividades normales y diarias se entorpecerán, causando daños y perjuicios a la sociedad, ya que la dependencia que se tiene de las computadoras es cada día más notoria, por lo que se debe aprender a protegerse de los virus informáticos, con medidas como las mencionadas.

1.8.2. ECONÓMICOS.

Un virus informático puede causar serios daños en los equipos de cómputo, como la pérdida de información (archivos o programas), daños que serían difíciles de cuantificar, ya que la información de una persona física o moral es el resultado de largas jornadas de trabajo, de esfuerzo, de investigación, etc.

Cuando un virus entra al equipo de una persona, los daños que se pueden causar son múltiples, desde la lentitud de los equipos, hasta daños y perdida de los archivos y programas en el disco duro, con lo que el usuario tendrá que solicitar la reparación de su equipo, tratando de rescatar la información perdida. Inmediatamente habrá que desfragmentar la computadora y reinstalar los programas y la información que haya logrado salvarse.

Si se trata de compañías o empresas grandes, un virus puede hacer que las inversiones en la bolsa y otras operaciones de crédito sufran atrasos y con ello, pérdidas considerables, inclusive, causar caídas severas en el plano económico.

1.8.3. POLÍTICOS.

La creación de virus informáticos puede ser el resultado de tácticas o estrategias políticas de algún grupo o partido, por ejemplo, hace dos años la página de Internet de la Presidencia de la República se vio dañada momentáneamente por un virus que se propagó en la misma web, el cual inhabilitó la página, lo que fue el producto de mentes criminales que deseaban causar un daño. A estas personas se les llama “hackers”

En la actualidad, donde las campañas políticas se basan en los medios de comunicación, es posible que se puedan crear virus informáticos con la finalidad de causar daño o desacreditar a los otros contrincantes políticos, sobretodo, previo a una elección.

1.8.4. INTERNACIONALES.

Los virus informáticos que han podido dar la vuelta al mundo como los ya mencionados: El “Anna Kournikova”, el “I love you” y otros más, sacudieron a muchos países, ya que miles de usuarios en todo el orbe resultaron perjudicados.

En la actualidad que se habla del terrorismo en varias de sus manifestaciones, como son la militar o armada, la biológica, la química, etc., habría que tener en cuenta que la creación de virus informáticos podría ser tranquilamente una nueva forma de causar daño en los equipos de cómputo de las personas y de las instituciones. Es por esta razón que personas como el señor Bill Gates siempre está interesado en encontrar y contratar a los creadores de virus informáticos, como una forma de prevenirlos.

No se exagera al decir que el mundo debe tener en cuenta la posibilidad de que los virus informáticos se conviertan en una nueva forma de terrorismo cibernético y más si se toma en cuenta que los mismos nacieron con la finalidad de causar daño a los extranjeros.

CAPÍTULO 2.
EL NUEVO CÓDIGO PENAL PARA EL DISTRITO FEDERAL. ASPECTOS GENERALES.

2.1. NUESTRO NUEVO CÓDIGO PENAL 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 Nuevo 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, Jefe de Gobierno de esta ciudad.

El Nuevo Código Penal 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 Nuevo Código 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 Nuevo Código Penal significa más retos, algunos de ellos complejos, sin embargo, su labor depende en mucho de la debida integración de las averiguaciones previas por parte del Ministerio Público de acuerdo a lo dispuesto en el artículo 36 del Código de Procedimientos Penales para el Distrito Federal:

"Artículo 36.- Cuando se haya negado la orden de aprehensión o de comparecencia, o dictado el auto de libertad por falta de elementos para procesar, por considerar que no están reunidos los requisitos del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos y 132 y 133 de este Código, el Juez penal deberá señalar aquellos requisitos que a su juicio no se encuentren satisfechos, fundando y motivando su resolución, y el Ministerio Público practicará las diligencias necesarias para integrar debidamente la averiguación previa correspondiente".

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

En los antecedentes del Proyecto de Decreto que contiene le Nuevo 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 Nuevo Código para el Distrito Federal se justifica plenamente en la necesidad 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 debían crear otros que no estaban tipificados como los delitos informáticos.

.

2.3. CLASIFICACIÓN DE LOS DELITOS QUE HACE EL NUEVO 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 Nuevo Código Penal para el Distrito Federal.

El Nuevo 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 Nuevo 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 Nuevo Código es precisamente contar con una normatividad sustantiva más moderna y adecuada a los tiempos de cambio de esta ciudad.

2.4. SU ESTRUCTURA.

Una de las principales innovaciones del Nuevo Código Penal para el Distrito Federal es la reclasificación de los delitos ya conocidos y, por otra parte, la creación de nuevos tipos penales y principios jurídicos sobre ellos, contenidos en los artículos 1º al 8º : principio de legalidad (artículo 1º); principio de tipicidad y prohibición de la aplicación retroactiva, analógica y por mayoría desazón (artículo 2º); principio de la prohibición de la responsabilidad objetiva (artículo 3º); principio del bien jurídico y de la antijuricidad material (artículo 4º); principio de culpabilidad (artículo 5º); principio de la jurisdiccionalidad (artículo 6º); principio de la

territorialidad (artículo 7º) y, principio de aplicación extraterritorial de la ley penal (artículo 8º).

2.5. LOS NUEVOS TIPOS PENALES QUE ESTABLECE.

Una de las principales características del Nuevo Código Penal para el Distrito Federal es que incorpora nuevos tipos penales, los cuales obedecen a una ratio legis y social que resultaba ya insoslayable e impostergable. La sociedad reclamaba que se sancionara de manera más efectiva y con penas más duras ciertas conductas que han lesionado seriamente a la misma. De esta manera, si bien, el Nuevo 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 tipos penales interesantes por su alcance y contenidos.

Para efecto de una mejor comprensión de los tipos nuevos que establece la ley penal sustantiva vigente para el Distrito Federal, enumeramos los contenidos del Libro Segundo y resaltamos con negrillas los tipos que recién se incorporaron al referido Código:

LIBRO SEGUNDO
Parte especial
TÍTULO PRIMERO
Delitos contra la vida y la integridad corporal
CAPÍTULO I
Homicidio 123 al 129
CAPÍTULO II
Lesiones 130 al 135

CAPÍTULO VI

Retención y sustracción de menores o incapaces 171 al 173

TÍTULO QUINTO

Delitos contra la libertad y la seguridad sexuales y el normal desarrollo psicosexual

CAPÍTULO I

Violación 174 y 175

CAPÍTULO II

Abuso sexual 176 al 178

CAPÍTULO III

Hostigamiento sexual 179

CAPÍTULO IV

Estupro 180

CAPÍTULO V

Incesto 181

CAPÍTULO VI

Disposiciones generales 182

TÍTULO SEXTO

Delitos contra la moral pública

CAPÍTULO I

Corrupción de menores e incapaces 183 al 186

CAPÍTULO II

Pornografía infantil 187 y 188

CAPÍTULO III

Lenocinio 189 y 190

CAPÍTULO IV

Disposiciones comunes 191 y 192

TÍTULO SÉPTIMO

Delitos contra la seguridad de la subsistencia familiar

CAPÍTULO ÚNICO 193 al 199

TÍTULO OCTAVO

Delitos contra la integridad familiar

CAPÍTULO ÚNICO

Violencia familiar 200 al 202

TÍTULO NOVENO

Delitos contra la filiación y la institución del matrimonio

CAPÍTULO I

Estado civil 203 y 204

CAPÍTULO II

Bigamia 205

TÍTULO DÉCIMO

Delitos contra la dignidad de las personas

CAPÍTULO ÚNICO

Discriminación 206

TÍTULO DÉCIMO PRIMERO

Delitos contra las normas de inhumación y exhumación y contra el respeto a los cadáveres o restos humanos

CAPÍTULO ÚNICO

Inhumación, exhumación y respeto a los cadáveres o restos humanos207 y 208

TÍTULO DÉCIMO SEGUNDO

Delitos contra la paz, la seguridad de las personas y la inviolabilidad del domicilio

CAPÍTULO I

Amenazas 209

CAPÍTULO II

Allanamiento de morada, despacho, oficina o establecimiento mercantil 210 y 211

TÍTULO DÉCIMO TERCERO

Delitos contra la intimidad personal y la inviolabilidad del secreto

CAPÍTULO I

Violación de la intimidad personal 212

CAPÍTULO II

Revelación de secretos 213

TÍTULO DÉCIMO CUARTO

Delitos contra el honor

CAPÍTULO I

Difamación 214 y 215

CAPÍTULO II

Calumnia 216 al 218

CAPÍTULO III

Disposiciones comunes 219

TÍTULO DÉCIMO QUINTO

Delitos contra el patrimonio

CAPÍTULO I

Robo 220 al 226

CAPÍTULO II

Abuso de confianza 227 al 229

CAPÍTULO III

Fraude 230 al 233

CAPÍTULO IV

Administración fraudulenta 234

CAPÍTULO V

Insolvencia fraudulenta en perjuicio de acreedores 235

CAPÍTULO VI

Extorsión 236

CAPÍTULO VII

Despojo 237 y 238

CAPÍTULO VIII

Daño a la propiedad 239 al 242

CAPÍTULO IX

Encubrimiento por receptación 243 al 245

CAPÍTULO X

CAPÍTULO III
Sabotaje 363
CAPÍTULO IV
Motín 364
CAPÍTULO V
Sedición 365
ARTÍCULOS TRANSITORIOS I al V.

2.6. LA AUSENCIA DE UN TIPO PENAL QUE REGULE Y SANCIONE LA CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICOS.

De la lectura de los diferentes delitos y sus respectivos numerales que contiene el Nuevo Código Penal vigente para el Distrito Federal, se puede observar que no hay ninguno que se refiera a los delitos 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 y sus asesores, 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.

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 cuyo artículo 217 se dispone que:

"Comete delito informático, la persona que dolosamente y sin derecho:

Use o entre a una base de datos, sistemas 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 intercepte, interfiera, reciba, use, 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".

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.

Este tipo penal hace alusión a los delitos informáticos en general y de manera particular, a la creación y propagación de virus informáticos.

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. En

el caso de las simples personas físicas, éstas también suelen hacer compras mediante la red, utilizando un tarjeta de crédito internacional, la cual puede ser utilizada ilegalmente por un hacker y despojar de los fondos a su titular. 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 Nuevo 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. El párrafo segundo del artículo 14 constitucional establece el principio penal *nullum poena sine lege*, es decir, que no puede haber delito si no hay un tipo penal anterior que sancione una determinada conducta como ilícita:

"No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querella de un hecho que la ley señale como delito, sancionado cuando menos con pena privativa de libertad y existan datos que acrediten el cuerpo del delito y que hagan probable la responsabilidad del indiciado".

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 advertir 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, sin embargo, se considera que por tratarse de conductas que constantemente evolucionan (casi diariamente sala a la luz un virus diferente), por lo que es menester que los legisladores profundicen más en el problema y adapten los tipos penales a los tipos de delitos informáticos, por ejemplo, la creación y propagación de virus informáticos, la destrucción o el robo de información a través de ellos, etc.

Los tipos descritos carecen de elementos de carácter técnico-informático que permita integrar adecuadamente la averiguación previa y en el caso de la consignación, para que el juzgador pueda imponer la pena adecuada al infractor de la norma penal.

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.

La legislación debe estar a la par de países como los Estados Unidos de América, España, Alemania o Francia donde la lucha contra los delitos informáticos es algo que ya cuenta con cinco o diez años por lo menos.

CAPÍTULO 3.
NECESIDAD DE CONTAR CON UN TIPO PENAL EN EL DISTRITO FEDERAL EN MATERIA DE CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICOS.

3.1. CONCEPTO DE DELITO.

Estos son algunos de los conceptos más importantes sobre el delito que han sido elaborados por los autores a través de los años.

El vocablo "delito", viene del latín: D*elictum, delinquo, delinquere*, que significa desviarse, resbalar, abandono de una ley.

El italiano Francesco Carrara manifiesta lo siguinete:

"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".[1]

Enrico Ferri dice: *"…los delitos son las acciones punibles determinadas por móviles individuales y antisociales que perturban las*

[1] Citado por Reynoso Dávila, Roberto. Teoría General del Delito. Editorial Porrúa S.A. 3ª edición, México, 1998, p. 13.

condiciones de vida y contravienen la moralidad media de un pueblo en un tiempo y lugar determinado".[2]

Fernando Castellanos Tena cita Carrara quien a su vez decía que: *"… 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 políticamente dañoso".*[3]

Después cita a Edmundo Mezger quien dice del delito que: *"… es una acción punible; esto es el conjunto de los presupuestos de la pena".*[4]

Eugenio Cuello Calón, igualmente citado por el maestro Castellanos Tena, dice que el delito es: *"la acción humana antijurídica, típica, culpable y punible".*[5]

Ernesto Beling señala: *"…la acción típica, antijurídica, culpable, sometida a una adecuada sanción penal y que llena las condiciones objetivas de penalidad".*[6]

No hay duda de que estos conceptos reflejan una época y concepción sobre el delito, sin embargo, hay que decir que a la fecha no existe un concepto que sea universalmente válido ya que esta figura jurídica está en constante transformación, sin embargo, muestran una idea clara sobre la actividad delictiva.

---

[2] Ibid. pp. 17 y 18.
[3] Vid. Castellanos Tena, Fernando. Lineamientos Elementales de Derecho Penal. Editorial Porrúa S.A. 43a edición, México, 2002, pp. 127 y 128.
[4] Idem.
[5] Idem.
[6] Citado por Jiménez de Asúa, Luis. Lecciones de Derecho Penal. Editorial Pedagógica Iberoamericana, México, 1995, p. 132.

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".[7]

No hay duda de que estos conceptos reflejan una época y concepción sobre el delito, sin embargo, hay que decir que a la fecha no existe un concepto que sea universalmente válido ya que esta figura jurídica está en constante transformación, sin embargo, nos muestran una idea clara sobre la actividad delictiva.

El anterior Código Penal para el Distrito Federal (de 1931), tenía el siguiente concepto legal del delito:

"Artículo 7º.-Delito es el acto u omisión que sancionan las leyes penales".

No obstante que este concepto ya no está vigente en el Nuevo Código Penal para el Distrito Federal, sí permanece en el Código Penal Federal vigente en el mismo artículo número 7º, toda vez que el Código Penal para el Distrito Federal de 1931 se aplicaba también supletoriamente en materia de delitos federales.

Francisco González de la Vega nos comenta:

"Aun cuando la mayor parte de los Códigos no se preocupan por definir el delito en general, nuestra legislación, siguiendo la tradición española, ha creído prudente hacerlo. Así el C.P. de 1871, art. 4º, decía: Delito es. La infracción voluntaria de una ley penal haciendo lo que ella prohíbe o dejando de hacer lo que

[7] Citado por Creus, Carlos. Derecho Penal. Parte General. Editorial Astrea, Buenos Aires, 1988, p. 26.

manda. El de 1929, art. 11, decía: Delito es: La lesión de un derecho protegido legalmente por una sanción penal".[8]

El autor agrega que el delito presenta las siguientes características:

"a) Es un acto humano entendiendo por él conducta actuante u omisa (acción u omisión);

b) Típico, es decir, previsto y descrito especialmente en la ley;

c) Antijurídico, o sea, contrario al derecho objetivo por ser violador de un mandato o a una prohibición contenidos en las normas jurídicas;

d) Imputable, entendiéndose aquí por imputabilidad la capacidad penal referida al sujeto;

e) Culpable, en cualquiera de las formas del elemento moral o subjetivo (intencionalidad o imprudencia);

f) Punible, amenazado con la aplicación de una pena; y

g) Conforme a sus condiciones objetivas de punibilidad, porque, en ocasiones, aparte de la reunión de los anteriores elementos, el legislador exige se cumpla un requisito externo a la acción criminal para que se integre la figura perseguible; ejemplo, en homicidio, se requiere que la muerte acontezca dentro de sesenta días (art. 303, frac. II). Jiménez de Asúa dice: 'El delito es una acto típico, antijurídico, imputable, culpable, sancionado con una pena adecuada y conforme a las condiciones objetivas de punibilidad'".[9]

El Nuevo Código Penal para el Distrito Federal ya no contiene un concepto legal del delito como su antecesor. Sin embargo, el Nuevo Código para el Distrito Federal señala:

*"**ARTÍCULO** 1 (Principio de legalidad). 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*

[8] Vid. González de la Vega, Francisco. El Código Penal Comentado. Editorial Porrúa, 12ª edición, México, 1996, p. 12.
[9] Idem.

la ley y la pena o la medida de seguridad se encuentren igualmente establecidas en ésta".

***"ARTÍCULO** 2 (Principio de tipicidad y prohibición de la aplicación retroactiva, analógica y por mayoría de razón). 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".*

El artículo 15 del Nuevo Código establece el principio de acto:

***"ARTÍCULO** 15 (Principio de acto). El delito sólo puede ser realizado por acción o por omisión".*

De la lectura de los anteriores artículos nos podemos percatar que se trata de una serie de principios que dan sustento a la averiguación previa y la actividad investigadora, pero también, la imposición de las penas que es una actividad del juzgador.

3.2. CLASIFICACIÓN DOCTRINAL DE LOS DELITOS.

Hay distintas clasificaciones de los delitos. Los autores se han dado a la tarea de clasificar los delitos con fines preponderantemente didácticos, lo que no significa que su tarea sea fácil, por el contrario, resulta una actividad complicada y que lleva mucho tiempo.

SEGÚN LA DOCTRINA.

Dentro de los variados autores penalistas quienes se ocupan de clasificar a los delitos está Francisco Torrejón quien dice:

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.[22]

Hay también delitos de comisión o acción, en los que se prohíbe llevar a cabo una determinada conducta como es el privar de la vida a alguien, robar, defraudar, etc. Los delitos de omisión, en los que la ley ordena una conducta determinada y el agente no la realiza, como sucede en los delitos de abandono de personas.[23]

Por el resultado que producen, los delitos pueden ser 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

[22] Torrejón, Francisco. Derecho Penal, tomo I.. Editorial Desalma, 2ª edición, Buenos Aires, 2001, p. 45.
[23] Idem.

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.

De conformidad al daño ocasionado a la víctima o, al bien jurídico tutelado, 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.

En cuanto a su duración, los delitos pueden ser instantáneos, contínuo o continuados. El Nuevo Código Penal para el Distrito Federal establece:

***"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

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

De acuerdo a su estructura o composición, lo delitos se clasifican en simples y complejos. Son simples aquellos en los cuales la lesión jurídica es única, como el homicidio. Son complejos aquellos 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.[24]

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.

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.

De acuerdo a la materia, los delitos pueden ser federales, comunes, militares y políticos (los cuales siguen siendo materia de polémicas doctrinales, ya que para muchos, no existen los delitos políticos).

DE ACUERDO AL NUEVO CÓDIGO PENAL PARA EL DISTRITO FEDERAL.

El Nuevo Código Penal para el Distrito Federal incorpora nuevos tipos penales que constituyen el anhelo y reclamo por parte de la población del Distrito Federal en materia de combate a la delincuencia.

[24] Ibid. p. 47.

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

a) Delitos contra la vida y la integridad corporal: Homicidio, lesiones, ayuda o inducción al suicidio y aborto.

b) Procreación asistida, inseminación artificial y manipulación genética.

c) Delitos de peligro para la vida o la salud de las personas: Omisión de auxilio o de cuidado y peligro de contagio.

d) 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.

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

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

g) Delitos contra la seguridad de la subsistencia familiar.

h) Delitos contra la integridad familiar: violencia familiar.

i) Delitos contra la filiación y la institución del matrimonio: Estado civil y bigamia.

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

k) 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.

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

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

n) Delitos contra el honor: difamación y calumnia.

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

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

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

q) 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.

r) 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.

s) 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.

t) 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.

u) Delitos cometidos en el ejercicio de la profesión: Responsabilidad profesional y técnica; usurpación de profesión; abandono, negación y práctica indebida del servicio 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.

v) 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.

w) 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.

x) Delitos ambientales: Alteración y daños al ambiente.

y) Delitos contra la democracia electoral: Delitos electorales.

z) Delitos contra la seguridad de las instituciones del Distrito Federal: Rebelión; ataques a la paz pública, sabotaje; motín y sedición.

Se desprende la existencia de nuevos tipos penales que hoy constituyen instrumentos importantes para combatir a las nuevas formas de delincuencia en el Distrito Federal que han encerrado a la sociedad en espacios

reducidos: la casa, oficina o lugar de trabajo, la escuela, etc., mientras que las calles son sólo para los delincuentes quienes se han apoderado de ellas.

3.3. LOS DELITOS INFORMÁTICOS:

En otros 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, según se ha visto, se ha extendido rápidamente a todos los círculos del país. Así, tanto 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 los delitos informáticos desde hace muchos años, sin embargo, parece que el Legislador tanto federal como de la mayoría de los Estados ha hecho caso omiso al respecto, posiblemente, menospreciando la importancia de tales ilícitos, sin embargo, se trata a todas luces 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 y los tratados que México ha suscrito con otras naciones, ha sido benéfico para que se desarrollen 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".

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.

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.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas. Y si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares, se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje.

No son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no 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)".[25]

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".*

[25] Téllez Valdez, Julio. Op. Cit. Pp. 103 y 104.

Nidia Callegari dice: *"aquél que se da con la ayuda de la informática o de las técnicas anexas".*[26]

Rafael Fernández Calvo señala: *"...la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1º de la Constitución Española".*[27]

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".*[28]

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".

De acuerdo con las anteriores opiniones de los doctrinarios, se puede 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

[26] www.tiny.uasnet.mx/prof/cin/der/silvis/INDEX.htm. Del 15 de abril del 2005 a las 20:45 horas.
[27] www.ctv.es/users/mqp/delitos.html. Del 15 de octubre del 2005 a las 20:53.
[28] www.colosus.rhon.itam.mx/-sriosma. Del 15 de abril del 2005 a las 21:03 horas.

operaciones fraudulentas, utilizando a la computadora y a sus programas como medio o instrumento de comisión.

3.3.2. CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS.

Según Julio Tellez 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".[29]

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 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. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS.

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

[29] Téllez Valdez, Julio. Op. Cit. Pp. 103 y 104.

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.

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.).

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

- **Acceso no autorizado:** Uso ilegitimo de 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.

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

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 imagenes)

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 loteria

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 logos 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.[30]

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 (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 computo 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

[30] www.delitosinformáticos.com.-estafas. 11 de abril del 2005, a las 21:34 horas.

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, aún **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 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.

3.3.6.1. 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 los delitos como el robo, abuso de confianza y el fraude, pues son de carácter patrimonial.

3.3.6.2. 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: fraude, robo, abuso de confianza 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 e inclusive, sus créditos y dinero guardado en una cuenta bancaria o varias y que puede ser objeto de un menoscabo total o parcial a través de Internet.

3.3.6.3. 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.[31]

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

[31] Hance, Oliver. Leyes y Negocios en Internet. Editorial McGraw Hill, México, 1997, p. 67.

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. 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.

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.

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. Se contempla también que el sujeto posea una cuenta bancaria y realice constantemente transacciones financieras en Internet, para que 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.

3.3.6.4. EL RESULTADO.

El delito de creación y propagación de virus informáticos es un ilícito penal de resultado eminentemente material ya que el sujeto pasivo recibe uno o varios daños ya sea 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 que puede recibir ya que la información que guarda en su equipo es uno de sus bienes más importantes, por ello, es aconsejable que siempre se

hagan copias o soportes de la misma para que en caso de ser atacado por un virus informático se pueda reponer la información.

El sujeto pasivo puede recibir un daño que consista en el robo o fraude de una o varias inversiones que estén en cuentas bancarias, ya que a través de Internet hemos dicho que ese dinero puede ser transferido fácilmente a otras cuentas.

3.3.6.5. 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, por lo que se trata de un ilícito que esencialmente admite el dolo como forma, aunque puede ser que una persona cree un virus informático y por accidente 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.

3.3.6.6. LA TENTATIVA.

La tentativa es el grado inacabado en la comisión de un delito. Esto significa que su autor intenta llevar a cabo todos y cada uno de los pasos planeados en el iter criminis, sin embargo, por causas ajenas al propio sujeto, el resultado no se logra.

En el caso del delito en cita, la tentativa sí 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.

Por lo anterior, se entiende perfectamente que el delito de creación y propagación de virus informáticos admite el grado de tentativa ante la gran gama de posibilidades de estar protegido contra tales programas y sus efectos o consecuencias.

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, incluyendo al Estado de Sinaloa, 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, por lo que resulta lógico que el Distrito Federal cuente con una regulación al respecto.

3.4.2. SU JUSTIFICACIÓN SOCIAL.

Se considera que el hecho de que se reforme y adicione el Nuevo Código Penal para el Distrito Federal para que contenga un tipo penal que sancione la creación y propagación de virus informáticos, obedece a una cuestión o razón social, dar seguridad a quienes acceden constantemente a Internet para fines de trabajo, de cultura, de amistad, recreación o diversión e incluso financieros.

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 VIRUS INFORMÁTICOS.

Como resultado de la presente investigación documental, se propone que se cree un nuevo tipo penal para el novel Código Sustantivo de la materia en el Distrito Federal en el rubro de la creación y propagación de virus informáticos, por todas y cada una de las razones ya explicadas. El texto que se pone a consideración del lector puede ser ubicado en el Título Décimo Tercero: Delitos contra la Intimidad Personal y la Inviolabilidad del Secreto, adicionándole un Capítulo, el Tercero que se denominaría: delitos informáticos. El texto del delito de creación y propagación de virus informáticos es el 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".

Se considera que 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.

Por otra parte, se considera 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 estima 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 están inmersos en este fenómeno, hay todavía quienes no conocen las ventajas de lasa computadoras, por lo que debe fomentarse su estudio a todos niveles.

CONCLUSIONES.

I.- Las computadoras constituyen uno de los inventos más extraordinarios que el hombre ha podido crear para hacer más fácil su vida diaria. Las computadoras han venido a modernizar el entorno del hombre de manera integral y definitiva.

II.- 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.

III.- 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.

IV.- 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.

V.- 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.

VI.- 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.

VII.- 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.

VIII.- 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.

IX.- 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.

X.- 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.

XI.- 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.

XII.- 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.

XIII.- 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.

XIV.- 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 Nuevo Código Penal para el Distrito Federal es omiso en cuanto a este tema importante.

XV.- 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.

XVI.- Ante la falta de una marco jurídico adecuado en el Nuevo 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".

Se estima 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 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, Luis. Lecciones de Derecho Penal. Editorial Pedagógica Iberoamericana, México, 1995, p. 132.

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

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

REYNOSO DÁVILA, Roberto. Teoría General del Delito. Editorial Porrúa S.A. 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, 2005.

CÓDIGO PENAL FEDERAL. Editorial SISTA S.A. México, 2005.

NUEVO CÓDIGO PENAL PARA EL DISTRITO FEDERAL. Editorial SISTA S.A. México, 2005.

OTRAS FUENTES.

Enciclopedia Encarta Microsoft 2004. Microsoft Corporation, 2004.

Revista: Vivir en Internet. Publicación mensual. Septiembre de 2001, México, mensual.

www.colosus.rhon.itam.mx/-sriosma. Del 15 de abril del 2005 a las 21:03 horas.

www.ctv.es/users/mqp/delitos.html. Del 15 de octubre del 2005 a las 20:53.

www.delitosinformáticos.com.-estafas. 11 de abril del 2005, a las 21:34 horas.

www.pandaantivirus.com. Día 22 de abril de 2005, a las 12:39 pm.

www.tiny.uasnet.mx/prof/cin/der/silvis/INDEX.htm. Del 15 de abril del 2005 a las 20:45 horas.