



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

PROPUESTA DE REFORMAS DE ALGUNOS ARTÍCULOS DEL CÓDIGO PENAL FEDERAL PARA LA SOLUCIÓN DE DELITOS INFORMÁTICOS

TESIS
QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN

PRESENTAN:

CONTRERAS JIMENEZ EDUARDO CARLOS
FLORES MEDINA PEDRO
RUIZ VAZQUEZ NOE JOB

DIRECTORA DE TESIS:
Ing. Lucila Patricia Arellano Mendoza



MÉXICO, D.F.

2008

AGRADECIMIENTOS

A Dios por haberme permitido vivir y lograr una meta más, y quien siempre ha estado conmigo en los momentos difíciles de mi vida.

A mi madre por todos estos años de trabajo, esfuerzo y sobre todo apoyo, ejemplo y cariño que siempre me ha brindado, y que ahora refleja en este logro.

A mi padre por todos estos años de trabajo, el gran apoyo que siempre me brindo, y por las bases para culminar este proyecto.

A mis hermanos Jesús, Dulce, Mari y Dalia, y mis sobrinos Nadia, Claudia, Víctor, Fernanda, Yoloatzin y Nicole, quienes con su inocencia y cariño me permitieron vislumbrar el camino para alcanzar esta meta que no solo es mía sino de toda la familia Flores Medina, a la que con mucho cariño dedico este trabajo.

A mis tíos y primos, quienes con su apoyo, ánimo y sus consejos me alentaron para seguir siempre adelante, pese a las dificultades.

A Paola, por todo cuanto estuvo en tu corazón dar, tuve el valor para tomar decisiones importantes que me llevaron a finalmente concluir este trabajo que significa tanto para mí, Dios te bendiga donde quiera que te lleven tus viajes.

A mis maestros, que siempre me acompañan a través de sus enseñanzas, me protegen y orientan aún cuando no este en el aula de clase, el legado maravilloso de la educación.

A mis compañeros Eduardo y Noe por todo el tiempo que compartimos juntos en la realización de este trabajo, el cual será inolvidable.

A todas aquellas personas que de alguna manera han influido y contribuido en mi preparación personal y profesional, en el trabajo, en la casa y en la escuela de la vida.

Sinceramente Gracias

Pedro Flores Medina

DEDICATORIAS

A Dios

A ti DIOS que me diste la oportunidad de vivir y de regalarme una familia maravillosa.

A Jesús

Por ser mi camino, mi verdad y mi vida.

A mi Madre

Ma. del Carmen Vázquez Montes

Por todo el apoyo físico, moral y económico que me ha dado durante toda mi formación académica e inculcarme el salir adelante, educarme y disciplinarme para ser alguien en la vida.

A mi Padre

José Andrés Ruiz Hernández

Con mucho cariño principalmente a mis padres que me dieron la vida y han estado conmigo en todo momento. Gracias por todo papá y mamá por darme una carrera para mi futuro y por creer en mí, aunque hemos pasado momentos difíciles siempre han estado apoyándome y brindándome todo su amor, por todo esto les agradezco de todo corazón el que estén conmigo a mi lado.

Los quiero con todo mi corazón y este trabajo que me llevó 4 meses hacerlo es para ustedes, por ser el hijo más chico que realizó Tesis, aquí está lo que ustedes me brindaron, solamente les estoy devolviendo lo que ustedes me dieron en un principio.

A mis hermanos y hermanas

José Andrés, Ignacio, Eduardo, Víctor Hugo,

Juana Lidia, Martha Alicia, Luz Raquel, Lorena y Erika Araceli

Por estar ahí en el momento que los necesite y hacerme ver que tengo a alguien por quienes luchar en la vida.

A mis sobrinos

Guillermo Iván, Andrés Adrian, Carmen, Lucia Cecilia, Josué Raziél, David Emmanuel, Barbará Sofía, Diego y Daniel Alberto.

Sobrinos, sobrinas y sobrinitos, quisiera nombrarlos a cada uno de ustedes sus nombres completos pero son muchos, pero eso no quiere decir que no me acuerde de cada uno, a todos, los quiero, nunca los olvidaré.

Gracias por hacerme feliz cuando convivo con ustedes y por enseñarme muchas cosas de la vida que son importantes en mi formación profesional.

A mis Amigos

Los cuales enumerarlos me llevaría muchísimas hojas pero que me apoyaron y me brindaron toda su amistad incondicional en todo momento. En especial a Raymundo Valentín López Quiroz por ser un gran amigo y apoyarme en esos momentos muy difíciles que pase en mi estancia en la Facultad de Ingeniería y a Monserrat Basilio Pérez por brindarme su total apoyo en uno de los momentos más difíciles de mi vida.

A todos mis amigos de la Facultad de Ingeniería

A Moisés, Manuel, Octavio, Isidro Omar, Roberto, Gabriel, †Hugo Luis, Federico Alejandro, Epifanio, Pedro, Eduardo Carlos, Ricardo Javier, Luis, Landeros, Jorge Faisal, Miguel Faisal, Alejandro Macario, y a cuantos más que participaron y que me hicieron gozar de triunfos, éxitos y popularidad que incluso aun después de varios años de habernos graduado de la Facultad nos siguen recordando con cariño.

Gracias a todos.

A mis profesores

A mis profesores por haberme compartido de sus conocimientos, por confiar en mí y por tenerme la paciencia necesaria. Agradezco el haber tenido unos profesores tan buenas personas en toda mi vida. En especial al Mat. Luis Alfonso León García y al Ing. Luis Cesar Vázquez Segovia, Secretario Académico de la División de Ciencias Básicas de la Facultad de Ingeniería.

Agradezco también al Lic. Cesar Augusto Méndez Cruz, Subdirector del Área de Mantenimiento, de la Dirección General de Sistemas de la Auditoría Superior de la Federación de la H. Cámara de Diputados (ASF), por haberme dado la oportunidad de realizar el servicio social en esta institución y por motivarme para que culminara el proceso de titulación, de antemano le doy las gracias por toda la ayuda que me brindo.

Y no me puedo despedir sin antes decirles, que sin ustedes a mi lado no lo hubiera logrado, tantas desveladas sirvieron de algo y aquí está el fruto. Les agradezco a todos ustedes con toda mi alma el haber llegado a mi vida y el compartir momentos agradables y momentos tristes, pero esos momentos son los que nos hacen crecer y valorar a las personas que nos rodean. Los quiero mucho y nunca los olvidaré.

Ing. Noé Job Ruíz Vázquez

DEDICATORIA

Lic. Cesar Augusto Méndez Cruz

Subdirector del Área de Mantenimiento

Dirección General de Sistemas

Auditoria Superior de la Federación (ASF)

H. Cámara de Diputados

Gracias por el apoyo que me has brindado a lo largo de este tiempo, por darme la oportunidad de realizar el servicio social y las prácticas profesionales en la Auditoria Superior de la Federación.

De igual manera te agradezco por los conocimientos que adquirí y por hacerme ver la importancia de la Titulación en la preparación profesional.

Ing. Noé Job Ruíz Vázquez

DEDICATORIA

Lic. Carlos Martínez Medina

Gracias por el apoyo y amistad que me brindas, los consejos y comentarios que me has dado en cuanto a mi persona, por enseñarme la mejor forma de lograr objetivos y metas en la vida, por ayudarme a descubrir esa parte de líder que tengo y mostrarme apoyo sincero en todo momento.

Ing. Noé Job Ruíz Vázquez

DEDICATORIA



Alfredo Rodríguez y Pacheco

Senador de la República de la LX legislatura

Integrante del Grupo Parlamentario del

Partido Acción Nacional

(PAN)

Gracias por su apoyo y colaboración para la elaboración de esta Tesis, por permitirnos expresar nuestras ideas y propuestas para el beneficio de los mexicanos y por ser un ejemplo para la sociedad.

Gracias también por generar propuestas y proyectos de decreto relacionados a la informática que nuestro país está comenzando a exigir y por comprometerse por generar acciones que beneficien a nuestro país.

Ing. Noé Job Ruíz Vázquez

ÍNDICE

INTRODUCCIÓN.....	1
--------------------------	----------

CAPÍTULO 1

Delitos informáticos

1.1 Definición de delitos Informáticos.....	4
1.2 Quien comete los delitos.....	6
1.3 Delitos Informáticos en México	8
1.4 Casos registrados.....	15

CAPÍTULO 2

La legislación mexicana sobre delitos informáticos

2.1 Tipos de delitos informáticos contemplados en nuestra legislación.....	17
2.2 Quiénes son culpables de los Delitos Informáticos.....	19
2.3 Análisis de las sanciones de los delitos.....	20
2.4 Reformas al Código Penal Federal en materia de Delitos Informáticos publicadas en el Diario Oficial de la Federación el 17 de Mayo de 1999....	21

CAPÍTULO 3

Industria del software en México

3.1 La industria del software en México.....	26
3.2 Servicios de seguridad.....	31
3.3 Fraudes cometidos mediante manipulación de información privada...	34
3.4 Falsificaciones informáticas.....	37

CAPÍTULO 4

Leyes e instituciones que rigen los programas de cómputo en México

4.1 Ley federal de derechos de autor.....	41
4.2 Ley de propiedad industrial.....	44
4.3 Código penal federal.....	47
4.4 Comparativas entre criterios de los tribunales norteamericanos y mexicanos para resolver conflictos por violaciones de derechos de autor.....	51

CAPÍTULO 5

Análisis de un caso específico ante las leyes mexicanas

5.1 Detección del delito.....	54
5.2 Flujo de la aplicación de la ley vigente.....	55
5.3 Problemas encontrados durante la aplicación de la ley.....	55
5.4 Sanciones aplicadas y conclusión del caso.....	58

CAPÍTULO 6

Propuesta de reforma del Código Penal federal en materia de delitos informáticos

6.1 Propuesta a las reformas del Código Penal federal en materia de delitos informáticos.....	61
---	----

CONCLUSIONES.....	70
--------------------------	-----------

BIBLIOGRAFÍA.....	74
--------------------------	-----------

GLOSARIO.....	76
----------------------	-----------

ANEXOS

ANEXO 1.....	87
--------------	----

ANEXO 2.....	92
--------------	----

PRÓLOGO

En la actualidad, el progreso de los sistemas computacionales permite procesar y poner a disposición de la sociedad una cantidad creciente de información de todos los ámbitos del conocimiento, al alcance concreto de millones de interesados y de usuarios.

En los últimos años, las tecnologías de la Información y la comunicación han revolucionado la vida social en numerosos aspectos: científicos, comerciales, laborales, profesionales, escolares, e incluso han cambiado los hábitos de entretenimiento y de interrelación de las personas al interior de la vida familiar, por estas razones se dice que la informática compone un fenómeno científico-tecnológico en las sociedades modernas.

Ciertamente resulta imposible que el Derecho vaya a la par que la Tecnología, regulando ipso facto cuanto fenómeno o conducta lícita o ilícita infiere en el ámbito jurídico, empezando porque es evidente que estos fenómenos y/o conductas tienen que manifestarse primero, ya que las leyes no pueden regular lo que aun no existe.

Si a esto le sumamos el carácter formal, escrito de nuestro sistema jurídico, las particularidades del proceso legislativo, la necesidad de que personas con formación de abogados comprendan lo necesario sobre tópicos técnicos y tecnológicos y las injerencias de intereses políticos, resulta que el Derecho y en especial, el Derecho Mexicano en cuanto a la legislación informática que es el que nos ocupa e interesa en esta tesis, se ha quedado por mucho rezagado en la regulación de una materia que lo ha rebasado y que exige atención inmediata y efectiva.

Con todo ello, se ha llevado esfuerzos mediante propuestas al Congreso de la Unión por legislar en la materia y algunos han fructificado.

En las siguientes líneas trataremos de dar un panorama general sobre la situación actual de la legislación informática en México, en especial nos enfocaremos a nuestro Código Penal Federal.

Para hacerlo de una manera ordenada, abarcaremos primero la definición de delito informático, la comparación de nuestra legislación informática con la de otros países para luego enfocarnos en nuestra legislación Mexicana.

Después, nos adentraremos en la situación de la legislación mexicana en referencia a los delitos informáticos, la industria del software en México, aquí se hablarán de los diferentes tipos de fraudes y la manipulación dolosa que ocurre cuando se comete un delito informático, así como algunas modalidades de delitos informáticos.

Tocaremos nuestra legislación informática en cuanto a nuestras leyes e instituciones que rigen lo referente a los delitos informáticos, como la Ley de Derechos de Autor, La ley de Propiedad Industrial y el mismo Código Penal Federal.

Así mismo, daremos algún ejemplo de un delito informático ocurrido en nuestro país y el proceso legal que se llevo a cabo para demostrar las carencias que nuestras leyes acusan, para finalmente presentar nuestra propuesta de reforma de algunos artículos del Código Penal Federal para la solución de los delitos informáticos.

INTRODUCCIÓN

El presente trabajo muestra un estudio detallado sobre los diferentes delitos que sufre la informática día con día, también se puede observar que es lo que se ha hecho y lo que se propone hacer para dar soluciones más acertadas y convincentes. Creemos que es necesario mejorar el mundo informático en beneficio de la sociedad.

Con el surgimiento y el desarrollo acelerado de la informática se han logrado muchos avances en distintos campos, principalmente en las últimas décadas. La enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, el uso de la misma es un instrumento que facilita a la sociedad su desarrollo económico, cultural y el crecimiento de la tecnología que es de gran importancia para el crecimiento de nuestro país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, etc. son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

En México, la Ley de Información Estadística y Geográfica, define en su artículo tercero a la informática, como la tecnología para el tratamiento sistemático y racional de información mediante el procesamiento electrónico de datos.

El avance logrado en los últimos años en este sector, ha permitido que un creciente número de personas tengan acceso a esta tecnología y la utilicen cotidianamente para realizar actividades de muy diversa índole, como las educativas, culturales, comerciales, industriales, financieras o de comunicación, entre muchas otras. Hoy en día tiene tal importancia, que muchas de esas actividades no podrían realizarse sin el uso de equipos y sistemas informáticos.

Junto a este importante avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica, «delitos informáticos».

Estas nuevas formas de conducta antisocial que han hecho de los equipos y sistemas informáticos instrumentos para delinquir. Adicionalmente, se presentan conductas en las que dichos equipos o sistemas constituyen el objeto o fin en sí mismo de la infracción.

Dentro de las conductas ilícitas más comunes que constituyen los llamados por la doctrina jurídica como "delitos informáticos", se encuentran: el acceso no autorizado a computadoras o sistemas electrónicos, la destrucción o alteración de información, el sabotaje por computadora, la interceptación de correo electrónico, el fraude electrónico y la transferencia ilícita de fondos.

En el contexto internacional, la Organización de las Naciones Unidas ha reconocido que los delitos por computadora constituyen un grave problema, ya que las leyes, los sistemas de impartición de justicia y la cooperación internacional no se han adecuado a los cambios tecnológicos. La propia Organización instó a los Estados miembros a intensificar sus esfuerzos para combatir este tipo de conductas, entre otras medidas, mediante la creación de

nuevos tipos penales y procedimientos de investigación. Para hacer frente a estas nuevas y sofisticadas formas de actividad criminal.

Países como Alemania, Austria y Francia han optado por crear una ley específica para combatir a los delitos informáticos, en tanto que otros países como Argentina, España y Estados Unidos de América, han optado por incluirlos en sus códigos penales.

En Nuestro país, el Estado mexicano está obligado a proteger los bienes jurídicos de los sectores que utilizan la informática como instrumento de desarrollo, por ello, requiere de un marco jurídico acorde al avance tecnológico.

Algunos estados de la República, conscientes de la necesidad de legislar en esta materia han adoptado en sus ordenamientos penales normas tendientes a la protección de la información; tal es el caso de Sinaloa, que tipifica al delito informático, o Morelos y Tabasco, que protegen la información mediante la tipificación de la violación a la intimidad personal.

La inexistencia a nivel federal de tipos penales exactamente aplicables a esas conductas ha dado lugar a que sus autores queden impunes, por lo que es imperativo prever en la ley estas nuevas formas de delincuencia.

La magnitud de los daños ocasionados por estas conductas depende de la información que se vulnere, al grado que puede tener un fuerte impacto en el desarrollo de la economía, en la seguridad nacional o en las relaciones comerciales.

Es necesario proteger la privacidad e integridad de la información contenida en sistemas y equipos de cómputo, de almacenamiento o procesamiento de información, por ello debe sancionarse a las personas que sin derecho, acceden a los equipos y sistemas de terceras personas para vulnerar la privacidad de la información, o dañarla, alterarla o provocar su pérdida.

Singapur, por ejemplo, enmendó recientemente su Ley sobre el Uso Indebido de las Computadoras. Ahora son más severos los castigos impuestos a todo el que interfiera con las "computadoras protegidas" --es decir, las que están conectadas con la seguridad nacional, la banca, las finanzas y los servicios públicos y de urgencia-- así como a los transgresores por entrada, modificación, uso o interceptación de material computadorizado sin autorización.

Hay países que cuentan con grupos especializados en seguir la pista a los delincuentes cibernéticos. Uno de los más antiguos es la Oficina de Investigaciones Especiales de la Fuerza Aérea de los Estados Unidos, creada en 1978. Otro es el de Investigadores de la Internet, de Australia, integrado por oficiales de la ley y peritos con avanzados conocimientos de informática. El grupo australiano recoge pruebas y las pasa a las agencias gubernamentales de represión pertinentes en el estado donde se originó el delito.

Pese a estos y otros esfuerzos, las autoridades aún afrontan graves problemas en materia de informática. El principal de ellos es la facilidad con que se traspasan las fronteras, por lo que la investigación, enjuiciamiento y condena de los transgresores se convierte en un dolor de cabeza jurisdiccional y jurídico. Además, una vez capturados, los oficiales tienen que escoger entre extraditarlos

para que se les siga juicio en otro lugar o transferir las pruebas --y a veces los testigos-- al lugar donde se cometieron los delitos.

Nuestra legislación

La secretaria de seguridad Pública encargada de los delitos informáticos ha creado la Policía Cibernética (a quien compete este tema), desafortunadamente solo podemos acceder la información que publican en su página en Internet donde no hay información de los casos que han registrado ni de los detenidos. Sin embargo, un estudio realizado bajo los auspicios de la Academia Mexicana de Derecho Informático, A.C., ha revelado cifras alarmantes: más de 843 sitios mexicanos han sido hackeados durante el último año y medio principalmente. Redondeando los números, tenemos que cada día más de 1.5 sitios mexicanos (o más bien dicho, el servidor en que éste se aloja) son penetrados y modificados por delincuentes cibernéticos

Las iniciativas que se presentan a nuestra Soberanía por parte de los senadores proponen adicionar un capítulo al Código Penal para sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad, con el propósito de conocer, copiar, modificar o provocar la pérdida de información que contengan.

Asimismo se propone establecer una pena mayor cuando las conductas son cometidas en agravio del Estado. pues la utilización de sistemas de cómputo, computadoras, bases de datos y programas Informáticos es cada vez mayor, como lo es su regulación por las leyes federales; tal es el caso de la Ley de Información Estadística y Geográfica, Ley del Mercado de Valores, Ley que Establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública, y Ley Federal para el Control de Precursores Químicos, Productos Químicos Esenciales y Máquinas para Elaborar Cápsulas, Tabletas o Comprimidos, entre otras.

Finalmente, se propone agravar las sanciones previstas para los tipos penales antes descritos, cuando con la comisión de dichos ilícitos se obtenga un provecho propio o ajeno.

Entrar a un servidor sin autorización para modificar, destruir, provocar la pérdida, conocer o copiar información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad es un delito. La práctica conocida como "defacement", desfiguración o cibergrafitti coincide perfectamente con este tipo penal (Art. 211 bis 1, Código Penal Federal).

La legislación mexicana en materia de delitos informáticos no es perfecta, tiene muchas carencias, es importante hacer algunos cambios que garanticen la estabilidad y seguridad de la información.

Por lo tanto es necesario hacer un estudio más detallado sobre estos problemas con la finalidad que la mayoría de la sociedad este consciente de lo que está pasando y de lo que se está tratando de hacer, que se conozcan los delitos informáticos y los daños que pueden causar.

CAPÍTULO 1

Delitos informáticos

1.1 Definición de delitos Informáticos

“Expresándonos en términos no legales, al hablar de delitos informáticos nos referimos a aquellas conductas que teniendo como instrumento o fin computadoras u otros bienes informáticos, lesionan o dañan bienes, intereses o derechos de personas físicas o morales”.¹

En términos jurídicos, para que exista delito es necesario un acto u omisión que sancionen las leyes penales, porque una de las características indispensables del delito es la tipicidad, es decir, que la conducta esté descrita en un tipo penal, en una ley penal, además de ser antijurídica, culpable y punible.

Los principales “delitos informáticos” son:

- 1.- Fraude mediante el uso de la computadora y la manipulación de la información que éstas contienen. (Técnica de salami u otras).
- 2.- Acceso no autorizado a sistemas o servicios. (Caballo de Troya, backdoors, etc.)
- 3.- Reproducción no autorizada de programas informáticos.
- 4.- Uso no autorizado de programas y de datos.
- 5.- Intervención de correo electrónico.
- 6.- Obtención de información que pasa por el medio (sniffer).

Analicemos uno por uno según la ley vigente en México:

1. Fraude mediante el uso de la computadora y la manipulación de la información que éstas contienen. (Técnica de salami u otras).-

El artículo 230 y 231 del código penal disponen: a quien: ... XIV. Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución...”

2. Acceso no autorizado a sistemas o servicios y destrucción de programas o datos.- Ésta conducta se encuentra regulada en los artículos 211 bis 1 a 211 bis 7, que determinan en resumen lo siguiente:

CONDUCTA	PENA
<p>Modificar, destruir o provocar pérdida de información contenida en sistemas o equipos informáticos protegidos sin autorización.</p> <p>Si se trata de sistemas o equipos del Estado.</p> <p>Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero</p>	<p>6 meses a dos años prisión y de 100 a 300 días multa</p> <p>1 a 4 años y 200 a 600 días multa</p> <p>6 meses a 4 años prisión y 100 a 600 días multa</p>
<p>Conocer o copiar información contenida en sistemas o equipos informáticos protegidos sin autorización</p> <p>Si se trata de sistemas o equipos del Estado.</p> <p>Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero.</p>	<p>3 meses a 1 año prisión y 50 a 150 días multa</p> <p>6 meses a 2 años prisión y 100 a 300 días multa</p> <p>3 meses a 2 años prisión y 50 a 300 días multa</p>
<p>Modificar, destruir o provocar pérdida de información contenida en sistemas o equipos informáticos cuando se tenga autorización para el acceso.</p> <p>Si se trata de sistemas o equipos del Estado.</p> <p>Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero.</p>	<p>2 a 8 años prisión y 300 a 900 días multa</p> <p>6 meses a 4 años prisión y 100 a 600 días multa</p>
<p>Conocer o copiar información contenida en sistemas o equipos informáticos cuando se tenga autorización para el acceso.</p> <p>Si se trata de sistemas o equipos del Estado.</p> <p>Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero.</p>	<p>1 a 4 años prisión y 150 a 450 días multa</p> <p>3 meses a 2 años prisión y 50 a 300 días multa</p>

Como se observa en el cuadro anterior, se puede notar cuales son las penas que se aplican a cada una de las violaciones a la ley con respecto a la información. De acuerdo con esto se especifica también que: las penas se incrementarán en una mitad cuando las conductas se realicen por empleados del sistema financiero y se incrementarán hasta en una mitad cuando la información obtenida se realice en provecho.

3. Reproducción no autorizada de programas informáticos.- Regulada en la Ley Federal del Derecho de Autor (desarrollada en capítulo 4 del presente trabajo). La Ley amplía la protección a los programas, autoriza al usuario legítimo a hacer las copias que le permita la licencia, o bien, una sola que sea indispensable para la utilización del programa o sea destinada exclusivamente como resguardo. El autor tiene el derecho de autorizar o prohibir además de la reproducción, la traducción, adaptación, arreglo o cualquier modificación al programa o reproducción del resultante, la distribución, la decompilación (proceso para revertir la ingeniería del programa) y el desembalaje.

4. Uso no autorizado de programas y de datos.- Además de las disposiciones relacionadas en párrafos precedentes sobre el uso no autorizado de programas, con respecto a los datos, la Ley Federal del Derecho de Autor, en sus artículos 107 al 110, protege como compilaciones a las bases de datos legibles por medio de máquinas que por razones de disposición de su contenido constituyan obras intelectuales, otorgándole a su organizador el uso exclusivo por cinco años; asimismo, exceptuando las investigaciones de autoridades, la información privada de las personas contenida en bases de datos no podrá ser divulgada, transmitida ni reproducida salvo con el consentimiento de la persona de que se trate.

5. Intervención de correo electrónico.- Éste delito, que atenta contra la privacidad como derecho fundamental de las personas, se equipara con el de violación de correspondencia que sanciona tanto en el Código Penal Federal, (art.173) como

en el local del D.F. (art. 333) al que abra o intercepte una comunicación escrita que no esté dirigida a él. Sin embargo, en estricto sentido esto aplica para la correspondencia postal solamente, por lo que en la Iniciativa de reformas y adiciones sobre diversas disposiciones del Código Penal para el Distrito federal en materia del fuero común y para toda la República en materia del fuero federal del 22 de marzo del 2000, se proponía una redacción que incluyera el acceso de las comunicaciones a través de medios electrónicos, electromagnéticos u ópticos.

Además, el artículo 167 fr.VI del Código Penal Federal sanciona con uno a cinco años de prisión y 100 a 10000 días de multa al que dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

6. Obtención de información que pasa por el medio (sniffer).- Este tipo de conductas, que se refiere a interceptar datos que las personas envían a través de la red (cuando hacen una compra por internet, por ejemplo, enviando datos personales y de crédito) se tipifican en el artículo 167 Fr. VI del Código Penal Federal.

Se han descrito cada uno de los delitos informáticos más frecuentes en la actualidad, por tal motivo podemos ver que la gran mayoría de la información de cada uno de nosotros está expuesta y que en cualquier momento puede sufrir alteraciones o pérdidas parciales o totales.

Por otro lado los delitos informáticos no se originan por si solos, existen muchas personas que están tratando de manipular información principalmente ajena. Para darnos una idea de los autores de este tipo de conductas bien podemos citar algunas definiciones que nos indiquen bajo que características operan los infractores, sus perfiles psicológicos y las razones por las que efectúan estos actos.

1.2 Quién comete los delitos

Los delitos informáticos son provocados por personas que no son tan comunes, es decir, que tienen amplios conocimientos sobre la informática y sobre ciertos métodos para poder interferir en información ajena. A continuación se muestran algunas definiciones que se han dado a este tipo de personas:

El criminólogo estadounidense Edwin Sutherland dice que: "El sujeto activo del delito informático 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".

Esta definición nos da la idea de que los sujetos no tienen problemas económicos y tienen una preparación muy elevada y quizás algún título de estudios universitarios, esta misma definición también nos deja pensar que los sujetos bien pueden realizar estos actos por el reto de "Poder Hacerlo", es evidente entonces que cuando estos autores realizan un acto de robo por botín económico es común que sea por asociaciones delictivas con personas que en efecto si carezcan de algún elemento dado en la definición.

Este trabajo no tiene el alcance de comprobar dicha idea, solo conservaremos el hecho de que los daños económicos son altísimos; además 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".

Existe otro punto importante sobre este nivel de criminalidad, que 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.

Según el mexicano Julio Tellez Valdez, "los delincuentes informáticos son un determinado número de personas con ciertos conocimientos (en este caso técnicos) los que pueden llegar a cometerlas".²

Estas acciones son principalmente ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

Entre los principales infractores tenemos:

a. Los hackers. Los jóvenes que se pasan horas frente a la computadora intentando husmear, penetrar y dañar computadoras ajenas, son sin duda los principales responsables.

b. Las universidades. Las universidades, a través de sus directivos, suelen ser las principales cómplices de los hackers por varias razones, entre ellas:

- No fomentan valores éticos en sus estudiantes, principalmente de las carreras técnicas o ingenierías.

- En ocasiones, el conocimiento técnico de los alumnos sobrepasa por mucho el de sus profesores, lo cual provoca en el estudiante un sentido de frustración educativa, lo que lo conduce a buscar o "aprender" por sus propios medios.

- Muy probablemente, una buena parte de las penetraciones o delitos informáticos los perpetran desde la escuela y/o con equipo informático de la propia universidad.

- Lo más importante, cuando la universidad se da cuenta de que uno de sus alumnos ha atacado/penetrado su propio servidor o uno ajeno, se convierten en cómplices al no dar parte a la autoridad, con tal de que la sociedad no se entere de que la universidad está preparando (y encubriendo) a delincuentes (hackers), en lugar de profesionistas o empresarios.

- Por las razones anteriores, no es de sorprenderse que la mayoría de los hackers tienen entre 16 y 24 años aproximadamente. En otras palabras, todos

son estudiantes o desarrollan el máximo de sus capacidades durante su etapa de estudios de bachillerato o profesional.

c. Los proveedores de hosting son culpables porque, a pesar de estar obligados por ley a usar mecanismos de seguridad para proteger la información de sus clientes, no lo hacen. La seguridad no suele ser uno de sus "argumentos de venta", ni parte del valor agregado que ofrecen a sus clientes.

d. Los fabricantes de software. Las estadísticas nos permiten observar que más del 60% de los servidores hackeados corren bajo el Sistema Operativo de Windows. Noticias recientes han anunciado que "usar servidores web IIS tiene un alto costo. Nimda ha mostrado nuevamente el alto riesgo de usar IIS y el esfuerzo involucrado en mantenerse al día con tantos patches de seguridad de Microsoft".

Veamos ahora algunos delitos ocurridos en nuestro país, para evidenciar la dificultad de su prevención por falta de bases legales.

1.3 Delitos Informáticos en México

Los delitos informáticos en México, están directamente ligados a fenómenos sociales y políticos que se desarrollan cada año, además de los clásicos delitos que buscan como fin la obtención de los bienes económicos de los afectados, las víctimas buscan reducir los ilícitos por cualquier medio, ya sea pagando seguridad a empresas privadas o bien comprando caro software y hardware de seguridad.

Este tipo de eventos son muy comunes en la actualidad, debido a esto se ha despertado un gran interés a nivel mundial por tratar de solucionar esto. Es necesario conocer un poco más de lo que pasa con estos problemas. Los siguientes recuadros nos muestran información sobre los delitos informáticos.

FUENTE	NOTA
<p>Estudio de Percepción sobre Seguridad en Informática México 2007 Fuente: JFS Autor: JFS</p>	<p>Las personas que utilizan soluciones informáticas están más sensibles y han tomado mayor conciencia respecto de la seguridad en informática, como parte de su vida cotidiana.</p> <p>Aspectos como políticas, procedimientos, privacidad y manejo de identidad, están más presentes que antes, en la mente tanto de los usuarios comunes como la de los especialistas en Sistemas.</p> <p>Creció significativamente la preocupación por la seguridad en transacciones en línea y el uso de banca electrónica.</p> <p>Los usuarios solicitan a los proveedores de tecnología mayor difusión y mejores productos.</p> <p>Joint Future Systems y La Cámara Nacional de la Industria, Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) presentaron el tercer Estudio de Percepción sobre Seguridad en Informática en México, con el propósito de generar estadísticas del entorno de nuestro país en la materia y de contar con parámetros que permitan comparar las variaciones (avances o rezagos percibidos por los entrevistados), desde el año 2004 a la fecha.</p> <p>El estudio fue realizado por Joint Future Systems y contó con el apoyo de la</p>

Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la Información (CANIETI), la Asociación Latinoamericana de Profesionales en Seguridad Informática, A.C. (ALAPSI), la Cámara Mexicano-Alemana de Comercio e Industria, A.C. (CAMEXA), Computer Associates México, la International Association of Financial Crimes Investigators (IAFCI) Capítulo México, Intel México, QoS Labs de México, Sun Microsystems de México, Técnica Comercial Vilsa, y Tralix.

Los alcances del estudio fueron los siguientes:

1. Conocer los niveles de conciencia que se tienen en las empresas mexicanas, acerca de la Seguridad en Informática.
2. Detectar el grado de conocimiento que se tiene con respecto a los diferentes ámbitos de la Seguridad en Informática (Seguridad Física, Seguridad frente a Agresores Externos y Seguridad frente a Agresores Internos).
3. Identificar aquellos elementos relacionados con la Seguridad en Informática, que son considerados más importantes por los responsables de su implementación dentro de sus organizaciones.+
4. Conocer la percepción que tienen algunos expertos en la materia, respecto del grado de conocimientos y penetración de esta cultura entre las organizaciones de nuestro país.
5. Conocer cuáles normas y regulaciones relacionadas con seguridad en informática están presentes en la mente de los usuarios en general.
6. Contar con una herramienta que permita fomentar la conciencia y desmitificación de la Seguridad en Informática, apoyando las labores educativas del país a nivel corporativo e institucional.
7. Crear un entorno que impulse el crecimiento del mercado de productos y servicios de seguridad, así como la correcta implementación de soluciones especializadas.

Algunos de los resultados más interesantes del estudio son los siguientes:

El 18.7% de todos los entrevistados mencionaron que lo que más les preocupa respecto de la seguridad en informática, son los virus, seguido de la pérdida de información, 10.3%, la invasión a su privacidad 9.3% y el uso de comercio y banca electrónica, con el 8.8%.

El 26.8% de todos los respondientes, al preguntarles “Qué es para usted la seguridad en informática”, consideraron que, en sí, este concepto está relacionado directamente con la privacidad y confidencialidad, así como con la transmisión segura de datos (20.4%).

Al comparar con años anteriores, es claro que los virus siguen siendo la principal preocupación para el usuario, así como la posibilidad de perder información. Sin embargo, llama la atención el aumento importante en la preocupación por la invasión a la privacidad. Denota que los usuarios están cada vez más conscientes del hecho que la seguridad en informática está cada vez más ligada a elementos personales, y que el comprometer los datos privados, tanto de una empresa como de una persona, es un riesgo sumamente importante.

Si bien las medidas principales para enfrentar los retos de seguridad en informática mencionadas siguen siendo antivirus, firewalls y medidas de identificación de usuarios, llama poderosamente la atención que el 13.5% de todos los entrevistados mencionaron las políticas y procedimientos adecuados, como uno de los aspectos primordiales y, entre usuarios que trabajan en áreas de informática, el 33.5% están conscientes de la importancia de este rubro.

Hablando específicamente de mecanismos para el manejo de identidad, fue interesante ver que muchos usuarios (27.6%) mencionaron algún tipo de biométrico (huella digital, reconocimiento de iris, reconocimiento de voz, etc.), aunque el uso de claves (passwords) fue el rubro más mencionado, con el 46.2%, es claro que los usuarios están percibiendo las posibilidades de los dispositivos biométricos y su lugar dentro del mundo de seguridad en informática.

Existe un alto grado de desconocimiento de las normas y regulaciones relacionadas con seguridad en informática. De hecho, el 85.9% de todos los usuarios y el 68.3% de usuarios que trabajan en áreas de informática, no pudieron mencionar ninguna de ellas.

El 22.8% de todos los usuarios pide a los proveedores de tecnología mayor difusión de conocimiento y, en muchos casos, se hace el comentario de que los proveedores deben poner a disposición de los usuarios información que sea fácil de entender. El 10.1% pidió a los proveedores de tecnología que tengan mejores productos, el 7.5% mencionó que se requieren precios más accesibles y el 6.7%

expresó que se requiere mayor honestidad y compromiso con los usuarios.

El 6.3% mencionó que le gustaría saber más acerca de políticas y procedimientos. Comparando con años anteriores, es un avance importante, e indica que la cultura en seguridad en informática está aumentando en nuestro país.

Los usuarios quieren más información, de cualquier fuente. El 31.1% de los entrevistados mencionó que les gustaría conocer más acerca de todos los aspectos de seguridad y el 15.3% especificó que le gustaría estar al tanto de novedades y actualizaciones en el tema.

El reto es claro. Si bien se perciben avances en la cultura sobre seguridad informática en general, se nota claramente una falta de difusión en este sentido, principalmente en algunas áreas que presentan huecos importantes. La preocupación en aspectos como virus, spyware y firewalls, muestra que los usuarios siguen considerando que gran parte del problema se resuelve con soluciones tecnológicas, haciendo a un lado la responsabilidad personal que tiene cada usuario de llevar a cabo las prácticas adecuadas. Esta difusión y adquisición de conocimiento no sólo debe recaer en los proveedores de tecnología, sino en las áreas respectivas

Empresas y asociaciones interesadas en aumentar la cultura informática en nuestro país, deben buscar e implementar medios para la difusión clara y concreta de la información respecto de la problemática y las soluciones que todos los usuarios deben conocer, así como medidas para que ésta información se pueda obtener de manera continua y actualizada de la informática y, de manera importante, en cada usuario.

Es un hecho que el manejo de identidad y la privacidad cobra cada vez más importancia en el mundo actual. Este estudio refleja que si bien la consciencia en este sentido empieza a presentar una tendencia creciente en México, hay mucho por hacer. Empresas de tecnología, asociaciones, gobierno, instituciones educativas y los usuarios de tecnología, en primer término, todos debemos trabajar para que México sea un país seguro en este sentido y, quizás aún más importante, que sea percibido como tal por otros países.

FUENTE

NOTA

Regulación a hackers **Fuente: NOTIMEX** **Autor: Agencia**

Expertos coinciden en la urgencia de contar con una legislación que garantice la seguridad informática.

CIUDAD DE MÉXICO, México, ene. 2003.- En México no existe el conocimiento técnico ni legal para castigar a los hackers, por lo que es urgente una legislación que regule este tipo de prácticas irregulares, aseguró el consultor en seguridad informática, Andrés Velásquez.

En entrevista con Notimex, recordó que existen países como Estados Unidos o China donde hay un control y una regulación rígida hacia los hackers, e incluso dicha práctica se condena con pena de muerte en la citada nación oriental.

Explicó que en el caso de México, el hacking se considera en el aspecto legal como robo de información y entra en el rubro de propiedad intelectual, derechos de autor y allanamiento.

A pesar de la diversidad de definiciones, un hacker es un individuo capaz de establecer una comunicación entre su computadora y la de otro usuario, usualmente en contra de la voluntad de este último, y para lo cual es necesario que ambas máquinas estén conectadas a Internet.

Los daños causados van desde una simple incursión, hasta el mal uso, robo o pérdida total de información.

Para el especialista, "desgraciadamente no hay una legislación ni el conocimiento total, ni técnico ni legal, para regular esta actividad" en México.

Dijo que países como Colombia ya tienen un área de gobierno que regula el comercio electrónico a nivel nacional por medio de certificados digitales.

No obstante, manifestó, en México ya se han dado pasos en este aspecto, "por lo menos ya hay algunas leyes en cuestión de seguridad informática, como la propuesta de certificados digitales y transacciones validadas por una entidad certificadora".

El también miembro de la Asociación Latinoamericana de Profesionales de la Seguridad Informática (Alapsi) comentó que las empresas deben crear conciencia

	<p>sobre seguridad informática y preguntarse cuánto vale su activo más importante que es la información.</p> <p>"Las empresas suben a la red información muy importante como contratos, si estos documentos caen en otras manos, alguien puede copiar información o firmas y ocasionar problemas".</p>
FUENTE	NOTA
<p>Combate México "ciberataques" Fuente: EL UNIVERSAL Autor: Nelly Acosta Vázquez</p>	<p>Después de la excesiva popularidad que se le hizo al virus Blaster, muchos se preguntan si México está preparado, legal y técnicamente, para enfrentar ataques cibernéticos. La respuesta aún es ambigua, sobre todo porque no existe una ley específica que responda a este tipo de problemas, además de que aún son muy pocos los expertos que están involucrados en este campo.</p> <p>"Pero no significa que estemos con los brazos cruzados", dijo Andrés Velázquez, consultor independiente en seguridad, quien parte del hecho de que ningún sistema, base de datos, computadora o vacuna está exento de ser atacado, aunque insista en presumir lo contrario.</p> <p>"Lo único seguro es una PC apagada, desconectada, guardada dentro de una caja de seguridad, rodeada de gas venenoso y resguardada por un equipo de guaruras. Y quizás también corra el riesgo de ser robada", indica el consultor, bromeando y acentuando que las promesas de protección absoluta de la mercadotecnia informática no son certeras.</p> <p>Los errores de ley.</p> <p>Es Jorge Navarro, maestro en derecho informático del ITAM y experto en delitos cibernéticos en México, quien indica que el Código Penal del país ha provocado que el rastreo y penalización de criminales cibernéticos sea aún una labor difícil.</p> <p>"Calculo que 40 por ciento de los códigos penales estatales carecen de artículos o menciones a este tipo de delitos (14 estados), y los que sí lo incluyen, no cuentan con la suficiente claridad de redacción y de términos que permitan aplicarla con prontitud", dijo Navarro.</p> <p>El experto en informática señala que sólo el estado de Sinaloa cuenta dentro de su código penal definiciones de los términos de seguridad informática, ciberdelito o hacker , pero aún así, son confusos.</p> <p>"El problema es que dichas leyes no fueron elaboradas por expertos en informática y por tanto, regulan algo que aún se desconoce y que en la práctica resulta totalmente contradictorio", agregó Jorge Navarro.</p> <p>Añade: "Los códigos del estado de México y del Distrito Federal son la prueba de que en este tema están regidos por la inconstitucionalidad, olvidando que los delitos digitales son un problema federal que requiere de esfuerzos conjuntos".</p> <p>De igual manera, existe la falta de regulaciones internacionales que indiquen cómo castigar y rastrear ataques multiregión: que el hacker que se encuentra en Estados Unidos, por ejemplo, ataque un servidor que está en China y que afectó a ciudadanos en París.</p> <p>Solución en manos de DC México (Delitos Cibernéticos México)</p> <p>Para consuelo de la industria mexicana de TI y de los usuarios, ya existe el Grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos (DC México), que trabaja en la creación de un marco jurídico y consultoría especializadas en el tema, hace labor de prevención e investigación, mide los valores, políticas de uso y regulaciones del web, desarrolla un concepto nacional de e-seguridad , crea programas de contingencia informática, además de sistemas de capacitación para entidades gubernamentales como la AFI.</p> <p>DC cuenta con el apoyo de la Secretaría de Economía, la Policía Cibernética y la Policía Federal Preventiva (PFP), y cuando detecta a algún delincuente cibernético (que para muchos es sinónimo de hacker), lo denuncia ante la Policía Federal Preventiva e inicia una averiguación para levantar el castigo correspondiente.</p> <p>"Con esto, nos enfrentamos a otro problema: las evidencias digitales. Son pocos jueces los que reconocen como prueba un disco duro, en donde está toda la bitácora del hacker, o un mensaje electrónico con señales de amenaza", explicó Velázquez.</p> <p>En promedio, México castiga con multas de 300 días y entre seis meses y dos años</p>

de cárcel a los desarrolladores de virus y con tres meses y un año de prisión, así como con 50 a 150 días de multa, a los hackers.

FUENTE

NOTA

Persigue Interpol al Ejército Popular Revolucionario por la red

Fuente: Excélsior

Autor: Lemic Madrid

En lo que va de 2007, la mayoría de los ataques cibernéticos de tipo phishing siguen siendo hacia instituciones financieras, como Banamex, Scotiabank y Santander, aunque las medidas de seguridad que han implementado dichas instituciones han ayudado a disminuir los casos y a usuarios afectados. Sin embargo, "aún así no es suficiente porque los intrusos están sofisticando sus técnicas para poder seguir defraudando", dijo Juan Carlos Guel, jefe del departamento de seguridad en Cómputo, de la Universidad Nacional Autónoma de México (UNAM-CERT).

Entrevistado en el marco del evento Seguridad, Compliance y Marcos Regulatorios, que llevó a cabo la empresa Cisco, el especialista señaló que en internet todos los usuarios e instituciones están expuestas a sufrir ataques a la seguridad informática como la negación de servicios, virus, troyanos y phishing.

Indicó que se observan casos de phishing dirigidos a Telcel y Boletazo, entre otras instituciones mexicanas. Mediante correos electrónicos falsos, con frases como: "Eres ganador del sistema Boletazo", los cibercriminales instalan malware o códigos maliciosos en las computadoras, combinando técnicas de intrusión.

Dijo que uno de los casos más recientes es el de un correo, el cual aparentemente está avalado por Profeco para bajar un estudio sobre gasolineras, pero cuando el internauta baja el archivo adjunto se instala un troyano y se realiza el fraude. También hay correos que dicen: "Te ha llegado una tarjeta de felicitación", y cuando se da acceso a la liga de internet se encuentra con un malware.

Aunque el entrevistado indicó que no hay un estimado real en cuanto a los montos de los fraudes y el número de usuarios defraudados, por los casos que han investigado dijo que los ilícitos varían desde "cinco mil pesos, hasta empresas que les han vaciado las cuentas y los dejan sin nómina".

En su ponencia, Guel explicó que los intrusos aprovechan las vulnerabilidades del "día cero" (si conocen el problema antes de que exista una solución, lo aprovechan para hacer ataques), implementan códigos maliciosos, virus, troyanos, entre otros. Tienen la capacidad para deshabilitar antivirus, esconden los procesos, crean virus que son invisibles para los usuarios finales e inclusive para los fabricantes. Intentan ataques masivos, usan códigos móviles o sobre los navegadores de internet, usan correos electrónicos y técnicas de ingeniería como el phishing y el spam.

En lo que va del año, a través de RedUnam, han descubierto cerca de 600 códigos maliciosos y muchos de ellos no son detectados por los sistemas de seguridad.

También han detectado pharming a través de malware. Mediante archivos ejecutables que se instalan en el equipo, cuando el usuario intenta abrir una página el sistema lo redirige a un sitio falso.

Otros ejemplos son software espías que se instalan dentro del equipo; software que permiten controlar las computadoras desde otros lugares y el vishing (ataques a Voz sobre IP), variante del phishing.

Por otra parte, el directivo destacó que los phishers ya están atacando los tokens o sistemas para autenticar el acceso, que en México se usa sobre todo para la banca en línea.

En 2006 fueron detectados 2 mil 50 casos de phishing que estaban afectando a instituciones mexicanas, 2% con dominios registrados.

Hasta el 30 de abril de 2007 se han registrado 589 casos de phishing que estaban afectando a instituciones mexicanas.

FUENTE	NOTA
<p>Bancos, objeto de los ataques Cibernéticos Fuente: El Universal Autor: Aída Ulloa</p>	<p>Durante el segundo semestre del 2006 se encontraron en México un total de 270 páginas fraudulentas según cifras de Mattica (laboratorio de cómputo forense), delito cibernético conocido como "phishing". De acuerdo con este estudio cuantitativo sobre el origen, número y tipo de phishing registrados en México, durante diciembre pasado se registró el mayor número de páginas web falsas superando incluso la cantidad detectada en todo el semestre.</p> <p>Andrés Velázquez, director de Investigaciones Digitales de Mattica, informa que aunque estos 270 phishing estén en español y navegando entre usuarios mexicanos, no necesariamente fueron creados en el país. De hecho, su origen –en origen de incidencia- resultó ser en su mayoría en Estados Unidos, Alemania, Rusia y Francia.</p> <p>Explicó que el phishing busca engañar al usuario para obtener de manera fraudulenta información sensible como contraseñas y detalles de tarjetas de crédito a través de un correo electrónico o página de Internet falso suplantando la identidad de alguna organización, comercio o institución financiera para que el usuario deposite su confianza en un sitio apócrifo, registre sus datos y así el delincuente suplante la identidad del usuario y robe su patrimonio en línea.</p> <p>Este tipo de robo de identidad es cada vez más popular por la facilidad con la que algunas personas divulgan información personal como números de tarjetas de crédito. Los ladrones de identidad también pueden obtener información de registros públicos para crear cuentas falsas a nombre de la víctima, arruinar su crédito o incluso impedir que la víctima acceda a sus cuentas propias.</p> <p>Se estima que entre mayo del 2004 y mayo del 2005, aproximadamente 1.2 millones de usuarios sufrieron pérdidas causadas por phishing. Se calcula que los negocios en Estados Unidos pierden un total de dos billones de dólares al año. En el Reino Unido, las pérdidas por fraude bancario vía web, en su mayoría phishing se duplicaron de 12.2 millones de libras a 23.3 millones de libras.</p> <p>Por su parte, Oscar Gutiérrez, director general de Mattica, comentó que algunos elementos para detectar un correo phishing son: Saludo genérico, link falso, solicitud de información personal y sentido de urgencia.</p> <p>Algunas recomendaciones para combatir el phishing son: Estar al tanto de la lista actualizada de phishing conocidos, contar con soluciones de detección de intrusos y programas antivirus instalados y actualizados, capacitar a los usuarios para que puedan reconocer los intentos de phishing., respetar y promover de forma masiva las medidas de seguridad que ofrecen los bancos e instituciones financieras durante las transacciones en línea y no prestar atención a ningún mensaje o correo electrónico de remitentes desconocidos y menos de instituciones financieras con el pretexto de actualizar los datos, ya que ningún banco envía por correo electrónico la actualización de su base de usuarios.</p> <p>Al continuar con las investigaciones sobre fraudes a cuentahabientes realizados a través de transferencias bancarias, fueron detenidas seis personas, una de ellas de origen argentino, relacionadas con movimientos ilícitos, cuyo monto asciende a 463 millones 500 mil pesos.</p> <p>Elementos de la Unidad Especializada en Delitos Cibernéticos, recién creada en esta administración, adscrita a la Segunda Sección del Estado Mayor Policial lograron el aseguramiento de Raúl Rodríguez Monte Agudo, Juan Hernández Pérez, Alma Brenda Acevedo Pérez, José Rubén Molina Martínez, Alejandro Morales Isidro y Ricardo Hugo Ramírez Romero, de 68, 50, 32, 52, 49 y 44 años de edad, respectivamente.</p> <p>Entre las víctimas de los detenidos se encuentran las empresas: Jhonson and Jhonson SA de CV, por un desvío de 129 millones 500 mil pesos, de los cuales, de acuerdo con autoridades bancarias, hasta el momento se han cobrado un millón de pesos.</p> <p>Asimismo, Universidad Tecnológica de México, Universidad Del Valle de México, Autotab SA de CV, Fresenius Kabim SA de CV, Hulera Automotriz SA de CV, Petronaval y Maple Urbanizadora SA de CV, entre otras.</p> <p>Cabe mencionar que los inculpados invirtieron en la compañía Cuenta Stanford Grupo México SA de CV, 350 millones de pesos, es decir, una parte de los recursos que obtuvieron ilícitamente.</p> <p>Las diligencias ministeriales indicaron que los implicados fueron contactados por Ricardo Hugo Ramírez Romero, pseudo abogado, quien fue reconocido como el autor que fraguó los fraudes cometidos.</p>

La manera de contactar a sus cómplices fue mediante la publicación de anuncios que aparecen en los diarios de circulación nacional, donde ofrecía préstamos y el único requisito era que tuvieran una cuenta bancaria.

Para convencer a los interesados, les ofreció a cambio el 10 por ciento de las cantidades que tenían que retirar de la sucursal acordada.

Dicho sujeto realizaba disposiciones en cuentas a través de transferencias, por lo que sus cómplices posteriormente acudían al banco y retiraban las sumas pactadas.

A su vez, Raúl Rodríguez, originario de Buenos Aires, Argentina, Alma Brenda Acevedo y Juan Hernández, Pérez fueron sorprendidos en Santander Serfín de la calle de Oslo, número 81, esquina avenida Félix Cuevas, colonia Del Valle Sur.

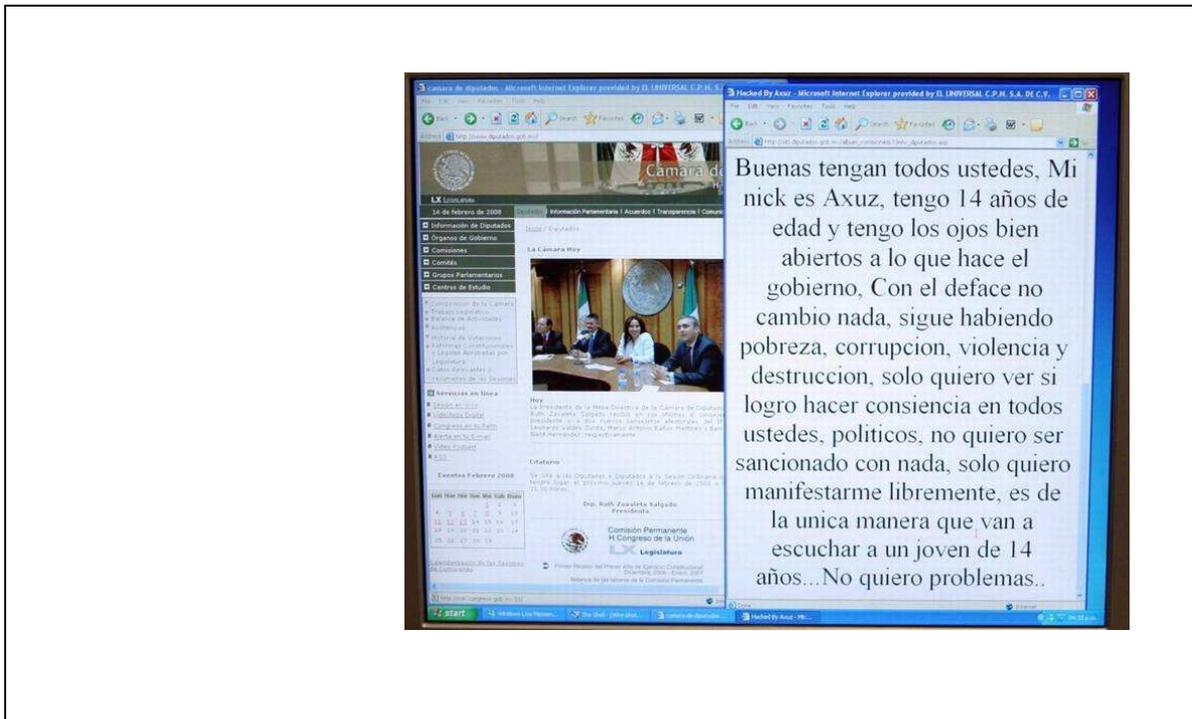
Ejecutivos bancarios detectaron que los 250 mil pesos que retiraron Raúl y Alma provenían de cuentas monitoreadas, relacionadas con movimientos ilícitos; en tanto, su cómplice Juan Hernández, quien los esperaba en la sala del banco, al ser investigado, se descubrió que obtuvo recursos de cuentahabientes por transferencias electrónicas que realizó en conjunto con Ricardo Hugo Ramírez.

Asimismo, las investigaciones revelaron que ese día también acudieron a la sucursal Santander Serfín ubicada en avenida Insurgentes Sur, número 1357, colonia Insurgentes Mixcoac, donde cambiaron dos cheques, uno por 50 mil y otros 100 mil pesos.

Paralelamente, José Rubén Molina y Alejandro Morales Isidro cobraron dos cheques por 150 mil pesos de otra sucursal del mismo banco, localizada en Paseo de la Reforma esquina Río Mississippi, colonia Juárez.

En las próximas horas Rodríguez Monte Agudo, Hernández Pérez, Acevedo Pérez, Molina Martínez, Morales Isidro y Ramírez Romero, serán puestos a disposición del juez penal en turno del Reclusorio Preventivo Norte, acusados de fraude.

FUENTE	NOTA
<p>ULTIMO CASO REGISTRADO EN MÉXICO</p> <p>Hackean sitio web de la H. Cámara de Diputados</p> <p>EL Universal</p> <p>Ciudad de México</p> <p>Jueves 14 de febrero de 2008</p> <p>Ricardo Gómez y Andrea Merlos</p>	<p>Un link de la página de internet de la Cámara de Diputados (www.diputados.gob.mx) se volvió loco: en lugar de divulgar información de las actividades de los legisladores, mostró un texto de repudio a la clase política.</p> <p>“Buenas tengan todos ustedes. Mi nick es Axuz, tengo 14 años de edad y tengo los ojos bien abiertos. Con el ace (sic) no cambié nada, sigue habiendo pobreza, corrupción, violencia, destrucción, sólo quiero ver si logro hacer conciencia (sic) en todos ustedes políticos, no quiero ser sancionado con nada, sólo quiero manifestarme libremente, es la única manera que van a escuchar a un joven de 14 años... No quiero problemas”, decía el texto.</p> <p>La violación a la página ocurrió a las 15:30 horas de ayer. “No fue un hackeo, la información está intacta, simplemente se cambió el index”, aseguró Miguel Ángel Vega, director General de Tecnologías de Información del Palacio Legislativo.</p> <p>Especialistas en informática de la Cámara de Diputados iniciaron una investigación para determinar si el atentado se dio dentro o fuera de San Lázaro, pues se conoció que la persona que cometió la violación usó claves que exclusivamente tiene personal interno.</p> <p>El funcionario rechazó que se haya tratado de un ataque masivo y dijo que no será necesaria la intervención de la Policía Cibernética, perteneciente a la Policía Federal Preventiva.</p> <p>Aseguró que a más tardar en una semana se tendrán datos fidedignos que permitan conocer de qué zona geográfica del país se violó la página web. Explicó que la alteración al portal sólo duró 15 minutos. Por lo pronto, dijo, se cambiarán las claves de acceso a la página de internet para evitar más ataques. Asimismo, reconoció que cada mes se registran diez mil intentos por hackear la página de la Cámara, sin éxito.</p>



Con respecto al cuadro, podemos notar que se ha tratado de solucionar la delincuencia informática, pero la sociedad sigue preocupada porque no ha desaparecido esta amenaza, exige seguridad.

Con una preocupación de prevención de la actividad de delitos informáticos, empieza a desarrollarse una conciencia sobre el público afectado que se informa y exige medidas que le garanticen seguridad por parte de sus gobernantes.

Toda la sociedad está expuesta a cualquier tipo de delincuencia informática, principalmente las empresas o agrupaciones que manejan una gran cantidad de información a través de la red (internet). Es indispensable que la sociedad no tenga este tipo de problemas y pueda realizar sus actividades cotidianas sin el temor de ser afectados posteriormente. Existen muchos casos de delitos informáticos que han sucedido y que de alguna manera todavía no hay una sanción que castigue adecuadamente dichos delitos.

1.4 Casos registrados

Cada año, cada día se tienen nuevos eventos que desatan investigaciones por parte de nuestra secretaría de seguridad pública, algunos de los casos jamás salen a luz por no convenir a las empresas afectadas, aquí presentamos algunos casos que están documentados en el periódico Excélsior.

Los delitos que se mencionan en el cuadro anterior, son algunos casos que muestran aun más la falta de leyes que castiguen más rigurosamente estos actos para que la seguridad de nuestra información sea garantizada.

Con estos elementos y definiciones expuestos en este capítulo así como las relaciones mundiales entorno a los cibercrimes, las leyes y las tendencias de otros países a renovar sus legislaciones, los casos de estos ilícitos presentados en los que no está claro el alcance de las leyes mexicanas, vamos a examinar lo

que en materia de delitos informáticos dictamina nuestra legislación, depositando principal atención en los puntos débiles que pueda tener y dando lugar al desarrollo del siguiente capítulo.

CAPÍTULO 2

La legislación mexicana sobre delitos informáticos

Después de haber conceptualizado lo que es un delito informático los legisladores encontraron que había varios delitos, así que los clasificaron, pero al igual que la definición de delito, la clasificación la han realizado varios autores exponiendo sus ideas sobre el porqué de esa clasificación, a continuación mencionaremos algunas clasificaciones.

2.1 Tipos de delitos informáticos contemplados en nuestra legislación

Julio Téllez Valdés clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio, o como fin u objetivo.

Como instrumento o medio: se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito. Algunos ejemplos son:

1. Falsificación de documentos vía computarizada (tarjetas de crédito).
2. Planeación o simulación de delitos convencionales (robos, homicidios).
3. Robo de tiempo de computadora.
4. Modificación de datos tanto de entrada como de salida.
5. Método del caballo de Troya, violación de un código para penetrar a un sistema con el fin de introducir instrucciones inapropiadas.
6. Técnica del Salami, desviación del destino de pequeñas cantidades de dinero hacia una cuenta bancaria fingida.
7. Alteración de funcionamiento de los sistemas.
8. Acceso a áreas informatizadas en forma no autorizada.

Como medio y objetivo: en esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

1. Programación de instrucciones que producen un bloqueo total al sistema.
2. Destrucción de programas por cualquier método.
3. Daño a la memoria.
4. atentado físico contra la máquina o sus accesorios.
5. Sabotaje político o terrorismo en que se destruyan o surja un apoderamiento de los centros neurálgicos computarizados
6. Secuestro de soportes magnéticos en los que figure información valiosa.

María de la Luz Lima, presenta una clasificación, de lo que ella llama "delitos electrónicos", diciendo que existen tres categorías:

Los que utilizan la tecnología electrónica como método;
Los que utilizan la tecnología electrónica como medio; y
Los que utilizan la tecnología electrónica como fin.

Como método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

Como medio: son conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

Como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

Por otro lado tenemos la clasificación que utiliza Palazzi en su libro y está basada en la reforma al código penal en materia de delitos informáticos que contemplan verdaderas necesidades que requiere nuestra legislación criminal, menciona Palazzi:

1. Delitos contra el patrimonio.
2. Delitos contra la intimidad.
3. Delitos contra la seguridad pública y las comunicaciones.
4. Falsificaciones Informáticas.
5. Contenidos Ilegales en Internet.

Partes que actúan en el Delito Informático.

Al tener una definición y una clasificación se dan cuenta de que actúan varios sujetos en todo lo que implica el delito informático, así que tienen que dar nombre a los participantes, y los nombran: Sujeto activo y Sujeto pasivo, ahora mencionaremos quiénes son y sus características.

1. Sujeto Activo.

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.

La siguiente tabla, recopilada del libro de Palazzi, muestra los grupos, que en base a la experiencia, son los autores de los delitos informáticos:

Clase de Delito.	Sujetos.
Delitos patrimoniales contra bancos y entidades financieras.	Empleados, en especial cajeros o personal del área de sistemas, desempleados, terceros en complicidad.
Delitos de acceso ilegítimo o delito de daños menores.	Hackers, crackers o usuarios descontentos.
Daño o sabotaje informático.	Empleados de la empresa, o espías profesionales o industriales.
Violaciones a la privacidad, tratamiento ilícito de datos personales.	Investigadores privados, empresas de marketing, agencias de informes crediticios t de solvencia patrimonial.
Violaciones a la propiedad intelectual del software y bancos de datos, con informes o compilaciones de datos.	Piratas informáticos, o también usuarios ("la copia amigable"), empresas que realizan competencia "parasitaria"

2. Sujeto Pasivo.

Se debe distinguir también al sujeto pasivo o víctima del delito quien es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos, las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

A continuación se presentan los principales culpables de los delitos informáticos.

2.2 Quiénes son culpables de los Delitos Informáticos

- a. Los hackers. Los jóvenes que se pasan horas frente a la computadora intentando husmear, penetrar y dañar computadoras ajenas, son sin duda los principales responsables.
- b. Las universidades. Las universidades, a través de sus directivos, suelen ser las principales cómplices de los *hackers* por varias razones, entre ellas:
 - No fomentan valores éticos en sus estudiantes, principalmente de las carreras técnicas o ingenierías.
 - En ocasiones, el conocimiento técnico de los alumnos sobrepasa por mucho el de sus profesores, lo cual provoca en el estudiante un sentido de frustración educativa, lo que lo conduce a buscar o "aprender" por sus propios medios.
 - Muy probablemente, una buena parte de las penetraciones o delitos informáticos los perpetran desde la escuela y/o con equipo informático de la propia universidad.
 - Lo más importante, cuando la universidad se da cuenta de que uno de sus alumnos ha atacado/penetrado su propio servidor o uno ajeno, se convierten en cómplices al no dar parte a la autoridad, con tal de que la sociedad no se entere de que la universidad está preparando (y encubriendo) a delincuentes (*hackers*), en lugar de profesionistas o empresarios.
 - Por las razones anteriores, no es de sorprenderse que la mayoría de los *hackers* tienen entre 16 y 24 años aproximadamente. En otras palabras, todos son estudiantes o desarrollan el máximo de sus capacidades durante su etapa de estudios de bachillerato o profesional.
- c. Los proveedores de hosting. Los proveedores de hosting son culpables porque, a pesar de estar obligados por ley a usar mecanismos de seguridad para proteger la información de sus clientes, no lo hacen. La seguridad no suele ser uno de sus "argumentos de venta", ni parte del valor agregado que ofrecen a sus clientes.
- d. Los fabricantes de *software*. Las estadísticas no nos dejan mentir, más del 60% de los servidores *hackeados* corren bajo el Sistema Operativo de Windows. Noticias recientes han anunciado que "usar servidores web IIS tiene un alto costo... Nimda ha mostrado nuevamente el alto riesgo de usar IIS y el esfuerzo involucrado en mantenerse al día con tantos patches de seguridad de Microsoft".
- e. Las punto com. El comercio electrónico es una útil herramienta para hacer negocios, pero los fraudes han puesto en duda su desarrollo. se habla de las transacciones fraudulentas que se han generado en Internet debido a la facilidad de realizar compras con tarjetas de crédito. Y no se hablan de

barbaridades ni mentiras. Bases de datos enteras han sido robadas con datos de suma importancia de consumidores, muchas empresas han duplicado cobros al realizarse una transacción, y en fin, la lista continúa.

- f. Los legisladores. Al no crear una Legislación Informática que reforme las leyes y las actualice a los nuevos delitos informáticos que se están dando en nuestro País recientemente y al no aplicar sanciones a quienes realizan dichos delitos, los Legisladores del Congreso de la Unión tanto de la Cámara de Diputados como de la de Senadores tienen mucha responsabilidad en los delitos informáticos que suceden en este País.
- g. El gobierno. También una mayor parte de culpabilidad de este ilícito recae en el Gobierno Federal y en los Gobiernos Estatales, pues al no proponer iniciativas de reformas de Leyes Informáticas para que sean discutidas y llevadas al Congreso de la Unión para ser aprobadas resultan ser estos uno de los principales culpables para que siga en aumento los delitos informáticos en México.

2.3 Análisis de las sanciones de los delitos

En México los delitos informáticos se dividen en tres categorías: acceso ilícito a sistemas y equipos informáticos de particulares, de gobierno y del sistema financiero mexicano. La única variante son las sanciones y algunas agravantes especiales (Libro Segundo, Título Noveno.- Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática, Código Penal Federal).

Sistema o Equipo Informático:	Privado		Del Estado		Sistema Financiero		
	Sin agravante	Provecho propio o ajeno	Sin agravante	Provecho propio o ajeno	Sin agravante	Empleado o Funcionario	Provecho propio o ajeno*
Sin autorización, modifique, destruya o provoque pérdida de la información	Prisión: 6 m - 2 a Multa: 100 a 300 d	Prisión: 9 m - 3 a Multa: 150 a 450 d	Prisión: 1 a - 4 a Multa: 200 a 600 d	Prisión: 1.5 a - 6 a Multa: 300 a 900 d	Prisión: 6 m - 4 a Multa: 100 a 600 d	Prisión: 9 m - 6 a Multa: 150 a 900 d	Prisión: 13.5m - 9a Multa: 225 a 1350 d
Sin autorización, conozca o copie información	Prisión: 3 m - 1 a Multa: 50 a 150 d	Prisión: 4.5m-1.5a Multa: 75 a 225 d	Prisión: 6 m - 2 a Multa: 100 a 300 d	Prisión: 9 m - 3 a Multa: 150 a 450 d	Prisión: 3 m - 2 a Multa: 50 a 300 d	Prisión: 4.5 m - 3 a Multa: 75 a 450 d	Prisión: 6.75m-4.5a Multa: 112 a 675 d
Con autorización, modifique, destruya o provoque pérdida de la información	N/A	N/A	Prisión: 2 a - 8 a Multa: 300 a 900 d	Prisión: 3 a - 12 a Multa: 450 a 1350 d	Prisión: 6 m - 4 a Multa: 100 a 600 d	Prisión: 9 m - 6 a Multa: 150 a 900 d	Prisión: 13.5m - 9a Multa: 225 a 1350 d
Con autorización, conozca o copie información	N/A	N/A	Prisión: 1 a - 4 a Multa: 150 a 400 d	Prisión: 1.5a - 6 a Multa: 225 a 600 d	Prisión: 3 m - 2 a Multa: 50 a 300 d	Prisión: 4.5 m - 3 a Multa: 75 a 450 d	Prisión: 6.75m-4.5a Multa: 112 a 450 d

* Penas de esta columna, suponiendo se den las dos agravantes (empleado o funcionario Y en provecho propio o ajeno). Si sólo se da el agravante de "en provecho propio o ajeno", las penas serían iguales a la columna de "empleado o funcionario".

m = meses, a = años, d = días multa, N/A = No Aplica

2.4. Reformas al Código Penal Federal en materia de Delitos Informáticos publicadas en el Diario Oficial de la Federación el 17 de Mayo de 1999.

Situación Nacional (Legislación).

Así como en la ONU reconocen ciertos delitos, México también necesita regular los delitos informáticos, y los reglamenta a través de los siguientes tratados, acuerdos y códigos:

A. Tratado de Libre Comercio de América del Norte (TLC)

Este instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, en la 6a. parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En este tratado se establecen como parte de las obligaciones de los Estados partes, que deberán proteger los programas de cómputo como obras literarias y las bases de datos como compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo. También contemplaron la defensa de los derechos de propiedad intelectual a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.

B. Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio, incluso el comercio de mercancías falsificadas.

El Gobierno de México es parte de este acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio (GATT), manteniendo su vigencia hasta nuestros días.

En el artículo 10, relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias, y que las compilaciones de datos posibles de ser legibles serán protegidas como creaciones de carácter intelectual.

En la sección denominada procedimientos penales, en particular el artículo 61, se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial, se establecerán procedimientos y sanciones penales además de que, "los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias".

En el artículo 69 relativo a la cooperación internacional, se establece el intercambio de información y la cooperación entre las autoridades de aduanas, por este motivo a las conductas ilícitas relacionadas con las computadoras es en el marco del derecho de autor.

C. Ley Federal del derecho de Autor y Código Penal Federal.

Los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran reguladas en la Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997.

Los derechos autorales exigían una reforma con objeto de aclarar las conductas que podían tipificarse como delitos y determinar las sanciones que resultarían más efectivas para evitar su comisión, por ello se propuso la adición de un título Vigésimo denominado "De los delitos en materia de derechos de autor".

Esta Ley regula todo lo relativo a la protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos. Se define lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento, casos en los que el usuario podrá realizar copias del programa que autorice el autor del mismo, las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece las infracciones y sanciones que en materia de derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etcétera.

Los artículos 102 y 231 de la presente Ley. El primero, regula la protección de los programas de computación y señala además que los programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos, lógicamente no serán protegidos. El segundo en su fracción V sanciona el comercio de programas de dispositivos o sistemas cuya finalidad sea desactivar dispositivos electrónicos de protección de un programa de cómputo.

El artículo 424, fracción IV del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal del que se infiere la sanción al uso de programas de virus.

Por otra parte, el artículo 104 se refiere a la facultad del titular de los derechos de autor sobre un programa de computación o sobre una base de datos, de conservar aún después de la venta de ejemplares de los mismos el derecho de autorizar o prohibir el arrendamiento de dichos programas.

El Artículo 109, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada que individuos inescrupulosos pueden hacer con esta información.

Nuestra legislación en materia de delitos informáticos resulta insuficiente en comparación a los avances tecnológicos que se han suscitado en el mundo, por lo que se torna complicada la persecución y sanción de los delincuentes que utilizan las computadoras como instrumento para cometer actos ilícitos.

Por lo anterior se resume que la legislación mexicana en materia de delitos informáticos dista mucho de ser perfecta, es sólo el primer paso para lograr un ambiente sano y seguro para los negocios y comunicaciones electrónicas en nuestro país. Algunos de los defectos del Código Penal Federal en esta área son los siguientes:

- Contempla que constituye el delito sólo si se accesa un sistema informático protegido por un mecanismo de seguridad. Esto es tan absurdo como si dijéramos que para que se diera el delito de allanamiento de morada es necesario que la casa habitada cuente con un candado, llave, portón o cadena protectora. La justicia no puede reducirse sólo a aquellos quienes tienen los medios económicos para proteger su computadora con un mecanismo de seguridad.

- El Código Penal no define qué debe entenderse por "mecanismo de seguridad". ¿Qué es un mecanismo de seguridad de un sistema informático? ¿Un *password*? ¿Un candado contra robo (físico)? ¿Un *firewall*? ¿Un sistema criptográfico de llave pública? o simplemente ¿Tener la computadora encerrada en un cuarto bajo llave o con un guardia de seguridad a un lado? Esta vaga redacción sin duda traerá innumerables problemas de interpretación a la hora de que le toque a un juez analizar un caso concreto.

- Nuestro Código no contempla todos los tipos más comunes de ataques informáticos. El capítulo II adicionado en virtud de la reforma del 17 de mayo de 1999, de entrada está titulado de manera incorrecta: "Acceso Ilícito a Sistemas y Equipos de Informática". Aunque su articulado (Arts. 211 bis 1 al 7) no habla en todo momento de *acceso ilícito*, el título del capítulo sí enfoca su contenido a *accesos ilícitos* precisamente. El problema radica en que muchos *ataques informáticos* se perpetran sin necesidad alguna de acceder directamente un sistema informático. El mejor ejemplo es el ataque de "Denegación de Servicios" (*Denial of Services* o *Distributed Denial of Services*), cuyo objetivo no es "modificar, destruir o provocar pérdida de información" como reiteradamente lo establece el Código Penal Federal, sino simplemente imposibilitar o inhabilitar un servidor temporalmente para que sus páginas o contenidos no puedan ser vistos por los cibernautas mientras el servidor esta *caído*.

Por lo antes visto, ahora mencionaremos a la legislación internacional en cuanto a los delitos informáticos de algunos países con la finalidad de realizar una comparación entre nuestra ley con la de otras naciones, las cuales se describen a continuación.

➤ Situación Internacional (Legislación).

Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre delitos informáticos, sin embargo con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países como México, a continuación se presenta los siguientes casos particulares:

Alemania

En Alemania para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

- Espionaje de datos (202 a);
- Estafa informática (263 a);
- Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño

- en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273);
- Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible;
- Sabotaje informático (303 b), destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa;
- Utilización abusiva de cheques o tarjetas de crédito (266 b).

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

Por otra parte, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistema informáticos. El tipo de daños protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.

Austria

Ley de reforma del Código Penal de 22 de diciembre de 1987.

Esta ley contempla los siguientes delitos:

- Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
- Estafa informática (148). En este artículo se 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 por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

Francia

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

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

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

- Destrucción de datos (462-4). En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informatizados (462-5). En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.
- Uso de documentos informatizados falsos (462-6). En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

Estados Unidos

Es importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modificó el Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un Caballo de Troya, etcétera y en que difieren de los virus, la nueva acta proscribire la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programas. (18 U.S.C. Sec. 1030 [a][5][A]). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley.

Las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de \$10,000 por cada persona afectada y hasta \$50,000 el acceso imprudencial a una base de datos, etcétera.

Uno de los apartados de esta ley, contempla la regulación de los virus (computer contaminant) conceptualizándose aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

CAPÍTULO 3

Industria del software en México

Desde hace varios años, resulta evidente que México requiere cambiar el paradigma con el que se ha construido la etapa de crecimiento y consolidación del Estado moderno, cuya sentencia es: frente a la emergencia de las economías asiáticas, México no puede competir con base al precio de sus recursos humanos, ni debe interesarle mantenerlo deprimido; tampoco puede continuar apoyando sus finanzas internacionales en la exportación de materias primas con escaso o nulo valor agregado.

El paradigma de ser un país con mano de obra barata, escasamente calificada, exportador de materias primas o de bienes con escaso o nulo valor agregado debe ser sustituido por uno que nos permita competir en un mercado mundial globalizado con bienes y servicios de calidad, generados por recursos humanos competentes y bien remunerados que fortalezcan el mercado interno, al ofrecer alternativas laborales en todo el territorio para ampliar los niveles de bienestar de toda la población, lo cual cimentará un México con miras a integrarse a una economía globalizada.

La naciente industria del software en México está congelada y muy dispersa, donde prevalecen las estructuras administrativas familiares o informales, compuestas por un reducido número de profesionales, que en su mayoría y salvo excepción, están fuera de cualquier modelo de calidad reconocido internacionalmente (el Modelo de Madurez de Capacidades de la Universidad Carnegie Mellon CMM, el modelo ISO 15504, entre otros).

La existencia de aproximadamente más de 390 empresas desarrolladoras de software en el país representa una base muy importante para impulsar el crecimiento de la industria de software, así como la gran magnitud de demanda internacional, que favorece la creación de una gran cantidad de nuevas empresas desarrolladoras de software.

La gran demanda de mercado externo orientado hacia la industria de software puede ser un trampolín para el crecimiento de nuevas empresas competitivas internacionalmente que puedan dar solución no solo al mercado interno sino también a la falta de atracción por parte de empresas líderes internacionales.

La presente exposición de este CAPÍTULO tiene como objetivo analizar la industria de software en México en la actualidad (año 2007) para determinar si es competitiva internacionalmente y pronosticar su crecimiento a largo plazo.

La finalidad de este capítulo es demostrar que México es un país con vocación de líder en el desarrollo de software. Determinará los mercados de software emergentes que no han sido atacados por soluciones de software existentes y así facilitar la unión de esfuerzos y capacidades existentes para el desarrollo de éste.

3.1 La industria del software en México

El escaso desarrollo de la Industria del Software en México se debe a varias razones, entre ellas se encuentran la ausencia de medidas eficientes que aumenten la oferta y la demanda interna, así como en el poco interés por parte de las empresas mexicanas en incursionar en el marco internacional.

El pobre desarrollo de la industria de software en México se ha dado gracias a los esfuerzos de empresas privadas, sin apoyo alguno que facilite su buen desarrollo, de las empresas públicas existe muy poco apoyo para su desarrollo.

México en el plano internacional esta conceptualizado como un país incapaz de desarrollar cualquier tipo de tecnología entre ellas la del software.

Son pocas las empresas que cuentan con capacidad de procesos al desarrollar software para que pueda ser competente en la demanda del mercado internacional. Por lo que, pocas de estas empresas son las que realmente tienen la experiencia de competir en este mercado.

Hay mucha escasez de programadores, desarrolladores e ingenieros con algún tipo de certificación en alguna tecnología que dificulta que se pueda llevar a cabo ese desarrollo tanto en calidad como en cantidad.

Los planes de estudio en escuelas y universidades no está a la altura de la demanda productiva de software ni a la demanda de las tecnologías informáticas emergentes.

Las empresas dedicadas al desarrollo de software requieren que sus recursos humanos cuenten con el dominio del idioma inglés más allá del que se tiene hoy día.

Se carece de un marco legal que apoye y regule el buen desarrollo de tecnologías de información, y desconoce los beneficios que se pueden obtener a partir de la aplicación de nuevas tecnologías.

El gobierno y la industria de software no han podido ponerse de acuerdo para llevar a cabo una estrategia para unir esfuerzos públicos y privados para desarrollar el mercado interno de software. Lo que provoca una competencia desfavorable para las empresas privadas para ofrecer sus servicios de software contra las instituciones de gobierno sin obligar a participar en procesos de licitación.

Las áreas de informática en algunos departamentos del Gobierno Federal cuentan con poca productividad y representan costos elevados dejando a un lado sus servicios informáticos y dejando poca oportunidad para la iniciativa privada.

No se cuenta con un apoyo o financiación para las empresas privadas con el fin de ampliar sus servicios y llevar a cabo planes de expansión, además de que se cuenta con un volumen reducido de proyectos de software a nivel interno. Desarrollando soluciones sin visión sin hacer frente a las necesidades reales del mercado interno.

La productividad de las empresas desarrolladoras de software es en general baja, debido a la falta de uso de procesos avanzados como CMMI o ISO. Esto

les impone una fuerte desventaja para competir frente a otros países que trabajan con este tipo de procesos.

Se carece de modelos, leyes, normas y de organismos evaluadores de la capacidad de procesos de la producción de software y las evaluaciones internacionales de capacidad de procesos son costosas.

La industria de software es una actividad que se caracteriza por generar un alto valor agregado aportando a la economía nacional servicios esenciales para su modernización.

Esta se basa en el conocimiento, desarrolla habilidades, propicia la innovación tecnológica y genera empleos bien remunerados, no contamina y requiere de relativamente poco capital para iniciar.

La industria del software es una de las actividades económicas que componen a las tecnologías de información (TI).

Éstas se integran además por la industria de hardware y los servicios. Junto con las comunicaciones componen lo que se conoce como TIC (tecnologías de información y comunicación).

El uso de TIC en los procesos de producción, comercialización, de servicios, de educación y de administración pública es un factor importante para mejorar la competitividad de las empresas y los países.

El Mercado Mundial

El mercado de TIC representa el 6.6% del valor de la producción económica mundial. Durante la década de los noventa la mayor parte de los países, aún los que enfrentaron crisis financieras y recesiones económicas, incrementaron su gasto en tecnologías de información y comunicación.

En la actualidad, el gasto en tecnologías de información ha trasladado su énfasis del hardware al software, provocando que la relación entre el segundo y el primero suba de 32.5% en 1996 a 40% en 1999.

El mercado mundial de productos de software rebasa los 153,000 millones de dólares anuales. Estados Unidos es el principal consumidor, con un gasto superior a los 75,000 millones de dólares anuales y una participación de 48.8% en el total mundial.

Una cantidad cada vez más creciente en producción mundial en cuanto a desarrollo software se refiere se realiza en países en vías de desarrollo, tal es el caso de la India, la cual representa el mayor éxito de creación y crecimiento basadas en la exportación y sobre todo se software.

La India se ha encargado de desarrollar software para Estados Unidos por más de 15 años.

El gobierno de la India ha invertido muchos billones de dólares en apoyo a capacitación, certificación, promoción e infraestructura para su correcto desarrollo de software.

Gran parte de esta producción de software se debe a que la India contó con ingenieros indios residentes en Estados Unidos trabajando para grandes empresas consumidoras de software.

La India utilizó un gran capital humano bien formado y capacitado, que se podía mantener con una baja remuneración para desarrollar proyectos en Estados Unidos, lo que la llevó a alcanzar grandes exportaciones de software al año.

Otro caso de éxito es Irlanda, la cual se enfocó al desarrollo de software atrayendo a empresas extranjeras con programas de apoyo que lograron un rápido desarrollo que aumentó su tasa de crecimiento anual de una manera sorprendente.

Por otro lado, la industria del software en Canadá está dedicada en su gran parte a la exportación.

La mayor parte de las empresas canadienses tienen a Estados Unidos como un mercado local, basando su producción de software a las necesidades de este mercado externo, enfocando su desarrollo a productos enfocados en gran medida a la animación, a los gráficos, a la administración de documentos, a la extracción inteligente de datos y a la administración de escuelas.

En cambio, la industria del software en Australia, se considera sublíder mundial como proveedor de contenidos de Internet, servicios de administración; servicios en línea hacia otros países, etc.

De acuerdo con la UNCTAD (Conferencia de las Naciones Unidas sobre Comercio y Desarrollo) el desarrollo de la industria del software en los países emergentes se puede llevar a cabo a través de dos alternativas de políticas estratégicas.

La primera estrategia; atención de demanda interna, se basa en el uso de software libre como una herramienta para el fortalecimiento de la infraestructura económica a fin de soportar el desarrollo de otros sectores de la economía y, la segunda estrategia generación de un proveedor internacional, se orienta a considerar a la industria del software como sector prioritario por la generación de nuevos empleos y el crecimiento industrial basado en la creación de oferta de software para exportación.

Una manera alternativa para el desarrollo de la industria de software consiste en implementar estas dos estrategias secuencialmente: valiéndose del software libre como una herramienta que con el tiempo sería reemplazada por una buena y planeada estrategia de desarrollo de software para exportación.

Entorno Productivo Nacional e Industria de Software

Para cumplir con la expectativa nacional de tecnologías de información y así mantener un entorno productivo nacional en cuanto a la industria de software se requiere, se debe tomar en cuenta lo siguiente:

- Recursos humanos emprendedores bien capacitados.
- Empresas incubadoras y aceleradoras de nuevos recursos.
- Fomentar a la industria ya existente.

Así como el Gobierno crea oportunidades en sus diversos programas de apoyo, de esa misma manera deberían existir apoyos para desarrollar la industria de software.

La manera idónea para lograr estas oportunidades sería la mejora de la industria local existente.

En México se cuenta actualmente con un programa que cumple con dichas características, este es conocido como el Programa para el desarrollo de la industria de Software (PROSOFT), el cual, es un plan a largo plazo que trata de impulsar a la industria de software.

Este programa se encarga de apoyar económicamente a empresas dedicadas a la industria nacional de software.

Lo que pretende este programa, es la de incrementar el nivel de competitividad de las empresas que se caracterizan por un lado, por el uso adecuado de tecnologías de información, lo cual genera mejoras y aumenta la productividad; y las empresas con mejor desarrollo en el entorno productivo de software nacional.

Es bueno tener en cuenta las etapas de evolución de las empresas, para determinar su nivel de competitividad, es esta la razón de este programa.

Un modelo de evolución empresarial basado en el nivel de competitividad del entorno productivo se describe a continuación.

Modelo de Evolución Empresarial.

Fuente: CONACYT

En este modelo se observa que en las últimas tres categorías los elementos relacionados con las tecnologías de información (TI) y su competitividad, estos son: eficiencia de procesos, diversificación de productos, expansión e innovación.

En México, el 98% de las empresas, que son el mercado objetivo local de las empresas de software locales, son de carácter emergente en términos de competitividad; esto significa que la gran mayoría de las unidades productivas consumen poco software y de baja sofisticación.

La misma clasificación pero ahora aplicada a las empresas mexicanas de software da como resultado la siguiente descripción:

Modelo de Evolución Empresarial. Empresas de Software.

Fuente: CONACYT

Si analizamos podemos ver que las empresas desarrolladoras de software presentan características similares a las del entorno productivo en general, es decir, hay un porcentaje que supera al 90% de empresas de software que pueden clasificarse en la categoría de emergentes.

El decir que son emergentes, indica dos cosas: una sería la necesidad de empresas por consumir software y otra, la gran área de oportunidad por

empresas para desarrollar software, es decir, estable una relación estrecha entre empresas usuarias y empresas productoras de software.

Ya dependiendo del papel que juegue una empresa de software, su mercado primario puede variar en dos tangentes:

- La Construcción de software es una competencia clave para todas las empresas de software.
- La Administración de proyectos y la atención a clientes son papeles importantes en el desarrollo de aplicaciones y de servicios.

La industria del software es diferente a las demás empresas porque en realidad no es un producto como tal lo que ofrecen, sino que viene siendo la aplicación de un proceso a un negocio, esto es, que aplicaciones desarrolladas generalmente son muy diversas.

El software puede abarcar desde la producción de reportes, una contestadora telefónica, el sistema GPS de un automóvil, etc.

Es por ello que las empresas dedicadas a la industria de software basan sus capacidades en ofrecer ya sea tanto productos como servicios.

Estas dos capacidades son buenas, y lo mejor es adoptar una especie de modelo combinado para convertir sus productos y servicios en un producto con gran aplicación de la tecnología en su totalidad.

Esta especie de modelo combinado es punto de debate para las nuevas empresas que desean incursionar a la industria de software ya que tienen que decidir si deciden ser empresas de productos, de servicios o combinadas.

De cualquier manera, el buen desarrollo de cualquier empresa dedicada al desarrollo de software debe de tener un buen capital humano, relaciones y proyectos y planes de desarrollo.

Lo que se pretende es llegar al ya sabido dicho: “un excelente programador al volverse líder de proyecto provoca que se gane un pésimo líder y se pierda un excelente desarrollador”, lo que provoca que el desarrollo de una empresa dedicada a la industria de software pueda echar abajo su propia estrategia de negocio.

3.2. Servicios de seguridad

La seguridad de software aplica los principios de la seguridad de información al desarrollo de software. **Information security** (La seguridad de información) se refiere a la seguridad de información comúnmente como la protección de sistemas de información contra el acceso desautorizado o la modificación de información, si está en una fase de almacenamiento, procesamiento o tránsito.

También la protege contra la negación de servicios a usuarios desautorizados y la provisión de servicio a usuarios desautorizados, incluyendo las medidas necesarias para detectar, documentar, y contrariar tales amenazas.

Muchas preguntas con respecto a la seguridad, son relacionadas al ciclo vital de software. En particular, la seguridad del código y el proceso de software; deben de ser considerados durante la fase del diseño y desarrollo.

Además, la seguridad debe de ser preservada durante la operación y el mantenimiento para asegurar la integridad de una parte (pedazo) de software.

Una gran cantidad de seguridad usada en los Sistemas de Redes de hoy, nos pueden engañar en la creencia que nuestros trabajos como diseñadores de sistema de seguridad ya han sido realizados. Sin embargo, las cadenas y computadoras son increíblemente inseguras.

La falta de seguridad se origina en dos problemas fundamentales: Los sistemas que son teóricamente seguros pueden ser inseguros en la práctica, además, los sistemas son cada vez más complejos. La complejidad proporciona más oportunidades para los ataques. Es mucho más fácil probar que un sistema es inseguro que demostrar que uno es seguro -- probar la inseguridad, simplemente una toma ventaja de ciertas vulnerabilidades del sistema. Por otra parte, probando un sistema seguro, requiere demostrar que todas las hazañas posibles puedan ser defendidas contra (muy desalentadora), si no imposible, la tarea –.

Actualmente, no hay ninguna solución singular para asegurar la ingeniería de software. Sin embargo, hay métodos específicos que mejoran la seguridad de los sistemas. En particular, podemos mejorar la confiabilidad de software. También podemos mejorar nuestra comprensión de los requisitos de un pedazo de software.

Buena Práctica

La seguridad requiere más manejo y riesgo de mitigación, de la que requiere la tecnología. Como un desarrollador, uno primero debe de determinar los riesgos de una aplicación particular. Por ejemplo, el Web site típico de hoy puede ser sujeto de una variedad de riesgos; la desfiguración o la negación distribuida de ataques del servicio.

Una vez que se identifiquen los riesgos, identificar medidas de seguridad apropiadas llega a ser manejable. En particular, al definir los requisitos, es importante considerar cómo la aplicación será utilizada. Con ese conocimiento uno puede decidir, si o no, utilizar características complejas como contabilidad, auditoría etc.

Otro asunto potencialmente importante es como soportar el nombramiento del producto. El aumento de los sistemas distribuidos ha hecho el nombramiento cada vez más importante. Típicamente, el nombramiento esta manejado por rendezvous: un principal exporta un nombre y lo anuncia en alguna parte, y alguien que desea utilizar el nombre lo busca en los libros y directorios de teléfono. Por ejemplo, en un sistema como el sistema del descubrimiento del recurso, los recursos y los individuos que usan esos recursos deben ser nombrados. A menudo hay cosas buenas y malas con respecto al nombramiento: mientras que el nombramiento puede proporcionar a un nivel de indirección, también puede crear problemas adicionales si los nombres no son estables. Los nombres pueden permitir que los directores desempeñen diversos papeles en un sistema determinado que pueda también ser útil.

Confiabilidad de software

La confiabilidad de software significa que un programa particular debe de seguir funcionando en la presencia de errores. Los errores pueden ser relacionados al diseño, a la implementación, a la programación, o el uso de errores. Así como los sistemas llegan a ser cada vez más complejos, aumenta la probabilidad de errores. Como mencionamos, es increíblemente difícil demostrar que un sistema sea seguro. Ross Anderson dice que la seguridad de computación es como programar la computadora del Satán. Software seguro debe de funcionar abajo de un ataque. Aunque casi todo el software tenga errores, la mayoría de los errores nunca serán revelados debajo de circunstancias normales. Un atacante busca esta debilidad para atacar un sistema.

Muchos de los problemas de la seguridad de hoy son relacionados con el código defectuoso. Por ejemplo, el **Morris Internet Worm** (el gusano Internet de Morris) utilizó overflow en un programa de UNIX para ganar acceso a las computadoras que ejecutaron el programa. Los ataques de **buffer overflow** han sido el tipo de ataque más común en los últimos diez años e implican el sobregresar instrucciones en el programa. Específicamente, una cantidad fija de memoria en la pila, puede ser reservado por el usuario; si la entrada de información del utilizador es más grande que este espacio reservado, el usuario puede sobregresar los instrucciones de la programa. Si esto se hace cuidadosamente, el usuario puede insertar sus propias instrucciones en el código del programa, así haciendo la máquina receptora realizar operaciones arbitrarias dictados por el atacante. Mientras que tales ataques se pueden prevenir típicamente con **bounds checking** (revisando el tamaño de la entrada de información antes de copiarla), ésta es una cuestión de práctica de programación que confiamos en que el programador mismo seguirá. El aspecto difícil de **buffer overflows** es que pueden ocurrir en una gran cantidad de lugares en cualquier programa, y es difícil de prevenir el suceso por todas partes. Este ha sido el caso en el pasado, especialmente, en los últimos 10 años.

"Confiando en la Confianza"

En particular, la lectura de Ken Thompson "Reflections on Trusting Trust" (reflexiones en confiar en confianza) nos da a pensar en la integridad de una parte de software. Específicamente, nos enseña un ejemplo donde un compilador de C puede ser hackeado por un Trojan horse. Para el propósito de esta demostración, Thompson inserta su propia versión de UNIX "login" código, cuando un usuario trataba de compilar el código de fuente. El valor de la lectura de Thompson es que no se puede confiar en el código de fuente que no hayas creado tu mismo. Este incluye el código del compilador, del ensamblador, y micro códigos de hardware. Thompson también nos dice que cuando el nivel de los "bugs" llega a un nivel bajo los " fallos de funcionamiento " serán más difíciles de detectar.

De hecho, no tenemos que compilar software para ser víctima del mensaje de Thompson. Cada vez que bajamos un programa por internet o instalar software nuevo, confiamos en un número de cosas. Primero, confiamos que la máquina en la que estamos bajando el software es realmente la máquina que demanda ser. Proyectos como **Self-Certifying File System** han tratado de arreglar este problema. Aunque nos confiamos en que la máquina con la cual estamos hablando es la que pensamos que es, debemos de comprobar que los archivos

fueron preparados apropiadamente. Así como cuando bajamos un programa por internet confiamos en el proceso de desarrollo del software.

Mientras que los sistemas de UNIX parece generar más interés en las comunidades académicas, otros sistemas de operación no son inmunes. Los ataques de buffer overflow son extensos, desde los servidores ftpd de Windows a los procesos ocultados que capturan cada golpe de teclado del usuario. No importa cuánto énfasis ponemos en el diseño y la seguridad de la ingeniería del software, debe de ser una cierta cantidad básica de software y de hardware que no vamos a poder confiar totalmente.

La Negación Distribuida del servicio

Los ataques de la negación distribuida del servicio **Distributed denial of service (DDoS)** es a menudo la causa de la preocupación ética. Algunas medidas de seguridad se han tomado contra ataques de DDoS, tales como filtración, **IP traceback mechanisms** mecanismos del traceback del IP, dando el FBI mayores potencias para la búsqueda y el asimiento, a etc., pero más de éstos se usan para la negación estándar de los ataques del servicio, más bien que los ataques de DDoS.

Los ataques de la negación distribuida del servicio **DDoS** comienzan con un "maestro" que es responsable de comprometer un número de máquinas "esclavas". Estos esclavos son responsables del ataque. A menudo "daemons" están instalados en múltiples ordenadores principales. Un cliente identifica una blanco a los daemons y cada uno de los clientes mandan una negación del ataque del servicio. El problema de DDoS llega a ser mucho más serio mientras que aumente el número de usuarios conectado constantemente con los módems de cable directos Internet o las líneas del DSL. En general, hay menos probabilidad para detectar una intrusión al sistema, así aumentando la probabilidad para ser un esclavo en un ataque de DDoS.

Hasta con el desarrollo sistemático del software "seguro", nosotros, como usuarios de computadoras en un mundo de Sistemas de Redes, no operamos en aislamiento -- somos dependientes de los otros, los cuales están haciendo su parte en desarrollando, diseñando, y utilizando software "seguro".

3.3. Fraudes cometidos mediante manipulación de información privada

No obstante, que en nuestro país no se contemplan muchos los delitos informáticos en la legislación penal, consideramos que es importante adicionar estas conductas antijurídicas, para evitar, grandes daños tanto a las personas físicas, como las entidades públicas y demás sujetos, que utilizan la informática como medio de trabajo y desarrollo de sus actividades cotidianas.

Como ya lo hemos mencionado con antelación en los capítulos pasados, en varios países sobre todo los más desarrollados ya se ha legislado al respecto, quizás el legislador nacional no está preparado todavía para introducirse en esta área y crear las normas jurídicas respectivas, empero, es de suma importancia que ya se comience a hacer algo al respecto, pues hay muchas conductas que implican responsabilidad para aquellos que las cometen, sin embargo, y en vista de que en México no existen muchas leyes al respecto, permite que éstas

queden impunes o bien se tipifiquen en otro delito que no es aplicable muchas veces al caso concreto.

Consistente en el derecho que tiene una persona de no ser molestada o sufrir invasión a su persona o a su información personal, así como a sus relaciones y comunicaciones privadas, entre las que cuenta las comunicaciones electrónicas en este caso el Internet, el Derecho Mexicano no ha reglamentado esta garantía individual que se deduce de las libertades de la persona en el aspecto espiritual, o sea la libertad de intimidad. Es decir, no puede violarse la intimidad de ningún individuo sin un mandamiento judicial escrito, conforme a derecho y con fundamento a la ley. Desafortunadamente, la realidad es otra en cuanto a este derecho, por falta de regulación; es uno de los menos respetados, tanto por violaciones del orden común como de la misma autoridad.

El concepto de vida privada, en relación con la informática, tiene un doble significado. Por un lado la protección de la vida privada, estricto sensu, se refiere al problema de la información sensible, definida aquella como relativa al origen racial, a las opiniones públicas, religiosas y memberships sindicales, información que no puede ser recopilada ni procesada electrónicamente salvo que exista autorización expresa del autor; por el otro lado, el manejo y registro de otro tipo de información puede también causar atentados a la vida privada estricto sensu, pero en relación con el ámbito social al que pertenece. En México, es necesario reconocer la importancia del Internet como un medio de comunicación de tecnología avanzada además de fomentarse la defensa del derecho de autodeterminación informática.

En la actualidad por medio de las computadoras y del Internet, las personas físicas cuentan en sus bases de datos con información confidencial, la cual hace referencia a muchas cuestiones personales, sin embargo, existen sujetos que son capaces de introducirse a dicha información electrónica evadiendo las contraseñas e introduciéndose a nuestro sistema informático sin la autorización de su creador o de mandamiento judicial, lo que implica un gran riesgo personal a la privacidad, por esto se debe de proteger la base de datos que pudiera tener una persona, ya que ésta es confidencial, lo cual atacaría el bien jurídico tutelado de la privacidad, y por las características de dicha conducta, además pueden provocar pérdidas económicas, con o sin un beneficio para los que la cometen; pudiendo ser cometidos imprudencialmente, pero en la mayoría de los casos, es una conducta que se realiza con la intención de transformar o difundir una información contenida en una base de datos; siendo importante señalar que son muchos los casos en que se produce este tipo de conductas, por lo cual consideramos adecuada la penalidad que pretendemos modificar en algunos artículos del Código Penal Federal de nuestra tesis.

Al respecto, de no imponer una sanción menor es porque se ha visto en la práctica desafortunadamente que la imposición de sanciones menores no desalienta la comisión de estos delitos, es por ello que sancionar con una pena más elevada implica que el sujeto, en caso de que realice su conducta e intente hacerlo de nuevo es sabedor de que será una pena elevada que le causará más perjuicio, que el beneficio que haya obtenido de su conducta.

Los delitos informáticos constituyen una gran laguna en nuestras leyes penales, así pues, el derecho comparado nos permite hacer una lista de los delitos que no están contemplados en el Código Penal y que requieren análisis urgente por

parte de nuestros académicos, penalistas y legisladores. A continuación se mencionan los diferentes tipos de fraudes de los delitos informáticos.

Tipos de Delitos Informáticos reconocidos por la Organización de las Naciones Unidas:

Las conductas o acciones que considera las Naciones Unidas como delitos informáticos son las siguientes:

I) Los Fraudes cometidos mediante manipulación de computadoras: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común.

II) La manipulación de programas; este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas que tienen conocimiento especializados en programación informática.

III) La Manipulación de datos de salida; se efectúa fijando un objetivo al funcionamiento del sistema informático, el ejemplo más común es el fraude que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

IV) Fraude efectuado por manipulación informáticas de los procesos de cómputo.

V) Falsificaciones informáticas; cuando se alteran datos de los documentos almacenados en forma computarizada.

VI) Como instrumentos; las computadoras pueden utilizarse también para efectuar falsificación de documentos de uso comercial

VII) Sabotaje Informático; es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

VIII) Los Virus; Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos.

IX) Los Gusanos; los cuales son análogos al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

X) La Bomba lógica o cronológica; la cual exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

XI) Acceso no autorizado a servicios u sistemas informáticos; esto es por motivos diversos desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

XII) Piratas Informáticos o Hackers; este acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones.

XIII) Reproducción no autorizada de programas informáticos de protección legal; la cual trae una pérdida económica sustancial para los propietarios legítimos.

3.4. Falsificaciones informáticas.

Se dividen en dos rubros que son los siguientes:

Como objeto. Cuando se alteran datos de los documentos almacenados en forma computarizada.

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

Si bien en el Código Penal Federal se tipifica el fraude y la falsificación de documentos es importante destacar que los tipos penales tradicionales no son suficientes para proteger el patrimonio, y por ello se debe ampliar la protección para cubrir las lagunas jurídicas.

En el fraude informático la conducta típica consiste en sancionar la introducción de datos incorrectos o las manipulaciones de los programas con la finalidad de lesionar el patrimonio.

En la actualidad esta conducta no se puede tipificar como fraude si falta el engaño y el error en una persona, por lo que es necesario sancionar la acción engañosa, la causación del error y la disposición patrimonial, mediante el uso de sistemas informáticos.

Los métodos utilizados para causar daños patrimoniales mediante los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detención.

El fraude relacionado con la informática consiste en la introducción, la alteración, el borrado o la supresión de datos o de programas informáticos u otra interferencia en el curso del procesamiento de datos que cause una pérdida económica o de bienes a otra persona, con la intención de obtener una ganancia económica ilícita para sí mismo o para otra persona.

La falsificación informática consiste en introducir o alterar datos o programas informáticos, u otra interferencia en el curso del procesamiento de datos de manera o en condiciones tales que constituirían un delito de falsificación, si se hubieran cometido con respecto a un objeto tradicional de dicho delito. La finalidad de la norma es tipificar como delito la falsificación de datos informáticos.

La conducta que se tipifica no se subsume en los tipos penales descritos en los artículos 211 bis 1 a 211 bis 7, ya que en los mismos se habla de modificación, alteración o destrucción. Según el diccionario de la Real Academia Española el verbo alterar significa cambiar la esencia o forma de algo, el verbo modificar

significa transformar o cambiar algo mudando alguno de sus accidentes, en ambos supuestos se cambia o transforma algo que ya existe, como es la alteración de información.

En la falsificación informática lo que se busca sancionar es la fabricación de algo contrario a las disposiciones legales, crear algo falso, simulado, falso de ley o realidad en términos del Diccionario de la Real Academia Española.

Obtención ilícita de servicios de telecomunicaciones

Se trata de conductas en las que para obtener servicios sin pagarlos, el autor recurre a la manipulación técnica de determinados dispositivos o de elementos electrónicos de los dispositivos.

Uso ilícito de instrumentos de pago.

La tipificación de esta conducta resulta de primordial importancia ya que en México al igual que en diversos países de América Latina, la obtención de un lucro indebido mediante el uso ilícito de tarjetas de crédito, de débito u otros instrumentos de pago con banda magnética o dispositivo técnico de almacenamiento de datos ha ido en aumento, generando fuertes pérdidas no sólo para los usuarios de los servicios financieros, sino incluso para las Instituciones de Crédito.

Según información disponible, el "número total de reclamaciones presentadas por los usuarios en los rubros de tarjetas de crédito y débito" se ha incrementado de forma considerable entre el año 2002 y 2003.

En el año 2002, los fraudes mediante el uso tarjetas de crédito y débito fueron absorbidos por dos instituciones bancarias en nuestro país, que representan más del 70% del monto total en dinero, y como resultado también en número de fraudes.

Con relación a la distribución del monto (en dinero) defraudado por tarjetas ya sea de débito o crédito, las de débito representan alrededor del 60% del total (en dinero); y tomando en cuenta el número de fraudes por tipo de tarjeta, las de crédito representan aproximadamente el 60%.

En otras palabras, el número de fraudes por tarjetas de débito aunque representan un menor número muestran mayores cantidades de dinero defraudadas.

El número de quejas presentadas en la materia ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros fue de 629.

Por lo que se refiere al año 2003, los fraudes por institución bancaria que emiten tarjetas de crédito y débito, al igual que en el año 2002, son absorbidas principalmente por dos instituciones bancarias, que representan más del 70% del monto total en dinero y en el número de fraudes.

Con relación a la distribución del monto defraudado por tarjetas ya sea de débito o crédito, se experimentó un aumento en el monto (de dinero) de los fraudes por tarjetas de crédito, y como consecuencia el número de fraudes por tipo de tarjeta

de crédito se incrementó. Es decir, tanto la cantidad en pesos y en el número de fraudes en tarjetas de crédito, van en ascenso.

El número de quejas presentadas ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, que para 2002 fueron 629, para 2003 alcanzaron la cifra de 896 casos.

De lo anterior podemos concluir que:

- Los montos en dinero por defraudación en tarjetas de crédito o débito van en ascenso.
- El número de fraudes en tarjetas de crédito se está incrementando comparándolo con las de débito.
- En su totalidad, el número de casos por defraudación en tarjetas de débito o crédito aumenta.

Es así como estas cifras muestran claramente que el índice delictivo se está incrementando en detrimento del patrimonio, no sólo de los usuarios de los servicios bancarios sino también de las instituciones de crédito.

Por lo expuesto, resulta ineludible legislar sobre la materia a fin de tipificar las conductas que mediante el uso de códigos falsos o generación de números válidos de tarjetas de crédito o de débito se obtenga una ganancia financiera ilícita.

Adicionalmente a la necesidad de tipificar el fraude informático, la falsificación informática, obtención ilícita de servicios de telecomunicaciones y el uso indebido de instrumentos de pago, los integrantes de mi Grupo Parlamentario consideramos que también se deben sancionar otras conductas que no se adecuan a los tipos penales de los delitos de acceso ilícito a sistemas y equipos informáticos que actualmente se prevén en el CAPÍTULO II del Título Noveno del Código Penal Federal.

Por ello, proponemos tipificar el acceso ilícito a un sistema informático aún cuando no se altere, destruya o modifique información contenida en sistemas o equipos de informática protegida por mecanismos de seguridad, ya que en los términos en que actualmente se sanciona esta conducta, el acceso ilícito constituye un acto preparatorio de la conducta típica.

En todo caso se debe considerar como un tipo penal autónomo ya que con la realización de la conducta delictiva se lesiona la privacidad.

Asimismo, consideramos necesario tipificar la interceptación ilícita de sistemas informáticos, así como la venta, compra, importación u otra forma de puesta a disposición de terceros de programas informáticos, contraseñas, códigos de acceso o datos informáticos, en virtud de que actualmente en la fracción II del artículo 424 Bis del Código Penal Federal sólo se sanciona a quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

De acuerdo a los graves efectos que producen la comisión de delitos cibernéticos y su incremento tanto en el ámbito nacional como internacional, en un mundo globalizado donde se requiere la cooperación internacional para la

investigación, persecución y sanción de los ciber delincuentes, es fundamental considerar las Recomendaciones que a nivel hemisférico ha emitido el Grupo de Expertos Gubernamentales en materia de delito cibernético de la Organización de los Estados Americanos.

CAPÍTULO 4

Leyes e instituciones que rigen los programas de cómputo en México

Situándonos de lleno en nuestro país, los esfuerzos por mantener los derechos de todos los ciudadanos ha generado nuevas y cada vez más adecuadas leyes, de las que podemos extraer aquellas que protegen a los autores de cualquier elemento que resulte de su trabajo intelectual (música, literatura, ciencia, tecnología, etc.), en nuestro caso únicamente mencionaremos aquellas relacionadas con la informática.

Sin duda uno de los mejores esfuerzos es el siguiente:

4.1 Ley federal de derechos de autor.



Cámara de Diputados del H. Congreso de la Unión

Secretaría General

Secretaría de Servicios Parlamentarios

Dirección General de Bibliotecas

LEY FEDERAL DEL DERECHO DE AUTOR

Nueva Ley publicada en el Diario Oficial de la Federación el 24 de diciembre de 1996

TEXTO VIGENTE

Última reforma publicada DOF 23-07-2003

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Presidencia de la República.

ERNESTO ZEDILLO PONCE DE LEON, Presidente de los Estados Unidos Mexicanos, a sus habitantes sabed:

Que el Honorable Congreso de la Unión, se ha servido dirigirme el siguiente

DECRETO

"EL CONGRESO DE LOS ESTADOS UNIDOS MEXICANOS, DECRETA:

LEY FEDERAL DEL DERECHO DE AUTOR

TÍTULO I

Disposiciones Generales

Capítulo Único

Artículo 1o.- La presente Ley, reglamentaria del artículo 28 constitucional, tiene por objeto la salvaguarda y promoción del acervo cultural de la Nación; protección de los derechos de los autores, de los artistas intérpretes o ejecutantes, así como de los editores, de los productores y de los organismos de radiodifusión, en relación con sus obras literarias o artísticas en todas sus manifestaciones, sus interpretaciones o ejecuciones, sus ediciones, sus

fonogramas o videogramas, sus emisiones, así como de los otros derechos de propiedad intelectual.

Capítulo IV

De los Programas de Computación y las Bases de Datos

A continuación podemos observar algunos de los artículos que existen dentro de la legislación para regular el desarrollo y manejo de software. Estos artículos se definen con mayor detalle como sigue:

Artículo 101.- Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

Artículo 102.- Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

Artículo 103.- Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.

Como excepción a lo previsto por el artículo 33 de la presente Ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.

Artículo 104.- Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o sobre una base de datos conservará, aún después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.

Artículo 105.- El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:

- I. Sea indispensable para la utilización del programa, o
- II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.

Artículo 106.- El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:

- I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;
- II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;
- III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y

IV. La decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

Artículo 107.- Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

Artículo 108.- Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.

Artículo 109.- El acceso a información de carácter privado relativa a las personas contenidas en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.

Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

Artículo 110.- El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

- I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;
- II. Su traducción, adaptación, reordenación y cualquier otra modificación;
- III. La distribución del original o copias de la base de datos;
- IV. La comunicación al público, y
- V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

Artículo 111.- Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

Artículo 112.- Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

Artículo 113.- Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.

Artículo 114.- La transmisión de obras protegidas por esta Ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.

De esta forma la ley protege a los desarrolladores de software ya sea siendo estos individuos ajenos a una empresa o perteneciendo a una.

4.2 Ley de propiedad industrial

En caso de empresas desarrolladoras de software se amplía todavía más la regulación de derechos de autor, incluyendo en las leyes los casos de espionaje industrial y robo de secretos, como veremos a continuación.



Cámara de Diputados del H. Congreso de la Unión
Secretaría General
Secretaría de Servicios Parlamentarios
Dirección General de Bibliotecas

LEY DE LA PROPIEDAD INDUSTRIAL
Nueva Ley publicada en el Diario Oficial de la Federación el 27 de junio de 1991

TEXTO VIGENTE
Última reforma publicada DOF 25-01-2006

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Presidencia de la República.

CARLOS SALINAS DE GORTARI, Presidente Constitucional de los Estados Unidos Mexicanos, a sus habitantes, sabed:

Que el H. Congreso de la Unión, se ha servido dirigirme el siguiente

DECRETO

"EL CONGRESO DE LOS ESTADOS UNIDOS MEXICANOS, DECRETA:

LEY DE LA PROPIEDAD INDUSTRIAL

TITULO PRIMERO

Disposiciones Generales

Capítulo Único

Artículo 1o.- Las disposiciones de esta Ley son de orden público y de observancia general en toda la República, sin perjuicio de lo establecido en los Tratados Internacionales de los que México sea parte. Su aplicación administrativa corresponde al Ejecutivo Federal por conducto del Instituto Mexicano de la Propiedad Industrial.

Artículo 2o.- Esta ley tiene por objeto:

I.- Establecer las bases para que, en las actividades industriales y comerciales del país, tenga lugar un sistema permanente de perfeccionamiento de sus procesos y productos.

II.- Promover y fomentar la actividad inventiva de aplicación industrial, las mejoras técnicas y la difusión de conocimientos tecnológicos dentro de los sectores productivos.

III.- Propiciar e impulsar el mejoramiento de la calidad de los bienes y servicios en la industria y en el comercio, conforme a los intereses de los consumidores.

IV.- Favorecer la creatividad para el diseño y la presentación de productos nuevos y útiles.

V. Proteger la propiedad industrial mediante la regulación y otorgamiento de patentes de invención; registros de modelos de utilidad, diseños industriales, marcas, y avisos comerciales; publicación de nombres comerciales; declaración de protección de denominaciones de origen, y regulación de secretos industriales.

VI. Prevenir los actos que atenten contra la propiedad industrial o que constituyan competencia desleal relacionada con la misma y establecer las sanciones y penas respecto de ellos

TITULO TERCERO

De los Secretos Industriales

Capítulo Único

Artículo 82.- Se considera secreto industrial a toda información de aplicación industrial o comercial que guarde una persona física o moral con carácter confidencial, que le signifique obtener o mantener una ventaja competitiva o económica frente a terceros en la realización de actividades económicas y respecto de la cual haya adoptado los medios o sistemas suficientes para preservar su confidencialidad y el acceso restringido a la misma.

La información de un secreto industrial necesariamente deberá estar referida a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción; o a los medios o formas de distribución o comercialización de productos o prestación de servicios.

No se considerará secreto industrial aquella información que sea del dominio público, la que resulte evidente para un técnico en la materia, con base en información previamente disponible o la que deba ser divulgada por disposición legal permisos, autorizaciones, registros, o cualesquiera otros actos de autoridad o por orden judicial. No se considerará que entra al dominio público o que es divulgada por disposición legal aquella información que sea proporcionada a cualquier autoridad por una persona que la posea como secreto industrial, cuando la proporcione para el efecto de obtener licencias,

Artículo reformado DOF 02-08-1994

Artículo 83.- La información a que se refiere el artículo anterior, deberá constar en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros instrumentos similares.

Artículo 84.- La persona que guarde un secreto industrial podrá transmitirlo o autorizar su uso a un tercero. El usuario autorizado tendrá la obligación de no divulgar el secreto industrial por ningún medio.

En los convenios por los que se transmitan conocimientos técnicos, asistencia técnica, provisión de ingeniería básica o de detalle, se podrán establecer cláusulas de confidencialidad para proteger los secretos industriales que contemplen, las cuales deberán precisar los aspectos que comprenden como confidenciales.

Artículo 85.- Toda aquella persona que, con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a un secreto industrial del cual se le haya prevenido sobre su confidencialidad, deberá abstenerse de revelarlo sin causa justificada y sin consentimiento de la persona que guarde dicho secreto, o de su usuario autorizado.

Artículo 86.- La persona física o moral que contrate a un trabajador que esté laborando o haya laborado o a un profesionista, asesor o consultor que preste o haya prestado sus servicios para otra persona, con el fin de obtener secretos industriales de ésta, será responsable del pago de daños y perjuicios que le ocasione a dicha persona.

También será responsable del pago de daños y perjuicios la persona física o moral que por cualquier medio ilícito obtenga información que contemple un secreto industrial.

Artículo 86 BIS.- La información requerida por las leyes especiales para determinar la seguridad y eficacia de productos farmoquímicos y agroquímicos que utilicen nuevos componentes químicos quedará protegida en los términos de los tratados internacionales de los que México sea parte.

Artículo adicionado DOF 02-08-1994

Artículo 86 BIS 1.- En cualquier procedimiento judicial o administrativo en que se requiera que alguno de los interesados revele un secreto industrial, la autoridad que conozca deberá adoptar las medidas necesarias para impedir su divulgación a terceros ajenos a la controversia.

Ningún interesado, en ningún caso, podrá revelar o usar el secreto industrial a que se refiere el párrafo anterior.

Con estas leyes se pretende dar mayor seguridad al sector informático, tanto en sus desarrollos intelectuales como en sus creaciones mercantiles a nivel internacional.

4.3 Código penal federal.

Nuestro código penal juega un papel muy importante en el desarrollo de los establecimientos legales en cuanto a que establece las penas en las que incurrir los delincuentes que violan las leyes, define a las personas responsables de los delitos.



Cámara de Diputados del H. Congreso de la Unión
Secretaría General
Secretaría de Servicios Parlamentarios
Dirección General de Bibliotecas
CÓDIGO PENAL FEDERAL

Nuevo Código Publicado en el Diario Oficial de la Federación el 14 de agosto de 1931

TEXTO VIGENTE
Última reforma publicada DOF 28-06-2007

Al margen un sello que dice: Poder Ejecutivo Federal.- Estados Unidos Mexicanos.-México.- Secretaría de Gobernación.

El C. Presidente Constitucional de los Estados Unidos Mexicanos, se ha servido dirigirme el siguiente Decreto:

PASCUAL ORTIZ RUBIO, Presidente Constitucional de los Estados Unidos Mexicanos, a sus habitantes, sabed:

Que en uso de las facultades que le fueron concedidas por Decreto de 2 de enero de 1931, ha tenido a bien expedir el siguiente

CÓDIGO PENAL FEDERAL

LIBRO PRIMERO

TITULO PRELIMINAR

Artículo 1o.- Este Código se aplicará en toda la República para los delitos del orden federal.

Artículo 2o.- Se aplicará, asimismo:

I. Por los delitos que se inicien, preparen o cometan en el extranjero, cuando produzcan o se pretenda que tengan efectos en el territorio de la República; o bien, por los delitos que se inicien, preparen o cometan en el extranjero, siempre

que un tratado vinculativo para México prevea la obligación de extraditar o juzgar, se actualicen los requisitos previstos en el artículo 4o. de este Código y no se extradite al probable responsable al Estado que lo haya requerido, y

II.- Por los delitos cometidos en los consulados mexicanos o en contra de su personal, cuando no hubieren sido juzgados en el país en que se cometieron.

CAPÍTULO III

Personas responsables de los delitos

Artículo 13.- Son autores o partícipes del delito:

- I.- Los que acuerden o preparen su realización.
- II.- Los que los realicen por sí;
- III.- Los que lo realicen conjuntamente;
- IV.- Los que lo lleven a cabo sirviéndose de otro;
- V.- Los que determinen dolosamente a otro a cometerlo;
- VI.- Los que dolosamente presten ayuda o auxilien a otro para su comisión;
- VII.- Los que con posterioridad a su ejecución auxilien al delincuente, en cumplimiento de una promesa anterior al delito y
- VIII.- los que sin acuerdo previo, intervengan con otros en su comisión, cuando no se pueda precisar el resultado que cada quien produjo.

Los autores o partícipes a que se refiere el presente artículo responderán cada uno en la medida de su propia culpabilidad.

CAPÍTULO II

Acceso ilícito a sistemas y equipos de informática

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.

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 6.- 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 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

TITULO VIGESIMO SEXTO

De los Delitos en Materia de Derechos de Autor

Artículo 424.- Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa:

I. Al que especule en cualquier forma con los libros de texto gratuitos que distribuya la Secretaría de Educación Pública;

II. Al editor, productor o grabador que a sabiendas produzca más números de ejemplares de una obra protegida por la Ley Federal del Derecho de Autor, que los autorizados por el titular de los derechos;

III. A quien use en forma dolosa, con fin de lucro y sin la autorización correspondiente obras protegidas por la Ley Federal del Derecho de Autor.

Artículo 424 bis.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, video gramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, video gramas o libros a que se refiere el párrafo anterior, o

II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Artículo 424 ter.- Se impondrá prisión de seis meses a seis años y de cinco mil a treinta mil días multa, a quien venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa, con fines de especulación comercial, copias de obras, fonogramas, video gramas o libros, a que se refiere la fracción I del artículo anterior.

Si la venta se realiza en establecimientos comerciales, o de manera organizada o permanente, se estará a lo dispuesto en el artículo 424 Bis de este Código.

Artículo 425.- Se impondrá prisión de seis meses a dos años o de trescientos a tres mil días multa, al que a sabiendas y sin derecho explote con fines de lucro una interpretación o una ejecución.

Artículo 426.- Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, en los casos siguientes:

I. A quien fabrique, importe, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal, y

II. A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.

Artículo 428.- Las sanciones pecuniarias previstas en el presente título se aplicarán sin perjuicio de la reparación del daño, cuyo monto no podrá ser menor al cuarenta por ciento del precio de venta al público de cada producto o de la prestación de servicios que impliquen violación a alguno o algunos de los derechos tutelados por la Ley Federal del Derecho de Autor.

Artículo 429.- Los delitos previstos en este título se perseguirán por querrela de parte ofendida, salvo el caso previsto en el artículo 424, fracción I, que será perseguido de oficio. En el caso de que los derechos de autor hayan entrado al dominio público, la querrela la formulará la Secretaría de Educación Pública, considerándose como parte ofendida.

De esta manera se establece en las leyes las multas y castigos que habrá que aplicarse a los infractores, sin embargo para darnos una idea de si estas son suficientes es necesario hacer comparativas con países que tienen una legislación más experimentada en el mundo de la tecnología informática, aquí presentamos algunas comparativas con los Estados Unidos.

4.4 Comparativas entre criterios de los tribunales norteamericanos y mexicanos para resolver conflictos por violaciones de derechos de autor.

Hoy en día se están gestando transformaciones importantes en los criterios para la solución de violaciones al derecho de autor, tenemos grandes brechas que se abren al enfrentar el poder de los grandes monopolios internacionales que controlan los medios de comunicación y quieren controlar la información y el conocimiento.

Estas experiencias podrán convertirse en el paradigma de un nuevo modelo de producción y distribución culturales.

Esto afecta a México a la hora de incluir la protección al derecho de autor dentro de los acuerdos comerciales, ya que los productos y servicios culturales se ven como una mercancía más sujeta al "libre comercio" entre desiguales.

Los Aspectos de propiedad intelectual relacionados con el comercio, la propiedad intelectual mexicana se vinculo a los acuerdos comerciales.

Un ejemplo de estas comparativas se discuten en tratados comerciales como el TLC. El objetivo fue lograr la homogenización de las legislaciones con independencia de las necesidades y posibilidades de los países subdesarrollados y con ello la garantía a la protección de las inversiones y el dominio de los mercados por parte de los países desarrollados. Sin embargo esto también refuerza en la actualidad la desigualdad, arruina las economías y pone en grave peligro las culturas nacionales.

En México la aplicación del TLC impidió que se aprobaran estímulos fiscales a las producciones cinematográficas nacionales.

Se vio que para los países de pocos recursos, aplicar y hacer cumplir un régimen de derechos de propiedad intelectual diseñado por y para países desarrollados, ejerce presión sobre sus débiles administraciones y ya escasas economías, colocándolos en una posición desventajosa. Esto debido a que es necesario para México no sólo la adopción de normas de mayor severidad, sino todo un sistema para garantizar su cumplimiento.

A países cuya situación económica es pésima y cuyas culturas, incluidas sus lenguas y el patrimonio material e inmaterial nacional se encuentran en peligro de ser extinguido, se les exige la implementación de medidas en frontera, formación de personal calificado, y otras acciones que no están en disposición ni en posibilidades de cumplir, so pena de ser sancionados económicamente o incluidos en una lista negra de los países donde los intereses comerciales de los EEUU y otros países desarrollados "no se encuentran debidamente protegidos".

En los EEUU cada vez que están a punto de expirar los plazos del copyright los grupos de presión aumentan su actividad.

Los plazos del copyright en los Estados Unidos han sido extendidos por el Congreso en 1831, 1909, 1962 y luego más y más, once veces en cuarenta años.

Estas prolongaciones de los plazos de protección de los derechos de autor perjudican a los usuarios de la información, aleja en tiempo a las fuentes creativas e intelectuales del dominio público, y distorsiona el equilibrio que debe existir entre los derechos de los titulares y los de la sociedad

Además en la legislación norteamericana, el límite borroso de la ley, unido a las extraordinarias responsabilidades legales si se cruzan estos límites, conllevan a que en muy pocas ocasiones pueda ser ejercido efectivamente, sin temor a ser reclamado. Por ejemplo, los abogados de las universidades americanas elaboran directrices sobre el status legal de las diapositivas utilizadas en las clases por los profesores e incluso prohíben a los bibliotecarios el uso de algunas, para evitar que demanden a la universidad. O sea, excepciones que en la ley han sido fijadas, en la práctica se hace muy difícil poder utilizarlas.

Las revistas científicas que antes eran adquiridas por las bibliotecas y podían ser usadas libremente por los clientes, al cambiar al formato digital en muchas ocasiones no pueden ser utilizadas sin pagar.

También las leyes del copyright dificultan e impiden la digitalización de obras a los fines de su conservación para la investigación, aún cuando no tienen ya un interés comercial.

Sobre la protección a los programas de ordenador, de la forma en que se establece, no tiene antecedente, ya que aún cuando se tiene licencia para explotarse legítimamente la "obra", su código no puede ser conocido. Este tipo de protección tiene que ver más con la promoción de la dependencia tecnológica que con la creación, aunque la propuesta y ya extendida protección

por medio de patentes, constituye otra barbaridad de mayor gravedad.

Igualmente se tiende a englobar derechos de autor y derechos conexos como titulares de derechos de propiedad intelectual, al igual que titulares originarios y titulares derivados.

La Ley contra el robo electrónico de EEUU convirtió en delito poseer o distribuir copias de material en línea registrado, fuera en beneficio propio o no. Sobre la base de la nueva ley norteamericana entre cuarenta y sesenta millones de ciudadanos de los EE UU pueden ser considerados criminales por este concepto.

De esta manera las leyes americanas son muy estrictas comparadas con las mexicanas, el cómo se puedan establecer relaciones entre ellas resulta muy difícil en un ámbito comercial igualitario.

En México este concepto representa un problema ya que la copia ilegal de programas de cómputo no tiene un control plenamente garantizado.

En cuanto a la apropiación por parte de las empresas de los conocimientos, informaciones, e investigaciones que pertenecen al dominio público y financiados por fondos públicos, sucede que la protección legal a las bases de datos no puede revertirse en limitaciones para acceder a los datos públicos. Los servicios relacionados con datos públicos no pueden ser asumidos por entes privados pues privatizan y encarecen de hecho el acceso a los mismos. por ejemplo: En 1985, todos los datos del programa público americano de observación de la tierra por satélite Landsat fueron traspasados a una filial de General Motors y de General Electric. Resultado: el coste de acceso a los datos fue multiplicado por veinte y las universidades públicas no pudieron acceder a los datos aun cuando estos habían sido obtenidos gracias a una financiación íntegramente pública. Su explotación favoreció principalmente a las grandes compañías petrolíferas, subvencionadas así directamente.

Si bien es cierto en México la venta de la información del padrón electoral en discos por parte de funcionarios públicos causo expectación por el significado publico de los intereses comerciales, hasta que punto todo el material cultural y de carácter público podrá ser protegido ante el creciente mercado internacional. No hay una conclusión definitiva, solo el paso del tiempo dará a conocer las consecuencias de estas diferencias legales entre países comercialmente unidos.

CAPÍTULO 5

Análisis de un caso específico ante las leyes mexicanas

5.1 Detección del delito.

Si bien es cierto detectar un delito informático, darle seguimiento y aplicar las leyes vigentes para su solución resulta algo muy difícil, la mayoría de estos nunca son rebelados a la luz pública, los afectados se ven solos y buscan el amparo de la ley, veamos de que manera actúa esta y que problemas enfrentan las partes involucradas en los delitos.

Noviembre 21, 2006

05:18 PM

NOTIMEX

México, 21 Nov. (Notimex).- El notario público 185 del Distrito Federal, Humberto Hassey Perezcano, denunció que Banco Santander de México actúa en forma "irresponsable y negligente", en la investigación y solución de un fraude cibernético por 3.5 millones de pesos, ejercido en su contra.

La institución por su parte se negó a depositar el dinero sustraído, así como resarcir los gastos que implicó investigar el ilícito, además exigió retirar la denuncia penal (averiguación previa número T 3/02240/06-09 P.G.R.), presentada ante las autoridades ministeriales de la capital del país.

En conferencia de prensa, el notario detalló que el pasado 29 de agosto recibió la llamada de una ejecutiva del banco citado, para aclarar la ejecución inusual de tres retiros en forma consecutiva que sumaban 3.5 millones de pesos, mismos que no fueron reconocidos por él y por lo tanto exigió cancelar.

Aunque el banco tuvo oportunidad de suspender las transferencias, que según versiones de la institución tenían la encomienda de pagar la nómina del personal de la notaría, lo cual es inverosímil pues esta sólo es utilizada para pagar impuestos, los ejecutivos del banco rehusaron cancelarlas.

5.2 Flujo de la aplicación de la ley vigente

A través de la firma Infocorp, representante de Norton Symantec en México, se logró comprobar que las transacciones no fueron realizadas desde las instalaciones de la notaría o lugar público alguno que pudiera facilitar la entrada de un hacker.

"El artículo 267 de la Ley de Títulos y Operaciones de Crédito establece que en el depósito bancario de dinero, la suma depositada transfiere la propiedad al depositario, Santander Serfín no reconoce que el fraude fue en su contra, y no en contra del depositante".

Tras días de "mentiras" y gestiones ante el banco, Hassey Perezcano notario afectado, decidió levantar una denuncia penal en contra de quién resulte responsable, ante la Procuraduría General del Distrito Federal, misma que fue turnada a la Procuraduría General de la República por considerarse delito del fuero federal.

La apatía de los funcionarios del banco por resolver el fraude, obligó al notario hacer público este ilícito a través de la colocación de dos espectaculares ubicados en las inmediaciones del D.F.

5.3 Problemas encontrados durante la aplicación de la ley.

En algunos robos a cuentahabientes en el mismo banco existen dos alternativas, que los fondos sean desviados por empleados del mismo banco o que sea obra de un hacker por Internet, estos ilícitos son responsabilidad tanto de los bancos, las autoridades y de los mismos clientes, cuando sucede un ilícito se trata de establecer quien fue el refractor, por parte de los bancos se tiene en contra que los sistemas utilizados por estos dicen ser muy avanzados y los empleados, pese a lo que se dice de que no tienen acceso a las claves de los clientes. Cada banco cuenta con una certificación notarial para probarlo, se demostró por el Lic. Adolfo Posadas, ante Notario Público que las claves de las cuentas si pueden cambiarse por el banco, esto faculta que los empleados de los bancos puedan ser delincuentes.

En otro punto en contra los bancos se comportan individualistas sobre la información de las previsiones y los cuidados que deben tener los clientes, entre algunas fallas los especialistas consultados aseguraron que los bancos no verifican si la credencial que les presentan es falsa o verdadera, cuando se abre una cuenta.

Esta característica aunada a que cada banco tiene sus propios sistemas de seguridad, propicia que efectivamente hay algunos bancos que tienen menos cuidado en la apertura de cuentas; piden menos datos, por ejemplo para abrir cuentas falsas que van a servir como recaudadoras de lo robado. Pero en eso, cada banco tiene que hacer su trabajo.

A la ley le toca enfrentar que bajo el cobijo del secreto bancario, el banco se niega a aclarar quienes y de qué forma llevan a cabo los delitos, y aunque autoridades ministeriales citaron a representantes del banco en el caso del robo de los 3.5 millones, nadie se presentó a aclarar los hechos".

Lo raro de este asunto fue que después de los espectaculares, el banco dijo que ya había recuperado el dinero robado, y se negó a dar detalles de cómo paso todo, también se negó a pagar daños y perjuicios, exigió el retiro de la denuncia penal, y rechazó esclarecer la forma y los propietarios de la cuenta a donde fueron transferidos los 3.5 millones de pesos hurtados.

El notario Hassey Perezcano aseguró desconocer si el banco actuó por negligencia, irresponsabilidad o "encubrimiento", sin embargo advirtió que ante el silencio del director general del banco, Marcos Martínez, la demanda se mantuvo con el fin de esclarecer los hechos, además de sacar a luz pública otros casos de fraude relacionados con esta institución.

El análisis legal de estas conductas se considera en las fracciones III, IV y V del artículo 400 del Código Penal Federal, que remiten expresamente a las conductas desarrolladas por los directivos de las entidades financieras. En la fracción III, que se refiere a las acciones de favorecer el ocultamiento del sujeto activo (en este caso el defraudador), impone una obligación genérica de cualquier ciudadano de denunciar a las autoridades a quien se sabe o se sospecha pudo haber cometido un delito.

La fracción IV refiere que, escudándose en el artículo 117 de la Ley de Instituciones de Crédito que ampara el secreto bancario, los bancos se niegan a colaborar con los defraudados y con las autoridades, lo que hace que el tipo penal se cumpla de manera cabal para quienes, so pretexto legal, pretendan paralizar las investigaciones. La razón de esta falta de cooperación, acusan defraudados y especialistas, es que los bancos tienden a proteger a sus empleados, ya que las estadísticas del FBI marcan que en 80 por ciento de estos casos, empleados o funcionarios bancarios están involucrados.

Prueba pericial de los fraudes bancarios

Cuando los bancos afirman que algún servicio es considerado una firma electrónica avanzada, en el caso de la banca electrónica y por ende es imposible hacer movimientos sin las claves del cliente, mismas que solo el cliente tiene en su poder, y por consiguiente, todo es responsabilidad del cliente.

Los análisis de los clientes se basan principalmente en los siguientes puntos, para decidir si el banco es responsable o no.

Sabiendo que el banco como administrador del sistema:

1.-Puede hacer movimientos en las cuentas del cliente

2.-Puede cambiar las claves del cliente, haciéndose así pasar por el cliente, al hacer los movimientos (ya que su sistema dice que siempre que se acceda con claves validas, entonces es el cliente el que supuestamente esta haciendo los movimientos).

Entonces, a la ley solo le queda solicitar una prueba pericial al sistema del banco en cuestión, con la esperanza de proveer apoyo a los clientes que quedan indefensos ante los silencios bancarios.

DICTAMEN PERICIAL

El dictamen pericial versará sobre los siguientes puntos y cuestionamientos:

a) El perito Determinará si el sistema de servicio de Internet de Banco es seguro como para ser considerado como firma electrónica avanzada según los términos del código de comercio.

b) Constatará si el sistema de servicio de Internet de Banco y/o las cuentas pueden ser accedidas por algún empleado desde la sucursal bancaria o desde fuera de ella y en su caso si para ello precisa de las claves del titular de la cuenta o puede hacerlo sin ellas.

c) Determinará si un tercero puede acceder al sistema de servicio de Internet de Banco y/o a las cuentas desde dentro o fuera de la sucursal bancaria o desde fuera de ella y, en su caso si requiere de las claves del titular de la cuenta o puede hacerlo sin ellas.

d) Determinará si los medios de transmisión de las claves y las operaciones del sistema de servicio de Internet de Banco son seguras, si los datos viajan abiertos o encriptados y si alguien puede interferir desde dentro o fuera del banco esas operaciones y si pueden ser borradas las claves.

e) Determinarán si el usuario, número de cuenta y clave de usuario o password del sistema de servicio de Internet de Banco pueden ser capturados por terceras personas y utilizado haciéndose pasar por el titular.

f) Constatará desde que dirección IP o dirección de Internet se realizaron las operaciones que se reclaman y si las mismas fueron hechas desde la computadora del titular de la cuenta, desde una computadora del banco o desde una computadora de fuera de ambos y, en su caso desde que dirección IP y que dirección física.

g) Al finalizar las pruebas se emitirán las conclusiones.

Estos puntos, fueron una sugerencia que realizo él:

Dr. Gabriel Campoli, Especialista en Delitos Informáticos

Desempeñándose como Profesor Investigador en el INACIPE (Instituto Nacional de Ciencias Penales)

5.4 Sanciones aplicadas y conclusión del caso.

Desafortunadamente durante esta investigación no se pudo saber cuáles son las cifras de los fraudes cometidos por Internet, sólo se sabe de cifras hipotéticas. Los bancos cuidan muy celosamente este tema; sin embargo en las fuentes podemos citar que quien está a la cabeza, según las estadísticas de nuestros casos es Bancomer.

Y sus directivos se enfrentarían en cada caso a la fracción V del artículo 400 del Código Penal Federal que señala que se otorgará prisión de tres meses a tres años y de 15 a 60 días multa, a quien "no procure, por los medios lícitos que tenga a su alcance, y sin riesgo para su persona, impedir la consumación de los delitos que sabe van a cometerse o se están cometiendo".

CASOS REGISTRADOS EN robosbancarios.com*

CLIENTE	BANCO	MONTO DEFRAUDADO
Alejandro Sánchez	BBVA Bancomer	2.9 Millones de pesos
Hugo Guerra	BBVA Bancomer	10.5 Millones de Pesos
Ivan Quezada	BBVA Bancomer	49 mil pesos
Francisco Agüero	BBVA Bancomer	155 mil pesos
Ricardo Rocha	BBVA Bancomer	145 mil pesos
Gerardo Porras	BBVA Bancomer	255 mil pesos
Carmen Valdez	BBVA Bancomer	94 mil pesos
Grupo Corporativo Diamante	BBVA Bancomer	262 mil pesos
Fernando de la Torre	BBVA Bancomer	75 mil pesos
Mario Pesquera Ostos, Bufete Ostos, Ostos y Pesquera Asociados S.C.	BBVA Bancomer	N/D

*Elaboración propia con datos de robosbancarios.com.

En el caso del artículo 400 bis, "existen al menos tres conductas muy claras, ya que son los empleados y directivos de una institución financiera los que administran y transfieren los fondos obtenidos de la actividad ilícita de las transferencias electrónicas no autorizadas". Esto, con el fin de ocultar el origen y destino de los fondos; aunque aquí el problema es la falta de investigación de la SHCP en la materia para hacer las denuncias correspondientes, ya que, según el texto legal, esto es indispensable para su procedencia.

Mostramos algunas leyes que son de utilidad saber, en el caso de algún fraude bancario, en este caso mostramos el CAPÍTULO II del Depósito, de la Ley de Instituciones de Crédito:

LEY GENERAL DE TITULO Y OPERACIONES DE CREDITO

TITULO CUARTO DE LAS DISPOSICIONES GENERALES Y DE LA CONTABILIDAD

CAPÍTULO II - Del depósito

Sección Primera - Del Depósito Bancario de Dinero

Artículos 267, 268, 269, 270, 271, 272, 273, 274 y 275

Artículo 267.- El depósito de una suma determinada de dinero en moneda nacional o en divisas o monedas extranjeras, transfiere la propiedad al depositario y lo obliga a restituir la suma depositada en la misma especie, salvo lo dispuesto en el artículo siguiente.

Artículo 268.- Los depósitos que se constituyan en caja, saco o sobre cerrados, no transfieren la propiedad al depositario, y su retiro quedará sujeto a los términos y condiciones que en el contrato mismo se señalen.

Artículo 269.- En los depósitos a la vista, en cuenta de cheques, el depositante tiene derecho a hacer libremente remesas en efectivo para abono de su cuenta y a disponer, total o parcialmente, de la suma depositada, mediante cheques girados a cargo del depositario. Los depósitos en dinero constituidos a la vista en instituciones de crédito, se entenderán entregados en cuenta de cheques, salvo convenio en contrario.

Para que el depositante pueda hacer remesas conforme a este artículo, en títulos de crédito, se requerirá autorización del depositario. Los abonos se entenderán hechos salvo buen cobro.

Artículo 270.- Los depósitos recibidos en cuentas colectivas en nombre de dos o más personas, podrán ser devueltos a cualquiera de ellas o por su orden, a menos que se hubiere pactado lo contrario.

Artículo 271.- Los depósitos bancarios podrán ser retirables a la vista, a plazo o previo aviso. Cuando al constituirse el depósito previo aviso no se señale plazo, se entenderá que el depósito es retirable al día hábil siguiente a aquél en que se dé el aviso. Si el depósito se constituye sin mención especial de plazo, se entenderá retirable a la vista.

Artículo 272.- Salvo estipulación en contrario, los depósitos serán pagaderos en la misma oficina en que hayan sido constituidos.

Artículo 273.- Salvo convenio en contrario, en los depósitos con interés, éste se causará desde el primer día hábil posterior a la fecha de la remesa y hasta el último día hábil anterior a aquél en que se haga el pago.

Artículo 274.- Los depósitos en cuenta de cheques se comprobarán únicamente con recibos del depositario o con anotaciones hechas por él en las libretas que al efecto deberá entregar a los depositantes, salvo lo que previene la Ley General de Instituciones de Crédito.

Artículo 275.- Las entregas y los reembolsos hechos en las cuentas de depósito a plazo o previo aviso, se comprobarán únicamente mediante constancias por escrito, precisamente nominativas y no negociables, salvo lo dispuesto en la Ley General de Instituciones de Crédito.

Recomendaciones para cuenta habientes bancarios, para evitar fraudes cibernéticos de sus cuentas.

Es necesario destacar la labor conjunta que realizan la Comisión Nacional de Defensa de los Usuarios del Servicio Financiero (Condusef), que preside Oscar Levín Coppel; la Asociación Mexicana de Bancos presidida por Marcos Martínez; y la PGR, a través de la nueva policía cibernética, para combatir el creciente número de fraudes electrónicos a cuenta habientes bancarios.

RECOMENDACIONES:

No hacer caso de los e-mail que llegan a los usuarios de bancos, en los que se les pide que verifiquen urgentemente sus datos para supuestamente evitar que se pierdan, porque hay un proceso de renovación del portal o algún otro pretexto similar.

No hacer caso de los e-mail que llegan, en el que se pide a los clientes que actualicen los datos de su cuenta para evitar que sean reportados al Buró de Crédito por irregularidades en la información de un crédito.

Verificar constantemente el saldo de las cuentas, cambiar en forma frecuente la clave de acceso y el NIP, y nunca utilizar un servicio público de Internet para realizar transacciones bancarias vía electrónica.

En síntesis la recomendación de la Condusef y de la ABM es que nunca se proporcionen datos vía electrónica, ya que ningún banco solicita por correo electrónico a sus clientes que confirmen la información de su cuenta y mucho menos su clave de acceso.

Para detectar el robo de identidad, la Condusef recomienda que por lo menos una vez al año se solicite al Buró de Crédito el reporte crediticio, al cual se tiene derecho en forma gratuita.

CAPÍTULO 6

Propuesta de reforma del Código Penal federal en materia de delitos informáticos

6.1 Propuesta a las reformas del Código Penal federal en materia de delitos informáticos

La importancia de la Información es tal que la Constitución Política de los Estados Unidos Mexicanos, en su reforma de 1977 reconoce el Derecho a la Información, por adiciones a los artículos 6º y 41, "de tal suerte, resultando, que estructuralmente hablando se consagra como garantía individual, y también como garantía formalmente política y materialmente social" .

En México las leyes ya consideran y castigan los delitos cibernéticos. Tal es el caso del código de comercio que acepta los mensajes digitales como prueba. La Agencia Federal de Investigación (AFI) cuenta con la unidad de delitos informáticos, la Policía Federal Preventiva (PFP) con la policía cibernética, hay peritos especializados en la Procuraduría General de la República (PGR) y existen algunas unidades estatales.

El Código Penal Federal vigente fue reformado el 17 de mayo de 1999 (DOF). Aunque el lapso de tiempo que ha transcurrido desde entonces es relativamente corto, los avances tecnológicos han sido vertiginosos y radicales en algunos casos.

La legislación mexicana en materia de delitos informáticos dista mucho de ser perfecta, es sólo el primer paso para lograr un ambiente sano y seguro para los negocios y comunicaciones electrónicas en nuestro país.

Algunos de los defectos del Código Penal Federal en esta área son los siguientes:

- A) Contempla que constituye el delito sólo si se accesa un sistema informático protegido por un mecanismo de seguridad. Esto es tan absurdo como si dijéramos que para que se diera el delito de allanamiento de morada es necesario que la casa habitada cuente con un candado, llave, portón o cadena protectora. La justicia no puede reducirse sólo a aquellos quienes tienen los medios económicos para proteger su computadora con un mecanismo de seguridad.

¿O qué acaso el que tu computadora esté conectada al Internet significa que cualquiera puede justificadamente entrar en ella, husmear y merodear tranquilamente, borrar o destruir archivos, sólo porque no está protegida por algún mecanismo de seguridad?

- B) El Código Penal no define qué debe entenderse por "mecanismo de seguridad". ¿Qué es un mecanismo de seguridad de un sistema informático? ¿Un password? ¿Un candado contra robo (físico)? ¿Un Firewall? ¿Un sistema criptográfico de llave pública? o simplemente ¿Tener la computadora encerrada en un cuarto bajo llave o con un guardia de seguridad a un lado? Esta vaga redacción sin duda traerá innumerables problemas de interpretación a la hora de que le toque a un juez analizar un caso concreto.
- C) Nuestro Código no contempla todos los tipos más comunes de ataques informáticos. El capítulo II adicionado en virtud de la reforma del 17 de mayo de 1999, de entrada está titulado de manera incorrecta: "Acceso Ilícito a Sistemas y Equipos de Informática". Aunque su articulado (Arts. 211 bis 1 al 7) no habla en todo momento de acceso ilícito, el título del capítulo sí enfoca su contenido a accesos ilícitos precisamente. El problema radica en que muchos ataques informáticos se perpetran sin necesidad alguna de acceder directamente un sistema informático. El mejor ejemplo es el ataque de "Denegación de Servicios" (Denial of Services o Distributed Denial of Services), cuyo objetivo no es "modificar, destruir o provocar pérdida de información" como reiteradamente lo establece el Código Penal Federal, sino simplemente imposibilitar o inhabilitar un servidor temporalmente para que sus páginas o contenidos no puedan ser vistos por los cibernautas mientras el servidor está caído.

Derecho de la informática

El Doctor Juan José Ríos Estavillo plantea a manera de hipótesis en el libro "Derecho e Informática en México", lo siguiente: ¿Puede el Derecho de la informática ser objeto de estudio metodológico como rama autónoma en el campo jurídico?

Para esto señala los siguientes puntos positivos y negativos de tal presunta existencia.

Elementos Negativos o que pueden determinar que no exista el Derecho de la Informática

- El Derecho de la Informática no puede extenderse como un cuerpo normativo con naturaleza propia e independiente, por lo que no se le da la validez a la existencia autónoma o científica.
- Todo cuerpo normativo desde su perspectiva de disciplina debe respaldarse de normas sustantivas como de normas adjetivas, o bien, reglas propias reguladoras del ser, hacer o no hacer, como de reglas propias para la solución de sus controversias.
- Considerando que en nuestro país es casi inexistente la localización de normas sustantivas que regulen la materia, también nos encontramos con un vacío formal de normas adjetivas.
- De ahí que sea prudente resaltar que el encuentro que sufran, por un lado, el avance de la tecnología y, por el otro, el derecho deberán ser resueltas por el aparato jurídico propiamente hablando y no por

las reglas informáticas de tal relación; esto es, el derecho no debe supeditarse a la informática; por tal motivo, el Derecho de la Informática como tal no existe.

- La norma jurídica tiene origen en el desarrollo y convivencia de individuos en una sociedad tales individuos o gobernados plantean una serie de hechos que el Derecho regula, por lo que el avance normativo depende propiamente del individuo y no del avance tecnológico. De esta interpretación se afirma que en una relación que puede derivar en lo jurídico, el hecho va primero que derecho; así, la sociedad no puede estar supeditada al derecho sino el derecho a la sociedad, y ante esto, el derecho de la informática no puede existir como tal, ni puede dárseles valores autónomos.

Conceptos de Derecho Informático

El Derecho de la Informática ha sido considerado por Carrascosa López como "el conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones."

Otros han señalado que la informática como objeto de regulación jurídica ha dado origen al llamado derecho de la informática.

Por otro lado, Julio Téllez ha afirmado que **"es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática"**.

Para Emilio Suñ, "es el conjunto de normas reguladoras del objeto informática o de problemas directamente relacionados con la misma."

Juan José Ríos nos dice que podríamos conceptualizar el derecho de la Informática como el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma en las que exista algún bien que es o deba ser tutelado jurídicamente por las propias normas.

Según Juan José Ríos, es cuestionable todavía hoy si en verdad existe esta disciplina como tal, por lo que una gran mayoría de estudiosos de la materia han preferido analizar algunos campos en los que, aplicando la informática, se podrían relacionar los resultados con el campo del derecho, y así han preferido mejor estudiar los puntos siguientes:

- La protección jurídica de la información personal
- La protección jurídica del software
- El flujo de datos fronterizos
- Los convenios o contratos informáticos
- Los delitos informáticos
- El valor probatorio de los documentos electromagnéticos laboral y la necesidad de una regulación jurídica sobre este aspecto

A éstos habrá que agregar otro aspecto a legislar y que el Doctor Julio Téllez marca en su libro "Derecho Informático":

- Ergonomía Informática, que nos muestra la importancia de la informática en el ámbito.

En base a todo esto, se propone la siguiente exposición de motivos de reformas de diversos artículos del Código Penal Federal que a continuación se detallan explícitamente, dichas propuestas fueron elaboradas detalladamente con la ayuda de gente que conoce las leyes de nuestro país y el Código Penal Federal, abogados y funcionarios públicos.

PROPUESTA PARA MODIFICAR DIVERSOS ARTÍCULOS DEL CÓDIGO PENAL FEDERAL

Propuesta para reformar el "Título Noveno" del Código Penal Federal

En la columna derecha se encontrará la exposición de motivos para cada propuesta.

Disposición (artículos)	Exposición de Motivos
<p><u>TITULO NOVENO</u></p> <p>Reforma: REVELACIÓN DE SECRETOS Y DELITOS INFORMÁTICOS</p> <p>CAPÍTULO II: Reforma: DELITOS INFORMÁTICOS</p>	<p>El nombre del Título 9º y su respectivo Capítulo I actual son incorrectos, ya que buena parte de los ataques informáticos se realizan "desde afuera", sin acceder a una computadora. El ejemplo más sencillo es el ataque de "denegación de servicios", el cual se realiza enviando "paquetes" de información a un servidor web para inhabilitarlo.</p> <p>Otro ejemplo podrían ser los "virus", ya que el diseñador no tiene acceso directo a ninguna computadora, ya que desencadena el daño enviando el virus por correo electrónico o de maneras similares.</p>
<p>(ARTICULADO: Se derogan los artículos 211 bis 1 al 211 bis 7 para que se adicionen los siguientes:)</p>	
<p>ARTÍCULO 211 bis 1.- Para los efectos de este título se entenderá por:</p> <p>I.- Computadora (s): Dispositivo, sistema, equipo de informática o aparato automático para el tratamiento de la información, que obedece a programas formados por sucesiones de operaciones aritméticas y lógicas. Una computadora comprende una parte física (hardware), constituida por circuitos electrónicos de alta integración, y una parte no física (software); el objetivo es realizar funciones lógicas, aritméticas, transmisión o de almacenamiento de datos, así como para el tratamiento sistemático de la información mediante el procesamiento automático de datos electrónicos o de cualquier otra tecnología. Esta definición incluye las redes públicas y privadas de computadoras.</p>	<p>El factor de especificar claramente los términos técnicos en esta definición se busca evitar que sea lo mas amplia posible debido a los constantes avances en cuanto a la Computación se refiere.</p>

<p>II.- Programa(s) de cómputo o computación: la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.</p>	<p>La intención de dejar la definición de "programa de computación" exacta e idéntica a la definición del artículo 101 de la Ley Federal del Derecho de Autor es la de buscar una homogeneidad en cuanto a los términos que se manejan en las Leyes de nuestro País.</p> <p>Se incluye que puede ser utilizado para controlar el comportamiento de un dispositivo o sistema en donde los programadores lo usan para comunicar instrucciones a una computadora y poder ejecutar un programa. Así mismo, se define como un sistema de escritura para la descripción precisa de algoritmos o programas informáticos.</p>
<p>III.- Daño: deterioro o menoscabo a la integridad, confidencialidad y/o disponibilidad de datos, información, programas de cómputo, o computadoras.</p>	<p>Fueron incluidos elementos básicos que se busca tener tanto en los documentos electrónicos como en las comunicaciones: integridad, confidencialidad y disponibilidad.</p>
<p>IV.- Información: archivos o datos contenidos y/o transmitidos a través de una computadora, o por medios electrónicos, ópticos o de cualquier otra tecnología.</p>	<p>Definición del principal bien jurídico protegido: la información. Se usó el lenguaje actualmente contemplado por las reformas publicadas en el DOF el 29 de Mayo de 2000.</p>
<p>V.- Mecanismo de seguridad: dispositivo físico y/o electrónico, palabra clave, código de acceso, programa de cómputo o equipo informático que tenga por objetivo proteger una computadora, un programa de cómputo y/o la información contenida en una computadora, sistema o equipo informático de o contra:</p> <p>a) accesos internos o externos no autorizados; b) borrado, alteración o daño de información; c) ataque informático de cualquier índole. d) repudio del emisor o receptor de la información.</p> <p>También se entenderá por mecanismo de seguridad, cualquier dispositivo técnico utilizado para proteger un programa de cómputo contra su copiado, distribución o uso ilícito.</p>	<p>Con esta definición se corrige uno de los principales defectos del actual Código Penal Federal, ya que no incluye una definición de "mecanismo de seguridad". Esta frase puede tener muy diversas acepciones según el especialista que la interprete, si no se cuenta con una guía o definición apropiada.</p> <p>Al incluir el término "dispositivo físico y/o electrónico, programa de cómputo" se cubre la posibilidad de que el mecanismo de protección consista en un elemento de <i>hardware</i> y/o de <i>software</i>, tal como ocurre en la realidad.</p> <p>Se contemplan los propósitos principales de cualquier <i>firewall</i>: proteger una computadora o red de computadoras en contra de accesos externos no autorizados, borrado o alteración de información, ataques informáticos diversos, etc. Además, se distingue uno de los objetivos fundamentales de un sistema criptográfico asimétrico (el cual también puede ser un "mecanismo de seguridad"): el no repudio del emisor o receptor.</p> <p>Como ventaja adicional, se clarificó que también se entiende por el referido término "cualquier dispositivo para proteger programas de cómputo", lo cual es un golpe directo en contra de la piratería de <i>software</i>.</p>
<p>VI.- Datos o información personal: Cualquier información relacionada a una persona física identificada o identificable. Los datos personales usualmente contienen información que directa o indirectamente puede ser relacionada o ligada a una persona física en particular.</p>	<p>Este término es un derivado del bien jurídico protegido que hablábamos con anterioridad, la "información". La definición fue tomada de las "Guías de la Organización para el Desarrollo y la Cooperación Económica (OECD) para la Protección de la Privacidad y Flujo Transfronterizo de Datos Personales". (Apartado "1. b" de las Guías y apartado "41" de su Memorando de Explicación).</p> <p>De manera indirecta, la definición también busca proteger otro bien jurídico distinto, éste recae directamente en la persona: el derecho a la privacidad e intimidad.</p>
<p>ARTÍCULO 211 bis 2.- Comete el delito informático, la persona que con intención y sin derecho:</p>	<p>Tengamos presente que todas las actividades descritas a continuación (fracciones) deben ser cometidas con intención y sin derecho.</p>
<p>I.- Accese a información o a una computadora sin autorización o excediendo su</p>	<p>Se refiere a la actividad genérica conocida como "hacking" perpetrada tanto desde afuera como desde adentro de la organización (<i>insiders</i>).</p>

acceso autorizado;	
II.- Intercepte, modifique, altere, borre, destruya, provoque daño o pérdida de información contenida en computadoras o programas de cómputo;	Este término se refiere específicamente al " cracking ". Además, la "intercepción" se relaciona con las prácticas en que se usan <i>network scanners</i> , <i>packet sniffers</i> e <i>IP spoofing</i> para interceptar y/o conocer información para poder penetrar computadoras y disimular el ataque con información falsa. Cumple con los Artículos 3 (<i>Illegal interception</i>) y 4 (<i>Data interference</i>) de la <u>CECD</u> .
III.- Conozca, copie, divulgue o distribuya a terceros información o comunicaciones no dirigidas a él, contenidas en computadoras;	Aquí el "conocer" también implica el uso de herramientas como <i>packet sniffers</i> para monitorear información útil para el delincuente. La divulgación no nada mas se relaciona con "revelación de información confidencial", por poner un ejemplo, sino además con el traficar o distribuir nombres de usuario y <i>passwords</i> para penetrar computadoras.
IV.- Diseñe, introduzca, programe, distribuya o provoque la transmisión o ejecución de programas de computación, datos, información, códigos, conjuntos de instrucciones o comandos informáticos, que tengan por objeto: a) Impedir el uso, funcionamiento apropiado, causar daños a información, computadoras o programas de computación; b) Alterar la información o programas de computación contenidos en una computadora; c) Causar la negación de servicios de naturaleza informática realizados por una computadora o una red de computadoras;	Sin duda esta es una de las principales innovaciones de la propuesta. La fracción IV contempla varios tipos de ataques informáticos muy comunes no previstos en el actual Código Penal, tales como : virus , gusanos (<i>worms</i>), caballos de troya, bombas lógicas y el ataque de denegación de servicios (DoS) . Cumple con los Artículos 4 (<i>Data interference</i>) y 5 (<i>System interference</i>) de la <u>CECD</u> .
V.- Diseñe, programe, comercialice, trafique, transmita, haga disponibles o distribuya programas de cómputo, números de serie o registro, palabras clave o códigos de acceso, o información de cualquier naturaleza que sirva para violar mecanismos de seguridad de computadoras o programas de cómputo;	Esta fracción penaliza el tráfico de <i>passwords</i> , números de serie y demás datos que sirvan para violentar mecanismos de seguridad que usualmente protege al <i>software</i> . También incluye el diseño de dispositivos o programas destinados a violar estos mecanismos de protección, prácticas conocidas como " cracking " y " regging ". Este numeral busca proteger la propiedad intelectual, o más concretamente, los derechos de autor de los creadores de los programas de cómputo. Este tipo de acciones no están penadas actualmente por el artículo 231 de la Ley Federal del Derecho de Autor (<i>De las Infracciones en materia de comercio</i>). De manera tangencial, la fracción V del citado artículo 231 podría contemplar parte de las acciones delimitadas en la fracción en comento de la propuesta, pero no está redactado con la amplitud y claridad suficiente, ya que ni siquiera usa el término que la propia LFDA define como "programa de cómputo", sólo habla de "dispositivo o sistema". Cumple con el Artículo 6 (<i>Misuse of devices</i>) de la <u>CECD</u> .
VI.- Amenace, hostigue, intimide, aceche o cause temor a personas físicas o morales, mediante mensajes electrónicos, el uso de computadoras u otros mecanismos tecnológicos similares.	El " ciberacoso " puede ser definido como una conducta amenazante o aproximaciones no deseadas dirigidas a otro usando el Internet y otras formas de comunicación "en línea". <u>49 Estados</u> de los Estados Unidos de América ya han adoptado o modificado leyes en contra del "ciberacoso". Este ataque es dirigido principalmente en contra de niños y mujeres. En EUA el problema se ha vuelto tan serio, que en 1999 el Vicepresidente Al Gore pidió al Procurador General de Justicia que realizara <u>una investigación y un reporte</u> con recomendaciones para combatir el " <i>cyberstalking</i> ".
VII.- Comercialice, trafique, transmita, difunda, distribuya o haga disponible a través de computadoras o redes de computadoras, y/o	Esta fracción pretende tipificar la conducta consistente en la publicación y distribución de material ofensivo y nocivo para la sociedad. La gran mayoría de los <u>Estados</u> de la Unión Americana ya han reformado sus leyes para luchar en contra de la pornografía infantil .

<p>dispositivos de almacenamiento magnéticos, ópticos, electrónicos o de cualquier otra tecnología:</p> <p>a) Pornografía infantil;</p> <p>b) Información xenofóbica, racista, o discriminatoria de cualquier naturaleza;</p> <p>c) Incitaciones o provocaciones para cometer delitos de cualquier índole;</p> <p>d) Información que explique cómo realizar cualesquiera de los delitos contemplados en este Capítulo.</p>	<p>En Mayo de 2002, el Consejo Europeo concluyó las negociaciones del Borrador del <u>Primer Protocolo Adicional a la Convención de Ciberdelitos</u> relacionado con la penalización de actos de naturaleza racista o xenofóbica cometidos a través de sistemas informáticos. La propuesta también está acorde al Artículo 9 (<i>Offences related to child pornography</i>) de la CECD.</p> <p>El inciso d) va en contra de una actividad muy común en el mundo de los <i>hackers</i>: la invitación e instrucción para delinquir". Hay muchas <u>páginas web</u> que publican información y consejos sobre cómo <i>hackear</i> y <i>crackear</i> sistemas informáticos y telefónicos.</p>
<p>VIII.- Obtenga sin consentimiento y/o mediante engaños datos o información personal de individuos para usarla con fines comerciales, obtenga un lucro directo o indirecto de dicha información, o la use o aproveche para cometer cualquier actividad ilícita;</p>	<p>Aquí se contemplan dos clases de situaciones. La primera, el "robo de identidad", actividad que consiste en obtener mediante engaños información de una persona, como número de tarjeta de crédito, domicilio y demás datos personales que el atacante puede usar para hacer compras por Internet o realizar actividades ilícitas.</p> <p>La segunda situación, puede ser aplicable a los defraudadores que mediante promesas falsas, como participar en una rifa de un viaje o una casa, invitan a consumidores a que proporcionen sus correos electrónicos y otros datos personales, no solo de ellos sino de amistades. Posteriormente se recopila toda esa información en una base de datos, la cual se comercializa para realizar prácticas reprobables como el <i>spamming</i> (envío de correos electrónicos comerciales no solicitados).</p>
<p>IX.- Transmita, publicite, distribuya o haga disponible a través de computadoras o redes de computadoras datos o información personal de terceros sin su consentimiento o que la haya obtenido mediante engaños.</p>	<p>Esta fracción está relacionada de alguna manera el "ciberacoso". Con relativa frecuencia, hombres que son terminados por su pareja, por coraje o rencor publican información personal de su novia o esposa, e inclusive fotografías comprometedoras, minando la reputación de la persona y violando su derecho a la intimidad y privacidad.</p>
<p>X.- Inserte, altere, borre o elimine información contenida en una computadora o programa de cómputo, lo cual resulte en información auténtica con la intención de que se considere para propósitos legales como si fuere auténtica, independientemente de si la información sea directamente legible o accesible para su consulta.</p>	<p>Texto traducido y adaptado del Artículo 7 (<i>Computer-related forgery</i>) de la CECD, relativo a la falsificación realizada mediante equipos o sistemas informáticos.</p> <p>Es posible falsificar contratos electrónicos, facturas electrónicas, firmas electrónicas, y prácticamente cualquier documento electrónico, con el fin de hacerlo pasar como legítimo.</p>
<p>XI.- Cause la pérdida de propiedad de una persona, o cualquier otro daño patrimonial, mediante la inserción, alteración, borrado o eliminación de información contenida en una computadora, o cualquier interferencia al funcionamiento de una computadora, con el propósito fraudulento o deshonesto de procurar, sin derecho, un beneficio económico en provecho propio o ajeno.</p>	<p>Texto traducido y adaptado del Artículo 8 (<i>Computer-related fraud</i>) de la CECD, relativo a la defraudación electrónica.</p> <p>Como ejemplo podemos mencionar un caso reciente en Europa. Se descubrió que un <i>hacker</i> había introducido un programa a una computadora de un banco, el cual tenía el propósito de redondear todas las cuentas para que los "centavos sobrantes" fueran depositados en una cuenta virtual. Miles de dólares diariamente eran depositados en la cuenta del <i>hacker</i>. Como eran cantidades muy pequeñas de muy diversas cuentas, difícilmente se percataban de los faltantes.</p>
<p>A quien comete los delitos previstos en las fracciones I, III, VI, VII, VIII, y IX se le impondrá la pena de prisión de seis meses a tres años y de doscientos a seiscientos días multa.</p> <p>A quien comete los delitos previstos en las fracciones II, IV, V, X y XI se le impondrá</p>	<p>Considerando la gravedad de cada una de las acciones, las penas se aumentaron moderadamente a las que actualmente establece el Código Penal Federal en sus artículos 211 bis 1 al 7.</p>

la pena de prisión de tres a diez años y de cuatrocientos a mil días multa.	
ARTÍCULO 211 bis 3.- Las penas previstas en este capítulo se aumentarán hasta en una mitad:	Este artículo contiene la primera parte de las agravantes a las acciones del artículo anterior.
I.- Para los casos previstos en las fracciones III y V del artículo 211 bis 2, cuando la información obtenida se utilice en provecho propio o ajeno;	La primera fracción emula algunas de las agravantes actuales del CPF.
II.- Para los casos previstos en la fracción IV del artículo 211 bis 2, cuando el daño se haya propagado masivamente, afectando a computadoras localizadas en varios Estados de la República Mexicana.	Esta sanción es para el caso concreto de virus, gusanos y programas similares.
<p>III.- Para cualquiera de los casos previstos en el artículo 211 bis 2,</p> <p>a) cuando las conductas sean cometidas por funcionarios, empleados o personas que presten sus servicios en la institución, organización o empresa a la que se le haya causado el daño;</p> <p>b) cuando el delito informático se haya cometido en contra de computadoras de gobierno o del sistema financiero;</p> <p>c) cuando dos o más individuos hayan actuado coordinadamente para perpetrar alguno de los delitos de este título</p> <p>d) cuando para cometer el delito informático haya violado algún mecanismo de seguridad;</p> <p>e) cuando con el fin de disimular su identidad y/o ubicación, se haya aprovechado de la computadora y/o datos o información personal de un tercero, o haya usado datos falsos para realizar cualesquiera de las conductas tipificadas en este capítulo;</p> <p>f) cuando bajo engaños o aprovechándose del error en que se encuentra una persona, obtiene de ésta información, códigos o claves de acceso, o logra instalar en su computadora programas de cómputo, que le permitan realizar cualesquiera de las conductas tipificadas en este capítulo.</p>	<p>a) Agravante equivalente a una de las actuales del CPF.</p> <p>b) Idem.</p> <p>c) Acción cometida por "pandillas" o "delincuencia organizada", por llamarlo de alguna manera.</p> <p>d) Condición indispensable en el CPF en vigor para que proceda cualquier delito informático. Esta propuesta elimina ese defecto, convirtiendo el requisito en agravante.</p> <p>e) Mediante técnicas como ingeniería social, "caballos de troya" y la inserción de programas similares en equipos de cómputo ajenos, los <i>hackers</i> pueden perpetrar y disfrazar sus ataques a otras computadoras para disimular su ubicación.</p> <p>f) Práctica usual conocida como "ingeniería social". En marzo de 2002, el <i>Computer Emergency Response Team</i> (CERT) de la Universidad <i>Carnegie Mellon</i> liberó un <u>reporte</u> que sintetiza varias quejas de este tipo de ataques. CERT concluye que decenas de miles de sistemas informáticos han sido comprometidos mediante ataques derivados de "ingeniería social".</p>
<p>ARTÍCULO 211 bis 4.- Las penas previstas en este capítulo se aumentarán hasta el doble:</p> <p>I.- Cuando se hayan dado dos o más agravantes de las mencionadas en el Artículo 211 bis 3.</p> <p>II.- Cuando el delito</p>	<p>Este artículo contiene la segunda parte de las agravantes a las acciones del artículo 211 bis 2.</p> <p>Se pretende incluir de manera genérica delitos como el <i>ciberterrorismo</i> y <i>hacktivismo</i>. La amenaza del <i>ciberterrorismo</i> es tan real, que el Departamento de Estado de los EUA tiene una "<u>Cyber-Terrorist Watch List</u>", la cual incluye a países como Cuba, Iran, Iraq, Libia, Sudán, Afganistán, Egipto, Kuwait, Pakistan y Arabia</p>

<p>informático haya sido motivado por cuestiones políticas, activistas o terroristas, o haya tenido cualquiera de los fines contemplados en el Libro Segundo, Título Primero "Delitos Contra la Seguridad de la Nación" de éste Código.</p>	<p>Saudita, entre otros.</p>
---	------------------------------

OTRAS PROPUESTAS

TÍTULO QUINTO.- DELITOS EN MATERIA DE VÍAS DE COMUNICACIÓN Y DE CORRESPONDENCIA CAPÍTULO II.- VIOLACIÓN DE CORRESPONDENCIA

ARTÍCULO 173.- Se impondrán de seis meses a dos años de prisión y de cien a trescientos días multa:

I.- Al que abra indebidamente una comunicación escrita que no esté dirigida a él; y

II.- Al que indebidamente intercepte una comunicación escrita que no esté dirigida a él, aunque la conserve cerrada y no se imponga de su contenido.

ARTICULO 350.- La difamación consiste: en comunicar por medios impresos, materiales, electrónicos, ópticos o de cualquier otra tecnología, dolosamente a una o más personas, la imputación que se le hace a otra persona física o persona moral, en los casos previstos por la ley, de un hecho cierto o falso, determinado o indeterminado, que pueda causarle deshonra, descrédito, perjuicio, o exponerlo al desprecio de alguien.

TÍTULO VIGÉSIMOSEGUNDO.- DELITOS EN CONTRA DE LAS PERSONAS EN SU PATRIMONIO CAPÍTULO I.- ROBO

ARTICULO 368.- Se equiparan al robo y se castigarán como tal:

III.- La copia, sustracción o el apoderamiento de documentos, datos o archivos electrónicos, ópticos o de cualquier otra tecnología que residan en computadoras o sistemas informáticos, o el aprovechamiento o utilización de dichos documentos, datos o archivos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

ANEXO I.

INSTITUCIONES DE LA ADMINISTRACIÓN PÚBLICA FEDERAL CON ATRIBUCIONES VINCULADAS CON LA INFORMÁTICA

En la Administración Pública Federal existen diversas instituciones con atribuciones que directa o indirectamente inciden en el ámbito de la informática, cuya participación es necesaria para promover el desarrollo nacional en la materia.

A continuación se señalan dichas instituciones y algunas atribuciones que inciden en la informática.

SECRETARÍA DE GOBERNACIÓN

Vigilar el cumplimiento de los preceptos constitucionales por parte de las autoridades del país, especialmente en lo que se refiere a las garantías individuales, y dictar las medidas administrativas que requiere ese cumplimiento.

SECRETARÍA DE RELACIONES EXTERIORES

Promover, propiciar y asegurar la coordinación de acciones en el exterior de las dependencias y entidades de la Administración Pública Federal; y sin afectar el ejercicio de las atribuciones que a cada una de ellas corresponda, conducir la política exterior para lo cual intervendrá en toda clase de tratados, acuerdos y convenciones en los que el país sea parte.

SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

- Determinar los criterios y montos globales de los estímulos fiscales, escuchando para ello a las dependencias responsables de los sectores correspondientes y administrar su aplicación en los casos en que no compete a otra Secretaría.
- Proyectar y calcular los egresos del Gobierno Federal y de la administración pública paraestatal, haciéndolos compatibles con la disponibilidad de recursos y en atención a las necesidades y políticas del desarrollo nacional.
- Formular el programa del gasto público federal y el proyecto del Presupuesto de Egresos de la Federación y presentarlos, junto con el del Departamento del Distrito Federal, a la consideración del Presidente de la República.
- Evaluar y autorizar los programas de inversión pública de las dependencias y entidades de la Administración Pública Federal.

- Coordinar y desarrollar los servicios nacionales de estadística y de información geográfica; establecer las normas y procedimientos para la organización, funcionamiento y coordinación de los sistemas nacionales estadísticos de información geográfica, así como normar y coordinar los servicios de informática de las dependencias y entidades de la Administración Pública Federal.
- Opinar, previamente a su expedición, sobre los proyectos de normas y lineamientos en materia de adquisiciones, arrendamientos y desincorporación de activos, servicios y ejecución de obras públicas de la Administración Pública Federal.
- Vigilar el cumplimiento de las obligaciones derivadas de las disposiciones en materia de planeación nacional, así como de programación, presupuestación, contabilidad y evaluación.

SECRETARÍA DE COMERCIO Y FOMENTO INDUSTRIAL

- Formular y conducir las políticas generales de industria, comercio exterior, interior, abasto y precios del país, con excepción de los precios de bienes y servicios de la Administración Pública Federal.
- Estudiar y determinar mediante reglas generales, conforme a los montos globales establecidos por la Secretaría de Hacienda y Crédito Público, los estímulos fiscales necesarios para el fomento industrial, el comercio interior y exterior y el abasto, incluyendo los subsidios sobre impuestos de importación, y administrar su aplicación, así como vigilar y evaluar sus resultados.
- Normar y registrar la propiedad industrial y mercantil, así como regular y orientar la inversión extranjera y la transferencia de tecnología;
- Establecer y vigilar las normas de calidad, pesas y medidas necesarias para la actividad comercial, así como las normas y especificaciones industriales;
- Promover, orientar, fomentar y estimular la industria nacional.
- Promover, orientar, fomentar y estimular el desarrollo de la industria pequeña, mediana y regular la organización de productores industriales.

SECRETARÍA DE COMUNICACIONES Y TRANSPORTES

- Formular y conducir las políticas y programas para el desarrollo del transporte y las comunicaciones de acuerdo a las necesidades del país;
- Otorgar concesiones y permisos previa opinión de la Secretaría de Gobernación para establecer y explotar sistemas de servicios telegráficos, telefónicos, sistemas y servicios de comunicación inalámbrica por telecomunicaciones y satélites, de servicio público de procesamiento remoto de datos, estaciones de radio experimentales, culturales y de aficionados y estaciones de radiodifusión

comerciales y culturales; así como vigilar el aspecto técnico del funcionamiento de tales sistemas, servicios y estaciones.

SECRETARÍA DE CONTRALORÍA Y DESARROLLO ADMINISTRATIVO

- Vigilar el cumplimiento, por parte de las dependencias y entidades de la Administración Pública Federal, de las disposiciones en materia de planeación, presupuestación, ingresos, financiamiento, inversión, deuda, patrimonio, fondos y valores.
- Organizar y coordinar el desarrollo administrativo integral en las dependencias y entidades de la Administración Pública Federal, a fin de que los recursos humanos, patrimoniales y los procedimientos técnicos de la misma, sean aprovechados y aplicados con criterios de eficiencia, buscando en todo momento la eficacia, descentralización, desconcentración y simplificación administrativa. Para ello, podrá realizar o encomendar las investigaciones, estudios y análisis necesarios sobre estas materias, y dictar las disposiciones administrativas que sean necesarias al efecto, tanto para las dependencias, como para las entidades de la Administración Pública Federal.
- Inspeccionar y vigilar, directamente o a través de los órganos de control, que las dependencias y entidades de la Administración Pública Federal cumplan con las normas y disposiciones en materia de sistemas de registro y contabilidad, contratación y remuneraciones de personal, contratación de adquisiciones, arrendamientos, servicios, y ejecución de obra pública, conservación, uso, destino, afectación, enajenación y baja de bienes muebles e inmuebles, almacenes y demás activos y recursos materiales de la Administración Pública Federal.
- Establecer normas, políticas y lineamientos en materia de adquisiciones, arrendamientos, desincorporación de activos, servicios y obras públicas de la Administración Pública Federal.

SECRETARÍA DE EDUCACIÓN PÚBLICA

- Vigilar que se observen y cumplan las disposiciones relacionadas con la educación preescolar, primaria, secundaria, técnica y normal, establecidas en la Constitución y prescribir las normas a que debe ajustarse la incorporación de las escuelas particulares del sistema educativo nacional.
- Promover la creación de institutos de investigación científica y técnica, y el establecimiento de laboratorios, observatorios, planetarios y demás centros que requiera el desarrollo de la educación primaria, secundaria, normal, técnica y superior; orientar, en coordinación con las dependencias competentes del Gobierno Federal y con las entidades públicas y privadas el desarrollo de la investigación científica y tecnológica.
- Organizar, controlar y mantener al corriente el registro de la propiedad literaria y artística.

- Vigilar con auxilio de las asociaciones de profesionistas, el correcto ejercicio de las profesiones.

COMISIÓN FEDERAL DE TELECOMUNICACIONES

- Expedir las disposiciones administrativas y las normas oficiales mexicanas en materia de telecomunicaciones, así como elaborar y administrar los planes técnicos fundamentales.
- Realizar estudios e investigaciones en materia de telecomunicaciones y elaborar anteproyectos de adecuación, modificación y actualización de las disposiciones legales y reglamentarias que resulten pertinentes.
- Establecer los procedimientos para la adecuada homologación de equipos, así como otorgar la certificación correspondiente o autorizar a terceros para que emitan dicha certificación, unidades de verificación, organismo de certificación y laboratorios de prueba en materia de telecomunicaciones, y acreditar peritos en dicha materia.
- Administrar el espectro radioeléctrico y promover su uso eficiente, así como elaborar y mantener actualizado el Cuadro Nacional de Atribución de Frecuencias.
- Promover y vigilar la eficiente interconexión de los equipos y redes públicas de telecomunicaciones, incluyendo la que se realice con redes extranjeras, y resolver las condiciones que, en materia de interconexión, no hayan podido convenirse entre los concesionarios de redes públicas de telecomunicaciones.
- Aprobar los convenios de interconexión entre redes públicas de telecomunicaciones con redes extranjeras y, en su caso, establecer las modalidades a que deberán sujetarse, así como autorizar la instalación de equipos de telecomunicaciones y medios de transmisión que crucen las fronteras del país.
- Dar seguimiento a los compromisos adquiridos por México ante organismos y otras entidades internacionales en el ámbito de competencia de la Comisión.
- Llevar a cabo la coordinación de la operación de satélites nacionales con satélites extranjeros e internacionales.
- Aplicar y ejercer las funciones de autoridad en las reglas, normas oficiales mexicanas y demás disposiciones administrativas en materia de telecomunicaciones.

CONSEJO NACIONAL DE CIENCIA Y TECNOLOGÍA

- Fungir como asesor del Ejecutivo Federal en la planeación, programación, coordinación, orientación sistematización, promoción y encausamiento de

las actividades relacionadas con la ciencia y la tecnología, su vinculación al desarrollo nacional y sus relaciones con el exterior.

- Fomentar y fortalecer las investigaciones básicas, tecnológicas y aplicadas que se necesiten y promover las acciones concertadas que se requieran con los institutos del sector público, instituciones académicas, centros de investigación y usuarios de las mismas, incluyendo al sector privado.

ANEXO 2



Convenio sobre cibercriminalidad

Budapest, 23.XI.2001

Traducción no oficial.

Preámbulo

Los Estados miembros del Consejo de Europa y los otros Estados firmantes,

Considerando que el objetivo del Consejo de Europa es lograr una unión más estrecha entre sus miembros;

Reconociendo el interés de intensificar la cooperación con los otros Estados parte en el Convenio;

Convencidos de la necesidad de llevar a cabo, con prioridad, una política penal común destinada a prevenir la criminalidad en el ciberespacio y, en particular, de hacerlo mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional;

Conscientes de los profundos cambios suscitados por el incremento, la convergencia y la mundialización permanente de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer infracciones penales y que las pruebas de dichas infracciones sean almacenadas y transmitidas por medio de esas redes;

Reconociendo la necesidad de una cooperación entre los Estados y la industria privada en la lucha contra la cibercriminalidad y la necesidad de proteger los intereses legítimos vinculados al desarrollo de las tecnologías de la información;

Estimando que una lucha bien organizada contra la cibercriminalidad requiere una cooperación internacional en materia penal acrecentada, rápida y eficaz;

Convencidos de que el presente Convenio es necesario para prevenir los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos, como los descritos en el presente Convenio, y la atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando la detección, la investigación y la persecución, tanto a nivel nacional como internacional, y previendo algunas disposiciones materiales al objeto de una cooperación internacional rápida y fiable;

Persuadidos de la necesidad de garantizar un equilibrio adecuado entre los intereses de la acción represiva y el respeto de los derechos fundamentales del hombre, como los garantizados en el Convenio para la protección de los derechos del hombre y de las libertades fundamentales del Consejo de Europa (1950), en el Pacto internacional relativo a los derechos civiles y políticos de las Naciones Unidas (1966), así como en otros convenios internacionales aplicables en materia de derechos del hombre, que reafirman el derecho de no ser perseguido por la opinión, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar informaciones e ideas de toda naturaleza, sin consideración de fronteras, así como el derecho al respeto de la vida privada;

Conscientes, igualmente, de la protección de los datos personales, como la que confiere, por ejemplo, el Convenio de 1981 del Consejo de Europa para la protección de las personas en lo referente al tratamiento automatizado de los datos de carácter personal;

Considerando el Convenio de Naciones Unidas relativo a los derechos del niño y el Convenio de la Organización Internacional del Trabajo sobre la prohibición de las peores formas de trabajo infantil (1999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre la cooperación en materia penal, así como otros tratados similares suscritos entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el presente Convenio tiene por objeto completarlos con el fin de hacer más eficaces las investigaciones y procedimientos penales relativos a las infracciones penales vinculadas a sistemas y datos informáticos, así como permitir la recogida de pruebas electrónicas de una infracción penal;

Felicitándose por las recientes iniciativas destinadas a mejorar la comprensión y la cooperación internacional para la lucha contra la criminalidad en el ciberespacio y, en particular, las acciones organizadas por las Naciones Unidas, la OCDE, la Unión europea y el G8;

Recordando la Recomendación N.º (85) 10 sobre la aplicación práctica del Convenio europeo de ayuda mutua judicial en materia penal respecto a las comisiones rogatorias para la vigilancia de las telecomunicaciones, la Recomendación N.º (88) 2 sobre medidas dirigidas a combatir la piratería en el ámbito de los derechos de autor y de los derechos afines, la Recomendación N.º (87) 15 dirigida a regular la utilización de datos de carácter personal en el sector de la policía, la Recomendación N.º (95) 4 sobre la protección de los datos de carácter personal en el sector de los servicios de telecomunicación, teniendo en cuenta, en particular, los servicios telefónicos y la Recomendación N.º (89) 9 sobre la delincuencia relacionada con el ordenador, que indica a los legisladores nacionales los principios directores para definir ciertas infracciones informáticas, así como la Recomendación N.º (95) 13 relativa a los problemas de procedimiento penal vinculados a las tecnologías de la información;

Vista la Resolución N.º 1, adoptada por los Ministros europeos de Justicia, en su 21ª Conferencia (Praga, junio 1997), que recomienda al Comité de Ministros mantener las actividades organizadas por el Comité europeo para los problemas penales (CDPC) relativas a la cibercriminalidad a fin de acercar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces

en materia de infracciones informáticas, así como la Resolución N.º 3, adoptada en la 23ª Conferencia de Ministros europeos de Justicia (Londres, junio 2000), que anima a las partes negociadoras a persistir en sus esfuerzos al objeto de encontrar soluciones adecuadas, que permitan al mayor número posible de Estados ser partes en el Convenio y reconoce la necesidad de disponer de un mecanismo rápido y eficaz de cooperación internacional, que tenga en cuenta las específicas exigencias de la lucha contra la cibercriminalidad;

Tomando igualmente en cuenta el Plan de acción adoptado por los Jefes de Estado y de gobierno del Consejo de Europa, con ocasión de su Décima Cumbre (Estrasburgo, 10-11 octubre 1997) a fin de buscar respuestas comunes al desarrollo de las nuevas tecnologías de la información, fundadas sobre las normas y los valores del Consejo de Europa;

Han convenido lo siguiente:

Capítulo I – Terminología

Artículo 1 – Definiciones

A los efectos del presente Convenio, la expresión:

a. "sistema informático" designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos;

b. "datos informáticos" designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función;

c. "prestador de servicio" ⁽¹⁾ designa:

i. toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático;

ii. cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios;

d. "datos de tráfico" ⁽²⁾ designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Capítulo II – Medidas que deben ser adoptadas a nivel nacional

Sección 1 – Derecho penal material

Título 1 – Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2 – Acceso ilícito

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso ⁽³⁾ y sin autorización a todo o parte de un sistema informático. Las Partes podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 3 – Interceptación ilícita

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos – en transmisiones no públicas– en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Las Partes podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 4 – Atentados contra la integridad de los datos

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero ocasione daños que puedan calificarse de graves.

Artículo 5 – Atentados contra la integridad del sistema

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6 – Abuso de equipos e instrumentos técnicos ⁽⁴⁾

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a. la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición:

i. de un dispositivo, incluido un programa informático, principalmente concebido o adaptado

para permitir la comisión de una de las infracciones establecidas en los artículos 2 a 5 arriba citados;

ii. de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5; y

b. la posesión de alguno de los elementos descritos en los párrafos (a) (1) o (2) con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2-5. Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad penal ⁽⁵⁾.

2. Lo dispuesto en el presente artículo no generará responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión u otras formas de puesta a disposición mencionadas en el párrafo 1 no persigan la comisión de una infracción prevista en los artículos 2 a 5 del presente Convenio, como en el caso de ensayos autorizados o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho de no aplicar el párrafo 1, a condición de que dicha reserva no recaiga sobre la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el párrafo 1 (a)(2).

Título 2 – Infracciones informáticas

Artículo 7 – Falsedad informática

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles. Las Partes podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal.

Artículo 8 – Estafa informática

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de:

a. la introducción, alteración, borrado o supresión de datos informáticos,

b. cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.

Título 3 – Infracciones relativas al contenido

Artículo 9 – Infracciones relativas a la pornografía infantil

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

- a. la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;
- b. el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático;
- c. la difusión o la transmisión de pornografía infantil a través de un sistema informático;
- d. el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático;
- e. la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 arriba descrito, la «pornografía infantil» comprende cualquier material pornográfico que represente de manera visual:

- a. un menor adoptando un comportamiento sexualmente explícito;
- b. una persona que aparece como un menor adoptando un comportamiento sexualmente explícito ⁽⁶⁾;
- c. unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito ⁽⁷⁾.

3. A los efectos del párrafo 2 arriba descrito, el término «menor» designa cualquier persona menor de 18 años. Las Partes podrán exigir un límite de edad inferior, que debe ser como mínimo de 16 años.

4. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, los párrafos 1 (d) y 1 (e) y 2 (b) y 2 (c).

Título 4 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

Artículo 10 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a la propiedad intelectual definida por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Universal sobre los Derechos de Autor, revisada en París el 24 de julio de 1971, del Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a los derechos afines definidos por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, hecha en Roma (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre interpretación o ejecución y fonogramas, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

3. Las Partes podrán, de concurrir determinadas circunstancias, reservarse el derecho de no imponer responsabilidad penal en aplicación de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos eficaces para su represión y que dicha reserva no comporte infracción de las obligaciones internacionales que incumban al Estado por aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Título 5 – Otras formas de responsabilidad y sanción

Artículo 11 – Tentativa y complicidad

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, cualquier acto de complicidad que sea cometido dolosamente y con la intención de favorecer la perpetración de alguna de las infracciones establecidas en los artículos 2 a 10 del presente Convenio.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la tentativa dolosa de cometer una de las infracciones establecidas en los artículos 3 a 5, 7, 8, 9 (1) a y 9 (1) c del presente Convenio.

3. Las Partes podrán reservarse el derecho de no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

Artículo 12 – Responsabilidad de las personas jurídicas

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las personas jurídicas puedan ser tenidas por

responsables de las infracciones establecidas en el presente Convenio, cuando éstas sean cometidas por una persona física, actuando ya sea a título individual, ya sea como miembro de un órgano de la persona jurídica, que ejerce un poder de dirección en su seno, cuyo origen se encuentre en:

- a. un poder de representación de la persona jurídica;
- b. una autorización para tomar decisiones en nombre de la persona jurídica;
- c. una autorización para ejercer control en el seno de la persona jurídica.

2. Fuera de los casos previstos en el párrafo 1, las Partes adoptarán las medidas necesarias para asegurar que una persona jurídica puede ser tenida por responsable cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de las infracciones descritas en el párrafo 1 a través de una persona física que actúa bajo autorización de la persona jurídica.

3. La responsabilidad de la persona jurídica podrá resolverse en sede penal, civil o administrativa, dependiendo de los principios jurídicos propios del Estado.

4. Esta responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido la infracción.

Artículo 13 – Sanciones y medidas

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las infracciones penales establecidas en los artículos 2 a 11 sean castigadas con sanciones efectivas, proporcionadas y disuasorias, incluidas las penas privativas de libertad.

2. Las Partes velarán para que las personas jurídicas que hayan sido declaradas responsables según lo dispuesto en el artículo 12 sean objeto de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas las sanciones pecuniarias.

Sección 2 – Derecho procesal

Título 1 – Disposiciones comunes

Artículo 14 – Ámbito de aplicación de las medidas de derecho procesal

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para instaurar los poderes y procedimientos previstos en la presente sección a los efectos de investigación o de procedimientos penales específicos.

2. Salvo disposición en contrario, prevista en el artículo 21, las Partes podrán aplicar los poderes y procedimientos mencionados en el párrafo 1:

- a. a las infracciones penales establecidas en los artículos 2 a 11 del presente Convenio;
- b. a cualquier otra infracción penal cometida a través de un sistema informático; y
- c. a la recogida de pruebas electrónicas de cualquier infracción penal.

3. a. Las Partes podrán reservarse el derecho de aplicar la medida mencionada en el artículo 20 a las infracciones especificadas en sus reservas, siempre que el número de dichas infracciones no supere el de aquellas a las que se aplica la medida mencionada en el artículo 21. Las Partes tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de la medida mencionada en el artículo 20.

b. Cuando un Estado, en razón de las restricciones impuestas por su legislación vigente en el momento de la adopción del presente Convenio, no esté en condiciones de aplicar las medidas descritas en los artículos 20 y 21 a las comunicaciones transmitidas en un sistema informático de un prestador de servicios que

i. es utilizado en beneficio de un grupo de usuarios cerrado, y

ii. no emplea las redes públicas de telecomunicación y no está conectado a otro sistema informático, público o privado, ese Estado podrá reservarse el derecho de no aplicar dichas medidas a tales comunicaciones. Los Estados tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de las medidas mencionadas en los artículos 20 y 21.

Artículo 15 – Condiciones y garantías

1. Las Partes velarán para que la instauración, puesta en funcionamiento y aplicación de los poderes y procedimientos previstos en la presente sección se sometan a las condiciones y garantías dispuestas en su derecho interno, que debe asegurar una protección adecuada de los derechos del hombre y de las libertades y, en particular, de los derechos derivados de las obligaciones que haya asumido en aplicación del Convenio para la protección de los derechos humanos y libertades fundamentales del Consejo de Europa (1950) y del Pacto internacional de derechos civiles y políticos de Naciones Unidas (1966) o de otros instrumentos internacionales relativos a los derechos del hombre, y que debe integrar el principio de proporcionalidad.

2. Cuando ello sea posible, en atención a la naturaleza del poder o del procedimiento de que se trate, dichas condiciones y garantías incluirán, entre otras, la supervisión judicial u otras formas de supervisión independiente, la motivación justificante de la aplicación, la limitación del ámbito de aplicación y la duración del poder o del procedimiento en cuestión.

3. Las Partes examinarán la repercusión de los poderes y procedimientos de esta Sección sobre los derechos, responsabilidades e intereses legítimos de terceros, como exigencia dimanante del interés público y, en particular, de una correcta administración de justicia.

Título 2 – Conservación inmediata de datos informáticos almacenados

Artículo 16 – Conservación inmediata de datos informáticos almacenados

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación inmediata de datos electrónicos especificados, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para pensar que son particularmente susceptibles de pérdida o de modificación.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a una persona a conservar y proteger la integridad de los datos – que se encuentran en su poder o bajo su control y respecto de los cuales exista un mandato previo de conservación en aplicación del párrafo precedente – durante el tiempo necesario, hasta un máximo de 90 días, para permitir a las autoridades competentes obtener su comunicación. Los Estados podrán prever que dicho mandato sea renovado posteriormente.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar al responsable de los datos o a otra persona encargada de conservarlos a mantener en secreto la puesta en ejecución de dichos procedimientos durante el tiempo previsto por su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Artículo 17 – Conservación y divulgación inmediata de los datos de tráfico

1. A fin de asegurar la conservación de los datos de tráfico, en aplicación del artículo 16, las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para:

a. procurar la conservación inmediata de los datos de tráfico, cuando uno o más prestadores de servicio hayan participado en la transmisión de dicha comunicación; y

b. asegurar la comunicación inmediata a la autoridad competente del Estado, o a una persona designada por dicha autoridad, de datos de tráfico suficientes para permitir la identificación de los prestadores de servicio y de la vía por la que la comunicación se ha transmitido.

2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Título 3 – Mandato de comunicación

Artículo 18 – Mandato de comunicación

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar:

a. a una persona presente en su territorio que comunique los datos informáticos especificados, en posesión o bajo el control de dicha persona, y almacenados en un sistema informático o en un soporte de almacenaje informático; y

b. a un prestador de servicios que ofrezca sus prestaciones en el territorio del Estado firmante, que comunique los datos en su poder o bajo su control relativos a los abonados y que conciernan a tales servicios;

2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

3. A los efectos del presente artículo, la expresión «datos relativos a los abonados» designa cualquier información, expresada en datos informáticos o de cualquier otro modo, poseída por un prestador de servicio y que se refiere a los abonados de sus servicios, así como a los datos de tráfico o relativos al contenido, y que permite establecer:

a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el tiempo del servicio;

b. la identidad, la dirección postal o geográfica y el número de teléfono del abonado o cualquier otro número de acceso, los datos relativos a la facturación y el pago, disponibles por razón de un contrato o de un alquiler de servicio;

c. cualquier otra información relativa al lugar donde se ubican los equipos de comunicación, disponible por razón de un contrato o de un alquiler de servicio.

Título 4 – Registro y decomiso de datos informáticos almacenados

Artículo 19 – Registro y decomiso de datos informáticos almacenados

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para registrar o acceder de un modo similar:

a. a un sistema informático o a una parte del mismo, así como a los datos informáticos que están almacenados; y

b. a un soporte de almacenamiento que permita contener datos informáticos en su territorio.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para procurar que, cuando sus autoridades registren o accedan de un modo similar a un sistema informático específico o a una parte del mismo, conforme al párrafo 1 (a), y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son igualmente accesibles a partir del

sistema inicial o están disponibles a través de ese primer sistema, dichas autoridades estén en condiciones de ampliar inmediatamente el registro o el acceso y extenderlo al otro sistema.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para decomisar u obtener de un modo similar los datos informáticos cuyo acceso haya sido realizado en aplicación de los párrafos 1 o 2. Estas medidas incluyen las prerrogativas siguientes:

- a. decomisar u obtener de un modo similar un sistema informático o una parte del mismo o un soporte de almacenaje informático;
- b. realizar y conservar una copia de esos datos informáticos;
- c. preservar la integridad de los datos informáticos almacenados pertinentes; y
- d. hacer inaccesibles o retirar los datos informáticos del sistema informático consultado.

4. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar a cualquier persona, que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione todas las informaciones razonablemente necesarias, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2.

5. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Título 5 – Recogida en tiempo real de datos informáticos

Artículo 20 – Recogida en tiempo real de datos informáticos

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para:

- a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio;
- b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a
 - i. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o
 - ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio a través de un sistema informático.

2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Artículo 21 – Interceptación de datos relativos al contenido

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes respecto a infracciones consideradas graves conforme a su derecho interno para:

a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio; y

b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a

i. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar,

en tiempo real, los datos relativos al contenido de concretas comunicaciones en su territorio, transmitidas a través de un sistema informático.

2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos relativos al contenido de concretas comunicaciones transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Sección 3 – Competencia

Artículo 22 – Competencia

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para atribuirse la competencia respecto a cualquier infracción penal establecida en los artículos 2 a 11 del presente Convenio, cuando la infracción se haya cometido:

- a. en su territorio;
- b. a bordo de una nave que ondee pabellón de ese Estado;
- c. a bordo de una aeronave inmatriculada en ese Estado;
- d. por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado.

2. Las Partes podrán reservarse el derecho de no aplicar, o de aplicar sólo en ciertos casos o condiciones específicas, las reglas de competencia definidas en los párrafos 1b a 1d del presente artículo o en cualquiera de las partes de esos párrafos.

3. Las Partes adoptarán las medidas que se estimen necesarias para atribuirse la competencia respecto de cualquier infracción mencionada en el artículo 24, párrafo 1 del presente Convenio, cuando el presunto autor de la misma se halle en su territorio y no pueda ser extraditado a otro Estado por razón de la nacionalidad, después de una demanda de extradición.

4. El presente Convenio no excluye ninguna competencia penal ejercida por un Estado conforme a su derecho interno.

5. Cuando varios Estados reivindiquen una competencia respecto a una infracción descrita en el presente Convenio, los Estados implicados se reunirán, cuando ello sea oportuno, a fin de decidir cuál de ellos está en mejores condiciones para ejercer la persecución.

Capítulo III – Cooperación internacional

Sección 1 – Principios generales

Título 1 – Principios generales relativos a la cooperación internacional

Artículo 23 – Principios generales relativos a la cooperación internacional

Las Partes cooperarán con arreglo a lo dispuesto en el presente capítulo, aplicando para ello los instrumentos internacionales relativos a la cooperación internacional en materia penal, acuerdos basados en la legislación uniforme o recíproca y en su propio derecho nacional, de la forma más amplia posible, con

la finalidad de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o para recoger pruebas electrónicas de una infracción penal.

Título 2 – Principios relativos a la extradición

Artículo 24 – Extradición

1. a. El presente artículo se aplicará a la extradición por alguna de las infracciones definidas en los artículos 2 a 11 del presente Convenio, siempre que éstas resulten punibles por la legislación de los dos Estados implicados y tengan prevista una pena privativa de libertad de una duración mínima de un año.

b. Aquellos Estados que tengan prevista una pena mínima distinta, derivada de un tratado de extradición aplicable a dos o más Estados, comprendido en la Convención Europea de Extradición (STE nº 24), o de un acuerdo basado en la legislación uniforme o recíproca, aplicarán la pena mínima prevista en esos tratados o acuerdos.

2. Las infracciones penales previstas en el apartado 1 del presente artículo podrán dar lugar a extradición si entre los dos Estados existe un tratado de extradición. Las Partes se comprometerán a incluirlas como tales infracciones susceptibles de dar lugar a extradición en todos los tratados de extradición que puedan suscribir.

3. Si un Estado condiciona la extradición a la existencia de un tratado y recibe una demanda de extradición de otro Estado con el que no ha suscrito tratado alguno de extradición, podrá considerar el presente Convenio fundamento jurídico suficiente para conceder la extradición por alguna de las infracciones penales previstas en el párrafo 1 del presente artículo.

4. Las Partes que no condicionen la extradición a la existencia de un tratado podrán llevar a cabo la extradición siempre que prevean como infracciones las previstas en el párrafo 1 del presente artículo.

5. La extradición quedará sometida a las condiciones establecidas en el derecho interno del Estado requerido o en los tratados de extradición vigentes, quedando asimismo sometidos a estos instrumentos jurídicos los motivos por los que el país requerido puede denegar la extradición.

6. Si es denegada la extradición por una infracción comprendida en el párrafo 1 del presente artículo, alegando la nacionalidad de la persona reclamada o la competencia para juzgar la infracción del Estado requerido, éste deberá someter el asunto – la demanda del Estado requirente — a sus autoridades competentes a fin de que éstas establezcan la competencia para perseguir el hecho e informen de la conclusión alcanzada al Estado requirente. Las autoridades en cuestión deberán adoptar la decisión y sustanciar el procedimiento del mismo modo que para el resto de infracciones de naturaleza semejante previstas en la legislación de ese Estado.

7. a. Las Partes deberán comunicar al Secretario General del Consejo de Europa, en el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de las autoridades

responsables del envío y de la recepción de una demanda de extradición o de arresto provisional, en caso de ausencia de tratado.

b. El Secretario General del Consejo de Europa creará y actualizará un registro de autoridades designadas por las Partes. Las Partes deberán garantizar la exactitud de los datos obrantes en el registro

Título 3 – Principios generales relativos a la colaboración ⁽⁸⁾

Artículo 25 – Principios generales relativos a la colaboración

1. Las Partes acordarán llevar a cabo una colaboración mutua lo más amplia posible al objeto de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o al de recoger pruebas electrónicas de una infracción penal.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que estimen necesarias para dar cumplimiento a las obligaciones establecidas en los artículos 27 a 35.

3. Las Partes podrán, en caso de emergencia, formular una demanda de colaboración, a través de un medio de comunicación rápido, como el fax o el correo electrónico, procurando que esos medios ofrezcan las condiciones suficientes de seguridad y de autenticidad (encriptándose si fuera necesario) y con confirmación posterior de la misma si el Estado requerido lo exigiera. Si el Estado requerido lo acepta podrá responder por cualquiera de los medios rápidos de comunicación indicados.

4. Salvo disposición en contrario expresamente prevista en el presente capítulo, la colaboración estará sometida a las condiciones fijadas en el derecho interno del Estado requerido o en los tratados de colaboración aplicables y comprenderá los motivos por los que el Estado requerido puede negarse a colaborar. El Estado requerido no podrá ejercer su derecho a rehusar la colaboración en relación a las infracciones previstas en los artículos 2 a 11, alegando que la demanda se solicita respecto a una infracción que, según su criterio, tiene la consideración de fiscal.

5. Conforme a lo dispuesto en el presente capítulo, el Estado requerido estará autorizado a supeditar la colaboración a la exigencia de doble incriminación. Esa condición se entenderá cumplida si el comportamiento constitutivo de la infracción - en relación a la que se solicita la colaboración — se encuentra previsto en su derecho interno como infracción penal, resultando indiferente que éste no la encuadre en la misma categoría o que no la designe con la misma terminología.

Artículo 26 – Información espontánea

1. Las Partes podrán, dentro de los límites de su derecho interno y en ausencia de demanda previa, comunicar a otro Estado las informaciones obtenidas en el marco de investigaciones que puedan ayudar a la Parte destinataria a iniciar o a concluir satisfactoriamente las investigaciones o procedimientos relativos a las infracciones dispuestas en el presente Convenio, o a que dicha parte presente una demanda de las previstas en el presente capítulo.

2. Antes de comunicar dicha información, ese Estado podrá solicitar que la información sea tratada de forma confidencial o que sea utilizada sólo en ciertas circunstancias. Si el Estado destinatario no pudiera acatar las condiciones impuestas, deberá informar al otro Estado, quien habrá de decidir si proporciona o no la información. Una vez aceptadas estas condiciones por el Estado destinatario, éste quedará obligado a su cumplimiento.

Título 4 – Procedimientos relativos a las demandas de asistencia en ausencia de acuerdo internacional aplicable

Artículo 27 – Procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional aplicable

1. En ausencia de tratado o acuerdo en vigor de asistencia basado en la legislación uniforme o recíproca, serán aplicables los apartados 2 al 9 del presente artículo. Éstos no se aplicarán cuando exista un tratado, acuerdo o legislación sobre el particular, sin perjuicio de que las partes implicadas puedan decidir someterse, en todo o parte, a lo dispuesto en este artículo.

2. a. Las Partes designarán una o varias autoridades centrales encargadas de tramitar las demandas de colaboración, de ejecutarlas o de transferirlas a las autoridades competentes para que éstas las ejecuten.

b. Las autoridades centrales se comunicarán directamente las unas con las otras.

c. Las Partes, en el momento de la firma o del depósito de sus instrumentos de ratificación, aceptación, de aprobación o de adhesión, comunicarán al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en aplicación del presente párrafo.

d. El Secretario General del Consejo de Europa creará y actualizará un registro de autoridades designadas por las partes. Las Partes deberán garantizar la exactitud de los datos obrantes en el registro.

3. Las demandas de asistencia basadas en el presente artículo serán ejecutadas conforme al procedimiento especificado por el Estado requirente, siempre que resulte compatible con la legislación del Estado requerido.

4. Al margen de los motivos previstos en el artículo 15 párrafo 4 para denegar la asistencia, ésta podrá ser rechazada por el Estado requerido:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que, de acceder a la colaboración, se pondría en peligro su soberanía, seguridad, orden público o otro interés esencial.

5. El Estado requerido podrá aplazar la ejecución de la demanda cuando ésta pueda perjudicar investigaciones o procedimientos en curso llevados a cabo por las autoridades nacionales.

6. Antes de denegar o retrasar la asistencia, el Estado requerido deberá examinar, tras consultar al Estado requirente, si es posible hacer frente a la demanda de forma parcial o si es posible establecer las reservas que estime necesarias.

7. El Estado requerido informará inmediatamente al Estado requirente del curso que pretende dar a la demanda de asistencia. De denegar o retrasar la tramitación de la demanda, el Estado requerido hará constar los motivos. Asimismo, dicho Estado deberá informar al Estado requirente sobre los motivos que hacen imposible, de ser así, la ejecución de la demanda o que retrasan sustancialmente su ejecución.

8. El Estado requirente podrá solicitar que el Estado requerido mantenga en secreto la propia existencia y objeto de la demanda interpuesta al amparo de este capítulo, salvo en aquellos aspectos necesarios para la ejecución de la misma. Si el Estado requirente no pudiera hacer frente a la petición de confidencialidad, éste deberá informar inmediatamente al otro Estado, quien decidirá si la demanda, pese a ello, debe ser ejecutada.

9. a. En caso de urgencia, las autoridades judiciales del Estado requirente podrán dirigir directamente a las autoridades homólogas del Estado requerido las demandas de asistencia y las comunicaciones. En tales casos, se remitirá simultáneamente una copia a las autoridades del Estado requerido con el visado de la autoridad central del Estado requirente.

b. Todas las demandas o comunicaciones formuladas al amparo del presente párrafo podrán ser tramitadas a través de la Organización Internacional de la Policía Criminal (INTERPOL).

c. Cuando una demanda haya sido formulada al amparo de la letra (a) del presente artículo, y la autoridad que le dio curso no sea la competente para ello, deberá transferir la demanda a la autoridad nacional competente y ésta informará directamente al Estado requerido.

d. Las demandas o comunicaciones realizadas al amparo del presente párrafo que no supongan la adopción de medidas coercitivas podrán ser tramitadas directamente por las autoridades del Estado requirente y las del Estado requerido.

e. Las Partes podrán informar al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que, por motivos de eficacia, las demandas formuladas al amparo del presente párrafo deberán dirigirse directamente a su autoridad central.

Artículo 28 – Confidencialidad y restricciones de uso

1. En ausencia de tratado o acuerdo en vigor de asistencia basados en la legislación uniforme o recíproca, será aplicable lo dispuesto en el presente artículo. Éste no se aplicará cuando exista un tratado, acuerdo o legislación sobre el particular, sin perjuicio de que las partes implicadas puedan decidir someterse, en todo o parte, a lo dispuesto en este artículo.

2. El Estado requerido podrá supeditar la comunicación de la información o del material requerido en la demanda al cumplimiento de las siguientes condiciones:

a. que se mantenga la confidencialidad sobre las mismas, siempre que la demanda corra el riesgo fracasar en ausencia de dicha condición; o

b. que éstas no sean utilizadas en investigaciones o procedimientos diversos a los establecidos en la demanda.

3. Si el Estado requirente no pudiera satisfacer alguna de las condiciones establecidas en el apartado 2 del presente artículo, la otra parte informará al Estado requerido, el cual decidirá si la información debe ser proporcionada. Si el Estado requirente acepta esta condición, dicho Estado estará obligado por la misma.

4. Todo Estado parte que aporte información o material supeditado a alguna de la condiciones previstas en el apartado 2, podrá exigir de la otra parte la concreción de las condiciones de uso de la información o del material.

Sección 2 – Disposiciones específicas

Título 1 – Cooperación en materia de medidas cautelares

Artículo 29 – Conservación inmediata datos informáticos almacenados

1. Las Partes podrán ordenar o imponer de otro modo la conservación inmediata de datos almacenados en sistemas informáticos que se encuentren en su territorio, en relación a los cuales el Estado requirente tiene intención de presentar una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos.

2. Una demanda de conservación formulada en aplicación del párrafo 1 deberá contener:

a. la identificación de la autoridad que solicita la conservación;

b. la infracción objeto de investigación con una breve exposición de los hechos vinculados a la misma;

c. los datos informáticos almacenados que deben conservarse y su vinculación con la infracción;

d. todas aquellas informaciones disponibles que permitan identificar al responsable de los datos informáticos almacenados o el emplazamiento de los sistemas informáticos;

e. justificación de la necesidad de conservación; y

f. la acreditación de que el Estado requirente está dispuesto a formular una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos.

3. Después de recibir la demanda, el Estado requerido deberá adoptar las medidas necesarias para proceder sin dilaciones a la conservación de los datos solicitados, conforme a su derecho interno. Para hacer efectiva la demanda de conservación no resultará condición indispensable la doble incriminación.

4. Si un Estado exige la doble incriminación como condición para atender a una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos, por infracciones diversas a las establecidas en los artículos 2 a 11 del presente Convenio, podrá negarse a la demanda de conservación, al amparo del presente artículo, si tiene fundadas sospechas de que, en el momento de la comunicación de los datos, el otro Estado no cumplirá la exigencia de la doble incriminación.

5. Al margen de lo anterior, una demanda de conservación únicamente podrá ser denegada:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que de acceder a la demanda se pondría en peligro su soberanía, su seguridad, orden público o otro interés esencial.

6. Cuando el Estado requerido considere que la simple conservación no será suficiente para garantizar la disponibilidad futura de los datos informáticos o que ésta podría comprometer la confidencialidad de la investigación o podría hacerla fracasar de otro modo, deberá informar inmediatamente al Estado requirente, quien decidirá la conveniencia de dar curso a la demanda.

7. Todas las conservaciones realizadas al amparo de una demanda de las previstas en el párrafo 1 serán válidas por un periodo máximo de 60 días, para permitir, en ese plazo de tiempo, al Estado requirente formular una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos. Después de la recepción de la demanda, los datos informáticos deberán mantenerse hasta que ésta se resuelva.

Artículo 30 – Comunicación inmediata de los datos informáticos conservados

1. Si, en ejecución de una demanda de conservación de datos de tráfico relativos a una concreta comunicación al amparo del artículo 29, el Estado requerido descubriera que un prestador de servicios de otro Estado ha participado en la transmisión de la comunicación, comunicará inmediatamente al Estado requirente los datos informáticos de tráfico, con el fin de que éste identifique al prestador de servicios y la vía por la que la comunicación ha sido realizada.

2. La comunicación de datos informáticos de tráfico prevista en el párrafo 1 únicamente podrá ser denegada:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que de acceder a la demanda se pondría en peligro su soberanía, su seguridad, orden público o otro interés esencial.

Título 2 – Asistencia en relación a los poderes de investigación

Artículo 31 – Asistencia concerniente al acceso a datos informáticos almacenados

1. Cualquier Estado podrá solicitar a otro el registro o acceso de otro modo, el decomiso u obtención por otro medio, o la comunicación de datos almacenados en un sistema informático que se encuentre en su territorio, incluidos los datos conservados conforme a lo dispuesto en el artículo 29.

2. El Estado requerido dará satisfacción a la demanda aplicando los instrumentos internacionales, convenios y la legislación mencionada en el artículo 23 siempre que no entre en contradicción con lo dispuesto en el presente capítulo.

3. La demanda deberá ser satisfecha lo más rápidamente posible en los siguientes casos:

a. cuando existan motivos para sospechar que los datos solicitados son particularmente vulnerables por existir riesgo de pérdida o modificación; o

b. cuando los instrumentos, convenios o legislación referida en el párrafo 2 prevean una cooperación rápida.

Artículo 32 – Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso

Cualquier Estado podrá sin autorización de otro:

a. acceder a los datos informáticos almacenados de libre acceso al público (fuentes abiertas), independientemente de la localización geográfica de esos datos; o

b. acceder a, o recibir a través de un sistema informático situado en su territorio, los datos informáticos almacenados situados en otro Estado, si se obtiene el consentimiento legal y voluntario de la persona autorizada para divulgarlos a través de ese sistema informático.

Artículo 33 – Asistencia para la recogida en tiempo real de datos de tráfico

1. Las Partes podrán acordar colaborar en la recogida, en tiempo real, de datos de tráfico, asociados a concretas comunicaciones llevadas a cabo en sus territorios, a través un sistema informático. Dicha colaboración se someterá a las condiciones y procedimientos previstos en el derecho interno, salvo que alguna de las partes se acoja a la reserva prevista en el párrafo 2.

2. Las Partes deberán acordar colaborar respecto a aquellas infracciones penales para las cuales la recogida en tiempo real de datos de tráfico se encuentra prevista en su derecho interno en situaciones análogas.

Artículo 34 – Asistencia en materia de interceptación de datos relativos al contenido

Las Partes podrán acordar colaborar, en la medida en que se encuentre previsto por tratados o leyes internas, en la recogida y registro, en tiempo real, de datos relativos al contenido de concretas comunicaciones realizadas a través de sistemas informáticos.

Título 3 – Red 24/7

Artículo 35 – Red 24/7

1. Las Partes designarán un punto de contacto localizable las 24 horas del día, y los siete días de la semana, con el fin de asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recogida de pruebas electrónicas de una infracción penal. Esta asistencia comprenderá, si lo permite el derecho y la práctica interna, facilitar la aplicación directa de las siguientes medidas:

- a. aportación de consejos técnicos;
- b. conservación de datos según lo dispuesto en los artículos 29 y 30; y
- c. recogida de pruebas, aportación de información de carácter jurídico y localización de sospechosos.

2. a. Un mismo punto de contacto podrá ser coincidente para dos Estados, siguiendo para ello un procedimiento acelerado.

b. Si el punto de contacto designado por un Estado no depende de su autoridad o autoridades responsables de la colaboración internacional o de la extradición, deberá velarse para que ambas autoridades actúen coordinadamente mediante la adopción de un procedimiento acelerado.

3. Las Partes dispondrán de personal formado y dotado a fin de facilitar el funcionamiento de la red.

Capítulo IV – Cláusulas finales

Artículo 36 – Firma y entrada en vigor

1. El presente Convenio está abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.

2. El presente Convenio está sometido a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación deberán ser entregados al Secretario General del Consejo de Europa.

3. El presente Convenio entrará en vigor el primer día del mes transcurridos tres meses desde que cinco Estados, de los cuales al menos tres deberán ser miembros del Consejo de Europa, presten su consentimiento a vincularse al Convenio, conforme a lo dispuesto en los párrafos 1 y 2.

4. Para todos los Estados que hayan prestado su consentimiento a vincularse al Convenio, éste entrará en vigor el primer día del mes transcurridos tres meses desde que hayan expresado su consentimiento, conforme a lo dispuesto en los párrafos 1 y 2.

Artículo 37 – Adhesión al Convenio

1. Después de entrar en vigor el presente Convenio, el Comité de Ministros del Consejo de Europa podrá, tras consultar a las Partes del Convenio y habiendo obtenido el asentimiento unánime de los mismos, invitar a todos los Estados no miembros del Consejo de Europa que no hayan participado en la elaboración del mismo a adherirse al Convenio. Esta decisión deberá tomarse mediante la mayoría prevista en el artículo 20.d del Estatuto del Consejo de Europa y el asentimiento unánime de los Estados Partes que tengan derecho a formar parte del Comité de Ministros.

2. Para todos aquellos Estados que se adhieran al Convenio conforme a lo previsto en el párrafo precedente, el Convenio entrará en vigor el primer día del mes transcurridos tres meses después del depósito del instrumento de adhesión ante el Secretario General del Consejo de Europa.

Artículo 38 – Aplicación territorial

1. Las Partes podrán, en el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, designar el territorio al que resultará aplicable el presente Convenio.

2. Las Partes podrán, en cualquier momento, a través de una declaración dirigida al Secretario General del Consejo de Europa, extender la aplicación del presente Convenio a otros territorios diversos a los designados en la declaración. En tal caso, el Convenio entrará en vigor en dichos territorios el primer día del mes transcurridos tres meses desde la recepción de la declaración por el Secretario General.

3. Toda declaración realizada al amparo de los párrafos precedentes podrá ser retirada, en lo que concierne al territorio designado en la citada declaración, a través de una notificación dirigida al Secretario General del Consejo de Europa. El retracto surtirá efecto el primer día del mes transcurridos tres meses desde la recepción de la notificación por el Secretario General.

Artículo 39 – Efectos del Convenio

1. El objeto del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales existentes entre las partes, y comprende las disposiciones:

– del Convenio Europeo de extradición abierto a la firma el 13 de diciembre de 1957 en París (STE nº 24)

- del Convenio Europeo de Cooperación judicial en materia penal abierto a la firma el 20 de abril de 1959 en Estrasburgo (STE nº 30),
- del Protocolo Adicional del Convenio Europeo de Cooperación judicial en materia penal abierto a la firma el 17 de marzo de 1978 en Estrasburgo (STE nº 99).

2. Si dos o más Estados han concluido un acuerdo o un tratado relativo a la materia objeto de este Convenio o si han establecido de otro modo la relación entre ellos, o si lo hacen en el futuro, dispondrán igualmente de la facultad de aplicar el citado acuerdo o de establecer sus relaciones con base en el mismo, en lugar del presente Convenio. Siempre que los Estados hayan establecido sus relaciones concernientes a la materia objeto del presente Convenio de forma diversa, éstas deberán llevarse a cabo de forma compatible con los objetivos y principios del Convenio.

3. Lo dispuesto en el presente Convenio no afectará a otros derechos, restricciones, obligaciones y responsabilidades de los Estados.

Artículo 40 – Declaraciones

A través de una declaración escrita dirigida al Secretario General del Consejo de Europa, las Partes podrán, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, declarar que se reservan el derecho a exigir, llegado el caso, uno o varios elementos suplementarios de los dispuestos en los artículos 2, 3, 6 del párrafo 1 (b), 7, 9 párrafo 3 y 27 del párrafo 9 (e).

Artículo 41 – Cláusula federal

1. Un Estado federal podrá reservarse el derecho de desempeñar sus obligaciones, en los términos previstos en el capítulo II del presente Convenio, en la medida en que éstas sean compatibles con los principios que presiden las relaciones entre el gobierno central y los Estados federados u otros territorios análogos, siempre que se garantice la cooperación en los términos previstos en el capítulo III.

2. Un Estado federal no podrá hacer uso de la reserva adoptada según lo dispuesto en el párrafo 1 para excluir o disminuir de forma substancial las obligaciones contraídas en virtud del capítulo II. En todo caso, el Estado federal deberá dotarse de los medios necesarios para dar cumplimiento a las medidas previstas en el citado capítulo.

3. En todo lo que concierne a las disposiciones de este Convenio cuya aplicación dimana de la competencia de cada uno de los Estados federados u otras entidades territoriales análogas, que no están, en virtud del sistema constitucional de la federación, obligados a adoptar medidas legislativas, el gobierno central pondrá, con la aprobación de éstos, en conocimiento de las autoridades competentes de los Estados federados la necesidad de adoptar las citadas medidas animándolos a que las ejecuten.

Artículo 42 – Reservas

Los Estados podrán, a través de una notificación escrita dirigida al Secretario del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o de adhesión, declarar que invocan la reserva o reservas previstas en el art. 4, párrafo 2, artículo 6, párrafo 3, artículo 9, párrafo 4, artículo 10, párrafo 3, artículo 11, párrafo 3, artículo 14, párrafo 3, artículo 22, párrafo 2, artículo 29, párrafo 4 y en el artículo 41, párrafo 1. No podrá realizarse ninguna otra reserva diversa a las indicadas.

Artículo 43 – Mantenimiento y retirada de las reservas

1. El Estado que haya formulado una reserva conforme a lo dispuesto en el artículo 42 podrá retirarla total o parcialmente notificando tal extremo al Secretario General. La retirada se hará efectiva en la fecha de recepción por el Secretario General de la notificación. Si en la notificación se hiciera constar que la reserva deberá tener efecto en una determinada fecha, ello se hará efectivo siempre que sea posterior a la recepción por el Secretario General de la notificación.

2. El Estado que haya formulado una reserva conforme a lo dispuesto en el artículo 42, podrá retirarla total o parcialmente siempre que lo permitan las circunstancias.

3. El Secretario General del Consejo de Europa podrá solicitar periódicamente a los Estados, que hayan formulado una o varias reservas conforme a lo dispuesto en el artículo 42, información sobre la posibilidad de su retirada.

Artículo 44 – Enmiendas

1. Las enmiendas al presente Convenio podrán ser propuestas por las Partes, y deberán ser comunicadas al Secretario General del Consejo de Europa, a los Estados miembros del Consejo de Europa, a los Estados no miembros del Consejo de Europa que hayan tomado parte en la elaboración del Convenio así como a los Estados que se hayan adherido o que hayan sido invitados a adherirse conforme a lo dispuesto en el artículo 37.

2. Las enmiendas propuestas por uno de los Estados deberán ser comunicadas al Comité europeo para los problemas criminales (CDPC), quien deberá informar al Comité de Ministros sobre las mismas.

3. El Comité de Ministros examinará la enmienda propuesta y el informe del Comité europeo para los problemas criminales (CDPC) y, después de consultar con los Estados no miembros y partes del Convenio, podrá adoptar la enmienda.

4. El texto de la enmienda adoptado por el Comité de Ministros, conforme a lo dispuesto en el párrafo 3 del presente artículo, deberá comunicarse a los Estados para su aceptación.

5. Las enmiendas adoptadas conforme al párrafo 3 del presente artículo entrarán en vigor el trigésimo día después del que los Estados hayan informado al Secretario General de su aceptación.

Artículo 45 – Reglamento de controversia

1. El Comité europeo para los problemas criminales (CDPC) está obligado a informar de la interpretación y aplicación del presente Convenio.
2. En caso de diferencias entre los Estados sobre la interpretación o aplicación del presente Convenio, los Estados intentarán adoptar un reglamento de diferencia a través de la negociación o de cualquier otro medio pacífico, con el compromiso de someter la controversia al Comité europeo para los problemas criminales, a un tribunal arbitral que tomará las decisiones que los Estados le sometan, o a la Corte internacional de justicia, a partir de un acuerdo adoptado por los Estados en litigio.

Artículo 46 – Reuniones de los Estados

1. Las Partes deberán reunirse periódicamente a fin de facilitar:
 - a. el uso y el efectivo cumplimiento del presente Convenio, la identificación de los problemas en esta materia, así como el efecto de las declaraciones o reservas formuladas conforme al presente Convenio;
 - b. el intercambio de información sobre novedades jurídicas, políticas o técnicas observadas en la criminalidad informática y recogida de pruebas electrónicas;
 - c. el examen sobre la posible reforma del Convenio.
2. El Comité europeo para los problemas criminales (CDPC) deberá estar al corriente de las reuniones llevadas a cabo al amparo del párrafo 1.
3. El Comité europeo para los problemas criminales (CDPC) deberá facilitar las reuniones previstas en el párrafo 1 y adoptar las medidas necesarias para ayudar a los Estados a completar o modificar el Convenio. No más tarde de tres años a contar desde la entrada en vigor del presente Convenio, el Comité europeo para los problemas criminales (CDPC) procederá, en cooperación con los Estados, a un examen conjunto de las disposiciones de la Convención y propondrá, en su caso, las modificaciones pertinentes.
4. Salvo que el Consejo de Europa los asuma, los gastos que ocasione la aplicación de las disposiciones del párrafo 1 deberán ser soportados por los Estados del modo que ellos mismos determinen.

Artículo 47 – Denuncia

1. Las Partes podrán, en cualquier momento, denunciar el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.
2. La denuncia entrará en vigor el primer día del mes transcurridos tres meses desde la recepción de la notificación por el Secretario General.

Artículo 48 – Notificación

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan tomado parte en la elaboración del presente Convenio, así como a cualquier Estado que se haya adherido o que haya sido invitado a adherirse:

- a. cualquier firma;
- b. el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;
- c. la fecha de entrada en vigor del presente Convenio según lo dispuesto en los artículos 36 y 37;
- d. cualquier declaración hecha por mor de los artículos 40 y 41 o cualquier reserva formulada en virtud del artículo 42;
- e. cualquier acto, notificación o comunicación referida al presente Convenio.

En vista de lo cual, los abajo firmantes, debidamente autorizados al efecto, han firmado el presente Convenio.

Hecho en Budapest, el 23 noviembre 2001, en francés y en inglés, ambos textos con el mismo valor, y en un solo ejemplar que será depositado en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copia certificada a cada uno de los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del Convenio y a cualquier Estado invitado a adherirse.

(1) El Convenio recoge, en la versión francesa, la expresión «fournisseur de services», cuya traducción literal sería la de «proveedor de servicios». En la presente traducción, se ha optado por emplear el término «prestador de servicios», en la línea seguida por la Directiva 2000/31 y el Proyecto de LSSI, como concepto o categoría omnicomprendiva que hace referencia a aquellos sujetos que desempeñan, profesionalmente, la actividad de prestación y gestión de accesos y servicios en Internet.

(2) También suele emplearse, para aludir a este tipo de datos, el término «datos de tránsito».

(3) El Convenio emplea el término «intentionnel». Sin embargo, en este caso, se ha preferido utilizar el vocablo «doloso» por corresponderse mejor con la categoría jurídico-penal propia del derecho español.

(4) El original en francés rubrica este ciberdelito como «Abus de dispositifs», lo que ha dado lugar a una traducción literal del mismo como «Abuso de dispositivos», expresión a la que, sin embargo, se ha preferido renunciar, por estimarse más precisa la empleada en texto.

(5) La interpretación de este último inciso suscita algunos interrogantes. De la literalidad del precepto podría deducirse que la referencia «elementos» debe circunscribirse a los propios mecanismos o

instrumentos aludidos en el precepto. Sin embargo, también sería posible inferir que el término «elementos» alude a «ánimos» o «intenciones», de modo similar a lo exigido en relación a otros delitos. Esta ambigüedad es resuelta a favor de la primera de las interpretaciones indicadas, por el [Rapport explicatif](#) del Convenio, en su parágrafo 75.

(6) Esta descripción se corresponde con la denominada «pornografía técnica».

(7) Esta descripción se corresponde con la denominada «simulada» o «pseudopornografía».

(8) El Convenio emplea el término «entraide», cuya traducción en español resulta multívoca. Entre las distintas acepciones que puede asumir el vocablo (ayuda mutua, asistencia, colaboración), se han utilizado, de modo indistinto, «asistencia» y «colaboración».

BIBLIOGRAFIA

CAPÍTULO 1

<http://www.mattica.com/articulos.php?m=1&a=2005>

<http://www.delitosinformaticos.com.mx/ciberdelitos.htm>

http://www.delitosinformaticos.com.mx/smh/FAQ_delitosinformaticos.htm

<http://www.inegi.gob.mx/inegi/contenidos/espanol/transp/ley1.asp>

<http://info4.juridicas.unam.mx/ijure/tcfed/8.htm?s>

CAPÍTULO 2

<http://www.fing.uach.mx/MatDidactico/Legislacion/deliinfo.htm>

<http://www.delitosinformaticos.com.mx/>

CAPÍTULO 3

1. Digital Planet: The Global Information Economy. WITSA. Noviembre de 2000.
2. Business Software Alliance. Forecasting a robust future: An economic study of the U S software industry. BSA. 1999.
3. UNCTAD, Changing Dynamics of Global Computer Software and Services Industry: Implication for Developing Countries. Naciones Unidas, 2001.
4. Datos estimados por CONACYT con base en la información de empresas apoyadas por FIDETEC.
5. http://www.amazon.com/exec/obidos/tg/detail/-/074321580X/ref=pd_bxgy_img_2/104-1747865-4039125?v=glance&s=books
6. <http://web2.deskbook.osd.mil/valhtml/2/26/264/264J19.htm>
7. "Distributed Tools" <http://phrack.infonexus.com/search.phtml?view&article=p56-12>
8. <http://securityportal.com/articles/webdev20001103.html>
9. Thompson, K , "Reflections on Trusting Trust", Communications of the ACM, Vol. 27, No. 8, August 1984, pp. 761-763.
10. Documento de la OEA. CP/CSH/INF.15/02 add. 1 de 4 de diciembre de 2002.
11. Recomendación N° R (89) 9 del Consejo de Europa (1989).

CAPÍTULO 4

Alarcón de Quesada, Ricardo. Intervención ante la Cumbre de la Sociedad de la Información. Ginebra . Diciembre 2003.

Barahona, Jesús M. González El futuro de la información: ¿vamos hacia donde queremos? Revista Archipiélago N° 55, marzo de 2003.

Castro, Fidel. Discurso pronunciado en Guane, Pinar del Río, el 27 de abril de 1967. Periódico Granma de 30 de abril de 1967 Cervera, José " 216 segundos de mirada: la justificación económica del copyleft" Declaración de Ginebra sobre el futuro de la Organización Mundial de la Propiedad Intelectual <http://peru.cpsr.org/>

"Declaración de la sociedad civil a la Cumbre Mundial sobre la Sociedad de la Información", Adoptada por unanimidad en Plenaria por la sociedad civil de la CMSI el 8 de diciembre de 2003.

Documento No. 2 de la Campaña CRIS, ¿Por qué los Derechos de Propiedad Intelectual Importan a la Sociedad Civil? publicado el 28 de octubre de 2003 en la Comunidad Web de movimientos sociales.

<http://www.crisinfo.org/> Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas (IFLA) "Limitaciones y excepciones al derecho de autor y derechos afines en el entorno digital: Una perspectiva internacional de las bibliotecas". <http://www.ifla.org/>

CAPÍTULO 5

<http://mx.news.finance.yahoo.com/21112006/7/finanzas-demandan-fraude-cibern-tico-santander-m-xico.html>

<http://www.jornada.unam.mx/2006/11/22/?section=economia&article=032n2eco&partner=rss>

http://www.robosbancarios.com/2006/10/en_mexico_todo_es_al_reves.html

GLOSARIO

GLOSARIO

backdoor:

Puerta trasera. Permiten a un usuario remoto ingresar sin autorización a otros sistemas mediante la instalación de un programa de acceso considerado virus, esto permite realizar diversas acciones como revisar datos, borrar archivos, infectar con otro tipo de virus, tareas que generalmente no son percibidas por el sistema víctima.

bomba lógica:

es una pieza de código de programación agregada a un software de una aplicación o sistema operativo que permanece inactiva hasta que, transcurrido un cierto período de tiempo, o al ocurrir un determinado evento, se pone en acción.

Las bombas lógicas tienen generalmente intenciones maliciosas, actuando de la misma manera que un virus o troyano al activarse. De hecho, los virus que están programados para activarse a cierta hora se consideran bombas lógicas. Pueden realizar acciones tales como formatear un disco duro, alterar o borrar datos, cambiar la configuración del sistema, etc.

bounds checking:

En la programación informática, el control de fronteras (bounds chekings) es cualquier método de detectar si una variable esta dentro de algunos límites antes de su uso. Es especialmente relevante para una variable utilizada como un índice en un arreglo para asegurar su valor reside dentro de los límites de la matriz. Por ejemplo: un valor de 32768 a punto de ser asignado a una de dieciséis bits con signo variable (superior cuyos límites son -32768 a 32767), o acceder a elemento 25 en índice de un arreglo (array) con rango de 0 a 9 solamente. La primera es conocida también como serie de cheques, la segunda como índice de control.

buffer:

es un área de almacenamiento temporario, usualmente en la RAM. El propósito de casi todos los buffers es actuar como área de almacenamiento, permitiendo que el CPU manipule los datos antes de transferirlos a un dispositivo.

Dado que los procesos de leer y escribir datos a un disco son relativamente lentos, muchos programas mantienen la referencia de los cambios en los datos en un buffer y luego copian el buffer al disco. Por ejemplo, los procesadores de textos emplean un buffer para el seguimiento de los cambios en un documento. Entonces, cuando se guarda el archivo, el programa actualiza el archivo en disco con los contenidos del buffer. Esto es más eficiente que acceder al archivo en disco cada vez que se realiza un cambio en el mismo.

Nótese que como los cambios se almacenan inicialmente en un buffer, y no en el disco, todos ellos se perderán si la computadora falla durante la sesión de edición. Por esto, es buena idea guardar periódicamente los archivos sobre los que se trabaja. La mayoría de los procesadores de textos guardan los archivos periódicamente a intervalos regulares de tiempo, que incluso pueden predefinirse en su configuración.

Los buffers suelen usarse también cuando se queman datos en CD-ROM. Los datos a copiar se transfieren al buffer antes de escribirse al disco.

Otro uso común de los buffers es para la impresión de documentos. Cuando se imprime un documento, el sistema operativo copia éste a un buffer de impresión (un área libre en memoria o disco), desde donde la impresora podrá leer e imprimir los caracteres con su propio ritmo. Esto libera la computadora para realizar otras tareas mientras la impresora funciona de fondo. Este proceso se conoce como *spooling*.

La mayoría de los drivers de teclado contienen un buffer de modo que se pueden editar los errores de tipeado antes de enviar el comando a un programa. Muchos sistemas operativos, incluyendo DOS, usan también un buffer de disco para guardar datos temporales que se leyeron del disco. El buffer de disco se conoce como caché.

buffer overflow:

buffer overflow o desbordamiento de buffer es un error de sistema causado por un defecto de programación, de tal forma que el programa que lo sufre pretende escribir más información en el buffer (unidad de memoria) de la que este puede alojar.

Este desbordamiento es posible porque el autor del programa no incluyó el código necesario para comprobar el tamaño y capacidad del buffer en relación con el volumen de datos que tiene que alojar.

Los problemas comienzan cuando el exceso de datos se escribe en otras posiciones de memoria, con la pérdida de los datos anteriores.

Si entre los datos perdidos por la sobreescritura se encuentran rutinas o procedimientos necesarios para el funcionamiento del programa que estamos ejecutando, el programa dará error.

Cuando la memoria de un programa llega a sobrecribir en forma aleatoria, el programa generalmente se colgará.

El problema para la seguridad nace cuando este desbordamiento de buffer es provocado intencionalmente por alguien mediante envío de datos que incluyen porciones de código, calculando la cantidad de datos para poder predeterminedir cual es el sobrante que se va a sobrecribir y donde. Provocado el desbordamiento, contienen una instrucción que apunta a una posición de memoria distinta, donde se encuentra el código ejecutable enviado por el atacante. El programa, inducido a funcionar anormalmente por la pérdida de datos causada por el desbordamiento, ejecutará el código enviado por el atacante.

El buffer overflow es un problema de código defectuoso, por lo tanto como usuarios nada podemos hacer para evitarlo (salvo que además de usuarios seamos expertos programadores, y dispongamos del código fuente de la aplicación que sufre el desbordamiento). En realidad el único remedio es estar informado de los programas que sufran estos problemas, y tener el software actualizado.

bug:

bicho, insecto. Error de programación que genera problemas en las operaciones de una computadora. Se habla de bug si es un error de diseño, pero no cuando la falla es provocada por otra cosa.

ciber:

prefijo utilizado ampliamente en la comunidad de Internet para denominar conceptos relacionados con las redes (cibercultura, ciberespacio, cibernauta, etc.).

Su origen es la palabra griega kibernao, que significa "pilotear una nave".

ciberpolicía:

funcionario policial especializado en Internet o en utilizar la red para sus investigaciones.

ciberacoso:

conducta amenazante o aproximaciones no deseadas dirigidas a otro usando el Internet y otras formas de comunicación "en línea".

código fuente:

Son las instrucciones de un programa en su forma original. La palabra fuente diferencia el código de varias otras formas posibles (por ej., código del objeto y código ejecutable).

Inicialmente, un programador escribe un programa en un lenguaje de programación en particular. Esto es, genera el programa fuente, o más genéricamente, el código fuente. Para ejecutar el programa, es necesario que el programador traduzca todo esto a lenguaje de máquina, para que lo entienda la computadora. El primer paso de esta traducción se logra con una utilidad denominada compilador. Éste, traduce el código fuente a una forma llamada código del objeto. Muchas veces, dicho código es el mismo que el código de máquina, pero otras debe traducirse a lenguaje de máquina usando otra utilidad, el ensamblador.

El código fuente es el único formato legible por humanos. Al adquirir un programa, normalmente los recibimos en su formato ejecutable, en código de máquina. Lo cual significa que pueden correrse directamente en la computadora, pero no pueden "leerse" ni modificarse. Algunos fabricantes o desarrolladores proveen además el código fuente, pero esto sólo le es útil a un programador avanzado que desee modificarlo o mejorarlo a su gusto.

comercio electrónico:

es la utilización de redes de datos (entre ellas principalmente Internet) para la realización de actividades comerciales entre empresas, consumidores finales y entidades de gobierno. Se trata de un área de negocios que crece a pasos agigantados y cada vez más perfeccionado y estandarizado.

computadora:

dispositivo, sistema, equipo de informática o aparato automático para el tratamiento de la información, que obedece a programas formados por sucesiones de operaciones aritméticas y lógicas. Una computadora comprende una parte física (hardware), constituida por circuitos electrónicos de alta integración, y una parte no física (software); el objetivo es realizar funciones lógicas, aritméticas, transmisión o de almacenamiento de datos, así como para el tratamiento sistemático de la información mediante el procesamiento automático de datos electrónicos o de cualquier otra tecnología. Esta definición incluye las redes públicas y privadas de computadoras.

contraseña:

palabra secreta que permite el acceso a servicios o información codificada a un cliente en particular.

correo electrónico:

es la transmisión de mensajes sobre redes de comunicaciones. Estos mensajes pueden consistir en textos escritos o archivos guardados en disco. Pueden enviarse también a múltiples destinatarios, lo que se denomina "broadcasting". Los mensajes enviados se almacenan en casillas de correo electrónico hasta que el receptor los revise. Una vez leídos pueden guardarse en el disco de la computadora, reenviarlos a otros usuarios, imprimirlos o simplemente eliminarlos. Todos los proveedores de acceso a Internet y casi todos los grandes portales brindan servicios de e-mail a sus usuarios, en algunos casos, gratuitamente. Un e-mail demora en condiciones normales unos pocos segundos en alcanzar su destino.

cortafuego:

Ver firewall.

cracker:

un hacker con intenciones destructivas y/o delictivas.

cracking :

Penetración fraudulenta en los sistemas ya sea para obtener un beneficio o causar daño.

craquear:

es el hecho de copiar y/o utilizar software comercial ilegalmente rompiendo las distintas técnicas de protección o registro que utilicen.

daemon:

aplicación UNIX que está alerta permanentemente en un servidor de Internet para realizar determinadas tareas como, por ejemplo, enviar un mensaje de correo electrónico o servir una página Web.

Datos o información personal:

Cualquier información relacionada a una persona física identificada o identificable. Los datos personales usualmente contienen información que directa o indirectamente puede ser relacionada o ligada a una persona física en particular.

Daño Informático:

deterioro o menoscabo a la integridad, confidencialidad y/o disponibilidad de datos, información, programas de cómputo, o computadoras.

defacement:

es una forma de hacking malicioso en el que un sitio Web es vandalizado. Normalmente un hacker malicioso (cracker) reemplaza el contenido normal del sitio con un mensaje específico de carácter político o social o aún más, borran el contenido del sitio entero. Logran esto aprovechándose de vulnerabilidades de seguridad para acceder al contenido del sitio.

delito informático:

se define como aquella conducta que teniendo como instrumento o fin computadoras u otros bienes informáticos, lesionan o dañan bienes, intereses o derechos de personas físicas o morales.

DSL:

Digital Subscriber Line: Línea Digital de Suscripción. Tecnología que permite enviar mucha información a gran velocidad a través de líneas telefónicas..

firewall:

es un sistema diseñado para prevenir el acceso no autorizado a o desde una red privada, normalmente en el caso de intranets. Los firewalls pueden implementarse tanto en hardware, en software, o bien en conjunto. Todos los mensajes entrantes o salientes de la intranet pasan por el firewall, el cual

examina cada uno y bloquea aquellos que no cumplan los criterios de seguridad especificados.

Hay varios tipos de firewall:

- Filtrado de paquetes: analiza cada paquete entrante o saliente de la red y lo acepta o rechaza basado en reglas predefinidas. Este método es bastante efectivo y transparente a los usuarios, aunque es difícil de configurar. Además, es susceptible a ataques de IP spoofing.
- Portal de aplicaciones: aplica mecanismos de seguridad a aplicaciones específicas, tales como servidores FTP y Telnet. Es muy efectivo pero puede degradar el rendimiento del sistema.
- portal a nivel circuito: aplica mecanismos de seguridad cuando se establece una conexión TCP o UDP. Una vez que se logra autenticar la conexión los paquetes fluyen libremente entre los hosts sin chequeos posteriores.
- Servidor proxy: intercepta todos los mensajes entrantes o salientes de la red y efectivamente oculta todas las direcciones reales de la red.

En la práctica, muchos firewalls usan dos o más de estas técnicas en conjunto. El firewall es la primer línea de defensa para proteger información privada. Para mayor seguridad los datos pueden encriptarse.

GATT: Acuerdo General de Aranceles Aduaneros y Comercio

gusano:

programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. Generalmente suelen llegar a través del correo electrónico, en forma de archivo adjunto.

Los gusanos de redes fueron definidos por primera vez por Shoch & Hupp, de Xerox, en la revista ACM Communications (Marzo 1982). El primer gusano famoso de Internet apareció en Noviembre de 1988 y se propagó por sí solo a más de 6000 sistemas a lo largo de Internet.

hacker:

experto informático especialista en entrar en sistemas ajenos sin permiso, generalmente para mostrar la baja seguridad de los mismos o simplemente para demostrar que es capaz de hacerlo. Los Hackers son muy respetados por la comunidad técnica de Internet, y proclaman tener una ética y unos principios contestatarios e inconformistas pero no delictivos, a diferencia de los Crackers que utilizan sus conocimientos para fines destructivos o delictivos.

hacking:

Acción de piratear sistemas informáticos y redes de telecomunicación.

hacktivismo:

formado al combinar "hack" con "activismo", se refiere al hacking de un sitio Web o sistema de cómputo para comunicar un mensaje motivado política o socialmente. A diferencia de un hacker malicioso, que puede irrumpir en un

sistema para obtener información o causar daños, el hacktivista realiza las mismas acciones para llamar la atención a una causa. Para el hacktivista, es la forma electrónica de practicar su protesta y desobediencia civil.

Acción de piratear sistemas informáticos y redes de telecomunicación.

hardware:

se refiere a todos los componentes físicos (que se pueden tocar) de la computadora: discos, unidades de disco, monitor, teclado, mouse, impresora, placas, chips y demás periféricos. En cambio, el software es intocable, existe como ideas, conceptos, símbolos, pero no tiene sustancia. Una buena metáfora sería un libro: las páginas y la tinta son el hardware, mientras que las palabras, oraciones, párrafos y el significado del texto son el software. Una computadora sin software sería tan inútil como un libro con páginas en blanco.

hosting:

alojamiento. Servicio ofrecido por algunos proveedores, que brindan a sus clientes (individuos o empresas) un espacio en su servidor para alojar un sitio web.

Información:

archivos o datos contenidos y/o transmitidos a través de una computadora, o por medios electrónicos, ópticos o de cualquier otra tecnología.

Internet:

red de redes. Sistema mundial de redes de computadoras interconectadas. Fue concebida en 1969 por el Departamento de Defensa de los Estados Unidos; más precisamente, por la ARPA. Hasta 1974 se llamó ARPAnet y fue pensada para cumplir funciones de investigación. Su uso se popularizó a partir de la creación de la World Wide Web. Actualmente es un espacio público utilizado por millones de personas en todo el mundo como herramienta de comunicación e información.

IP:

Internet Protocol. Protocolo de Internet. Sistema que define el modo en que los sistemas intercambian información en Internet.

IP spoofing:

técnica que permite que un atacante tome la identidad de un host "confiable" (cambiando su dirección IP por la dirección de éste) y obtenga de este modo accesos no autorizados a otros sistemas. En numerosos sitios (bajo Unix o Linux), existe un archivo denominado .rhosts conteniendo una lista de nombres de hosts que se consideran de confianza. Si un atacante se hace pasar por una de esas direcciones, puede llegar a ejecutar comandos en forma remota o logearse en el sistema aún sin tener una contraseña.

Mecanismo de seguridad:

dispositivo físico y/o electrónico, palabra clave, código de acceso, programa de cómputo o equipo informático que tenga por objetivo proteger una computadora, un programa de cómputo y/o la información contenida en una computadora, sistema o equipo informático de o contra:

- a) accesos internos o externos no autorizados;
- b) borrado, alteración o daño de información;
- c) ataque informático de cualquier índole.
- d) repudio del emisor o receptor de la información.

NIMDA:

El gusano "Nimda" (ADMIN, sigla de ADMINistrador, invertido), tiene la capacidad de propagarse a una velocidad pocas veces vistas en Internet. Se vale de cuatro formas diferentes para hacerlo.

1. Utiliza la misma vulnerabilidad en los servidores IIS de Microsoft, que usa el CodeRed y otros posteriores, para tomar el control de sus víctimas. Una vez en un servidor infectado, puede propagarse a otros servidores que tengan la misma vulnerabilidad, usando el comando tftp para enviar su código (en un archivo **ADMIN.DLL**).
2. Puede propagarse a través del correo electrónico, distribuyéndose a todos los contactos de la libreta de direcciones y otros obtenidos del historial del navegador, en un mensaje con el virus en el archivo **README.EXE** adjunto.
3. Cuando un servidor Web está infectado, cada usuario que visita sus páginas puede descargar el gusano desde un supuesto archivo WAV (sonido), que en realidad se llama **README.EML**. Bajo ciertas condiciones el Internet Explorer querrá ejecutar automáticamente el archivo del gusano, causando la infección de su computadora.
4. Se puede propagar a través de recursos compartidos en red, siempre que aquellos recursos sean accesibles sin contraseñas. Esto incluye a los usuarios domésticos que tienen habilitada la opción "**Compartir impresoras y archivos para redes**".

Hay informes de algunos mensajes enviados desde direcciones falsas, pero se supone que alguien, intencionalmente, modificó esas direcciones para hacer creer al destinatario en un remitente confiable. Se especula que esto podría haber sido hecho intencionalmente para propagar el virus en sus comienzos. El gusano está escrito en Microsoft Visual C++.

ONU: Organización de la Naciones Unidas.

página web:

es una de las tantas páginas que pueden componer un sitio de la World Wide Web. Un sitio Web agrupa un conjunto de páginas afines. A la página de inicio se la llama "home page".

password:

Ver contraseña.

phishing:

phishing: pesca. Es el acto de enviar un mail fraudulento a un usuario en nombre de una empresa legítima para engañarlo respecto a algún tema de su información privada. El mail deriva al usuario a un sitio Web donde se le pregunta algún dato personal, como ser contraseñas, número de tarjeta de crédito, cuentas bancarias, etc, que la verdadera organización ya tiene. Ese sitio, obviamente, es un truco para robar los datos del usuario.

phreaking:

está íntimamente relacionado al hacking, y consiste en utilizar una computadora u otro dispositivo para engañar al sistema telefónico. Típicamente, el phreaking se usa para hacer llamadas gratuitas o cargar esas llamadas a una cuenta diferente.

piratería de software:

es la copia no autorizada de software. La mayoría de los programas a la venta se licencian para el uso en sólo una computadora o para ser usados solamente por un usuario a la vez. Al comprar el software, el usuario se convierte en un usuario licenciado y no en un propietario (véase EULA). El usuario licenciado tiene permiso para realizar copias del programa con propósitos de backup, pero va contra la ley el distribuir copias a amigos y colegas. La piratería de software es imposible de detener, sin embargo las compañías de software están abriendo cada vez más y más demandas contra grandes infractores. Originalmente, las compañías de software trataban de detener la piratería usando protecciones anticopia, pero esta estrategia falló porque era inconveniente para los usuarios legítimos y no es 100% eficiente. La mayoría del software requiere algún tipo de registro, el cual desalienta a potenciales piratas, pero no detiene realmente la piratería en sí.

Hay un enfoque enteramente distinto a la piratería, denominado shareware, y se basa en la honestidad de la gente. Los productores de shareware alientan a los usuarios a dar copias de los programas a sus amigos y colegas pero le pidan a cualquiera que use el software regularmente que pague una cuota de registro directamente al autor del programa.

Los programas comerciales que se ponen a disposición del público ilegalmente se conocen como warez.

Policía Cibernética:

Unidad derivada de la Policía Federal Preventiva de México (PFP), que además de las acciones preventivas en materia de delitos cometidos en Internet y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores, como existen en los países desarrollados.

Programa(s) de cómputo o computación:

la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

PROSOFT: Programa para el desarrollo de la industria de Software.

Self-Certifying File System:

SFS es un seguro, sistema de archivos de red global con control completamente descentralizado. SFS permite acceder a sus archivos desde cualquier lugar y compartirlos con cualquier persona y en cualquier lugar. Cualquiera puede crear un servidor de SFS, y cualquier usuario puede acceder a cualquier servidor desde cualquier cliente.

sniffer:

programa que monitorea y analiza el tráfico de una red para detectar problemas o congestiones (conocidos como "bottlenecks", cuellos de botella). Su objetivo es mantener la eficiencia del tráfico de datos. Pero también puede ser usado ilegítimamente para capturar datos en una red. Esto último, sumado al hecho de que son prácticamente imposibles de detectar, los convierten en las herramientas favoritas de los hackers.

software:

se refiere a instrucciones para computadoras o datos. Cualquier cosa que pueda almacenarse electrónicamente es software, por eso se designa con este término a los diversos tipos de programas usados en computación. Los dispositivos de almacenamiento y visualización son el hardware.

El software suele dividirse en estas dos categorías:

- i. sistemas: incluye el sistema operativo y todas las utilidades que hacen funcionar a la computadora.

- ii. aplicaciones: son los programas que trabajan para los usuarios: procesadores de texto, planillas de cálculo, administradores de archivos y/o bases de datos, etc.

spam:

envío de correo electrónico publicitario no solicitado que se envía a listas de cientos de miles de usuarios. Se lo considera muy poco ético, ya que el receptor paga por estar conectado a Internet y no debería tener que estar soportando estas prácticas. Este tipo de mensajes causa graves molestias y provoca importantes pérdidas de tiempo y recursos.

Técnica del salami:

La técnica del salami es una forma de delito automatizado que consiste en el robo de pequeñas cantidades de activos de un gran número de fuentes, de allí su nombre ya que el método equivale al hecho de tomar rebanadas muy delgadas de un trozo de salami sin reducir significativamente el trozo total, por lo que las víctimas de este tipo de delito no se dan cuenta que están siendo objeto de un robo, o las diferencias que perciben en sus balances (de nóminas, cuentas corrientes, inventarios, etc.)

Son tan pequeñas que no consideran que vale la pena reclamarlas.

TI: tecnologías de información

TLC: Tratado de Libre comercio de América del Norte.

troyano:

(Trojan horse); caballo de Troya. Programa que contiene un código dañino dentro de datos aparentemente inofensivos. Puede arruinar parte del disco rígido o provocar pérdidas de información.

virus:

1. Programa o código que se carga en la computadora sin conocimiento del usuario y que se ejecuta por sí mismo.
2. Programa o código capaz de replicarse, esto es, capaz de infectar otros programas, el sector de arranque, alguna partición, o documentos que pueden ejecutar macros u otro tipo de programas, bien adjuntándose o insertándose a ese medio.

ANEXO I.

INSTITUCIONES DE LA ADMINISTRACIÓN PÚBLICA FEDERAL CON ATRIBUCIONES VINCULADAS CON LA INFORMÁTICA

En la Administración Pública Federal existen diversas instituciones con atribuciones que directa o indirectamente inciden en el ámbito de la informática, cuya participación es necesaria para promover el desarrollo nacional en la materia.

A continuación se señalan dichas instituciones y algunas atribuciones que inciden en la informática.

SECRETARÍA DE GOBERNACIÓN

Vigilar el cumplimiento de los preceptos constitucionales por parte de las autoridades del país, especialmente en lo que se refiere a las garantías individuales, y dictar las medidas administrativas que requiere ese cumplimiento.

SECRETARÍA DE RELACIONES EXTERIORES

Promover, propiciar y asegurar la coordinación de acciones en el exterior de las dependencias y entidades de la Administración Pública Federal; y sin afectar el ejercicio de las atribuciones que a cada una de ellas corresponda, conducir la política exterior para lo cual intervendrá en toda clase de tratados, acuerdos y convenciones en los que el país sea parte.

SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

- Determinar los criterios y montos globales de los estímulos fiscales, escuchando para ello a las dependencias responsables de los sectores correspondientes y administrar su aplicación en los casos en que no compete a otra Secretaría.
- Proyectar y calcular los egresos del Gobierno Federal y de la administración pública paraestatal, haciéndolos compatibles con la disponibilidad de recursos y en atención a las necesidades y políticas del desarrollo nacional.
- Formular el programa del gasto público federal y el proyecto del Presupuesto de Egresos de la Federación y presentarlos, junto con el del Departamento del Distrito Federal, a la consideración del Presidente de la República.
- Evaluar y autorizar los programas de inversión pública de las dependencias y entidades de la Administración Pública Federal.

- Coordinar y desarrollar los servicios nacionales de estadística y de información geográfica; establecer las normas y procedimientos para la organización, funcionamiento y coordinación de los sistemas nacionales estadísticos de información geográfica, así como normar y coordinar los servicios de informática de las dependencias y entidades de la Administración Pública Federal.
- Opinar, previamente a su expedición, sobre los proyectos de normas y lineamientos en materia de adquisiciones, arrendamientos y desincorporación de activos, servicios y ejecución de obras públicas de la Administración Pública Federal.
- Vigilar el cumplimiento de las obligaciones derivadas de las disposiciones en materia de planeación nacional, así como de programación, presupuestación, contabilidad y evaluación.

SECRETARÍA DE COMERCIO Y FOMENTO INDUSTRIAL

- Formular y conducir las políticas generales de industria, comercio exterior, interior, abasto y precios del país, con excepción de los precios de bienes y servicios de la Administración Pública Federal.
- Estudiar y determinar mediante reglas generales, conforme a los montos globales establecidos por la Secretaría de Hacienda y Crédito Público, los estímulos fiscales necesarios para el fomento industrial, el comercio interior y exterior y el abasto, incluyendo los subsidios sobre impuestos de importación, y administrar su aplicación, así como vigilar y evaluar sus resultados.
- Normar y registrar la propiedad industrial y mercantil, así como regular y orientar la inversión extranjera y la transferencia de tecnología;
- Establecer y vigilar las normas de calidad, pesas y medidas necesarias para la actividad comercial, así como las normas y especificaciones industriales;
- Promover, orientar, fomentar y estimular la industria nacional.
- Promover, orientar, fomentar y estimular el desarrollo de la industria pequeña, mediana y regular la organización de productores industriales.

SECRETARÍA DE COMUNICACIONES Y TRANSPORTES

- Formular y conducir las políticas y programas para el desarrollo del transporte y las comunicaciones de acuerdo a las necesidades del país;
- Otorgar concesiones y permisos previa opinión de la Secretaría de Gobernación para establecer y explotar sistemas de servicios telegráficos, telefónicos, sistemas y servicios de comunicación inalámbrica por telecomunicaciones y satélites, de servicio público de procesamiento remoto de datos, estaciones de radio

experimentales, culturales y de aficionados y estaciones de radiodifusión comerciales y culturales; así como vigilar el aspecto técnico del funcionamiento de tales sistemas, servicios y estaciones.

SECRETARÍA DE CONTRALORÍA Y DESARROLLO ADMINISTRATIVO

- Vigilar el cumplimiento, por parte de las dependencias y entidades de la Administración Pública Federal, de las disposiciones en materia de planeación, presupuestación, ingresos, financiamiento, inversión, deuda, patrimonio, fondos y valores.
- Organizar y coordinar el desarrollo administrativo integral en las dependencias y entidades de la Administración Pública Federal, a fin de que los recursos humanos, patrimoniales y los procedimientos técnicos de la misma, sean aprovechados y aplicados con criterios de eficiencia, buscando en todo momento la eficacia, descentralización, desconcentración y simplificación administrativa. Para ello, podrá realizar o encomendar las investigaciones, estudios y análisis necesarios sobre estas materias, y dictar las disposiciones administrativas que sean necesarias al efecto, tanto para las dependencias, como para las entidades de la Administración Pública Federal.
- Inspeccionar y vigilar, directamente o a través de los órganos de control, que las dependencias y entidades de la Administración Pública Federal cumplan con las normas y disposiciones en materia de sistemas de registro y contabilidad, contratación y remuneraciones de personal, contratación de adquisiciones, arrendamientos, servicios, y ejecución de obra pública, conservación, uso, destino, afectación, enajenación y baja de bienes muebles e inmuebles, almacenes y demás activos y recursos materiales de la Administración Pública Federal.
- Establecer normas, políticas y lineamientos en materia de adquisiciones, arrendamientos, desincorporación de activos, servicios y obras públicas de la Administración Pública Federal.

SECRETARÍA DE EDUCACIÓN PÚBLICA

- Vigilar que se observen y cumplan las disposiciones relacionadas con la educación preescolar, primaria, secundaria, técnica y normal, establecidas en la Constitución y prescribir las normas a que debe ajustarse la incorporación de las escuelas particulares del sistema educativo nacional.
- Promover la creación de institutos de investigación científica y técnica, y el establecimiento de laboratorios, observatorios, planetarios y demás centros que requiera el desarrollo de la educación primaria, secundaria, normal, técnica y superior; orientar, en coordinación con las dependencias competentes del Gobierno Federal y con las entidades públicas y privadas el desarrollo de la investigación científica y tecnológica.
- Organizar, controlar y mantener al corriente el registro de la

propiedad literaria y artística.

- Vigilar con auxilio de las asociaciones de profesionistas, el correcto ejercicio de las profesiones.

COMISIÓN FEDERAL DE TELECOMUNICACIONES

- Expedir las disposiciones administrativas y las normas oficiales mexicanas en materia de telecomunicaciones, así como elaborar y administrar los planes técnicos fundamentales.
- Realizar estudios e investigaciones en materia de telecomunicaciones y elaborar anteproyectos de adecuación, modificación y actualización de las disposiciones legales y reglamentarias que resulten pertinentes.
- Establecer los procedimientos para la adecuada homologación de equipos, así como otorgar la certificación correspondiente o autorizar a terceros para que emitan dicha certificación, unidades de verificación, organismo de certificación y laboratorios de prueba en materia de telecomunicaciones, y acreditar peritos en dicha materia.
- Administrar el espectro radioeléctrico y promover su uso eficiente, así como elaborar y mantener actualizado el Cuadro Nacional de Atribución de Frecuencias.
- Promover y vigilar la eficiente interconexión de los equipos y redes públicas de telecomunicaciones, incluyendo la que se realice con redes extranjeras, y resolver las condiciones que, en materia de interconexión, no hayan podido convenirse entre los concesionarios de redes públicas de telecomunicaciones.
- Aprobar los convenios de interconexión entre redes públicas de telecomunicaciones con redes extranjeras y, en su caso, establecer las modalidades a que deberán sujetarse, así como autorizar la instalación de equipos de telecomunicaciones y medios de transmisión que crucen las fronteras del país.
- Dar seguimiento a los compromisos adquiridos por México ante organismos y otras entidades internacionales en el ámbito de competencia de la Comisión.
- Llevar a cabo la coordinación de la operación de satélites nacionales con satélites extranjeros e internacionales.
- Aplicar y ejercer las funciones de autoridad en las reglas, normas oficiales mexicanas y demás disposiciones administrativas en materia de telecomunicaciones.

CONSEJO NACIONAL DE CIENCIA Y TECNOLOGÍA

- Fungir como asesor del Ejecutivo Federal en la planeación, programación,

coordinación, orientación sistematización, promoción y encausamiento de las actividades relacionadas con la ciencia y la tecnología, su vinculación al desarrollo nacional y sus relaciones con el exterior.

- Fomentar y fortalecer las investigaciones básicas, tecnológicas y aplicadas que se necesiten y promover las acciones concertadas que se requieran con los institutos del sector público, instituciones académicas, centros de investigación y usuarios de las mismas, incluyendo al sector privado.

ANEXO 2



Convenio sobre cibercriminalidad

Budapest, 23.XI.2001

Traducción no oficial.

Preámbulo

Los Estados miembros del Consejo de Europa y los otros Estados firmantes,

Considerando que el objetivo del Consejo de Europa es lograr una unión más estrecha entre sus miembros;

Reconociendo el interés de intensificar la cooperación con los otros Estados parte en el Convenio;

Convencidos de la necesidad de llevar a cabo, con prioridad, una política penal común destinada a prevenir la criminalidad en el ciberespacio y, en particular, de hacerlo mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional;

Conscientes de los profundos cambios suscitados por el incremento, la convergencia y la mundialización permanente de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer infracciones penales y que las pruebas de dichas infracciones sean almacenadas y transmitidas por medio de esas redes;

Reconociendo la necesidad de una cooperación entre los Estados y la industria privada en la lucha contra la cibercriminalidad y la necesidad de proteger los intereses legítimos vinculados al desarrollo de las tecnologías de la información;

Estimando que una lucha bien organizada contra la cibercriminalidad requiere una cooperación internacional en materia penal acrecentada, rápida y eficaz;

Convencidos de que el presente Convenio es necesario para prevenir los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos, como los descritos en el presente Convenio, y la atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando la detección, la investigación y la persecución, tanto a nivel

nacional como internacional, y previendo algunas disposiciones materiales al objeto de una cooperación internacional rápida y fiable;

Persuadidos de la necesidad de garantizar un equilibrio adecuado entre los intereses de la acción represiva y el respeto de los derechos fundamentales del hombre, como los garantizados en el Convenio para la protección de los derechos del hombre y de las libertades fundamentales del Consejo de Europa (1950), en el Pacto internacional relativo a los derechos civiles y políticos de las Naciones Unidas (1966), así como en otros convenios internacionales aplicables en materia de derechos del hombre, que reafirman el derecho de no ser perseguido por la opinión, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar informaciones e ideas de toda naturaleza, sin consideración de fronteras, así como el derecho al respeto de la vida privada;

Conscientes, igualmente, de la protección de los datos personales, como la que confiere, por ejemplo, el Convenio de 1981 del Consejo de Europa para la protección de las personas en lo referente al tratamiento automatizado de los datos de carácter personal;

Considerando el Convenio de Naciones Unidas relativo a los derechos del niño y el Convenio de la Organización Internacional del Trabajo sobre la prohibición de las peores formas de trabajo infantil (1999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre la cooperación en materia penal, así como otros tratados similares suscritos entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el presente Convenio tiene por objeto completarlos con el fin de hacer más eficaces las investigaciones y procedimientos penales relativos a las infracciones penales vinculadas a sistemas y datos informáticos, así como permitir la recogida de pruebas electrónicas de una infracción penal;

Felicitándose por las recientes iniciativas destinadas a mejorar la comprensión y la cooperación internacional para la lucha contra la criminalidad en el ciberespacio y, en particular, las acciones organizadas por las Naciones Unidas, la OCDE, la Unión europea y el G8;

Recordando la Recomendación N.º (85) 10 sobre la aplicación práctica del Convenio europeo de ayuda mutua judicial en materia penal respecto a las comisiones rogatorias para la vigilancia de las telecomunicaciones, la Recomendación N.º (88) 2 sobre medidas dirigidas a combatir la piratería en el ámbito de los derechos de autor y de los derechos afines, la Recomendación N.º (87) 15 dirigida a regular la utilización de datos de carácter personal en el sector de la policía, la Recomendación N.º (95) 4 sobre la protección de los datos de carácter personal en el sector de los servicios de telecomunicación, teniendo en cuenta, en particular, los servicios telefónicos y la Recomendación N.º (89) 9 sobre la delincuencia relacionada con el ordenador, que indica a los legisladores nacionales los principios directores para definir ciertas infracciones informáticas, así como la Recomendación N.º (95) 13 relativa a los problemas de procedimiento penal vinculados a las tecnologías de la información;

Vista la Resolución N.º 1, adoptada por los Ministros europeos de Justicia, en su 21ª Conferencia (Praga, junio 1997), que recomienda al Comité de Ministros

mantener las actividades organizadas por el Comité europeo para los problemas penales (CDPC) relativas a la cibercriminalidad a fin de acercar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de infracciones informáticas, así como la Resolución N.º 3, adoptada en la 23ª Conferencia de Ministros europeos de Justicia (Londres, junio 2000), que anima a las partes negociadoras a persistir en sus esfuerzos al objeto de encontrar soluciones adecuadas, que permitan al mayor número posible de Estados ser partes en el Convenio y reconoce la necesidad de disponer de un mecanismo rápido y eficaz de cooperación internacional, que tenga en cuenta las específicas exigencias de la lucha contra la cibercriminalidad;

Tomando igualmente en cuenta el Plan de acción adoptado por los Jefes de Estado y de gobierno del Consejo de Europa, con ocasión de su Décima Cumbre (Estrasburgo, 10-11 octubre 1997) a fin de buscar respuestas comunes al desarrollo de las nuevas tecnologías de la información, fundadas sobre las normas y los valores del Consejo de Europa;

Han convenido lo siguiente:

Capítulo I – Terminología

Artículo 1 – Definiciones

A los efectos del presente Convenio, la expresión:

a. "sistema informático" designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos;

b. "datos informáticos" designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función;

c. "prestador de servicio" ⁽¹⁾ designa:

i. toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático;

ii. cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios;

d. "datos de tráfico" ⁽²⁾ designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Capítulo II – Medidas que deben ser adoptadas a nivel nacional

Sección 1 – Derecho penal material

Título 1 – Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2 – Acceso ilícito

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso ⁽³⁾ y sin autorización a todo o parte de un sistema informático. Las Partes podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 3 – Interceptación ilícita

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos – en transmisiones no públicas– en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Las Partes podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 4 – Atentados contra la integridad de los datos

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero ocasione daños que puedan calificarse de graves.

Artículo 5 – Atentados contra la integridad del sistema

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6 – Abuso de equipos e instrumentos técnicos ⁽⁴⁾

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a. la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición:

i. de un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los artículos 2 a 5 arriba citados;

ii. de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5; y

b. la posesión de alguno de los elementos descritos en los párrafos (a) (1) o (2) con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2-5. Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad penal ⁽⁵⁾.

2. Lo dispuesto en el presente artículo no generará responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión u otras formas de puesta a disposición mencionadas en el párrafo 1 no persigan la comisión de una infracción prevista en los artículos 2 a 5 del presente Convenio, como en el caso de ensayos autorizados o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho de no aplicar el párrafo 1, a condición de que dicha reserva no recaiga sobre la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el párrafo 1 (a)(2).

Título 2 – Infracciones informáticas

Artículo 7 – Falsedad informática

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles. Las Partes podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal.

Artículo 8 – Estafa informática

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de:

- a. la introducción, alteración, borrado o supresión de datos informáticos,
- b. cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.

Título 3 – Infracciones relativas al contenido

Artículo 9 – Infracciones relativas a la pornografía infantil

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

- a. la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;
- b. el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático;
- c. la difusión o la transmisión de pornografía infantil a través de un sistema informático;
- d. el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático;
- e. la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 arriba descrito, la «pornografía infantil» comprende cualquier material pornográfico que represente de manera visual:

- a. un menor adoptando un comportamiento sexualmente explícito;
- b. una persona que aparece como un menor adoptando un comportamiento sexualmente explícito ⁽⁶⁾;
- c. unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito ⁽⁷⁾.

3. A los efectos del párrafo 2 arriba descrito, el término «menor» designa cualquier persona menor de 18 años. Las Partes podrán exigir un límite de edad inferior, que debe ser como mínimo de 16 años.

4. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, los párrafos 1 (d) y 1 (e) y 2 (b) y 2 (c).

Título 4 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

Artículo 10 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a la propiedad intelectual definida por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Universal sobre los Derechos de Autor, revisada en París el 24 de julio de 1971, del Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a los derechos afines definidos por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, hecha en Roma (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre interpretación o ejecución y fonogramas, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

3. Las Partes podrán, de concurrir determinadas circunstancias, reservarse el derecho de no imponer responsabilidad penal en aplicación de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos eficaces para su represión y que dicha reserva no comporte infracción de las obligaciones internacionales que incumban al Estado por aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Título 5 – Otras formas de responsabilidad y sanción

Artículo 11 – Tentativa y complicidad

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, cualquier acto de complicidad que sea cometido dolosamente y con la intención de favorecer la perpetración de alguna de las infracciones establecidas en los artículos 2 a 10 del presente Convenio.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la tentativa dolosa de cometer una de las infracciones establecidas en los artículos 3 a 5, 7, 8, 9 (1) a y 9 (1) c del presente Convenio.

3. Las Partes podrán reservarse el derecho de no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

Artículo 12 – Responsabilidad de las personas jurídicas

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las personas jurídicas puedan ser tenidas por responsables de las infracciones establecidas en el presente Convenio, cuando éstas sean cometidas por una persona física, actuando ya sea a título individual, ya sea como miembro de un órgano de la persona jurídica, que ejerce un poder de dirección en su seno, cuyo origen se encuentre en:

- a. un poder de representación de la persona jurídica;
- b. una autorización para tomar decisiones en nombre de la persona jurídica;
- c. una autorización para ejercer control en el seno de la persona jurídica.

2. Fuera de los casos previstos en el párrafo 1, las Partes adoptarán las medidas necesarias para asegurar que una persona jurídica puede ser tenida por responsable cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de las infracciones descritas en el párrafo 1 a través de una persona física que actúa bajo autorización de la persona jurídica.

3. La responsabilidad de la persona jurídica podrá resolverse en sede penal, civil o administrativa, dependiendo de los principios jurídicos propios del Estado.

4. Esta responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido la infracción.

Artículo 13 – Sanciones y medidas

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las infracciones penales establecidas en los artículos 2 a 11 sean castigadas con sanciones efectivas, proporcionadas y disuasorias, incluidas las penas privativas de libertad.

2. Las Partes velarán para que las personas jurídicas que hayan sido declaradas responsables según lo dispuesto en el artículo 12 sean objeto de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas las sanciones pecuniarias.

Sección 2 – Derecho procesal

Título 1 – Disposiciones comunes

Artículo 14 – Ámbito de aplicación de las medidas de derecho procesal

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para instaurar los poderes y procedimientos previstos en la presente sección a los efectos de investigación o de procedimientos penales específicos.

2. Salvo disposición en contrario, prevista en el artículo 21, las Partes podrán aplicar los poderes y procedimientos mencionados en el párrafo 1:

- a. a las infracciones penales establecidas en los artículos 2 a 11 del presente Convenio;
- b. a cualquier otra infracción penal cometida a través de un sistema informático; y
- c. a la recogida de pruebas electrónicas de cualquier infracción penal.

3. a. Las Partes podrán reservarse el derecho de aplicar la medida mencionada en el artículo 20 a las infracciones especificadas en sus reservas, siempre que el número de dichas infracciones no supere el de aquellas a las que se aplica la medida mencionada en el artículo 21. Las Partes tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de la medida mencionada en el artículo 20.

b. Cuando un Estado, en razón de las restricciones impuestas por su legislación vigente en el momento de la adopción del presente Convenio, no esté en condiciones de aplicar las medidas descritas en los artículos 20 y 21 a las comunicaciones transmitidas en un sistema informático de un prestador de servicios que

- i. es utilizado en beneficio de un grupo de usuarios cerrado, y
- ii. no emplea las redes públicas de telecomunicación y no está conectado a otro sistema informático, público o privado, ese Estado podrá reservarse el derecho de no aplicar dichas medidas a tales comunicaciones. Los Estados tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de las medidas mencionadas en los artículos 20 y 21.

Artículo 15 – Condiciones y garantías

1. Las Partes velarán para que la instauración, puesta en funcionamiento y aplicación de los poderes y procedimientos previstos en la presente sección se sometan a las condiciones y garantías dispuestas en su derecho interno, que debe asegurar una protección adecuada de los derechos del hombre y de las libertades y, en particular, de los derechos derivados de las obligaciones que haya asumido en aplicación del Convenio para la protección de los derechos humanos y libertades fundamentales del Consejo de Europa (1950) y del Pacto internacional de derechos civiles y políticos de Naciones Unidas (1966) o de otros instrumentos internacionales relativos a los derechos del hombre, y que debe integrar el principio de proporcionalidad.

2. Cuando ello sea posible, en atención a la naturaleza del poder o del procedimiento de que se trate, dichas condiciones y garantías incluirán, entre otras, la supervisión judicial u otras formas de supervisión independiente, la

motivación justificante de la aplicación, la limitación del ámbito de aplicación y la duración del poder o del procedimiento en cuestión.

3. Las Partes examinarán la repercusión de los poderes y procedimientos de esta Sección sobre los derechos, responsabilidades e intereses legítimos de terceros, como exigencia dimanante del interés público y, en particular, de una correcta administración de justicia.

Título 2 – Conservación inmediata de datos informáticos almacenados

Artículo 16 – Conservación inmediata de datos informáticos almacenados

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación inmediata de datos electrónicos especificados, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para pensar que son particularmente susceptibles de pérdida o de modificación.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a una persona a conservar y proteger la integridad de los datos – que se encuentran en su poder o bajo su control y respecto de los cuales exista un mandato previo de conservación en aplicación del párrafo precedente – durante el tiempo necesario, hasta un máximo de 90 días, para permitir a las autoridades competentes obtener su comunicación. Los Estados podrán prever que dicho mandato sea renovado posteriormente.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar al responsable de los datos o a otra persona encargada de conservarlos a mantener en secreto la puesta en ejecución de dichos procedimientos durante el tiempo previsto por su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Artículo 17 – Conservación y divulgación inmediata de los datos de tráfico

1. A fin de asegurar la conservación de los datos de tráfico, en aplicación del artículo 16, las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para:

a. procurar la conservación inmediata de los datos de tráfico, cuando uno o más prestadores de servicio hayan participado en la transmisión de dicha comunicación; y

b. asegurar la comunicación inmediata a la autoridad competente del Estado, o a una persona designada por dicha autoridad, de datos de tráfico suficientes para permitir la identificación de los prestadores de servicio y de la vía por la que la comunicación se ha transmitido.

2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Título 3 – Mandato de comunicación

Artículo 18 – Mandato de comunicación

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar:

a. a una persona presente en su territorio que comunique los datos informáticos especificados, en posesión o bajo el control de dicha persona, y almacenados en un sistema informático o en un soporte de almacenaje informático; y

b. a un prestador de servicios que ofrezca sus prestaciones en el territorio del Estado firmante, que comunique los datos en su poder o bajo su control relativos a los abonados y que conciernan a tales servicios;

2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

3. A los efectos del presente artículo, la expresión «datos relativos a los abonados» designa cualquier información, expresada en datos informáticos o de cualquier otro modo, poseída por un prestador de servicio y que se refiere a los abonados de sus servicios, así como a los datos de tráfico o relativos al contenido, y que permite establecer:

a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el tiempo del servicio;

b. la identidad, la dirección postal o geográfica y el número de teléfono del abonado o cualquier otro número de acceso, los datos relativos a la facturación y el pago, disponibles por razón de un contrato o de un alquiler de servicio;

c. cualquier otra información relativa al lugar donde se ubican los equipos de comunicación, disponible por razón de un contrato o de un alquiler de servicio.

Título 4 – Registro y decomiso de datos informáticos almacenados

Artículo 19 – Registro y decomiso de datos informáticos almacenados

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para registrar o acceder de un modo similar:

a. a un sistema informático o a una parte del mismo, así como a los datos informáticos que están almacenados; y

b. a un soporte de almacenamiento que permita contener datos informáticos en su territorio.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para procurar que, cuando sus autoridades registren o accedan de un modo similar a un sistema informático específico o a una parte del mismo, conforme al párrafo 1 (a), y tengan motivos para creer que los datos buscados

se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son igualmente accesibles a partir del sistema inicial o están disponibles a través de ese primer sistema, dichas autoridades estén en condiciones de ampliar inmediatamente el registro o el acceso y extenderlo al otro sistema.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para decomisar u obtener de un modo similar los datos informáticos cuyo acceso haya sido realizado en aplicación de los párrafos 1 o 2. Estas medidas incluyen las prerrogativas siguientes:

- a. decomisar u obtener de un modo similar un sistema informático o una parte del mismo o un soporte de almacenaje informático;
- b. realizar y conservar una copia de esos datos informáticos;
- c. preservar la integridad de los datos informáticos almacenados pertinentes; y
- d. hacer inaccesibles o retirar los datos informáticos del sistema informático consultado.

4. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar a cualquier persona, que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione todas las informaciones razonablemente necesarias, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2.

5. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Título 5 – Recogida en tiempo real de datos informáticos

Artículo 20 – Recogida en tiempo real de datos informáticos

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para:

- a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio;
- b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a
 - i. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o
 - ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos de tráfico asociados a

comunicaciones específicas transmitidas en su territorio a través de un sistema informático.

2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Artículo 21 – Interceptación de datos relativos al contenido

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes respecto a infracciones consideradas graves conforme a su derecho interno para:

a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio; y

b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a

i. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar,

en tiempo real, los datos relativos al contenido de concretas comunicaciones en su territorio, transmitidas a través de un sistema informático.

2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos relativos al contenido de concretas comunicaciones transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Sección 3 – Competencia

Artículo 22 – Competencia

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para atribuirse la competencia respecto a cualquier infracción penal establecida en los artículos 2 a 11 del presente Convenio, cuando la infracción se haya cometido:

- a. en su territorio;
- b. a bordo de una nave que ondee pabellón de ese Estado;
- c. a bordo de una aeronave inmatriculada en ese Estado;
- d. por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado.

2. Las Partes podrán reservarse el derecho de no aplicar, o de aplicar sólo en ciertos casos o condiciones específicas, las reglas de competencia definidas en los párrafos 1b a 1d del presente artículo o en cualquiera de las partes de esos párrafos.

3. Las Partes adoptarán las medidas que se estimen necesarias para atribuirse la competencia respecto de cualquier infracción mencionada en el artículo 24, párrafo 1 del presente Convenio, cuando el presunto autor de la misma se halle en su territorio y no pueda ser extraditado a otro Estado por razón de la nacionalidad, después de una demanda de extradición.

4. El presente Convenio no excluye ninguna competencia penal ejercida por un Estado conforme a su derecho interno.

5. Cuando varios Estados reivindiquen una competencia respecto a una infracción descrita en el presente Convenio, los Estados implicados se reunirán, cuando ello sea oportuno, a fin de decidir cuál de ellos está en mejores condiciones para ejercer la persecución.

Capítulo III – Cooperación internacional

Sección 1 – Principios generales

Título 1 – Principios generales relativos a la cooperación internacional

Artículo 23 – Principios generales relativos a la cooperación internacional

Las Partes cooperarán con arreglo a lo dispuesto en el presente capítulo, aplicando para ello los instrumentos internacionales relativos a la cooperación internacional en materia penal, acuerdos basados en la legislación uniforme o recíproca y en su propio derecho nacional, de la forma más amplia posible, con la finalidad de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o para recoger pruebas electrónicas de una infracción penal.

Título 2 – Principios relativos a la extradición

Artículo 24 – Extradición

1. a. El presente artículo se aplicará a la extradición por alguna de las infracciones definidas en los artículos 2 a 11 del presente Convenio, siempre que éstas resulten punibles por la legislación de los dos Estados implicados y tengan prevista una pena privativa de libertad de una duración mínima de un año.

b. Aquellos Estados que tengan prevista una pena mínima distinta, derivada de un tratado de extradición aplicable a dos o más Estados, comprendido en la Convención Europea de Extradición (STE nº 24), o de un acuerdo basado en la legislación uniforme o recíproca, aplicarán la pena mínima prevista en esos tratados o acuerdos.

2. Las infracciones penales previstas en el apartado 1 del presente artículo podrán dar lugar a extradición si entre los dos Estados existe un tratado de extradición. Las Partes se comprometerán a incluirlas como tales infracciones susceptibles de dar lugar a extradición en todos los tratados de extradición que puedan suscribir.

3. Si un Estado condiciona la extradición a la existencia de un tratado y recibe una demanda de extradición de otro Estado con el que no ha suscrito tratado alguno de extradición, podrá considerar el presente Convenio fundamento jurídico suficiente para conceder la extradición por alguna de las infracciones penales previstas en el párrafo 1 del presente artículo.

4. Las Partes que no condicionen la extradición a la existencia de un tratado podrán llevar a cabo la extradición siempre que prevean como infracciones las previstas en el párrafo 1 del presente artículo.

5. La extradición quedará sometida a las condiciones establecidas en el derecho interno del Estado requerido o en los tratados de extradición vigentes, quedando asimismo sometidos a estos instrumentos jurídicos los motivos por los que el país requerido puede denegar la extradición.

6. Si es denegada la extradición por una infracción comprendida en el párrafo 1 del presente artículo, alegando la nacionalidad de la persona reclamada o la competencia para juzgar la infracción del Estado requerido, éste deberá someter el asunto – la demanda del Estado requirente —a sus autoridades competentes a fin de que éstas establezcan la competencia para perseguir el hecho e informen de la conclusión alcanzada al Estado requirente. Las autoridades en cuestión deberán adoptar la decisión y sustanciar el procedimiento del mismo modo que para el resto de infracciones de naturaleza semejante previstas en la legislación de ese Estado.

7. a. Las Partes deberán comunicar al Secretario General del Consejo de Europa, en el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de las autoridades responsables del envío y de la recepción de una demanda de extradición o de arresto provisional, en caso de ausencia de tratado.

b. El Secretario General del Consejo de Europa creará y actualizará un registro de autoridades designadas por las Partes. Las Partes deberán garantizar la exactitud de los datos obrantes en el registro

Título 3 – Principios generales relativos a la colaboración ⁽⁸⁾

Artículo 25 – Principios generales relativos a la colaboración

1. Las Partes acordarán llevar a cabo una colaboración mutua lo más amplia posible al objeto de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o al de recoger pruebas electrónicas de una infracción penal.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que estimen necesarias para dar cumplimiento a las obligaciones establecidas en los artículos 27 a 35.

3. Las Partes podrán, en caso de emergencia, formular una demanda de colaboración, a través de un medio de comunicación rápido, como el fax o el correo electrónico, procurando que esos medios ofrezcan las condiciones suficientes de seguridad y de autenticidad (encriptándose si fuera necesario) y con confirmación posterior de la misma si el Estado requerido lo exigiera. Si el Estado requerido lo acepta podrá responder por cualquiera de los medios rápidos de comunicación indicados.

4. Salvo disposición en contrario expresamente prevista en el presente capítulo, la colaboración estará sometida a las condiciones fijadas en el derecho interno del Estado requerido o en los tratados de colaboración aplicables y comprenderá los motivos por los que el Estado requerido puede negarse a colaborar. El Estado requerido no podrá ejercer su derecho a rehusar la colaboración en relación a las infracciones previstas en los artículos 2 a 11, alegando que la demanda se solicita respecto a una infracción que, según su criterio, tiene la consideración de fiscal.

5. Conforme a lo dispuesto en el presente capítulo, el Estado requerido estará autorizado a supeditar la colaboración a la exigencia de doble incriminación. Esa condición se entenderá cumplida si el comportamiento constitutivo de la infracción - en relación a la que se solicita la colaboración — se encuentra previsto en su derecho interno como infracción penal, resultando indiferente que éste no la encuadre en la misma categoría o que no la designe con la misma terminología.

Artículo 26 – Información espontánea

1. Las Partes podrán, dentro de los límites de su derecho interno y en ausencia de demanda previa, comunicar a otro Estado las informaciones obtenidas en el marco de investigaciones que puedan ayudar a la Parte destinataria a iniciar o a

concluir satisfactoriamente las investigaciones o procedimientos relativos a las infracciones dispuestas en el presente Convenio, o a que dicha parte presente una demanda de las previstas en el presente capítulo.

2. Antes de comunicar dicha información, ese Estado podrá solicitar que la información sea tratada de forma confidencial o que sea utilizada sólo en ciertas circunstancias. Si el Estado destinatario no pudiera acatar las condiciones impuestas, deberá informar al otro Estado, quien habrá de decidir si proporciona o no la información. Una vez aceptadas estas condiciones por el Estado destinatario, éste quedará obligado a su cumplimiento.

Título 4 – Procedimientos relativos a las demandas de asistencia en ausencia de acuerdo internacional aplicable

Artículo 27 – Procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional aplicable

1. En ausencia de tratado o acuerdo en vigor de asistencia basado en la legislación uniforme o recíproca, serán aplicables los apartados 2 al 9 del presente artículo. Éstos no se aplicarán cuando exista un tratado, acuerdo o legislación sobre el particular, sin perjuicio de que las partes implicadas puedan decidir someterse, en todo o parte, a lo dispuesto en este artículo.

2. a. Las Partes designarán una o varias autoridades centrales encargadas de tramitar las demandas de colaboración, de ejecutarlas o de transferirlas a las autoridades competentes para que éstas las ejecuten.

b. Las autoridades centrales se comunicarán directamente las unas con las otras.

c. Las Partes, en el momento de la firma o del depósito de sus instrumentos de ratificación, aceptación, de aprobación o de adhesión, comunicarán al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en aplicación del presente párrafo.

d. El Secretario General del Consejo de Europa creará y actualizará un registro de autoridades designadas por las partes. Las Partes deberán garantizar la exactitud de los datos obrantes en el registro.

3. Las demandas de asistencia basadas en el presente artículo serán ejecutadas conforme al procedimiento especificado por el Estado requirente, siempre que resulte compatible con la legislación del Estado requerido.

4. Al margen de los motivos previstos en el artículo 15 párrafo 4 para denegar la asistencia, ésta podrá ser rechazada por el Estado requerido:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que, de acceder a la colaboración, se pondría en peligro su soberanía, seguridad, orden público o otro interés esencial.

5. El Estado requerido podrá aplazar la ejecución de la demanda cuando ésta pueda perjudicar investigaciones o procedimientos en curso llevados a cabo por las autoridades nacionales.

6. Antes de denegar o retrasar la asistencia, el Estado requerido deberá examinar, tras consultar al Estado requirente, si es posible hacer frente a la demanda de forma parcial o si es posible establecer las reservas que estime necesarias.

7. El Estado requerido informará inmediatamente al Estado requirente del curso que pretende dar a la demanda de asistencia. De denegar o retrasar la tramitación de la demanda, el Estado requerido hará constar los motivos. Asimismo, dicho Estado deberá informar al Estado requirente sobre los motivos que hacen imposible, de ser así, la ejecución de la demanda o que retrasan sustancialmente su ejecución.

8. El Estado requirente podrá solicitar que el Estado requerido mantenga en secreto la propia existencia y objeto de la demanda interpuesta al amparo de este capítulo, salvo en aquellos aspectos necesarios para la ejecución de la misma. Si el Estado requirente no pudiera hacer frente a la petición de confidencialidad, éste deberá informar inmediatamente al otro Estado, quien decidirá si la demanda, pese a ello, debe ser ejecutada.

9. a. En caso de urgencia, las autoridades judiciales del Estado requirente podrán dirigir directamente a las autoridades homólogas del Estado requerido las demandas de asistencia y las comunicaciones. En tales casos, se remitirá simultáneamente una copia a las autoridades del Estado requerido con el visado de la autoridad central del Estado requirente.

b. Todas las demandas o comunicaciones formuladas al amparo del presente párrafo podrán ser tramitadas a través de la Organización Internacional de la Policía Criminal (INTERPOL).

c. Cuando una demanda haya sido formulada al amparo de la letra (a) del presente artículo, y la autoridad que le dio curso no sea la competente para ello, deberá transferir la demanda a la autoridad nacional competente y ésta informará directamente al Estado requerido.

d. Las demandas o comunicaciones realizadas al amparo del presente párrafo que no supongan la adopción de medidas coercitivas podrán ser tramitadas directamente por las autoridades del Estado requirente y las del Estado requerido.

e. Las Partes podrán informar al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que, por motivos de eficacia, las demandas formuladas al amparo del presente párrafo deberán dirigirse directamente a su autoridad central.

Artículo 28 – Confidencialidad y restricciones de uso

1. En ausencia de tratado o acuerdo en vigor de asistencia basados en la legislación uniforme o recíproca, será aplicable lo dispuesto en el presente

artículo. Éste no se aplicará cuando exista un tratado, acuerdo o legislación sobre el particular, sin perjuicio de que las partes implicadas puedan decidir someterse, en todo o parte, a lo dispuesto en este artículo.

2. El Estado requerido podrá supeditar la comunicación de la información o del material requerido en la demanda al cumplimiento de las siguientes condiciones:

a. que se mantenga la confidencialidad sobre las mismas, siempre que la demanda corra el riesgo fracasar en ausencia de dicha condición; o

b. que éstas no sean utilizadas en investigaciones o procedimientos diversos a los establecidos en la demanda.

3. Si el Estado requirente no pudiera satisfacer alguna de las condiciones establecidas en el apartado 2 del presente artículo, la otra parte informará al Estado requerido, el cual decidirá si la información debe ser proporcionada. Si el Estado requirente acepta esta condición, dicho Estado estará obligado por la misma.

4. Todo Estado parte que aporte información o material supeditado a alguna de la condiciones previstas en el apartado 2, podrá exigir de la otra parte la concreción de las condiciones de uso de la información o del material.

Sección 2 – Disposiciones específicas

Título 1 – Cooperación en materia de medidas cautelares

Artículo 29 – Conservación inmediata datos informáticos almacenados

1. Las Partes podrán ordenar o imponer de otro modo la conservación inmediata de datos almacenados en sistemas informáticos que se encuentren en su territorio, en relación a los cuales el Estado requirente tiene intención de presentar una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos.

2. Una demanda de conservación formulada en aplicación del párrafo 1 deberá contener:

a. la identificación de la autoridad que solicita la conservación;

b. la infracción objeto de investigación con una breve exposición de los hechos vinculados a la misma;

c. los datos informáticos almacenados que deben conservarse y su vinculación con la infracción;

d. todas aquellas informaciones disponibles que permitan identificar al responsable de los datos informáticos almacenados o el emplazamiento de los sistemas informáticos;

e. justificación de la necesidad de conservación; y

f. la acreditación de que el Estado requirente está dispuesto a formular una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos.

3. Después de recibir la demanda, el Estado requerido deberá adoptar las medidas necesarias para proceder sin dilaciones a la conservación de los datos solicitados, conforme a su derecho interno. Para hacer efectiva la demanda de conservación no resultará condición indispensable la doble incriminación.

4. Si un Estado exige la doble incriminación como condición para atender a una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos, por infracciones diversas a las establecidas en los artículos 2 a 11 del presente Convenio, podrá negarse a la demanda de conservación, al amparo del presente artículo, si tiene fundadas sospechas de que, en el momento de la comunicación de los datos, el otro Estado no cumplirá la exigencia de la doble incriminación.

5. Al margen de lo anterior, una demanda de conservación únicamente podrá ser denegada:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que de acceder a la demanda se pondría en peligro su soberanía, su seguridad, orden público o otro interés esencial.

6. Cuando el Estado requerido considere que la simple conservación no será suficiente para garantizar la disponibilidad futura de los datos informáticos o que ésta podría comprometer la confidencialidad de la investigación o podría hacerla fracasar de otro modo, deberá informar inmediatamente al Estado requirente, quien decidirá la conveniencia de dar curso a la demanda.

7. Todas las conservaciones realizadas al amparo de una demanda de las previstas en el párrafo 1 serán válidas por un periodo máximo de 60 días, para permitir, en ese plazo de tiempo, al Estado requirente formular una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos. Después de la recepción de la demanda, los datos informáticos deberán mantenerse hasta que ésta se resuelva.

Artículo 30 – Comunicación inmediata de los datos informáticos conservados

1. Si, en ejecución de una demanda de conservación de datos de tráfico relativos a una concreta comunicación al amparo del artículo 29, el Estado requerido descubriera que un prestador de servicios de otro Estado ha participado en la transmisión de la comunicación, comunicará inmediatamente al Estado requirente los datos informáticos de tráfico, con el fin de que éste identifique al prestador de servicios y la vía por la que la comunicación ha sido realizada.

2. La comunicación de datos informáticos de tráfico prevista en el párrafo 1 únicamente podrá ser denegada:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que de acceder a la demanda se pondría en peligro su soberanía, su seguridad, orden público o otro interés esencial.

Título 2 – Asistencia en relación a los poderes de investigación

Artículo 31 – Asistencia concerniente al acceso a datos informáticos almacenados

1. Cualquier Estado podrá solicitar a otro el registro o acceso de otro modo, el decomiso u obtención por otro medio, o la comunicación de datos almacenados en un sistema informático que se encuentre en su territorio, incluidos los datos conservados conforme a lo dispuesto en el artículo 29.

2. El Estado requerido dará satisfacción a la demanda aplicando los instrumentos internacionales, convenios y la legislación mencionada en el artículo 23 siempre que no entre en contradicción con lo dispuesto en el presente capítulo.

3. La demanda deberá ser satisfecha lo más rápidamente posible en los siguientes casos:

a. cuando existan motivos para sospechar que los datos solicitados son particularmente vulnerables por existir riesgo de pérdida o modificación; o

b. cuando los instrumentos, convenios o legislación referida en el párrafo 2 prevean una cooperación rápida.

Artículo 32 – Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso

Cualquier Estado podrá sin autorización de otro:

a. acceder a los datos informáticos almacenados de libre acceso al público (fuentes abiertas), independientemente de la localización geográfica de esos datos; o

b. acceder a, o recibir a través de un sistema informático situado en su territorio, los datos informáticos almacenados situados en otro Estado, si se obtiene el consentimiento legal y voluntario de la persona autorizada para divulgarlos a través de ese sistema informático.

Artículo 33 – Asistencia para la recogida en tiempo real de datos de tráfico

1. Las Partes podrán acordar colaborar en la recogida, en tiempo real, de datos de tráfico, asociados a concretas comunicaciones llevadas a cabo en sus territorios, a través un sistema informático. Dicha colaboración se someterá a las condiciones y procedimientos previstos en el derecho interno, salvo que alguna de las partes se acoja a la reserva prevista en el párrafo 2.

2. Las Partes deberán acordar colaborar respecto a aquellas infracciones penales para las cuales la recogida en tiempo real de datos de tráfico se encuentra prevista en su derecho interno en situaciones análogas.

Artículo 34 – Asistencia en materia de interceptación de datos relativos al contenido

Las Partes podrán acordar colaborar, en la medida en que se encuentre previsto por tratados o leyes internas, en la recogida y registro, en tiempo real, de datos relativos al contenido de concretas comunicaciones realizadas a través de sistemas informáticos.

Título 3 – Red 24/7

Artículo 35 – Red 24/7

1. Las Partes designarán un punto de contacto localizable las 24 horas del día, y los siete días de la semana, con el fin de asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recogida de pruebas electrónicas de una infracción penal. Esta asistencia comprenderá, si lo permite el derecho y la práctica interna, facilitar la aplicación directa de las siguientes medidas:

- a. aportación de consejos técnicos;
- b. conservación de datos según lo dispuesto en los artículos 29 y 30; y
- c. recogida de pruebas, aportación de información de carácter jurídico y localización de sospechosos.

2. a. Un mismo punto de contacto podrá ser coincidente para dos Estados, siguiendo para ello un procedimiento acelerado.

b. Si el punto de contacto designado por un Estado no depende de su autoridad o autoridades responsables de la colaboración internacional o de la extradición, deberá velarse para que ambas autoridades actúen coordinadamente mediante la adopción de un procedimiento acelerado.

3. Las Partes dispondrán de personal formado y dotado a fin de facilitar el funcionamiento de la red.

Capítulo IV – Cláusulas finales

Artículo 36 – Firma y entrada en vigor

1. El presente Convenio está abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.

2. El presente Convenio está sometido a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación deberán ser entregados al Secretario General del Consejo de Europa.

3. El presente Convenio entrará en vigor el primer día del mes transcurridos tres meses desde que cinco Estados, de los cuales al menos tres deberán ser miembros del Consejo de Europa, presten su consentimiento a vincularse al Convenio, conforme a lo dispuesto en los párrafos 1 y 2.

4. Para todos los Estados que hayan prestado su consentimiento a vincularse al Convenio, éste entrará en vigor el primer día del mes transcurridos tres meses desde que hayan expresado su consentimiento, conforme a lo dispuesto en los párrafos 1 y 2.

Artículo 37 – Adhesión al Convenio

1. Después de entrar en vigor el presente Convenio, el Comité de Ministros del Consejo de Europa podrá, tras consultar a las Partes del Convenio y habiendo obtenido el asentimiento unánime de los mismos, invitar a todos los Estados no miembros del Consejo de Europa que no hayan participado en la elaboración del mismo a adherirse al Convenio. Esta decisión deberá tomarse mediante la mayoría prevista en el artículo 20.d del Estatuto del Consejo de Europa y el asentimiento unánime de los Estados Partes que tengan derecho a formar parte del Comité de Ministros.

2. Para todos aquellos Estados que se adhieran al Convenio conforme a lo previsto en el párrafo precedente, el Convenio entrará en vigor el primer día del mes transcurridos tres meses después del depósito del instrumento de adhesión ante el Secretario General del Consejo de Europa.

Artículo 38 – Aplicación territorial

1. Las Partes podrán, en el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, designar el territorio al que resultará aplicable el presente Convenio.

2. Las Partes podrán, en cualquier momento, a través de una declaración dirigida al Secretario General del Consejo de Europa, extender la aplicación del presente Convenio a otros territorios diversos a los designados en la declaración. En tal caso, el Convenio entrará en vigor en dichos territorios el primer día del mes transcurridos tres meses desde la recepción de la declaración por el Secretario General.

3. Toda declaración realizada al amparo de los párrafos precedentes podrá ser retirada, en lo que concierne al territorio designado en la citada declaración, a través de una notificación dirigida al Secretario General del Consejo de Europa. El retracto surtirá efecto el primer día del mes transcurridos tres meses desde la recepción de la notificación por el Secretario General.

Artículo 39 – Efectos del Convenio

1. El objeto del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales existentes entre las partes, y comprende las disposiciones:

- del Convenio Europeo de extradición abierto a la firma el 13 de diciembre de 1957 en París (STE nº 24)
- del Convenio Europeo de Cooperación judicial en materia penal abierto a la firma el 20 de abril de 1959 en Estrasburgo (STE nº 30),
- del Protocolo Adicional del Convenio Europeo de Cooperación judicial en materia penal abierto a la firma el 17 de marzo de 1978 en Estrasburgo (STE nº 99).

2. Si dos o más Estados han concluido un acuerdo o un tratado relativo a la materia objeto de este Convenio o si han establecido de otro modo la relación entre ellos, o si lo hacen en el futuro, dispondrán igualmente de la facultad de aplicar el citado acuerdo o de establecer sus relaciones con base en el mismo, en lugar del presente Convenio. Siempre que los Estados hayan establecido sus relaciones concernientes a la materia objeto del presente Convenio de forma diversa, éstas deberán llevarse a cabo de forma compatible con los objetivos y principios del Convenio.

3. Lo dispuesto en el presente Convenio no afectará a otros derechos, restricciones, obligaciones y responsabilidades de los Estados.

Artículo 40 – Declaraciones

A través de una declaración escrita dirigida al Secretario General del Consejo de Europa, las Partes podrán, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, declarar que se reservan el derecho a exigir, llegado el caso, uno o varios elementos suplementarios de los dispuestos en los artículos 2, 3, 6 del párrafo 1 (b), 7, 9 párrafo 3 y 27 del párrafo 9 (e).

Artículo 41 – Cláusula federal

1. Un Estado federal podrá reservarse el derecho de desempeñar sus obligaciones, en los términos previstos en el capítulo II del presente Convenio, en la medida en que éstas sean compatibles con los principios que presiden las relaciones entre el gobierno central y los Estados federados u otros territorios análogos, siempre que se garantice la cooperación en los términos previstos en el capítulo III.

2. Un Estado federal no podrá hacer uso de la reserva adoptada según lo dispuesto en el párrafo 1 para excluir o disminuir de forma substancial las obligaciones contraídas en virtud del capítulo II. En todo caso, el Estado federal deberá dotarse de los medios necesarios para dar cumplimiento a las medidas previstas en el citado capítulo.

3. En todo lo que concierne a las disposiciones de este Convenio cuya aplicación dimana de la competencia de cada uno de los Estados federados u otras entidades territoriales análogas, que no están, en virtud del sistema constitucional de la federación, obligados a adoptar medidas legislativas, el gobierno central pondrá, con la aprobación de éstos, en conocimiento de las autoridades competentes de los Estados federados la necesidad de adoptar las citadas medidas animándolos a que las ejecuten.

Artículo 42 – Reservas

Los Estados podrán, a través de una notificación escrita dirigida al Secretario del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o de adhesión, declarar que invocan la reserva o reservas previstas en el art. 4, párrafo 2, artículo 6, párrafo 3, artículo 9, párrafo 4, artículo 10, párrafo 3, artículo 11, párrafo 3, artículo 14, párrafo 3, artículo 22, párrafo 2, artículo 29, párrafo 4 y en el artículo 41, párrafo 1. No podrá realizarse ninguna otra reserva diversa a las indicadas.

Artículo 43 – Mantenimiento y retirada de las reservas

1. El Estado que haya formulado una reserva conforme a lo dispuesto en el artículo 42 podrá retirarla total o parcialmente notificando tal extremo al Secretario General. La retirada se hará efectiva en la fecha de recepción por el Secretario General de la notificación. Si en la notificación se hiciera constar que la reserva deberá tener efecto en una determinada fecha, ello se hará efectivo siempre que sea posterior a la recepción por el Secretario General de la notificación.

2. El Estado que haya formulado una reserva conforme a lo dispuesto en el artículo 42, podrá retirarla total o parcialmente siempre que lo permitan las circunstancias.

3. El Secretario General del Consejo de Europa podrá solicitar periódicamente a los Estados, que hayan formulado una o varias reservas conforme a lo dispuesto en el artículo 42, información sobre la posibilidad de su retirada.

Artículo 44 – Enmiendas

1. Las enmiendas al presente Convenio podrán ser propuestas por las Partes, y deberán ser comunicadas al Secretario General del Consejo de Europa, a los Estados miembros del Consejo de Europa, a los Estados no miembros del Consejo de Europa que hayan tomado parte en la elaboración del Convenio así como a los Estados que se hayan adherido o que hayan sido invitados a adherirse conforme a lo dispuesto en el artículo 37.

2. Las enmiendas propuestas por uno de los Estados deberán ser comunicadas al Comité europeo para los problemas criminales (CDPC), quien deberá informar al Comité de Ministros sobre las mismas.

3. El Comité de Ministros examinará la enmienda propuesta y el informe del Comité europeo para los problemas criminales (CDPC) y, después de

consultar con los Estados no miembros y partes del Convenio, podrá adoptar la enmienda.

4. El texto de la enmienda adoptado por el Comité de Ministros, conforme a lo dispuesto en el párrafo 3 del presente artículo, deberá comunicarse a los Estados para su aceptación.

5. Las enmiendas adoptadas conforme al párrafo 3 del presente artículo entrarán en vigor el trigésimo día después del que los Estados hayan informado al Secretario General de su aceptación.

Artículo 45 – Reglamento de controversia

1. El Comité europeo para los problemas criminales (CDPC) está obligado a informar de la interpretación y aplicación del presente Convenio.

2. En caso de diferencias entre los Estados sobre la interpretación o aplicación del presente Convenio, los Estados intentarán adoptar un reglamento de diferencia a través de la negociación o de cualquier otro medio pacífico, con el compromiso de someter la controversia al Comité europeo para los problemas criminales, a un tribunal arbitral que tomará las decisiones que los Estados le sometan, o a la Corte internacional de justicia, a partir de un acuerdo adoptado por los Estados en litigio.

Artículo 46 – Reuniones de los Estados

1. Las Partes deberán reunirse periódicamente a fin de facilitar:

a. el uso y el efectivo cumplimiento del presente Convenio, la identificación de los problemas en esta materia, así como el efecto de las declaraciones o reservas formuladas conforme al presente Convenio;

b. el intercambio de información sobre novedades jurídicas, políticas o técnicas observadas en la criminalidad informática y recogida de pruebas electrónicas;

c. el examen sobre la posible reforma del Convenio.

2. El Comité europeo para los problemas criminales (CDPC) deberá estar al corriente de las reuniones llevadas a cabo al amparo del párrafo 1.

3. El Comité europeo para los problemas criminales (CDPC) deberá facilitar las reuniones previstas en el párrafo 1 y adoptar las medidas necesarias para ayudar a los Estados a completar o modificar el Convenio. No más tarde de tres años a contar desde la entrada en vigor del presente Convenio, el Comité europeo para los problemas criminales (CDPC) procederá, en cooperación con los Estados, a un examen conjunto de las disposiciones de la Convención y propondrá, en su caso, las modificaciones pertinentes.

4. Salvo que el Consejo de Europa los asuma, los gastos que ocasione la aplicación de las disposiciones del párrafo 1 deberán ser soportados por los Estados del modo que ellos mismos determinen.

Artículo 47 – Denuncia

1. Las Partes podrán, en cualquier momento, denunciar el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.
2. La denuncia entrará en vigor el primer día del mes transcurridos tres meses desde la recepción de la notificación por el Secretario General.

Artículo 48 – Notificación

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan tomado parte en la elaboración del presente Convenio, así como a cualquier Estado que se haya adherido o que haya sido invitado a adherirse:

- a. cualquier firma;
- b. el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;
- c. la fecha de entrada en vigor del presente Convenio según lo dispuesto en los artículos 36 y 37;
- d. cualquier declaración hecha por mor de los artículos 40 y 41 o cualquier reserva formulada en virtud del artículo 42;
- e. cualquier acto, notificación o comunicación referida al presente Convenio.

En vista de lo cual, los abajo firmantes, debidamente autorizados al efecto, han firmado el presente Convenio.

Hecho en Budapest, el 23 noviembre 2001, en francés y en inglés, ambos textos con el mismo valor, y en un solo ejemplar que será depositado en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copia certificada a cada uno de los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del Convenio y a cualquier Estado invitado a adherirse.

(1) El Convenio recoge, en la versión francesa, la expresión «fournisseur de services», cuya traducción literal sería la de «proveedor de servicios». En la presente traducción, se ha optado por emplear el término «prestador de servicios», en la línea seguida por la Directiva 2000/31 y el Proyecto de LSSI, como concepto o categoría omnicomprendiva que hace referencia a aquellos sujetos que desempeñan, profesionalmente, la actividad de prestación y gestión de accesos y servicios en Internet.

(2) También suele emplearse, para aludir a este tipo de datos, el término «datos de tránsito».

(3) El Convenio emplea el término «intentionnel». Sin embargo, en este caso, se ha preferido utilizar el vocablo «doloso» por corresponderse mejor con la categoría jurídico-penal propia del derecho español.

(4) El original en francés rubrica este ciberdelito como «Abus de dispositifs», lo que ha dado lugar a una traducción literal del mismo como «Abuso de dispositivos», expresión a la que, sin embargo, se ha preferido renunciar, por estimarse más precisa la empleada en texto.

(5) La interpretación de este último inciso suscita algunos interrogantes. De la literalidad del precepto podría deducirse que la referencia «elementos» debe circunscribirse a los propios mecanismos o instrumentos aludidos en el precepto. Sin embargo, también sería posible inferir que el término «elementos» alude a «ánimos» o «intenciones», de modo similar a lo exigido en relación a otros delitos. Esta ambigüedad es resuelta a favor de la primera de las interpretaciones indicadas, por el [Rapport explicatif](#) del Convenio, en su párrafo 75.

(6) Esta descripción se corresponde con la denominada «pornografía técnica».

(7) Esta descripción se corresponde con la denominada «simulada» o «pseudopornografía».

(8) El Convenio emplea el término «entraide», cuya traducción en español resulta multívoca. Entre las distintas acepciones que puede asumir el vocablo (ayuda mutua, asistencia, colaboración), se han utilizado, de modo indistinto, «asistencia» y «colaboración».

GLOSARIO

GLOSARIO

backdoor:

Puerta trasera. Permiten a un usuario remoto ingresar sin autorización a otros sistemas mediante la instalación de un programa de acceso considerado virus, esto permite realizar diversas acciones como revisar datos, borrar archivos, infectar con otro tipo de virus, tareas que generalmente no son percibidas por el sistema víctima.

bomba lógica:

es una pieza de código de programación agregada a un software de una aplicación o sistema operativo que permanece inactiva hasta que, transcurrido un cierto período de tiempo, o al ocurrir un determinado evento, se pone en acción.

Las bombas lógicas tienen generalmente intenciones maliciosas, actuando de la misma manera que un virus o troyano al activarse. De hecho, los virus que están programados para activarse a cierta hora se consideran bombas lógicas. Pueden realizar acciones tales como formatear un disco duro, alterar o borrar datos, cambiar la configuración del sistema, etc.

bounds checking:

En la programación informática, el control de fronteras (bounds chekings) es cualquier método de detectar si una variable esta dentro de algunos límites antes de su uso. Es especialmente relevante para una variable utilizada como un índice en un arreglo para asegurar su valor reside dentro de los límites de la matriz. Por ejemplo: un valor de 32768 a punto de ser asignado a una de dieciséis bits con signo variable (superior cuyos límites son -32768 a 32767), o acceder a elemento 25 en índice de un arreglo (array) con rango de 0 a 9 solamente. La primera es conocida también como serie de cheques, la segunda como índice de control.

buffer:

es un área de almacenamiento temporario, usualmente en la RAM. El propósito de casi todos los buffers es actuar como área de almacenamiento, permitiendo que el CPU manipule los datos antes de transferirlos a un dispositivo.

Dado que los procesos de leer y escribir datos a un disco son relativamente lentos, muchos programas mantienen la referencia de los cambios en los datos en un buffer y luego copian el buffer al disco. Por ejemplo, los procesadores de textos emplean un buffer para el seguimiento de los cambios en un documento. Entonces, cuando se guarda el archivo, el programa actualiza el archivo en disco con los contenidos del buffer. Esto es más eficiente que acceder al archivo en disco cada vez que se realiza un cambio en el mismo.

Nótese que como los cambios se almacenan inicialmente en un buffer, y no en el disco, todos ellos se perderán si la computadora falla durante la sesión de

edición. Por esto, es buena idea guardar periódicamente los archivos sobre los que se trabaja. La mayoría de los procesadores de textos guardan los archivos periódicamente a intervalos regulares de tiempo, que incluso pueden predefinirse en su configuración.

Los buffers suelen usarse también cuando se queman datos en CD-ROM. Los datos a copiar se transfieren al buffer antes de escribirse al disco.

Otro uso común de los buffers es para la impresión de documentos. Cuando se imprime un documento, el sistema operativo copia éste a un buffer de impresión (un área libre en memoria o disco), desde donde la impresora podrá leer e imprimir los caracteres con su propio ritmo. Esto libera la computadora para realizar otras tareas mientras la impresora funciona de fondo. Este proceso se conoce como *spooling*.

La mayoría de los drivers de teclado contienen un buffer de modo que se pueden editar los errores de tipeado antes de enviar el comando a un programa. Muchos sistemas operativos, incluyendo DOS, usan también un buffer de disco para guardar datos temporales que se leyeron del disco. El buffer de disco se conoce como caché.

buffer overflow:

buffer overflow o desbordamiento de buffer es un error de sistema causado por un defecto de programación, de tal forma que el programa que lo sufre pretende escribir más información en el buffer (unidad de memoria) de la que este puede alojar.

Este desbordamiento es posible porque el autor del programa no incluyó el código necesario para comprobar el tamaño y capacidad del buffer en relación con el volumen de datos que tiene que alojar.

Los problemas comienzan cuando el exceso de datos se escribe en otras posiciones de memoria, con la pérdida de los datos anteriores.

Si entre los datos perdidos por la sobrescritura se encuentran rutinas o procedimientos necesarios para el funcionamiento del programa que estamos ejecutando, el programa dará error.

Cuando la memoria de un programa llega a sobrescribir en forma aleatoria, el programa generalmente se colgará.

El problema para la seguridad nace cuando este desbordamiento de buffer es provocado intencionalmente por alguien mediante envío de datos que incluyen porciones de código, calculando la cantidad de datos para poder predeterminedir cual es el sobrante que se va a sobrescribir y donde. Provocado el desbordamiento, contienen una instrucción que apunta a una posición de memoria distinta, donde se encuentra el código ejecutable enviado por el atacante. El programa, inducido a funcionar anormalmente por la pérdida de datos causada por el desbordamiento, ejecutará el código enviado por el atacante.

El buffer overflow es un problema de código defectuoso, por lo tanto como usuarios nada podemos hacer para evitarlo (salvo que además de usuarios seamos expertos programadores, y dispongamos del código fuente de la aplicación que sufre el desbordamiento). En realidad el único remedio es estar informado de los programas que sufren estos problemas, y tener el software actualizado.

bug:

bicho, insecto. Error de programación que genera problemas en las operaciones de una computadora. Se habla de bug si es un error de diseño, pero no cuando la falla es provocada por otra cosa.

ciber:

prefijo utilizado ampliamente en la comunidad de Internet para denominar conceptos relacionados con las redes (cibercultura, ciberespacio, cibernauta, etc.).

Su origen es la palabra griega kibernao, que significa "pilotear una nave".

ciberpolicía:

funcionario policial especializado en Internet o en utilizar la red para sus investigaciones.

ciberacoso:

conducta amenazante o aproximaciones no deseadas dirigidas a otro usando el Internet y otras formas de comunicación "en línea".

código fuente:

Son las instrucciones de un programa en su forma original. La palabra fuente diferencia el código de varias otras formas posibles (por ej., código del objeto y código ejecutable).

Inicialmente, un programador escribe un programa en un lenguaje de programación en particular. Esto es, genera el programa fuente, o más genéricamente, el código fuente. Para ejecutar el programa, es necesario que el programador traduzca todo esto a lenguaje de máquina, para que lo entienda la computadora. El primer paso de esta traducción se logra con una utilidad denominada compilador. Éste, traduce el código fuente a una forma llamada código del objeto. Muchas veces, dicho código es el mismo que el código de máquina, pero otras debe traducirse a lenguaje de máquina usando otra utilidad, el ensamblador.

El código fuente es el único formato legible por humanos. Al adquirir un programa, normalmente los recibimos en su formato ejecutable, en código de máquina. Lo cual significa que pueden correrse directamente en la computadora, pero no pueden "leerse" ni modificarse. Algunos fabricantes o desarrolladores proveen además el código fuente, pero esto sólo le es útil a un programador avanzado que desee modificarlo o mejorarlo a su gusto.

comercio electrónico:

es la utilización de redes de datos (entre ellas principalmente Internet) para la realización de actividades comerciales entre empresas, consumidores finales y entidades de gobierno. Se trata de un área de negocios que crece a pasos agigantados y cada vez más perfeccionado y estandarizado.

computadora:

dispositivo, sistema, equipo de informática o aparato automático para el tratamiento de la información, que obedece a programas formados por sucesiones de operaciones aritméticas y lógicas. Una computadora comprende una parte física (hardware), constituida por circuitos electrónicos de alta integración, y una parte no física (software); el objetivo es realizar funciones lógicas, aritméticas, transmisión o de almacenamiento de datos, así como para el tratamiento sistemático de la información mediante el procesamiento automático de datos electrónicos o de cualquier otra tecnología. Esta definición incluye las redes públicas y privadas de computadoras.

contraseña:

palabra secreta que permite el acceso a servicios o información codificada a un cliente en particular.

correo electrónico:

es la transmisión de mensajes sobre redes de comunicaciones. Estos mensajes pueden consistir en textos escritos o archivos guardados en disco. Pueden enviarse también a múltiples destinatarios, lo que se denomina "broadcasting". Los mensajes enviados se almacenan en casillas de correo electrónico hasta que el receptor los revise. Una vez leídos pueden guardarse en el disco de la computadora, reenviarlos a otros usuarios, imprimirlos o simplemente eliminarlos. Todos los proveedores de acceso a Internet y casi todos los grandes portales brindan servicios de e-mail a sus usuarios, en algunos casos, gratuitamente. Un e-mail demora en condiciones normales unos pocos segundos en alcanzar su destino.

cortafuego:

Ver firewall.

cracker:

un hacker con intenciones destructivas y/o delictivas.

cracking :

Penetración fraudulenta en los sistemas ya sea para obtener un beneficio o causar daño.

craquear:

es el hecho de copiar y/o utilizar software comercial ilegalmente rompiendo las distintas técnicas de protección o registro que utilicen.

daemon:

aplicación UNIX que está alerta permanentemente en un servidor de Internet para realizar determinadas tareas como, por ejemplo, enviar un mensaje de correo electrónico o servir una página Web.

Datos o información personal:

Cualquier información relacionada a una persona física identificada o identificable. Los datos personales usualmente contienen información que directa o indirectamente puede ser relacionada o ligada a una persona física en particular.

Daño Informático:

deterioro o menoscabo a la integridad, confidencialidad y/o disponibilidad de datos, información, programas de cómputo, o computadoras.

defacement:

es una forma de hacking malicioso en el que un sitio Web es vandalizado. Normalmente un hacker malicioso (cracker) reemplaza el contenido normal del sitio con un mensaje específico de carácter político o social o aún más, borran el contenido del sitio entero. Logran esto aprovechándose de vulnerabilidades de seguridad para acceder al contenido del sitio.

delito informático:

se define como aquella conducta que teniendo como instrumento o fin computadoras u otros bienes informáticos, lesionan o dañan bienes, intereses o derechos de personas físicas o morales.

DSL:

Digital Subscriber Line: Línea Digital de Suscripción. Tecnología que permite enviar mucha información a gran velocidad a través de líneas telefónicas..

firewall:

es un sistema diseñado para prevenir el acceso no autorizado a o desde una red privada, normalmente en el caso de intranets. Los firewalls pueden implementarse tanto en hardware, en software, o bien en conjunto. Todos los mensajes entrantes o salientes de la intranet pasan por el firewall, el cual

examina cada uno y bloquea aquellos que no cumplan los criterios de seguridad especificados.

Hay varios tipos de firewall:

- Filtrado de paquetes: analiza cada paquete entrante o saliente de la red y lo acepta o rechaza basado en reglas predefinidas. Este método es bastante efectivo y transparente a los usuarios, aunque es difícil de configurar. Además, es susceptible a ataques de IP spoofing.
- Portal de aplicaciones: aplica mecanismos de seguridad a aplicaciones específicas, tales como servidores FTP y Telnet. Es muy efectivo pero puede degradar el rendimiento del sistema.
- portal a nivel circuito: aplica mecanismos de seguridad cuando se establece una conexión TCP o UDP. Una vez que se logra autenticar la conexión los paquetes fluyen libremente entre los hosts sin chequeos posteriores.
- Servidor proxy: intercepta todos los mensajes entrantes o salientes de la red y efectivamente oculta todas las direcciones reales de la red.

En la práctica, muchos firewalls usan dos o más de estas técnicas en conjunto. El firewall es la primer línea de defensa para proteger información privada. Para mayor seguridad los datos pueden encriptarse.

GATT: Acuerdo General de Aranceles Aduaneros y Comercio

gusano:

programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. Generalmente suelen llegar a través del correo electrónico, en forma de archivo adjunto.

Los gusanos de redes fueron definidos por primera vez por Shoch & Hupp, de Xerox, en la revista ACM Communications (Marzo 1982). El primer gusano famoso de Internet apareció en Noviembre de 1988 y se propagó por sí solo a más de 6000 sistemas a lo largo de Internet.

hacker:

experto informático especialista en entrar en sistemas ajenos sin permiso, generalmente para mostrar la baja seguridad de los mismos o simplemente para demostrar que es capaz de hacerlo. Los Hackers son muy respetados por la comunidad técnica de Internet, y proclaman tener una ética y unos principios contestatarios e inconformistas pero no delictivos, a diferencia de los Crackers que utilizan sus conocimientos para fines destructivos o delictivos.

hacking:

Acción de piratear sistemas informáticos y redes de telecomunicación.

hacktivismo:

formado al combinar "hack" con "activismo", se refiere al hacking de un sitio Web o sistema de cómputo para comunicar un mensaje motivado política o socialmente. A diferencia de un hacker malicioso, que puede irrumpir en un

sistema para obtener información o causar daños, el hacktivista realiza las mismas acciones para llamar la atención a una causa. Para el hacktivista, es la forma electrónica de practicar su protesta y desobediencia civil.

Acción de piratear sistemas informáticos y redes de telecomunicación.

hardware:

se refiere a todos los componentes físicos (que se pueden tocar) de la computadora: discos, unidades de disco, monitor, teclado, mouse, impresora, placas, chips y demás periféricos. En cambio, el software es intocable, existe como ideas, conceptos, símbolos, pero no tiene sustancia. Una buena metáfora sería un libro: las páginas y la tinta son el hardware, mientras que las palabras, oraciones, párrafos y el significado del texto son el software. Una computadora sin software sería tan inútil como un libro con páginas en blanco.

hosting:

alojamiento. Servicio ofrecido por algunos proveedores, que brindan a sus clientes (individuos o empresas) un espacio en su servidor para alojar un sitio web.

Información:

archivos o datos contenidos y/o transmitidos a través de una computadora, o por medios electrónicos, ópticos o de cualquier otra tecnología.

Internet:

red de redes. Sistema mundial de redes de computadoras interconectadas. Fue concebida en 1969 por el Departamento de Defensa de los Estados Unidos; más precisamente, por la ARPA. Hasta 1974 se llamó ARPAnet y fue pensada para cumplir funciones de investigación. Su uso se popularizó a partir de la creación de la World Wide Web. Actualmente es un espacio público utilizado por millones de personas en todo el mundo como herramienta de comunicación e información.

IP:

Internet Protocol. Protocolo de Internet. Sistema que define el modo en que los sistemas intercambian información en Internet.

IP spoofing:

técnica que permite que un atacante tome la identidad de un host "confiable" (cambiando su dirección IP por la dirección de éste) y obtenga de este modo accesos no autorizados a otros sistemas. En numerosos sitios (bajo Unix o Linux), existe un archivo denominado .rhosts conteniendo una lista de nombres de hosts que se consideran de confianza. Si un atacante se hace pasar por una de esas direcciones, puede llegar a ejecutar comandos en forma remota o logearse en el sistema aún sin tener una contraseña.

Mecanismo de seguridad:

dispositivo físico y/o electrónico, palabra clave, código de acceso, programa de cómputo o equipo informático que tenga por objetivo proteger una computadora, un programa de cómputo y/o la información contenida en una computadora, sistema o equipo informático de o contra:

- a) accesos internos o externos no autorizados;
- b) borrado, alteración o daño de información;
- c) ataque informático de cualquier índole.
- d) repudio del emisor o receptor de la información.

NIMDA:

El gusano "Nimda" (ADMIN, sigla de ADMINistrador, invertido), tiene la capacidad de propagarse a una velocidad pocas veces vistas en Internet. Se vale de cuatro formas diferentes para hacerlo.

1. Utiliza la misma vulnerabilidad en los servidores IIS de Microsoft, que usa el CodeRed y otros posteriores, para tomar el control de sus víctimas. Una vez en un servidor infectado, puede propagarse a otros servidores que tengan la misma vulnerabilidad, usando el comando tftp para enviar su código (en un archivo **ADMIN.DLL**).
2. Puede propagarse a través del correo electrónico, distribuyéndose a todos los contactos de la libreta de direcciones y otros obtenidos del historial del navegador, en un mensaje con el virus en el archivo **README.EXE** adjunto.
3. Cuando un servidor Web está infectado, cada usuario que visita sus páginas puede descargar el gusano desde un supuesto archivo WAV (sonido), que en realidad se llama **README.EML**. Bajo ciertas condiciones el Internet Explorer querrá ejecutar automáticamente el archivo del gusano, causando la infección de su computadora.
4. Se puede propagar a través de recursos compartidos en red, siempre que aquellos recursos sean accesibles sin contraseñas. Esto incluye a los usuarios domésticos que tienen habilitada la opción "**Compartir impresoras y archivos para redes**".

Hay informes de algunos mensajes enviados desde direcciones falsas, pero se supone que alguien, intencionalmente, modificó esas direcciones para hacer creer al destinatario en un remitente confiable. Se especula que esto podría haber sido hecho intencionalmente para propagar el virus en sus comienzos. El gusano está escrito en Microsoft Visual C++.

ONU: Organización de la Naciones Unidas.

página web:

es una de las tantas páginas que pueden componer un sitio de la World Wide Web. Un sitio Web agrupa un conjunto de páginas afines. A la página de inicio se la llama "home page".

password:

Ver contraseña.

phishing:

phishing: pesca. Es el acto de enviar un mail fraudulento a un usuario en nombre de una empresa legítima para engañarlo respecto a algún tema de su información privada. El mail deriva al usuario a un sitio Web donde se le pregunta algún dato personal, como ser contraseñas, número de tarjeta de crédito, cuentas bancarias, etc, que la verdadera organización ya tiene. Ese sitio, obviamente, es un truco para robar los datos del usuario.

phreaking:

está íntimamente relacionado al hacking, y consiste en utilizar una computadora u otro dispositivo para engañar al sistema telefónico. Típicamente, el phreaking se usa para hacer llamadas gratuitas o cargar esas llamadas a una cuenta diferente.

piratería de software:

es la copia no autorizada de software. La mayoría de los programas a la venta se licencian para el uso en sólo una computadora o para ser usados solamente por un usuario a la vez. Al comprar el software, el usuario se convierte en un usuario licenciado y no en un propietario (véase EULA). El usuario licenciado tiene permiso para realizar copias del programa con propósitos de backup, pero va contra la ley el distribuir copias a amigos y colegas. La piratería de software es imposible de detener, sin embargo las compañías de software están abriendo cada vez más y más demandas contra grandes infractores. Originalmente, las compañías de software trataban de detener la piratería usando protecciones anticopia, pero esta estrategia falló porque era inconveniente para los usuarios legítimos y no es 100% eficiente. La mayoría del software requiere algún tipo de registro, el cual desalienta a potenciales piratas, pero no detiene realmente la piratería en sí.

Hay un enfoque enteramente distinto a la piratería, denominado shareware, y se basa en la honestidad de la gente. Los productores de shareware alientan a los usuarios a dar copias de los programas a sus amigos y colegas pero le pidan a cualquiera que use el software regularmente que pague una cuota de registro directamente al autor del programa.

Los programas comerciales que se ponen a disposición del público ilegalmente se conocen como warez.

Policía Cibernética:

Unidad derivada de la Policía Federal Preventiva de México (PFP), que además de las acciones preventivas en materia de delitos cometidos en Internet y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores, como existen en los países desarrollados.

Programa(s) de cómputo o computación:

la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

PROSOFT: Programa para el desarrollo de la industria de Software.

Self-Certifying File System:

SFS es un seguro, sistema de archivos de red global con control completamente descentralizado. SFS permite acceder a sus archivos desde cualquier lugar y compartirlos con cualquier persona y en cualquier lugar. Cualquiera puede crear un servidor de SFS, y cualquier usuario puede acceder a cualquier servidor desde cualquier cliente.

sniffer:

programa que monitorea y analiza el tráfico de una red para detectar problemas o congestiones (conocidos como "bottlenecks", cuellos de botella). Su objetivo es mantener la eficiencia del tráfico de datos. Pero también puede ser usado ilegítimamente para capturar datos en una red. Esto último, sumado al hecho de que son prácticamente imposibles de detectar, los convierten en las herramientas favoritas de los hackers.

software:

se refiere a instrucciones para computadoras o datos. Cualquier cosa que pueda almacenarse electrónicamente es software, por eso se designa con este término a los diversos tipos de programas usados en computación. Los dispositivos de almacenamiento y visualización son el hardware.

El software suele dividirse en estas dos categorías:

- i. sistemas: incluye el sistema operativo y todas las utilidades que hacen funcionar a la computadora.

- ii. aplicaciones: son los programas que trabajan para los usuarios: procesadores de texto, planillas de cálculo, administradores de archivos y/o bases de datos, etc.

spam:

envío de correo electrónico publicitario no solicitado que se envía a listas de cientos de miles de usuarios. Se lo considera muy poco ético, ya que el receptor paga por estar conectado a Internet y no debería tener que estar soportando estas prácticas. Este tipo de mensajes causa graves molestias y provoca importantes pérdidas de tiempo y recursos.

Técnica del salami:

La técnica del salami es una forma de delito automatizado que consiste en el robo de pequeñas cantidades de activos de un gran número de fuentes, de allí su nombre ya que el método equivale al hecho de tomar rebanadas muy delgadas de un trozo de salami sin reducir significativamente el trozo total, por lo que las víctimas de este tipo de delito no se dan cuenta que están siendo objeto de un robo, o las diferencias que perciben en sus balances (de nóminas, cuentas corrientes, inventarios, etc.)

Son tan pequeñas que no consideran que vale la pena reclamarlas.

TI: tecnologías de información

TLC: Tratado de Libre comercio de América del Norte.

troyano:

(Trojan horse); caballo de Troya. Programa que contiene un código dañino dentro de datos aparentemente inofensivos. Puede arruinar parte del disco rígido o provocar pérdidas de información.

virus:

1. Programa o código que se carga en la computadora sin conocimiento del usuario y que se ejecuta por sí mismo.
2. Programa o código capaz de replicarse, esto es, capaz de infectar otros programas, el sector de arranque, alguna partición, o documentos que pueden ejecutar macros u otro tipo de programas, bien adjuntándose o insertándose a ese medio.