UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DIVISIÓN DE INGENIERÍA ELÉCTRICA

LEGISLACIÓN PARA EL INTERCAMBIO DE INFORMACIÓN A TRAVÉS DE REDES DE DATOS EN MÉXICO

T E S I S

QUE PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACION
P R E S E N T A

ANTONIO DÁVALOS DE LOS RÍOS

Asesor de Tesis: M. C. Cintia Quezada Reyes

México, D.F., Agosto, 2008

“Todo comportamiento humano debe ser regulado por el Derecho. Las redes de datos son una invención del hombre y por tanto deben ser reguladas por las especificaciones que la ciencia jurídica rige, si no es así viviríamos en la anarquía…”

Dr. Salazar Hernández

LEGISLACIÓN PARA EL INTERCAMBIO DE INFORMACION A TRAVÉS DE REDES DE DATOS EN MÉXICO

ÍNDICE DE CONTENIDO

Introducción

Planteamiento del Problema

En el mundo es cada vez más recurrente la necesidad de transferir información de un lugar a otro con el menor consumo de recursos posibles. Se vive en una sociedad que necesita de la información para mantener operando los procesos que rigen las principales actividades de los países, por ejemplo, telefonía, correo, mensajería, etcétera.

Actualmente es necesario transmitir información de una manera mucho más rápida y efectiva que por los medios anteriores, además de poder garantizar la fiabilidad de la misma que se envía, obteniendo este intercambio de información una importancia considerable con respecto a las actividades cotidianas.

El mundo actual es un mundo globalizado que exige la intercomunicación entre los habitantes de cualquier región. Uno de los métodos más eficaces y más empleados actualmente es el intercambio de información a través de Internet, ya que supone una manera rápida y efectiva de comunicación.

Debido a la importancia de intercambiar información de manera rápida, efectiva, y buscando que ésta sea íntegra, confiable y se encuentre disponible en el momento que un usuario autorizado lo requiera, es indispensable entrelazar los avances de la Ingeniería y la tecnología frente a la ciencia jurídica, lo que impone la actualización constante de las legislaciones para los intercambios de datos y de información sensible entre personas físicas y morales. Por tanto, es vital centrar el estudio en el intercambio de información vía electrónica, al emplear las redes de datos pues se busca como objetivo lograr la protección de los datos ante cualquier posible ataque y es digno de considerar cómo es que la ley protege a esta información.

Se parte de la base que en el mundo globalizado actual no puede dejarse de lado el hecho de incorporar en los estudios de investigación los avances de la ciencia y la técnica en el ámbito universal de conocimiento, lo que no es ajeno para la Ingeniería, que debe ocuparse también del avance en el manejo de las redes de datos y su información, que comunica a los pobladores del globo

terráqueo, que a decir de algunos autores, han concebido la idea de que la tierra es una sola sociedad de información.

Bajo esta óptica se entrelazan los avances de la Ingeniería frente a la ciencia jurídica, que impone la actualización de las legislaciones para lograr los intercambios de datos y de información sensible entre personas físicas y morales. En este contexto se pretende desprender la esencia de las redes de datos y proyectarla en su concepción original al mundo del Derecho, ya que es necesaria la articulación de leyes y reglamentos coherentes y operativos para proteger a la información que se intercambia haciendo uso de las redes.

Hipótesis Básica

Por todo lo anterior, allegándose del método deductivo e inductivo, sin olvidar los instrumentos que proporciona la actuaría, estadística y sobre todo los datos bibliográficos que se desprenden de la historia escrita en los libros que servirán de base, se plantea como hipótesis de arranque el siguiente cuestionamiento "¿Es necesario que la legislación mexicana actual se ocupe de los distintos derroteros que impone el avance cibernético, y dentro de éste la protección de la información que se intercambia, así como la seguridad que demanda la práctica del mundo globalizado actual?".

Estrategia de Comprobación

Para el análisis y comprobación de la hipótesis, se trata como primer punto los principios en los que operan las redes de datos hoy en día, definiendo los componentes principales de cada arquitectura.

Enseguida se abordan los factores de riesgo que existen alrededor de la información enviada a través de las redes de datos; estos factores de riesgo se traducen en ataques potenciales sobre los datos o información transferida.

Para gravitar el tercer punto define las principales herramientas con las que se cuenta en la actualidad para brindar protección a la información que circula a través de las redes de datos, las políticas

que se sugieren emplear y los análisis más representativos en este rubro.

Ya consolidada la teoría en los puntos anteriores, se hace un análisis profundo de la realidad de las redes de información mundialmente, considerando los mecanismos que la ciencia jurídica otorga para poder brindar una protección legal a la información que se transmite o se recibe.

Este trabajo está dirigido a toda persona que desee conocer el panorama actual del intercambio de información a través de las redes de datos, se parte de las bases estructurales que las conforman y se proveen los mecanismos que se tienen para poder proteger dicha información dentro de un marco jurídico específico, en este caso, la legislación mexicana.

Capítulo Primero

Arquitecturas para el Intercambio de Información a través de las Redes de Datos

1.1 Generalidades

El estudio de las comunicaciones a través de los siglos representa una evidencia fehaciente de la necesidad del ser humano de comunicarse con los demás. Desde los primeros asentamientos humanos, con las pinturas rupestres el hombre intercambiaba información sensible acerca de la ubicación de alimentos, de la caza y de sus propias experiencias.

La necesidad de intercambiar datos se desarrolló a su máxima expresión con los Mayas, Fenicios, Griegos, Etruscos, Hititas, Sumerios, Egipcios, Chinos, Incas, Persas y Asirios. Todas estas grandes civilizaciones compartieron un lazo en común, el desarrollo de tecnologías y técnicas como la escritura para poder transmitir un mensaje entre ellos.

Esta gran herencia milenaria se conserva hasta la época actual, donde se requiere mandar un mensaje en específico no sólo a personas de la misma región geográfica, sino a otras latitudes del planeta.

Aquí es donde se hace necesario un medio en el cual los seres humanos puedan intercambiar diversos tipos de datos de una manera rápida, eficiente y muy confiable; este medio son las redes de datos. La interconexión de redes de datos públicas y privadas da lugar a la comunicación internacional de un modo nuevo, en el que las referencias territoriales se pierden y también se difuminan los poderes que gobiernan cada trozo de espacio físico sobre el que están constituidos los Estados. Es un territorio abierto: **el ciberespacio**, un mundo sin fronteras.[1]

Por tanto, antes de describir a las redes de datos y cómo funcionan en lo general, se debe conocer su impacto en la sociedad del siglo XXI, esta sociedad que cambia a pasos acelerados y tiende a la migración total hacia las redes de datos.

[1] Muñoz Machado Santiago, La regulación de la red, Poder y Derecho en Internet, Primera Edición, Ed. Taurus, México, 2002, p.7

Ahora bien, aparece una interrogante que surgió casi con el origen mismo de las redes de datos, ¿por qué las redes no son seguras? Se podrían considerar varios aspectos que dan respuesta a esta interrogante.

Una razón, que resulta ser la principal que se puede dar es que la seguridad es molesta, esto se refleja en que muchos administradores de redes de datos no implementan mecanismos de seguridad eficientes e indispensables porque éstos resultan molestos a los usuarios. Considerando factores que más adelante se tratarán a detalle.

No se pueden concebir las redes de datos sin mencionar un poco de su historia y cómo es que a través de los años se han dirigido y sumado esfuerzos en implementar medidas que resten efectividad a los ataques más comunes hoy en día.

Antes de 1945, las computadoras no existían como tal. La verdadera necesidad de seguridad vino del aseguramiento del equipo militar para la comunicación. La criptografía moderna surgió como una medida de protección para el envío de mensajes con información sensible.

A inicios de la década de los cincuenta, se desarrollaron las primeras computadoras como tales. Consistían en máquinas gigantescas que requerían una manipulación muy específica para su correcto funcionamiento. La seguridad de la información no era un problema ya que se requería del acceso a la máquina y los conocimientos adecuados para poder operarla sin contratiempos.

Ya a fines de la década de los años setenta y comienzos de los ochentas, se dejó ver la gran falta de implementación de seguridad, cuando las compañías comenzaron a utilizar las terminales de acceso remoto con módems que operaban en el sistema telefónico público. El mayor problema fue, la aparición de ataques a los conmutadores telefónicos y a las grandes compañías, todo a una llamada de distancia.

Es a mediados de la década de los ochenta, donde ocurre una explosión en la necesidad de conectar a las computadoras

directamente entre ellas, formando las Redes de Área Local o LAN's. Estas redes, utilizaron versiones empresariales de las redes basadas en paquetes de los organismos militares, las cuales se optimizaron para redes pequeñas; la interconexión de estas redes dio paso a la creación de la red de redes, Internet. Para el año de 1995 las computadoras conectadas a Internet se habían convertido en elementos cruciales del mundo financiero.

Aquí, es donde aparecen los Bulletin Board Systems o BBS, los cuales consistían en conexiones de una gran computadora central con una gran cantidad de módems a los cuales se conectaban los usuarios, vía modo texto, para compartir información o conversar entre ellos. Éstos son los precursores de los foros de discusión que en estos tiempos se pueden encontrar en la red.

Es preciso indicar, que las universidades ya se encontraban realizando pruebas e investigaciones acerca de la protección de los paquetes de información enviados a través de estas redes. Estas investigaciones llevaron a generar avances como los del correo electrónico, el cual pasó de ser una herramienta simple de mensajería a un gran sistema de mensajes capaz de comunicar a personas y compañías de varias latitudes del planeta para poder hacer negocio.

La Internet, tuvo su gran crecimiento en la escena pública entre 1994 y 1996. Utilizado mayoritariamente para las utilidades de correo electrónico y visualización de páginas de la World Wide Web (o simplemente Web), forzó a los Bulletin Board Systems a conectarse a ella, generando así a los primeros proveedores de servicio de Internet o ISP (Internet Service Provider).

El "boom" de la Internet, se dio tan rápido, que ni siquiera potencias empresariales como Microsoft pudieron preverlo. Bill Gates, presidente de Microsoft, declaró en una conferencia que Internet no tendría éxito y que sólo se trataba de una moda.[2]

[2] Strebe Matthew, Network Security Foundations: Technology Fundamentals for IT Success, Primera Edición, Sybex, E.E.U.U., 2004, p. 12

Pronto dio cuenta de su error y lanzó una campaña de entrada de todos sus productos con la leyenda "Internet Enabled"[3]. La Internet y sus protocolos completamente inseguros dieron pie al desarrollo y proliferación de hackers que se habían cansado y aburrido de realizar ataques contra las centrales telefónicas, mismas que ya habían reforzado su seguridad.

La solución de los desarrolladores ante esta nueva ola de ataques a través de la red fue la de instalar cortafuegos o firewalls, los cuales mitigaron un poco los efectos de los ataques pero que presentaban una vulnerabilidad que hacía posible a los miembros de una red a compartir datos sin permisos especiales. Los perpetradores continuaron explotando a los protocolos inseguros, promoviendo el desarrollo de protocolos seguros.

Todavía en estos momentos, los trabajos de las compañías encargadas del desarrollo de software siguen en el desarrollo de nuevos protocolos capaces de proteger paquete a paquete, empleando algoritmos de cifrado y demás técnicas, para garantizar la integridad, confidencialidad y disponibilidad de la información enviada a través de las redes de datos, en especial en la Internet.

Es conveniente entonces definir lo que es una red de datos, siendo ésta un conjunto de dispositivos conectados entre sí mediante un medio de transmisión para permitir intercambiar información o compartir recursos de una manera confiable y eficiente.

Para lograr estos dos últimos puntos, confiabilidad y eficiencia, se han desarrollado tecnologías que la interconexión de equipos con un propósito específico; estas tecnologías acortan distancias entre sistemas de información, optimizan los recursos de una organización y en general permiten compartir información entre personas.

Conocer cómo se realiza el intercambio de información lleva a la necesidad de documentar las arquitecturas de conexión más importantes hasta el día de hoy, la arquitectura Cliente-Servidor y la punto a punto.

[3] Ídem. p12

1.2 Arquitectura Cliente - Servidor

Para poder conocer más de cómo es que se realizan los intercambios de información más comunes en el mundo, se debe referir al esquema Cliente-Servidor.

A lo largo de la última década del siglo pasado, el intercambio de información a través de Cliente-Servidor ha tenido un impacto muy considerable sobre todos los aspectos de diseño, desarrollo e implementación de los sistemas computacionales. Ha permitido a las organizaciones a abandonar el desarrollo *monolítico* centralizado para dar paso al procesamiento distribuido a través de una red de sistemas. Ésta flexibilidad permite a que la información pueda ser almacenada y que los procesos sean realizados en equipos centrales, locales o remotos. Computadoras personales y estaciones de trabajo pueden ser conectadas a las redes Cliente-Servidor aumentando las capacidades de los sistemas centrales y distribuidos.

El empleo de Cliente-Servidor permite el uso de equipos de bajo costo, incrementando la autonomía y pertenencia de la información compartida. Las primeras aplicaciones diseñadas bajo este esquema se enfocaron originalmente a aplicaciones de rápido procesamiento y desarrollo, siendo disminuido el costo en la utilización de recursos de Software y de Hardware; ahora, se cuentan con aplicaciones potentes que proveen de una gran capacidad de diseño y de implementación, fortaleciendo a las redes de datos como el principal elemento de intercomunicación entre personas y computadoras.

1.2.1 Definición

Existen varias definiciones de la Arquitectura Cliente-Servidor (C/S), con base en su concepción y su arquitectura. La empresa IBM define a este modelo o arquitectura como "La tecnología que proporciona al usuario final el acceso transparente a las aplicaciones, datos, servicios de cómputo o cualquier otro recurso del grupo de trabajo y/o, a través de la organización, en múltiples plataformas. El modelo soporta un ambiente distribuido en el cual los requerimientos de servicio hechos por estaciones de trabajo

inteligentes o *clientes*, resultan en un trabajo realizado por otras computadoras llamados servidores"[4]

Originalmente se designó con este término a un método de procesamiento distribuido. El ambiente de comunicación basado en redes de área local que sirvió como plataforma para la unión de dos bases de datos cliente – servidor es sólo una de las grandes ramificaciones de los que representan los sistemas de información con procesamiento distribuido.

De acuerdo con Olguín Romo se pueden citar tres características primordiales de las arquitecturas C/S[5]:

- "Los sistemas se crean ensamblando componentes independientes, los cuales poseen funciones específicas que hacen al sistema en su conjunto trabajar para un fin específico. Exponiéndose de una manera simple, los componentes de los clientes interactúan con el usuario y los servidores utilizan a los módulos cliente para pedir información necesaria para completar una tarea. A esta característica se le conoce como *modularidad*.

- Los clientes y servidores pueden utilizar hardware y software diseñado específicamente para funciones particulares; pero esto no significa que no puedan adaptarse herramientas prefabricadas a los sistemas ya implementados. Esto es lo que se conoce como la *adaptabilidad*.

- El poder descomponer al sistema completo en los elementos independientes para facilitar el mantenimiento de las aplicaciones representa la característica de *mantenimiento."*

Se puede concluir, que la arquitectura Cliente-Servidor representa un gran beneficio, ya que provee la disponibilidad de los servidores en el plano físico (hardware) que se pueden escalar desde una pequeña máquina con un solo procesador hasta las grandes máquinas con cientos o miles de procesadores. Las empresas ahora

[4] Cliente – Servidor: Tecnología, potencial y futuro
[5] Olguín Romo Heriberto, Dirección, Organización y Administración de Centros de Tecnología de Información, Primera Edición, U.N.A.M. Facultad de Ingeniería, 2005., p.293

pueden comparar el poder de cómputo o procesamiento de los servidores con el trabajo en proceso. Un servidor puede ser reemplazado de una manera *simple* por otro de mayor procesamiento. Este cambio puede realizarse sin afectar a las estaciones de trabajo de los clientes o las herramientas que emplean, proveyendo esto no sólo de escalabilidad, sino también flexibilidad en el manejo del crecimiento de hardware que se traduce a final de cuentas en una reducción en los costos de actualización de la tecnología de información.

1.2.2 Protocolos Característicos

La conexión entre clientes y servidores se realiza a partir de protocolos en común, es decir, varias reglas o comandos que especifican cómo es que se realiza el intercambio de información o datos entre las entidades.

Los sistemas C/S utilizan a la familia de protocolos TCP/IP (Transmision Control Protocol/Internet Protocol), los cuales son una familia de protocolos que se adoptaron como estándar al ser los más sencillos y útiles al implementarse. En la actualidad no existe un paquete completo que contenga a todas las aplicaciones de TCP/IP, esto es, debido a que los desarrolladores de software y, en general de tecnología de redes de datos, generaban sus propios protocolos para un objetivo específico, reemplazando o actualizando algunos para después liberarlos.

Es pertinente que se señalen los protocolos más característicos utilizados en una conexión Cliente/Servidor al nivel de aplicación, considerando que nos son los únicos, sino los más representativos de esta tecnología.

a) Hyper Text Transfer Protocol (HTTP)

Éste es de los protocolos más utilizados. Es el protocolo de transferencia de hiper texto es uno de los protocolos más empleados hoy en día, se usa para los sistemas de información distribuidos y colaborativos.[6] Maneja el concepto de hipertexto, el

[6] RFC 2616 Definición de HTTP 1.1

cual es un documento que puede enlazarse con otro para hacer una unidad de información.

Utiliza un lenguaje estandarizado de marcas para documentos Web, el *Hypertext Markup Language HTML.* Su funcionamiento básicamente es establecer una conexión del cliente a través del puerto lógico 80 por el cual es enviada una solicitud (mensaje). El servidor recibe esta solicitud y envía una respuesta al cliente, que en caso de ser afirmativa realiza tal conexión y la mantiene hasta que el cliente cierra la comunicación.

b) File Transfer Protocol (FTP)

El protocolo de transferencia de archivos es junto con HTTP uno de los protocolos más utilizados en las redes de datos, fue desarrollado por el *Massachussets Institute of Technology* en 1971 y ha sufrido de numerosas mejoras a través de su historia. Se describe detalladamente en el RFC 959[7].

Se utiliza para copiar archivos de una máquina a otra por medio de una identificación del usuario en el servidor. Se emplean dos conexiones, la primera para el login, seguida del protocolo TELNET. Después se realiza la segunda conexión que se encarga de gestionar la transferencia de datos. Todo esto en el puerto 21.

En ambos extremos del enlace, la aplicación FTP se compone de un intérprete de protocolo (PI), un proceso de transferencia de datos y una interfaz de usuario.

c) Simple Mail Transfer Protocol (SMTP)

El protocolo de transferencia de correo simple fue diseñado en 1982 para el intercambio de información en forma de correo. La comunicación entre el cliente y el servidor se realiza a través de caracteres ASCII con una longitud no mayor a cien caracteres por el puerto 25. Al momento de realizar la conexión el servidor envía una

[7] RFC 959 Definición de FTP en español

serie de códigos de confirmación, los cuales son interpretados por el cliente para seguir con el envío de la información restante.[8]

d) Finger

Este es un protocolo que muestra información sobre los usuarios de un equipo remoto. El cliente envía un comando en caracteres ASCII, que acaba en <CRLF>(\r) a través del puerto 79. El servidor responde con una o más cadenas del tipo ASCII con la información de usuario y cierra la conexión.

e) TELNET

Permite la conexión vía remota para acceder a los datos de un equipo determinado. Es de los protocolos más antiguos, ya que su desarrollo comenzó en 1969[9] . Su principal desventaja es que no provee de protección a los datos que envía, es decir, que toda la información se envía sin cifrar, lo que lo hace vulnerable a intercepción de datos.

f) Protocolos basados en Socket Secure Layer

Es una variante de los protocolos HTTP y FTP el cual utiliza los principios de la *Capa de Sockets Seguros SSL (Socket Secure Layer)*. Donde se mantiene un canal de comunicación cifrado entre el cliente y el servidor.

La conexión básicamente se realiza en tres pasos: *Handshake* o acuerdo de tres vías, en donde acuerdan los algoritmos criptográficos a utilizar, las claves a emplear y la identificación del servidor. *Envío de datos seguros* donde se transmiten los datos con el objetivo de cifrar y garantizar la integridad. *Cierre de la sesión* donde se termina la comunicación de la conexión segura.

[8] RFC 821 Definición de Simple Mail Transfer Protoco
[9] RFC 15 Definición de Telnet

1.3 Arquitectura Punto a Punto (P2P)

En las redes actuales no sólo se manejan los protocolos Cliente-Servidor. Hoy en día se acostumbra compartir cualquier tipo de información a través de las redes, lo que se realiza de una manera común por medio de las conexiones punto a punto.

1.3.1 Definición de Punto a Punto

Aquellas conexiones de computadoras que no siguen un esquema centralizado de servicio, es decir, que no existe un equipo que funja como servidor central.

Aunque los sistemas cliente/servidor sean los más utilizados hoy en día, la tecnología punto a punto utiliza el fundamento original de Internet: un medio de comunicación para máquinas que comparten recursos con otras máquinas al mismo nivel. [10]

Actualmente se utilizan las arquitecturas Punto a Punto para la transferencia de archivos de una manera rápida y eficiente. Se pueden localizar en las redes dedicadas al P2P un sin fin de archivos que van desde las fotografías hasta los reportes militares de soldados retirados, pasando por música, libros virtuales, etcétera.

1.3.2 Redes de Intercambio de Información por P2P

Se emplean las tecnologías P2P básicamente para compartir información, lo que implica la creación de redes completas dedicadas a la transferencia *libre* de archivos; las redes más empleadas para transferir información de esta manera son las redes Napster, Gnutella, Gnutella2, FastTrack, eDonkey, Overnet, DirectConect y MP2P. A continuación se muestran estas redes según las concibe Wallace Wang. [11]

a) Napster

[10] Oram Andy, Peer to Peer: Harnessing the Power of Disruptive Technologies, Primera Edición, Oreilly & Associates, E.E.U.U., 2001, p.13

[11] Wang, Wallace, Steal this File Sharing Book, No Starch Press, E.E.U.U., 2004 pp 17-39

La red Napster se originó en el año de 1999 como una alternativa para el intercambio de archivos de audio en Internet. Fue el servicio que fungió como parte aguas de las tecnologías P2P actuales.

Consiste en una red centralizada, donde el servidor central recopila la información de todas las máquinas de la red. Cuando un usuario quiere buscar un archivo de audio se conecta al servidor central, el cual le indica por medio de tablas la dirección del otro usuario que posee el archivo solicitado. Después de eso se realiza la conexión entre los dos clientes y se inicia la descarga. La figura 1.1 ejemplifica cómo es que el servidor central es el que dirige las conexiones.

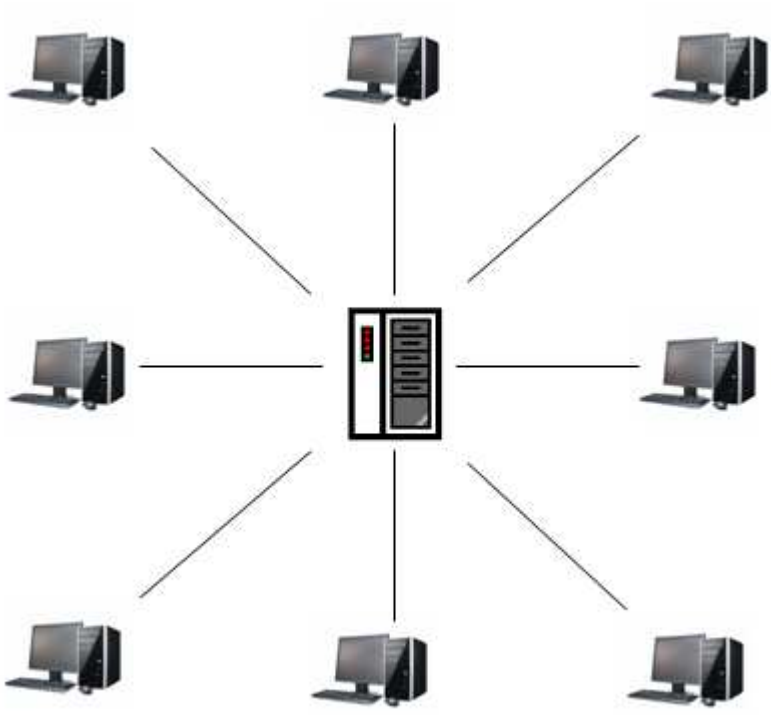

Figura 1.1 Esquema general de conexión de Napster

Cuando el problema se volvió legal por el uso de archivos de audio con derechos (copyright), fue muy sencillo para las autoridades estadounidenses dar de baja el servicio, sólo tuvieron que apagar al servidor central. Ése fue el problema principal de Napster, confiar toda la conexión de la red en un solo servidor central. Las redes P2P

subsecuentes lograron darle la vuelta a ese problema implementando otras medidas como las que se muestran a continuación.

b) Gnutella y Gnutella2

Gnutella surgió justo después del cierre del Napster original. Eliminó el uso del servidor central y creó una red completamente descentralizada donde todas las computadoras de esta red pudieran comunicarse directamente con las demás, como se muestra en la figura 1.2. A diferencia de Napster, cada computadora puede trabajar de manera independiente, así que tirar una computadora jamás podrá tirar a la red completa. Una ventaja que aportó Gnutella es que el código es libre, lo que significa que cualquier programador podía modificarlo para añadir mejoras, depurar errores, entre otros.

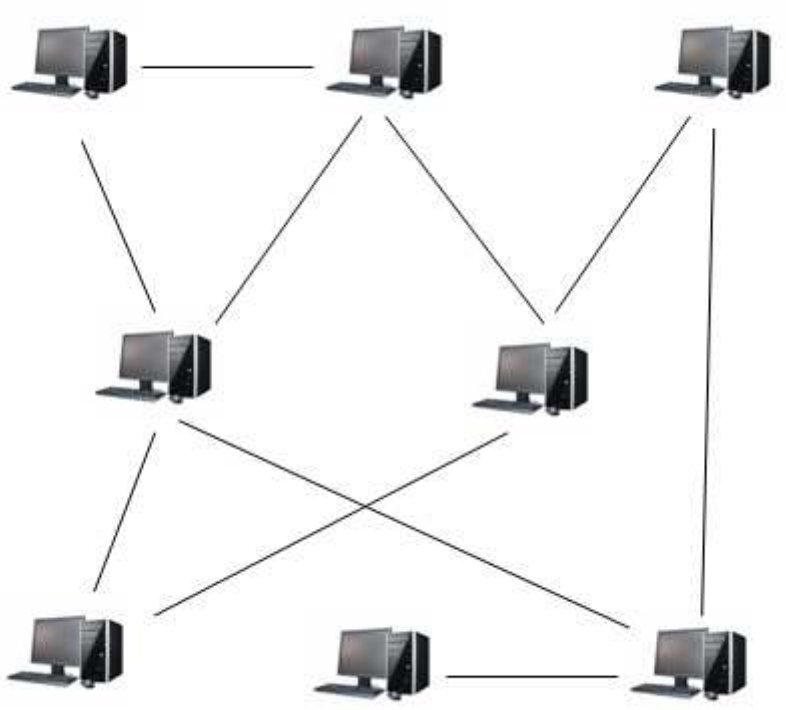

Figura 1.2 Esquema general de conexión de Gnutella

Gnutella mostró otra mejora ante Napster, no sólo compartía archivos de audio sino archivos de todo tipo. Es una de las redes más antiguas, conocidas y utilizadas para compartir información, pero las búsquedas pueden ser muy lentas. Cuando se busca un archivo, la petición pasa a través de todas las computadoras de la red, las cuales llegan a ser miles.

Como solución a este problema se diseñó una nueva red basada en Gnutella, la Gnutella2 que es software libre también e incorpora mecanismos eficientes de búsquedas de archivos.

c) FastTrack

Mientras que Gnutella es una red libre a la que cualquiera puede acceder, FastTrack es una red propietaria donde cierto número limitado de programas usuario pueden acceder.

Una compañía holandesa, Kazaa BV, creó la red FastTrack después del cierre de Napster. Se basó principalmente en el diseño libre de Gnutella y añadió un mecanismo mucho más eficaz de búsqueda de archivos.

Este método eficaz de búsqueda se basa en Supernodos, los cuales dividen a la gran red en varias subredes, realizando la búsqueda de una manera mucho más rápida. Cada uno de estos supernodos debe buscar en una parte específica de la red, no en toda. En la figura 1.3 se muestra que los supernodos son los encargados de dar las conexiones para localizar los archivos deseados.

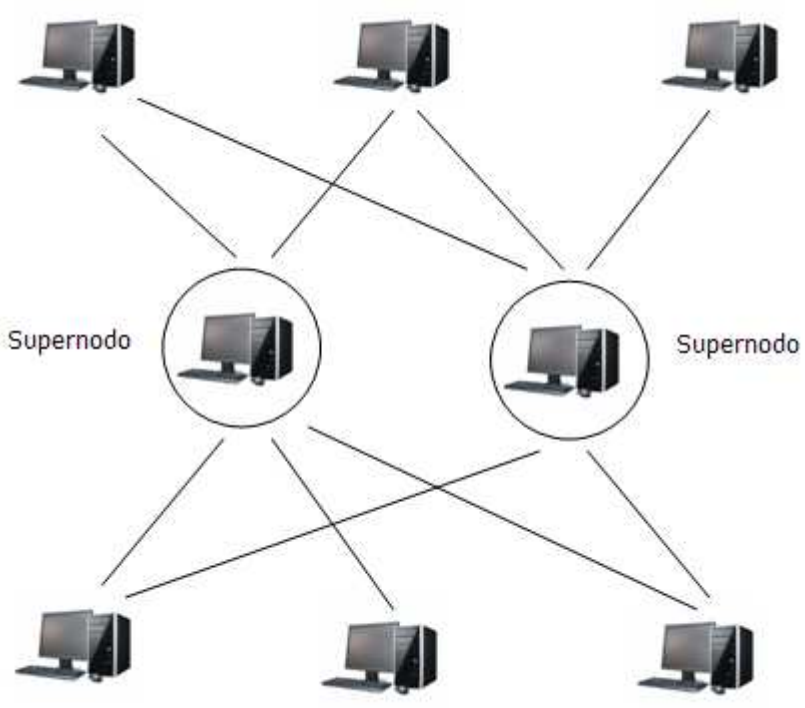

Figura 1.3 Esquema general de conexión de FastTrack

Además implementó la opción de descargar archivos de varias fuentes, lo cual es muy útil para archivos de gran tamaño. Otra de las innovaciones que presenta es que su protocolo está cifrado, lo que supone que se tiene que pagar cierta cantidad de dinero para poder modificarlo.

d) eDonkey y Overnet

Aunque Gnutella y FastTrack permiten a las personas el intercambio de cualquier tipo de archivo, los archivos más populares son los archivos de sonido que contienen una canción individual. En las redes eDonkey (ed2k) y Overnet se encontrarán archivos de tamaño mucho mayor, como películas o imágenes de CD's y DVD's.

Lo que hace a estas redes populares para los archivos de mayor tamaño es la capacidad para descargar un archivo desde diferentes fuentes. Al descargar un archivo de esta manera, se asegura que si un equipo con el archivo deseado se desconecta de la red se pueda continuar la descarga del resto del archivo de otra computadora.

Para evitar la confusión causada por la similitud de los nombres de los archivos, ambas redes examinan el contenido y tamaño del archivo y crea un cálculo único, llamado *hash checksum* o suma de verificación hash. Esta operación permite identificar a los archivos idénticos que puedan aparecer en la red con diferente nombre.

Para mejorar el desempeño en compartir los archivos de muy gran tamaño se permite compartir este archivo antes de descargarlo completamente. Eso quiere decir que se puede compartir un archivo justo desde el momento que se realiza la descarga, lo que implica que los clientes obtendrán el archivo en un tiempo menor.

La diferencia entre eDonkey y Overnet es que ed2k se basa en un servidor central (similar a como funciona Napster), mientras que Overnet no. Además de que Overnet tiene la capacidad de conectarse a las redes Overnet e eDonkey.

e) DirectConnect

Ésta es una red basada en servidores centrales esparcidos, no en una sola red unificada. En vez de compartir archivos entre ellos, cada servidor comparte sólo los archivos con los equipos que se conectan directamente a ese servidor en particular. Muchos de los servidores de DirectConnect no proporcionan acceso a conexión a menos de que se compartan al menos 10 o 20 GB de archivos.

Al permitir que cualquiera pueda crear un servidor propio se genera el concepto de servidores específicos, los cuales comparten archivos de un tipo especializado, como películas de un estilo en concreto, música, programas, etcétera.

f) MP2P

Mientras las redes analizadas anteriormente proveen videos, programas y archivos gráficos, la red Manolito P2P o MP2P se enfoca únicamente en archivos MP3. Es básicamente una aplicación similar a las anteriores, enfocada a los archivos de audio exclusivamente.

De esta manera se puede concluir que las redes punto a punto se han convertido en el medio de intercambio de archivos, sobre todo archivos multimedia. Esto ha traído como consecuencia que las empresas o agrupaciones creadoras de los archivos que se distribuyen de manera *ilimitada* por P2P busquen la manera y argumentos legales para poder detener el tráfico de estos archivos, un tráfico que no puede ser detenido, ya que al tratar de desaparecer una red de intercambio se generará otra, como lo ocurrido con la red Napster, que al caer dio paso al desarrollo de las demás redes P2P.

Punto a punto, como todas las tecnologías, envuelve una serie de cuestionamientos acerca de las personas y sus futuras direcciones para la tecnología. Se está dando el caso de que P2P está marcando la pauta de la información en un sentido que está contraponiéndose a los principios marcados por las compañías y los gobiernos.

La cuestión es ahora ver los usos de la tecnología y de la información. Un enfoque común proporciona a los usuarios de ésta tecnología con el máximo de control sobre la aplicación dada a la tecnología y a la información. El usuario puede decidir que contenido descargar y cómo utilizarlo, pudiendo importar si su origen va en contra de las leyes. A final de cuentas, un archivo de computadora no es más que una colección de impulsos eléctricos en forma de bits, los cuales al ser interpretados por un equipo dan origen a la información.

El mostrar la estructura básica de las arquitecturas Cliente-Servidor y Punto a punto permite definir el tipo de acciones que se realiza en ellas. El compartir información siempre conllevará riesgos a su integridad, confidencialidad y disponibilidad, puntos que como se mostrará más adelante, conllevan al resguardo y protección de la información.

No cabe duda que en un futuro no muy lejano, las arquitecturas Cliente-Servidor y Punto a punto coexistirán. Muchos sistemas formarán parte de ambos modelos y es menester que el flujo de datos que se origine sea protegido tanto de una manera técnica,

como legal, tomando como base a los modelos por separado para poder analizar y comprender los fundamentos de su utilización.

Capítulo Segundo

Seguridad y Protección de la Información

2.1 Aspectos Generales de Seguridad

Habiéndose definido las distintas arquitecturas que una red de datos emplea, es necesario saber qué es lo que maneja. Muchos autores discrepan entre sí acerca de una definición formal de lo que se transfiere en estas redes, pero todos concuerdan que es el mismo principio, la información.

Esta información es la que origina la necesidad de implementar seguridad en una red de datos. El desarrollar un ambiente de seguridad en la red requiere una gran cantidad de requerimientos que deben ser cubiertos y aplicados en todos los recursos de la red misma. Esto no puede realizarse si no se genera una cultura de seguridad en los miembros de la organización. Ya sea desde el Director General hasta el asistente, debe existir esa sensibilidad hacia la protección de la información que manejan a través de las redes de datos de la organización para poder evitar de esa manera generar un riesgo a la misma.

2.1.1 Definición de Información

Existe una gran cantidad de definiciones, pero la que mejor se adapta a la intención de este trabajo de investigación es la que define a la información como todo aquel conjunto de elementos que pueden ser interpretados por los seres humanos para un fin en específico.

Esto sin duda puede resultar muy general, pero si se analiza con detenimiento, la información no es otra cosa más que lo posiblemente interpretable por una persona para utilizar. De ahí se parte para poder especificar lo que se quiere transmitir a través de las redes de datos, información representada por datos electrónicos.

Esta información puede tener un cierto grado de sensibilidad para la persona que la envía o la recibe, por lo que no necesariamente se desea divulgarla a cualquier persona. Se tratará siempre de proteger la información de personas que no deban acceder a ella.

Tómese como ejemplo al tratamiento de la información en la Segunda Guerra Mundial. El ejército de los Estados Unidos ideó un sistema de comunicación basado en el lenguaje *navajo* con la finalidad de que los soldados japoneses, al realizar las intercepciones radiales de la comunicación, no pudieran entender la información compartida entre un batallón y otro. El idioma *navajo* en esencia es complicado y con una fonética similar a las lenguas orientales; de ahí su gran utilidad para confundir a las fuerzas enemigas.

El empleo de esta técnica se realizó con el objetivo de proteger a la información de una manera tal que no se comprometiera al enemigo, ejemplificando el concepto de seguridad.

2.1.2 Definición de Seguridad

La seguridad no es otra cosa más que el tratamiento que se le da a la información para poder resguardarla, es decir, evitar que se comprometa.

De aquí se desprende que la seguridad informática sea el tratamiento dado a la información que fluye a través de redes de datos, con el fin de resguardarla.

Resguardar a la información puede interpretarse de varias maneras, que la información no sea proporcionada a personas no autorizadas, que no sea modificada más que por la persona que la envía o recibe y que en el momento que se requiera esta información, se encuentre a la mano.

Estas interpretaciones mencionadas dan lugar a la descripción de los tres pilares fundamentales de la Seguridad en los sistemas de información, la confidencialidad, la disponibilidad y la integridad, la figura 2.1 muestra claramente cómo se complementan las tres para definir a la Seguridad Informática.

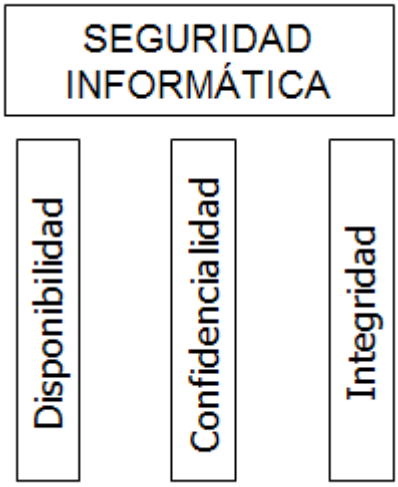

Figura 2.1 Pilares de la Seguridad Informática

La **confidencialidad** se refiere a la prevención del acceso a la información sensible a personas que no cuenten con la autoridad necesaria. Este acceso puede hacerse de manera intencional, rompiendo un cifrado para averiguar el contenido, o de manera involuntaria, por descuido del personal encargado de manipular esa información.

La **disponibilidad** asegura que la información siempre estará al alcance del usuario autorizado, al momento que lo requiera.

La **integridad** persigue tres metas principales, de acuerdo con Cole, Krutz y Conley[12]:

- Prevención de la modificación de la información por usuarios no autorizados.

- Prevención de la modificación no autorizada o no intencional de la información por personal autorizado.

- Prevención de la consistencia interna y externa. Por interna se entiende que los elementos de una organización concuerdan con los registrados. La externa

[12] Cole Eric, Krutz Donald, Conley James, Network Security Bible, Wiley Publishing Inc., E.E.U.U., 2005 p4

implica que los datos dentro de la organización tengan cierta congruencia con el mundo real.

Autores como Canavan argumentan la existencia de otra tercia de elementos fundamentales para la Seguridad Informática. Estos elementos los llama el **triángulo de la seguridad,** ejemplificado en la figura 2.2[13]**.**

Figura 2.2 El triángulo de la Seguridad

Siendo el primer elemento la prevención, es decir, que para proveer un cierto nivel de seguridad es necesaria la implementación de medidas que eviten que se exploten vulnerabilidades. En el desarrollo de esquemas de seguridad, las organizaciones deben enfatizar a las medidas preventivas sobre la detección y la respuesta. Es mucho más fácil, más eficiente y económicamente mejor prevenir una falla en la seguridad que detectarla o repararla.

El segundo elemento es la detección, la cual especifica los procedimientos necesarios para poder identificar problemas potenciales o fallas en la seguridad, en caso de que las medidas de prevención fallen. Mientras más rápido se detecta un problema, más sencillo será corregirlo.

Como último elemento se encuentra la respuesta, en la cual las organizaciones necesitan desarrollar un plan que identifique el tipo de acción a emplear en caso de que se aproveche una falla en la

[13] Canavan John, Fundamentals of Network Security, Primera Edición, Artech House, E.E.U.U., 2001 pp 9-10

seguridad. También se debería identificar al responsable de las acciones que atenten contra la organización y su nivel jerárquico.

2.1.3 Metodología

Teniendo las bases para definir la seguridad, sería demasiado irresponsable tratar de implementarla sin saber exactamente cómo, para qué y contra que elementos se implementa, lo cual lleva a especificar una metodología de seguridad.

Precisamente son estos tres elementos los que plantean el objetivo de la seguridad de la información. López y Quezada las formulan de la siguiente manera[14]

- ¿Qué es lo que se quiere proteger?
- ¿De qué se quiere proteger?
- ¿Cómo se va a proteger?

La primera cuestión responde a la identificación de los elementos que se quieren proteger o se les desea brindar seguridad. Lo que implica identificar a los elementos denominados activos de la organización, los cuales pueden ser elementos físicos y lógicos, componiendo así un **entorno de seguridad**. También es necesario saber dónde afectaría el que se presentara una amenaza y si se podría repetir o no la misma.

La segunda cuestión representa los posibles riesgos a los que se encuentran expuestos los elementos o activos, es decir, saber que es lo que podría afectar al entorno. Aquí es importante hacer la observación de que ningún entorno de seguridad se encuentra completamente seguro, siempre existirán vulnerabilidades, las cuales, por ínfimas que sean, pueden presentar un riesgo potencial contra el entorno antes descrito. Por ello es necesario basarse en el triángulo de Seguridad para evitar y mitigar una posible falla de seguridad.

[14] López B., Jaquelina y Quezada R., Cintia, Fundamentos de Seguridad Informática, Primera Edición, U.N.A.M. Facultad de Ingeniería, 2006 pp 3-6

La última cuestión es la culminación del análisis de seguridad en el entorno, es decir, con base en los elementos a proteger y sabiendo contra qué se van a proteger se pueden elegir las herramientas que se consideren más adecuadas para la protección.

Estas cuestiones forman parte de una metodología de seguridad, la cual, si llega a aplicarse de una manera efectiva, puede llevar al aseguramiento del entorno.

2.2 Amenazas

El simple hecho de manipular información sensible conlleva un riesgo, el cual puede poner en peligro alguno de los tres aspectos primordiales de la seguridad. Tómese un ejemplo de la vida diaria, un miembro del comité ejecutivo de cierta compañía "A" es despedido por situaciones que a su parecer considera injustas. Este personaje tiene en su poder el reporte de ventas de marketing de la compañía "A" al momento de ser despedido; es contratado por la organización competidora de la primera compañía (compañía "B"), la cual se encuentra en los mismos niveles de ventas. Este personaje puede utilizar el informe obtenido para poder plantear una estrategia de negocios mucho más efectiva y así atraer más clientes a la compañía "B".

Visto en lo anterior, la persona que es despedida tiene información sensible acerca de la compañía "A" y por tanto, al estar inconforme con ella, puede hacer uso del reporte para su propio beneficio y afectarla. Esta persona representa por tanto, una **amenaza** contra la compañía "A", ya que tiene en su poder información sensible no autorizada y la puede o no utilizar.

Por lo tanto, se puede deducir que una amenaza es todo aquel personaje o situación que puede destruir o que por lo menos lo pretende. Este peligro es latente y puede o no manifestarse.

Las amenazas se pueden considerar dentro de varias clasificaciones.

a) Amenazas Humanas

Puede decirse que este tipo de amenazas son las que más frecuentemente se presentan en una organización. Representan a la ignorancia, ineptitud o mala fe de las personas que pertenecen a la misma organización, pero también incluyen a los intereses personales o de grupo para afectar a la información.

Dentro de las amenazas humanas, Paquet y Saxe hacen una clasificación basados en las acciones que pueden llevar a cabo las personas que representan a estas amenazas[15].

- No estructuradas

  Estas amenazas describen la búsqueda de un atacante por una presa fácil. No atenta necesariamente contra algo en específico, sino que simplemente busca algo que atacar. Se puede realizar una analogía con un criminal en potencia que camina por las calles desiertas buscando qué robar.

- Estructuradas

  Estas amenazas tienen ya un fin específico, no son producto de la casualidad; todo parece estar planeado para intentar llevar a cabo un ataque. Por ejemplo, un atacante que pretenda entrar a un servidor un día específico con el fin de obtener información específica.

- Internas

  Son amenazas presentadas por alguien dentro de la organización. Pudiera ser un empleado con malicia o un empleado incompetente que no pretende causar daño alguno, pero que puede provocar un daño considerable.

- Externas

  Estas amenazas pueden ser estructuradas o no estructuradas y emanan de personas ajenas a la organización.

[15] Paquet Catherine, Saxe Warren, The Business Case For Network Security: Advocacy, Governance, And ROI, Primera Edición, Cisco Press, E.E.U.U., 2004 Sección Threats Classification

Un claro ejemplo de una amenaza de este tipo podría ser el siguiente caso. Un empleado de limpieza del área de servidores desconecta de la corriente eléctrica un cable de alimentación que se cruza en su camino. Al terminar la limpieza esta persona lo vuelve a conectar y se retira. El elemento que desconecta es uno de los servidores Web de la compañía que puede o no ser accedido por algún usuario en el momento en el que la persona de limpieza desconecta el cable, provocando la interrupción del servicio Web.

b) Amenazas por Errores en Hardware

Generalmente estas amenazas pueden causar problemas en los sistemas de información cuando uno de los dispositivos de red de la organización presenta anomalías o fallas en su operación.

En muchos casos no se observa el verdadero impacto de este tipo de amenazas hasta que se convierten en ataques; tómese como ejemplificación de esto al core switch de una red, el cual tiene un defecto de fabricación en el convertidor de la fuente de alimentación, aumentando un poco su temperatura al operar. Este calentamiento no es de consideración pero tampoco es normal, lo que puede llevar a la caída de la red completa del edificio si se presenta una sobrecarga de voltaje en el edificio tal que afecte al convertidor defectuoso.

c) Amenazas por Errores en la Red

Los paquetes de información fluyen de una red a otra utilizando mecanismos a nivel eléctrico-electrónico muy específicos, es decir, a nivel de cableado se realiza una conmutación de las señales eléctricas con el fin de transmitir en un mismo canal diferentes pulsos en sentidos diferentes. Cuando no se calcula correctamente el flujo de tráfico que se va a tener en la red se puede llegar a provocar conflictos a nivel de señales.

Una de las causas de estos conflictos es la mala planeación y diseño de la red, es decir, que no se cuenta con el estudio profundo de las necesidades de diseño en ellas.

d) *Amenazas Lógicas*

Desde un error de programación hasta un código malicioso no ejecutado, las amenazas lógicas representan, junto con las humanas, las más comunes fuentes de amenaza para una red de datos.

Un error de programación es un problema existente en el sistema desarrollado, el cual no ha sido encontrado o depurado por los analistas. Estos errores de programación a menudo representan negaciones en los servicios de la red, lo cual puede llevar a pérdidas del tipo económico. Piense en un error en la autenticación de un usuario en una conexión remota, si este error permite la entrada al sistema sin la validación adecuada, un atacante podría entrar al sistema y registrarse como usuario autorizado. Por otro lado, un error en el módulo de cambio de contraseña podría negar el acceso a un usuario autorizado y bien intencionado, con la premisa de que la contraseña proporcionada no es válida, dando como resultado una negación de servicio.

Los códigos maliciosos son todos aquellos programas informáticos diseñados para afectar a las redes de datos. Según el reporte de amenazas a la seguridad de Internet de Symantec, en el primer semestre del año 2007 se reportaron 212,101 códigos maliciosos nuevos, lo que implica un aumento del 185% con respecto al semestre anterior[16]. Esta cifra nos indica que los códigos maliciosos son un verdadero peligro para las redes de datos, entre estos encontramos a los Virus, los Gusanos, los Caballos de Troya y los Bots. Todos estos elementos maliciosos serán descritos a profundidad en el tercer capítulo.

e) Desastres Naturales

Son sucesos que no se pueden predecir a ciencia cierta y que pueden llegar a causar la destrucción completa de una red de Información. Tal es el caso del huracán Katrina, en el año 2004, el cuál destruyó más de la tercera parte de la infraestructura informática de la ciudad de Nueva Orleáns y cuyos estragos no

[16] Symantec Internet Security Threat Report, January-June 2007, Symantec, E.E.U.U. 2007 p 17

pudieron ser calculados antes de que tocara tierra en Estados Unidos.[17]

Estos desastres son de varios tipos: inundaciones, incendios, huracanes, terremotos, erupciones volcánicas, entre otros.

A este tipo de amenazas también se les conoce como actos de Dios (acts of God).

2.3 Vulnerabilidades

Habiendo hecho un análisis de las principales amenazas a la información, se debe conocer qué es lo que buscan explotar dichas amenazas, encontrar el posible hueco de seguridad o debilidad que pudiera poner en riesgo a la información de una red de datos.

Una de las definiciones más concretas menciona que "Una vulnerabilidad es un punto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo".[18]

Symantec encontró 2,461 vulnerabilidades en sistemas de información a lo largo del primer semestre de 2007, mostrando las brechas de seguridad que no se consideraban antes de ese periodo.[19]

Esto muestra que las vulnerabilidades existirán siempre. Mientras más se encuentre una persona o equipo cercano a cualquier tipo de interacción, sea una red de datos o cualquier aspecto de la vida diaria, la más vulnerable será la más propensa. La naturaleza del ser humano sugiere que siempre existirá una persona que tratará de buscar vulnerabilidades a explotar.

Acorde con López y Quezada se pueden citar las siguientes categorizaciones de las amenazas[20]:

[17] Huracán Katrina: la información continúa gracias a la red.
[18] López B., Jaquelina y Quezada R., Cintia, Ob. Cit. p100
[19] Symantec Internet Security Threat Report, January-June 2007, Symantec, E.E.U.U. 2007 p 52
[20] Ídem pp 100-103

a) Vulnerabilidades Físicas

Son todas aquellas que se presentan dentro del entrono físico donde se encuentra la red o sistema de información. Generalmente se asocia con el aseguramiento físico de los equipos que controlan a la red o al sistema de información. Básicamente se refieren al acceso presencial que pudiera tener un atacante en el seno mismo de la red. Para evitar vulnerabilidades de este tipo se implementan políticas y controles de acceso físico en las instalaciones de la organización.

Además del acceso físico a la instalación, una vulnerabilidad de este tipo incluye a los dispositivos físicos extraíbles, los cuales ya son de un tamaño reducido y con una capacidad asombrosa, lo que permite la extracción de información sin llamar mucho la atención.

b) *Vulnerabilidad Humana*

Las personas son susceptibles al compromiso de la información que poseen, utilizando técnicas como la ingeniería social, la cual se tratará a profundidad en el tercer capítulo de este trabajo de investigación. Generalmente estas vulnerabilidades obedecen a un esquema de descuido y desatención a los empleados de la organización, lo que puede provocar descontento, ignorancia o una mala relación entre los elementos de una empresa.

Se puede ejemplificar como aquel empleado de la compañía "A" el cual tiene a su cargo el control de acceso a las bases de datos del personal de la organización. Esta persona no tiene un conocimiento pleno del nivel de seguridad que deben tener estas bases y permite que cualquier persona que conozca utilice su computadora con acceso a la base para revisar correos electrónicos. Un atacante pudiera hacerse pasar por conocido de esta persona para acceder a la máquina sin ningún problema y obtener información sensible.

c) *Vulnerabilidades de Hardware*

Detalles tan sencillos como evitar dar mantenimiento a los equipos de una red representan un punto débil aprovechable por un

atacante. También dentro de este rubro se destacan los errores de fabricación o la falta de conocimiento del elemento de la red al momento de su instalación y operación.

d) *Vulnerabilidades de Red*

La promiscuidad de la información a través de redes tanto públicas como privadas, sugiere la existencia de un punto débil dentro de éstas. Si no se realiza un análisis sensible del tipo de seguridad a implementar en la red, se puede provocar que un atacante aproveche un recurso de la misma para provocar un daño. Ejemplo típico de esto son la intercepción de información que fluye a través de la red debido a la mala planeación de los elementos de seguridad y las vulnerabilidades en software que en conjunto existan con las de red.

e) *Vulnerabilidades de Software*

Las fallas en programación de los sistemas son con frecuencia los mayores causantes de caídas en una red o sistema. Mientras esto no ocurre tan seguido con el nuevo software, los programas más antiguos presentaban fallas en los mecanismos de seguridad, cuando se llegaban a implementar. Un equipo nuevo instalado en la organización pudiera no tener activado el servicio de autenticación, aunque hoy en día son más los equipos que cuentan con este servicio.

f) *Vulnerabilidades Naturales*

Dependen al cien por ciento de la ubicación y construcción del espacio físico de la red o sistema. Comprenden en sí los aspectos que no se contemplan en el diseño y construcción del espacio físico. No deben confundirse con las amenazas naturales, ya que las vulnerabilidades no engloban los actos de la Naturaleza en sí, sino lo que provoca que éstos afecten.

Por tanto, se puede concluir que las amenazas explotan vulnerabilidades para lograr un objetivo, en muchos de los casos, obtener información sensible de la organización o de una persona en particular.

2.4 Servicios de Seguridad

Mucho se ha hablado ya de lo que son las amenazas y las vulnerabilidades de una organización. De una manera global, en una red o en un sistema de información se busca brindar servicios a los usuarios y a los dueños de la información con el fin de garantizar los tres aspectos fundamentales de la seguridad Informática.

Estos servicios son generalizaciones de las herramientas utilizadas, es decir, son la noción general del tipo de protección que se quiere implementar en la red. Con base en esto se pretende conceptualizar el tipo de procedimiento que se requiere en la organización para poder proteger a la información de la red.

Considerando entonces servicios de seguridad de varios tipos, según lo que deseen implementar para proteger.

a) *Servicios de Confidencialidad*

Este tipo de servicios plantea que sólo la entidad que cuente con el permiso necesario pueda acceder a la información sensible. Por información sensible se entiende a los recursos informáticos que se encuentran almacenados en los dispositivos y el tráfico que fluye a través de la red; implicando esto que los Servicios de Confidencialidad no sólo regulen el acceso a la información almacenada, sino que también se regula el acceso al tráfico de la red.

Con base en esto se conocen dos tipos de Servicios de confidencialidad:

- Servicios de Confidencialidad de Contenido. Utilizan una técnica de cifrado para prevenir la interpretación de los datos por un tercero no autorizado. Como su nombre lo indica, afectan a la información en sí, cifrando todo el contenido.

- Servicios de Confidencialidad de Flujo de Mensaje. Ocultan a la información en bloques completos y no por contenido,

previniendo que por observación se obtenga información del emisor y el receptor de la información.

Se puede ver a estos servicios como un sistema de llave-cerradura, en el cual la llave representa un elemento imprescindible para el acceso a la información; es decir, que la entidad que cuenta con esa llave puede acceder a la información. Esto lleva a plantear el problema de que los servicios de confidencialidad se corrompen si la llave de acceso es comprometida, es decir, una persona o entidad que no tiene el permiso lo obtiene, porque obtuvo la llave que permite el acceso.

Como se menciona, para proveer estos servicios es necesario el cifrado de la información, de ahí que resulte fundamental la **criptografía** para poder implementarla correctamente y con certeza.

b) Servicios de Autenticación

Queda claro que no sólo se debe garantizar que la información sea confidencial, sino que también la entidad que tiene acceso a ella debe ser quien en verdad dice que es, esto es, que la entidad que desee tener acceso a la información compruebe su identidad. Por ello se emplea la autenticación, que según Mitch[21], es el proceso que verifica que las entidades son en verdad quienes dicen ser. Las entidades que puedan requerir autenticación son los usuarios, computadoras y procesos. En una red típica se realiza la autenticación durante el proceso de inicio de sesión donde un usuario introduce sus credenciales, usualmente un nombre de usuario y una contraseña.

No sólo es este tipo de autenticación el que existe, también se puede autenticar por algo que se sabe (por ejemplo, una clave secreta), por algo que se tiene (tarjetas o llaves físicas) o por lo que se es (huellas digitales o el iris). La información que proporciona la entidad es comparada con la información que el sistema de autenticación tiene sobre esa entidad.

[21] Tulloch Mitch, Microsoft Encyclopedia of Security, Primera Edición, Microsoft Press, E.E.U.U., 2003 p31

c) *Servicios de Integridad*

La integridad de la información se realiza a través de marcadores en la propia información, los cuales indican que ésta no ha sido alterada por alguna entidad que no sea la que creó la información misma o que tenga privilegios de modificación sobre ella. Para proporcionar este servicio se realizan métodos llamados mecanismos de detección de modificación, los cuales pueden afectar a la información bit a bit, por secuencia de mensajes o por mensajes en particular.

Se emplean técnicas como el código de detección de modificación, el cual es una suma para comprobar los datos a través de un algoritmo de cifrado. También existe el código de autenticación de mensaje, donde se realiza una suma de comprobación cifrada pero en el mensaje entero. Una de las técnicas más empleadas hoy en día es la Firma digital, la cual es un identificador del emisor y que se revisa cuando llega a su destino.

d) *Servicios de No Repudio*

El no repudio implica que no se rechacen mensajes transmitidos. Se puede dar el caso de que un mensaje del cual se comprobó su emisor, sea rechazado por el receptor debido a algún malentendido en la comunicación. Se aplica al problema de la denegación de servicio falsa de la información que se recibe de otros o de la que uno ha enviado a otros. Los servicios de no repudio suministran pruebas que pueden ser demostradas a una tercera entidad.[22]

e) *Control de Acceso*

Constituyen una importante ayuda para proteger a la información de la utilización o modificaciones no autorizadas; esto con el fin de mantener la integridad de la información y resguardar la confidencialidad de la misma de accesos no autorizados. Básicamente se encuentran tres elementos en todo mecanismo de

[22] López B., Jaquelina y Quezada R., Cintia, Ob. Cit. p.122

control de acceso, las entidades de red, los recursos de la red y los derechos de acceso.[23]

Una vez que la entidad se ha autenticado e iniciado sesión, el control de acceso limita al usuario la utilización del sistema. La manera más común de implementar este tipo de controles es a través de Listas de Control de Acceso (LCA o CAL), las cuales especifican una lista de protecciones de seguridad aplicadas a elementos informáticos, como una carpeta, un archivo o un proceso en específico. El control de acceso puede ser también administrado por medio de manejadores de políticas.

2.5 Mecanismos de Seguridad

Con la evolución de los sistemas de información, se desarrollaron técnicas para proveer de seguridad a todo el tráfico que se realiza en las redes de datos. Estos mecanismos se pueden implementar tanto física como lógicamente, originando un conjunto de herramientas enfocadas a proveer seguridad de tres formas generales.

a) Seguridad por Oscuridad

Origina la ocultación de la información como técnica de protección. Un ejemplo que resultará muy claro es el de los sistemas militares. Sólo filtran información acerca de cómo funcionan sus sistemas de información a personal que requiera expresamente esa información. Este tipo de seguridad incrementa la cantidad de esfuerzo que un atacante debe aportar para realizar un ataque al sistema, aunque a veces no sea suficiente para contrarrestarlo.

Es posible mantener un cierto nivel de seguridad por medio de la oscuridad en la información, pero no garantiza que un atacante no sepa cómo es que funciona el sistema que quiere atacar. Simplemente pudiera inferir el funcionamiento del sistema de información con el simple hecho de observar su comportamiento bajo condiciones *normales* y comparando resultados cuando se proporciona información que no es la esperada. El problema con este enfoque es que nunca funciona a largo plazo y una vez que se

[23] Ídem p.124

detecta una red, ésta se vuelve completamente vulnerable a ataques.

b) Defensa Perimetral

Las organizaciones refuerzan los sistemas perimetrales dentro de una red. Un ejemplo de esto es el aseguramiento de los routers de salida o el resguardo de la red detrás de un cortafuego o *firewall* que separa a la red protegida del exterior. Se asume que las defensas perimetrales son suficientes para detener un ataque de cualquier intruso, garantizando que los sistemas internos sean seguros.

Existen varias fallas en este concepto, este modelo no implementa protección alguna de los sistemas internos ante un potencial ataque desde dentro de la red *segura*. Otra es que la defensa perimetral puede fallar eventualmente; una vez que lo hace, los sistemas internos se quedan desprotegidos ante cualquier ataque.

c) *Defensa a Profundidad*

El enfoque más robusto para usar. Proporciona seguridad al asegurar y monitorear cada uno de los sistemas de la red; cada sistema es una isla que se defiende a sí misma, por verlo de una manera figurada. Se toman medidas extra para los sistemas perimetrales, pero la seguridad de la red interna no recae sólo en estos sistemas. Este enfoque es más difícil de alcanzar y requiere que todos los sistemas y los administradores de la red cumplan con su objetivo. La red interna es mucho más difícil de comprometer si un administrador comete un error de seguridad en el sistema. Además, la actividad de cualquier intruso dentro del perímetro sería más fácil de detectar que con los enfoques anteriores.

Los mecanismos a describir a continuación pueden entrar en cualquiera de los enfoques de implementación de seguridad mostrados y presentan un punto de vista objetivo del tipo de resguardo que proveen y ante qué es lo que protegen.

2.5.1 Mecanismos Físicos

La forma más elemental de protección de algo es la protección física. Es la implementación de herramientas tangibles con el fin de resguardar a la información.

Se emplea el concepto de *clave*, el cual es un elemento que permite el acceso a la información cuando se presenta. Esta *clave* puede ser un elemento externo a la persona o un rasgo físico que esa persona posee.

Muestra de éstos últimos son los dispositivos biométricos, los cuales permiten, a través de una característica física que una persona posee, el acceso a la información. La utilización de estos dispositivos significan un control mucho más estricto sobre los elementos físicos pero tienen como principal desventaja que pueden ser invasivos, es decir, violar la privacidad de una persona o hacerle sentir incómoda.

Los mecanismos de seguridad físicos presentan innovaciones tecnológicas considerables, pero también repercuten en el modo de actuar de los miembros de la organización, lo que a la larga presenta consecuencias como la incomodidad de los usuarios para utilizarla o su mal empleo. Además, la utilización de la información no siempre será presencial, sino que implicará el trabajo vía remota, haciendo inviables estos elementos.

Debido a estas razones es más conveniente implementar mecanismos que no requieran un acceso presencial a la información, de ahí surgen los mecanismos lógicos para protección de la información.

2.5.2 Mecanismos Lógicos

Los mecanismos lógicos generalmente son más prácticos de implementar que los mecanismos físicos y la gran ventaja que presentan es que pueden realizarse vía remota para acceder a la información sin mayores complicaciones más que el empleo de la red. Generalmente, una organización cuenta con más de uno de los siguientes mecanismos, con el fin de proveer la mayor seguridad posible.

a) Software para protección de Virus o Antivirus

Ayudan a proteger a las redes y a los equipos contra un número específico de código malicioso, incluyendo en él los virus. Estos programas asignan un nivel de amenaza a estos códigos basados en un criterio particular, en su mayoría es la velocidad de propagación o *infección* que tiene y el daño que provoca en el equipo o red infectado.

Muchos de los análisis son realizados a nivel de equipo pero también existen a nivel de red para poder monitorear la información que fluye a través de ella.

b) Filtrado de Tráfico y Cortafuegos *Firewall*

Analizan el contenido de las cabeceras del tráfico de datos de la red, así como el tipo de contenido que tiene cada uno de los paquetes. Contienen una serie de reglas que limitan el acceso y salida de la información a través de los puertos lógicos.

Generalmente se utilizan como barrera entre la red local y la Internet, lo que supone cierta vulnerabilidad si es que un código malicioso se ejecuta dentro del perímetro de seguridad marcado por el cortafuego.

c) Proxy

Los servidores Proxy son similares a los cortafuegos, ya que mantienen al tráfico no deseado lejos de la red local. Operando a nivel de software, un servidor Proxy intercepta el tráfico de salida a Internet, creando una *sesión* para posteriormente reenviarlo al destino. Cuando se envíen confirmaciones de envío, éstas se enviarán al Proxy y no a la máquina cliente, ocultando así la identidad del cliente.

d) Cifrado de Datos

El cifrado de datos representa uno de los métodos más confiables para el intercambio de información. Se define como todas aquellas técnicas que permiten ocultar la información por medio de algoritmos matemáticos, con el fin de que sólo las personas que lo envían y reciben puedan interpretarla.

En la actualidad se utiliza una c*lave* para poder generar el texto cifrado y la misma para obtener de nuevo el mensaje original; a este tipo de cifrado se le conoce como cifrado de clave compartida ya que se utiliza la misma clave para cifrar y descifrar.

Otras técnicas emplean dos claves distintas para el cifrado de la información, las cuales son empleadas por el emisor y el receptor de forma diferente para acceder a la información. Ésta es el cifrado de clave pública o asimétrica, ya que no se utiliza la misma clave para cifrar y descifrar, sino que se emplea una clave pública para cifrar y una clave privada para descifrar.

Algunos ejemplos de algoritmos empleados actualmente para realizar el cifrado de los datos son: DES, AES, RC4, RC5, MD4, MD5, SHA, curvas elípticas, entre otros.

Ahora bien, no sólo es el implementar medidas para la protección de la información la solución a las amenazas y vulnerabilidades de una organización y sus redes de datos, sino que también es necesario concienciar al personal de que estas medidas deben seguirse correctamente. Aquí es donde aparecen las políticas de seguridad.

2.6 Políticas de Seguridad

"Las políticas de seguridad son el conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de las mismas."[24]

[24] López B., Jaquelina y Quezada R., Cintia, Ob. Cit. p129

Aseguran que las medidas tomadas para proteger la información se implementen correctamente y consistentemente en toda la organización. Determinan qué recursos tangibles o intangibles se necesitan para proteger la información y cómo protegerla.

Si se implementan correctamente, proveen un área de trabajo donde los elementos de la organización pueden reducir los errores no reconocibles que pudieran aparecer. Establecer reglas ayuda a la organización a protegerse de la gran mayoría de las amenazas y vulnerabilidades descritas con anterioridad, lo cual las convierten en una herramienta efectiva de prevención y detección de errores de seguridad en la red.

Según la visión de Olguín Romo los elementos que deben contener las políticas de seguridad son las siguientes[25]:

- *Alcance de las políticas.* Es decir, indicar los sistemas, personas y lugares donde se aplican.

- *Objetivos de la Política*. Es una descripción del por qué se deben definir dichas políticas.

- *Responsabilidades por Servicios*. Incluir los niveles de responsabilidad del uso de los recursos informáticos.

- *Requerimientos Mínimos de Configuración*. Es saber lo que se necesita para implementar los servicios de seguridad.

- *Definición de Violaciones*. Plantear los casos donde se violan las políticas y las repercusiones que esto origina.

- *Responsabilidades de los Usuarios*. Con base en la información a la que tienen acceso se debe definir qué deben procurar hacer y no hacer.

- *Explicar Tomas de Decisiones*. Ejemplificar y demostrar que la seguridad de la información es prioritaria.

[25] Olguín Romo Heriberto, Ob. Cit. P 134

Las políticas de seguridad deben tener una actualización constante, debido a que el ritmo de la organización así lo requiere y el ritmo tecnológico lo demanda. El saber definirlas es la base de toda estrategia o marco de acción ante un ataque a la información.

Para poder formular políticas de seguridad, se deben considerar las siguientes cuatro áreas fundamentales:

- *Fiabilidad.* Las políticas deben proveer la confianza necesaria en los mecanismos de envío de información empleados. Además. Se debe garantizar que la información manejada dentro de la red sea la verdadera, esto es, garantizando la integridad de la información.

- *Acceso.* Controlar el acceso certifica que los usuarios autorizados serán los que manejen la información. Maneja tanto la integridad, como la confidencialidad de la información.

- *Constancia.* Representa la disponibilidad de la información cuando sea requerida. Las políticas deben proveer los mecanismos necesarios para respaldar la información de una red en caso de un ataque.

- *Responsabilidad.* Los análisis y monitoreos de la red deben ser revisados regularmente, con el fin de detectar y corregir posibles irregularidades en el comportamiento de la red. Permite el acceso directo a un área generadora de problemas potenciales.

Al momento de presentarse las políticas, se deberán plasmar en un documento específico, empleando un lenguaje claro y de fácil comprensión para los elementos de la organización a quienes van dirigidas.

Se pueden emplear diversas metodologías para la realización de políticas de seguridad, las cuales entran en los modelos abstractos (representan elementos simbólicos) y los concretos (representando elementos reales). A continuación se mencionan los modelos más populares.

- Modelos de Control de Acceso. Consisten en la especificación de las reglas de autorización a los recursos de un sistema.

- Modelos de Flujo de Información. Plantean la forma en que la información se intercambia entre los elementos de la organización.

- Modelos de Integridad. Proveen los mecanismos y conductas que permitan la protección de la información a modificaciones no autorizadas.

De acuerdo con López y Quezada, se deben considerar los siguientes aspectos para establecer una política de seguridad[26].

a) Es necesario especificar una filosofía básica. Lo más usual es indicar si las políticas serán permisivas (todo lo que no esté prohibido está permitido) o restrictivas (todo está prohibido excepto lo específicamente permitido). Se debe mantener una consistencia en el empleo de las filosofías.

b) Toda política debe ser holística, es decir, debe cubrir todos los aspectos relacionados con el sistema.

c) Debe proteger el sistema en todos los niveles: físico, humano, lógico y logístico. Se necesita asignar un dueño a cada equipo e información.

d) Debe tomar en cuenta los distintos componentes del sistema, así como la interacción entre los mismos. La creación de las políticas se debe realizar por todos los miembros de la organización, tanto el departamento de Informática como el Legal y de Recursos Humanos.

e) Debe tomar en cuenta el entorno del sistema.

f) Debe adecuarse a las necesidades y recursos de la organización, pensando en los usuarios sin ser necesariamente hostiles hacia el mismo.

[26] López B., Jaquelina y Quezada R., Cintia, Ob. Cit. pp 152-153

g) Al momento de redactarse, debe hacerse en un lenguaje claro y de preferencia ser de carácter positivo. Esto permite que el usuario entienda y acate mejor las políticas.

Sabiendo los factores que pueden causar problemas en la seguridad de la organización y más específicamente de las redes de datos, se puede entonces presentar en sí los ataques y cómo es que pueden llegar a afectar a nuestra red de datos.

Es necesario recalcar que los mecanismos de protección no tienen sentido de existir si no se comprende a fondo la necesidad de ellos, es decir, si no se comprende para qué se quieren implementar. Teniendo conocimiento de esto, se pueden elaborar entonces políticas de seguridad que garanticen y planteen el marco sobre el cual se van a realizar los mecanismos de seguridad y proveer la mayor cantidad de seguridad posible a la información.

Capítulo 3

Ataques Contra la Información

3.1 Definición

En el ámbito informático se le denomina *ataque* a la culminación de una amenaza explotando una o varias vulnerabilidades de la red de datos a través de la utilización de técnicas específicas.

Debe recordarse que la seguridad de la red no es absoluta, siempre existirán huecos en los sistemas de protección que podrían dar paso a que una amenaza atente contra los principios básicos descritos en el capítulo anterior.

Varios autores concuerdan en la existencia de dos tipos fundamentales de ataques.

- *Ataques Pasivos*. Estos ataques son difíciles de detectar debido a que no existen rastros que puedan permitir el monitoreo o la detección. El objetivo principal de los ataques pasivos es obtener información sensible, sin modificarla.

- *Ataques Activos*. Emplean una mayor cantidad de mecanismos sobre la red, por lo mismo son más sencillos de detectar, pero pueden ser mucho más devastadores para la organización. Se realiza una modificación de la información, por lo que se puede detectar cuando se realiza o después de realizada.

Dentro de esta clasificación entran todos los ataques a explicar más adelante. Como se puede entender, es necesario que el atacante, perpetrador, tercera entidad maliciosa o cómo se le describa a lo que quiere atentar contra la información, tenga acceso a alguno de los elementos de la red de datos, de manera presencial o remota.

Existen otras clasificaciones de los ataques basadas en la repercusión que tienen en el flujo de información. Con base en lo planteado por López y Quezada, se presenta la tabla 3.1 con la descripción de estos ataques[24].

[24] López B., Jaquelina y Quezada R., Cintia, Ob. Cit. pp103-105

Tabla 3.1 Clasificación de los Ataques según su repercusión en el flujo de información

Ataque	Contra que atenta	Descripción
Interrupción	Disponibilidad	Es la eliminación o la exclusión de un elemento de la red.
Intercepción	Confidencialidad	Acceso no autorizado de la información de un elemento de la red.
Modificación	Integridad	Alteración de los datos almacenados o transferidos por un elemento de la red.
Suplantación	Autenticación	Es la falsificación de un elemento de la red con la intención de conseguir acceso

Aquí se puede apreciar que la base de todo es acceder a la información, ya sea para negarla a otras entidades o para modificarla a beneficio del atacante.

Combinando ambas clasificaciones se puede deducir que los ataques activos son aquellos que atentan contra la confidencialidad, integridad y autenticación; y que los ataques pasivos básicamente atentan contra la confidencialidad de la información.

Una última clasificación que es muy utilizada en el medio informático es la que especifica el tipo de ataque que realizan[25]:

- *Ataques de Reconocimiento.* Son aquellos ataques donde se recolecta la mayor información posible sobre la red o sistema, como las direcciones de red, la topología, los sistemas operativos utilizados, conocer el tipo de aplicaciones que manejan. Estos ataques buscan fundamentalmente vulnerabilidades de la red o sistema.

[25] Paquet Catherine, Saxe Warren, Ob.Cit. Sección Categories of Attacks

- *Ataques de Acceso.* Se les considera a estos ataques como los más directos contra la red. Utilizando la información recolectada por los ataques de reconocimiento, para penetrar al sistema y explotar vulnerabilidades. Son actos no mitigados de acceso no autorizado al sistema.

- *Ataques de Negación de Servicio (DoS).* A diferencia del ataque de acceso donde el atacante busca penetrar las defensas de seguridad de la organización, en un DoS el objetivo es sobrecargar el sistema de alguna manera para poder evitar que provea el servicio que debiera. Pueden ir desde consumir el ancho de banda de la red, hasta el aislamiento de elementos en específico.

Los ataques en general contemplan tres etapas para su realización.

a) Planeación. Se recaba la información necesaria para poder llevar a cabo el ataque. Conocer la estructura de la red, los elementos que la conforman, en fin, recolectar información acerca de la red o sistema a atacar.

b) Activación. Es el momento en el que se realiza el ataque, es decir, cuando se intenta perpetrar o vulnerar la seguridad de la red. En este punto es donde el atacante hace uso de las vulnerabilidades recolectadas en la fase de planeación para conseguir su objetivo.

c) Ejecución. Es el objetivo que se logra después de realizado el ataque. Se llega a hacer el recuento de los daños causados por el atacante y averiguar qué información fue la que obtuvo, si era un registro de contraseñas o de correo electrónico, por ejemplo.

Con base en el concepto de ataque se puede entonces analizar las formas en que se afecta a la información, pero antes se debe sensibilizar de tal forma que se piense como un atacante, para poder comprender el fin de cada uno de los ataques y poder implementar una estrategia de seguridad adecuada en la red o el sistema.

Pero antes de describir a estos ataques es necesario hacer la diferenciación entre los términos más utilizados para describir a los atacantes de una red de datos.

a) Hacker. Es una persona dedicada al estudio y la investigación de tecnologías informáticas. Basa su motivación para realizar ataques en la premisa de alcanzar un conocimiento y satisfacción por burlar los perímetros de seguridad. En sentido estricto, un hacker no realiza ataques por dinero o remuneración alguna, simplemente por la satisfacción de realizarlas y por el aprendizaje derivado de este ataque.

Este término es el más deformado de todos, ya que generalmente se piensa que un hacker es cualquier persona que realiza ataques, concepto que, como se puede apreciar, es completamente erróneo ya que un hacker puede apoyar a las organizaciones para referirles sus brechas en la seguridad de la red o de un sistema en específico.

b) Cracker. Este tipo de personas se dedican a la informática con el fin de realizar un daño a otros. Generalmente está motivado por intereses económicos. La actividad de acceder al modo en que los programas funcionan para poder obtener un beneficio se le conoce como *cracking*.

c) Script Kiddies. Se emplea este término peyorativo contra aquellos individuos que utilizan herramientas de *cracking* disponibles por la Internet. En su gran mayoría son adolescentes que tienen un conocimiento medio-básico de las tecnologías informáticas y realizan los ataques para conocer cómo es que funcionan.

d) Lammer. La categoría más baja de todas. Describe a aquella persona que dice conocer mucho sobre ataques y técnicas de intrusión sin realmente conocerlas. Emplean cualquier herramienta que encuentren disponible para hacerse pasar por hackers o crackers.

Existen muchos más términos a personas que dicen relacionarse con los ataques, como los piratas, copyhackers, gurús, spammers, thrashers, newbie, entre otros.

3.2 Análisis de Ataques más comunes

Diariamente se realiza una cantidad incalculable de ataques a las redes de datos, los cuales forman parte de toda la clasificación de ataques vista con anterioridad.

A continuación se hace la descripción de los ataques más comunes en las redes de datos, presentando su definición, contra qué es lo que atentan y una breve descripción de cómo se realiza el ataque.

a) Ingeniería Social

Es la técnica más empleada por los atacantes por su *facilidad* de realización y por la gran cantidad de información que se obtiene a través de ella. Consiste en utilizar la persuasión o manipulación en vez de la tecnología para poder recabar información sensible para realizar un ataque mucho más dañino.

Dentro de las clasificaciones mostradas, encaja en los ataques pasivos y de reconocimiento. Atenta contra la confidencialidad de la persona a la que se le realiza el ataque, ya que por medio de abuso de confianza se puede obtener información que pueda emplearse para penetrar el perímetro de seguridad.

Presenta una variante, la *ingeniería social inversa*, la cual consiste en plantear a la víctima que el atacante es un ser de confianza, al cual se puede recurrir para resolver cualquier problema. Esto es aprovechado para acceder a la información que se desea obtener bajo la falsa idea de brindar un soporte.

La mejor manera de evitar la ingeniería social, es creando una cultura de seguridad entre los miembros de la organización, considerando como base las políticas de seguridad de la misma.

b) Suplantación de Identidad o *Phishing*

Es un ataque contra la identidad de una tercera entidad, donde se mandan correos electrónicos a la víctima o se realizan llamadas telefónicas, suplantando el nombre de la tercera entidad, solicitándole que llene formularios o conteste cuestionarios para así obtener información sensible como las contraseñas de acceso a un sistema o simplemente información personal.

En la actualidad se ha convertido en uno de los ataques preferidos para obtener información sensible. Generalmente el atacante se hace pasar por una entidad bancaria y pide al usuario -por medio de un correo electrónico falso- que se ingrese a un portal ficticio con apariencia similar al sitio real. Ya dentro del sitio ficticio se pide llenar formularios o confirmación de información, los cuales serán enviados al atacante para poder acceder a la información contenida en la cuenta bancaria. Otra forma es llamar al usuario a su casa para pedir información personal sobre cuentas bancarias, familia y demás información personal.

Según el estudio de Symantec de las amenazas de Internet del primer semestre del año 2007, se detectaron un total de 196,860 mensajes de phishing únicos, diferentes entre sí. También reporta que se bloquearon más de 2 300 millones de mensajes de este tipo en dicho lapso, siendo Estados Unidos, Alemania y Gran Bretaña los que cuentan con mayor cantidad de sitios Web de phishing[26].

Una opción para evitar estos ataques es el filtrar correos electrónicos a nivel de servidor dentro de la red, así como la implementación de bloqueos de DNS que no sean los verificados por la organización. Cuando se reciben llamadas de personas o instituciones solicitando información, se debe siempre averiguar sobre la autenticidad de la llamada. Un método sencillo es la colocación de identificadores de números telefónicos y pedir a la persona que realiza la llamada que se identifique con su número de empleado.

[26] Symantec Internet Security Threat Report, January-June 2007, Symantec, E.E.U.U. 2007 p 103

c) Fisgoneo o *Sniffing*

Se define como la captura y análisis del tráfico de una red. Implica el acceso al canal de comunicación de la red y la intercepción de los datos que fluyen a través de ella. Existen varias aplicaciones capaces de obtener el tráfico de una red, lo cual puede ser aprovechado por el atacante para tratar de interpretar el contenido de la información obtenida y así lograr obtener información sensible.

Es un ataque pasivo el cual es, en muchos casos, imposible de detectar, ya que no se afecta el flujo de la conversación entre los miembros de una red, sino que se capturan los paquetes sin modificarlos. El atacante recaba la información contenida en cada uno de los paquetes transmitidos con la finalidad de encontrar información como contraseñas o incluso texto en claro (es necesario recordar que algunos protocolos no manejan el cifrado de información, lo que implica que ésta viaja en claro a través de la red). Un típico ataque de fisgoneo es el que se muestra en la figura 3.1, donde se muestra un caso específico de sniffing a una red inalámbrica.

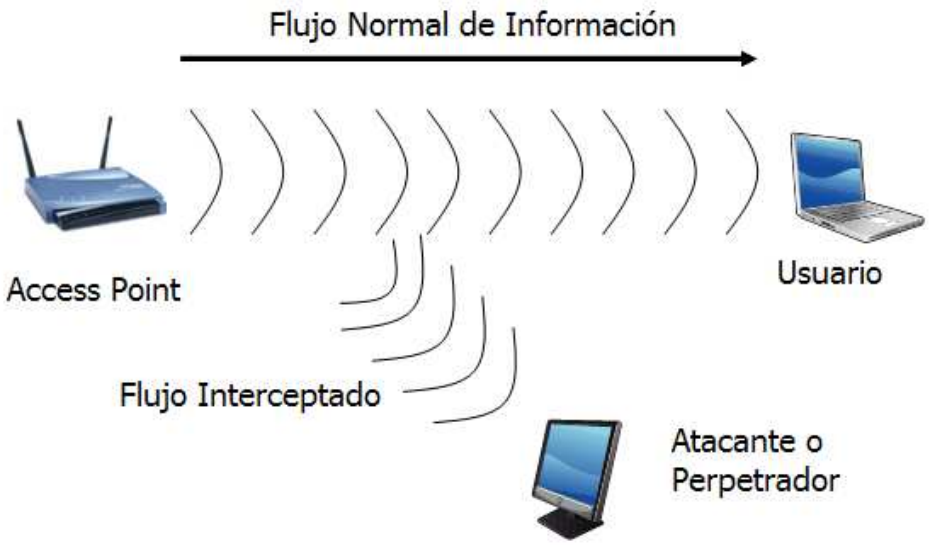

Figura 3.1 Esquematización de un ataque por sniffing

Es necesario destacar que el análisis del tráfico de una red no representa un riesgo si se realiza por personal autorizado para ello y con el fin de monitorear el rendimiento de la red de datos.

Para prevenir que personas no autorizadas tengan acceso a la información que fluye a través de la red se implementa el cifrado de los datos. En la época actual es muy común la promiscuidad del flujo de información de las redes inalámbricas, para asegurar su protección se implementan mecanismos de cifrado como WEP (*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access* o acceso protegido a Wi-Fi) y WPA2.

Además, se utilizan mecanismos de autenticación como EAP o TKIP, los cuales permiten garantizar la transferencia de datos a través de estas redes inalámbricas por los miembros autorizados. También se pueden emplear sistemas de detección o de prevención de intrusos (IDS o IPS) los cuales detectan cualquier posible intromisión al canal de comunicación de la red.

d) Ataques por virus

Se entiende por virus a todo código malicioso que afecta a los archivos, dañándolos, destruyéndolos u ocultándolos del usuario. Existen muchas clasificaciones de virus, entre ellas la de Tulloch, que muestra las siguientes observaciones[27]:

- Virus de Sector de Arranque: Infectan el arranque de una computadora, provocando que se carguen en memoria cada vez que se inicia el sistema.

- Virus de Archivo: Son llamados también programas parásitos, los cuales se adjuntan a programas ejecutables y se cargan en memoria cuando éstos lo hacen.
- Virus de Macro: Es un tipo específico de virus para los lenguajes macros como los de la suite Office de Microsoft. Infectan generalmente a los sistemas a través

[27] Tulloch Mitch, Ob. Cit. p358

de correo electrónico. Dado que se basan en aplicaciones, pueden ser multiplataforma, es decir, infectando diferentes sistemas operativos que corren las mismas aplicaciones.
- Virus Multipartito: Son combinaciones de los virus de archivo y de sector de arranque.
- Virus polimorfos: Son cualquiera de los virus anteriormente descritos, pero con la capacidad de mutar su propio código para hacerlos más difíciles de detectar y remover.

En el primer semestre de 2007 se detectó al virus Whybo, dentro de las redes de intercambio de archivos (generalmente P2P) el cual producía la descarga y ejecución de programas sin consentimiento del usuario. Este virus es considerado como el virus creado entre Enero y Junio de 2007 más peligroso. Infecta los archivos portables ejecutables de todas las unidades de disco, obteniendo un archivo cifrado y ejecutándolo en la máquina comprometida. Además de esto, abre ventanas dentro del ambiente gráfico con cadenas de texto referentes a aplicaciones de seguridad.

Teniendo como ejemplo a este virus, se puede determinar que son una amenaza muy considerable a la seguridad de la organización. Otro aspecto curioso de este tipo de código malicioso, es que se enfocan en su gran mayoría a los sistemas Windows, debido a la gran cantidad de equipos y redes conectadas con este sistema.

Para prevenir que se ejecute dentro de la red de datos, es necesario contar con mecanismos que detecten a estos elementos, estos elementos son los Antivirus. Mantenerlos actualizados debe ser prioridad de la organización, porque no sólo detecta virus, sino demás código malicioso, como los Caballos de Troya o los gusanos.

e) Ataques por Gusanos o *Worms*

Similares a los virus, estos códigos maliciosos presentan la característica de poder propagarse a otras redes de datos. Muchos gusanos simplemente se replican, saturando memoria y

consumiendo gran ancho de banda hasta negar los accesos de los usuarios legítimos a las redes. Algunos de estos gusanos son más dañinos e incluyen virus que pueden afectar a los archivos, destruyéndolos, mandándolos por correo electrónico o simplemente dejándolos inaccesibles al usuario.

A lo largo de la historia informática se han dado casos de gusanos que han pasado a ser tristemente célebres por el gran daño que causaron en las redes de datos y en los equipos a los que se propagaron. Algunos ejemplos de éstos son:

- *ADMw0rm*: Reportado en mayo de 1988, se considera como la base de la creación de los demás gusanos.

- *Code Red Worm:* El 19 de Julio de 2001 infectó a más de 359,000 equipos. Basa su ataque en vulnerabilidades del servidor Web de Microsoft IIS.

- *VBS/LoveLetter*: También conocido como gusano *I love you,* basa su funcionamiento en un script de Visual Basic que se propaga por correo electrónico. Cuenta con la característica de ser el primer gusano que explota la Ingeniería Social al máximo, ya que en el asunto del correo se encontraba el título *ILOVEYOU* o *te amo* en inglés. Se propagó por vez primera el 4 de mayo de 2000.

- *Gusano Melissa*: Se propaga a través del procesador de textos Microsoft Word 97, mandando correos electrónicos masivos en Outlook 97. Consiste en un virus de macro, el cual se activa al abrir el archivo infectado, recolectando las primeras 50 direcciones de correo electrónico de Outlook 97, para después mandarse a sí mismo.

- *Nimda*: Aparecido el 18 de Septiembre de 2001, se convirtió en el gusano propagado más rápido del mundo, afectando en 22 minutos a la gran mayoría de los equipos que atacó. Atacó vulnerabilidades de Microsoft IIS y se propagó por correo electrónico, redes P2P, sitios Web y por IIS.

Para poder prevenir y mitigar un ataque por gusano es necesario contar con mecanismos como el Antivirus y el firewall, los cuales pueden prevenir la entrada de estos códigos a través de puertos abiertos del equipo.

f) Caballos de Troya o Troyanos

Se distinguen de los virus y de los gusanos porque son sigilosos en su operación y ejecución, haciéndose pasar por programas y procesos legítimos. Además, no se propagan al mismo ritmo que lo hacen los gusanos.

Originalmente se le asignó el nombre de Troyano a código malicioso oculto en un programa legítimo. Actualmente son archivos ejecutables que son insertados en la red por los atacantes.

Pueden ser de varios tipos, dependiendo del tipo de acción que ejecuten[28]:

- *Robo de contraseñas*: Buscan las contraseñas guardadas en el equipo víctima y las envía por correo electrónico al atacante. Pueden realizar esto utilizando interfaces de programas legítimos para robar la información.

- *Registros de tecleo o Keystroke Loggers:* Monitorean toda las interrupciones de teclado del equipo, guardándose en archivos de texto plano que se envían por correo electrónico al atacante.

- *Herramientas de Administración Remota:* Permiten el acceso a todos los recursos del sistema víctima.

- *Zombies:* Provocan que el equipo víctima realice acciones que no son notificadas al usuario legítimo; generalmente coexisten atacante y víctima en el mismo equipo.

[28] Ídem p347.

Generalmente este tipo de código malicioso permite la entrada y ejecución de otra clase de códigos, como los virus y los gusanos. En su gran mayoría explotan las vulnerabilidades de una red o sistema para permitir el paso a demás aplicaciones dañinas.

g) Spam

Se ha convertido en la verdadera amenaza de la Internet y no existe una solución concreta contra el Spam. Consiste en el envío masivo de correos electrónicos no solicitados; estos correos electrónicos tienen la finalidad de anunciar productos o de atentar contra la información de una víctima (generalmente el phishing recurre al spam para el envío de los mensajes dañinos).

El problema principal del spam es de libertad de expresión y de la concepción de la Internet como un medio de propagación sin un control específico. De hecho se calcula que el 61% de todos los correos electrónicos de la Internet son spam[29].

Analizando con detenimiento el reporte de Symantec del primer semestre de 2007, se puede determinar que alrededor del 47% de todo el spam es generado en los Estados Unidos. Esto se debe a la gran cantidad de usuarios de Internet de banda ancha en ese país.[30]

h) Suplantación o Spoofing

Es el forzar paquetes de información dentro de la red para que aparenten ser de un cliente de confianza. Existen tres tipos básicos de suplantación:

- *Suplantación de Dirección IP:* Consiste en falsificar la dirección IP, modificando en cada paquete de información, el campo de dirección de origen de las cabeceras.

- *Suplantación de ARP:* El protocolo de resolución de direcciones es el encargado de interpretar las direcciones

[29] Symantec Internet Security Threat Report, January-June 2007, Symantec, E.E.U.U. 2007 p.107
[30] Ídem p. 107

MAC de las interfaces de red de los equipos. Este ataque consiste en utilizar una dirección MAC diferente de la original.

- *Suplantación de DNS:* El sistema de nombres de dominio es el encargado de traducir las direcciones IP de una computadora a los nombres entendibles por las personas. Cuando se realiza una suplantación de DNS se altera la traducción del nombre del host para redirigir al atacante.

  Considérese el sitio Web *www.sitiomuestra.com* con una dirección IP de *208.77.180.45*. Un atacante modifica las tablas de traducción de DNS para que un usuario que desee entrar a *www.sitiomuestra.com* sea dirigido a la dirección IP *199.45.15.13*, donde se encuentra una copia del sitio Web original donde el atacante es capaz de leer la información enviada por el usuario.

No debe confundirse el término *spoofing* con *phishing,* ya que éste último realiza el ataque a través de un correo electrónico mensaje instantáneo. Como medidas preventivas contra este ataque se pueden implementar medidas de seguridad robustas en los elementos activos de una red, así como la implementación de mecanismos como el firewall, que filtra y bloquea el tráfico hacia el interior de la red interna. De hecho, el *phishing* se vale del *spoofing* como técnica de ataque de reconocimiento.

i) Negación de Servicio Distribuida DDoS

Consiste en el envío masivo de peticiones a un servidor, las cuales provienen de varios hosts que intentan alcanzar al mismo servidor. En la gran mayoría de los casos, los equipos que realizan el envío de las peticiones son equipos comprometidos. Estos equipos fueron atacados por un gusano o por un virus, los cuales dejan en control a un equipo central, encargado de lanzar el ataque informando a los equipos el inicio del envío de peticiones. A los equipos comprometidos para realizar la negación de servicio distribuida se les conoce como *equipos zombie.*

El atacante manda una señal a las computadoras comprometidas previamente (Figura 3.2), las cuales comienzan el envío masivo de las peticiones al servidor víctima (Figura 3.3). Al no ser posible procesar tantas peticiones, el ancho de banda se consume y los usuarios auténticos no pueden acceder al servicio prestado por el servidor.

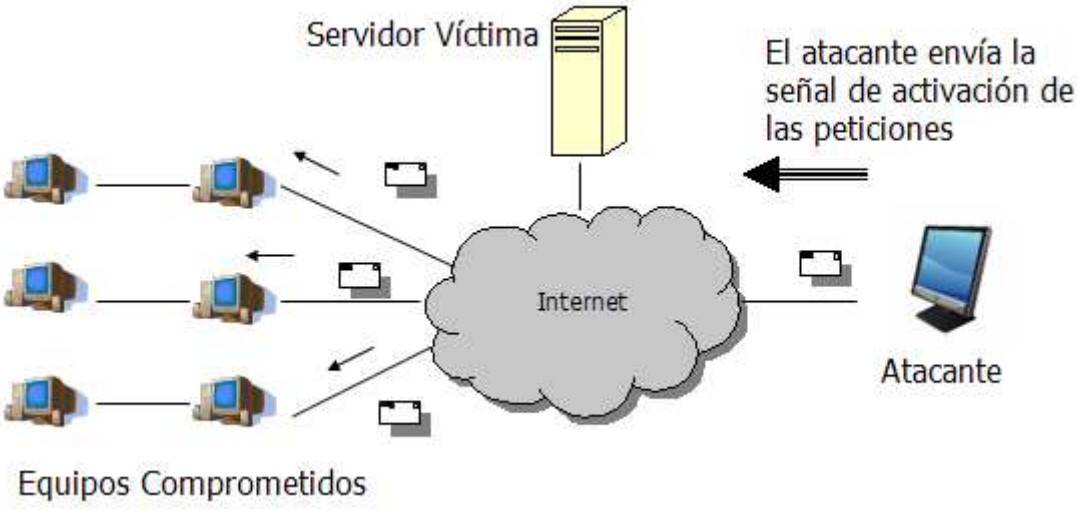

Figura 3.2 Envío de la activación de una DDoS

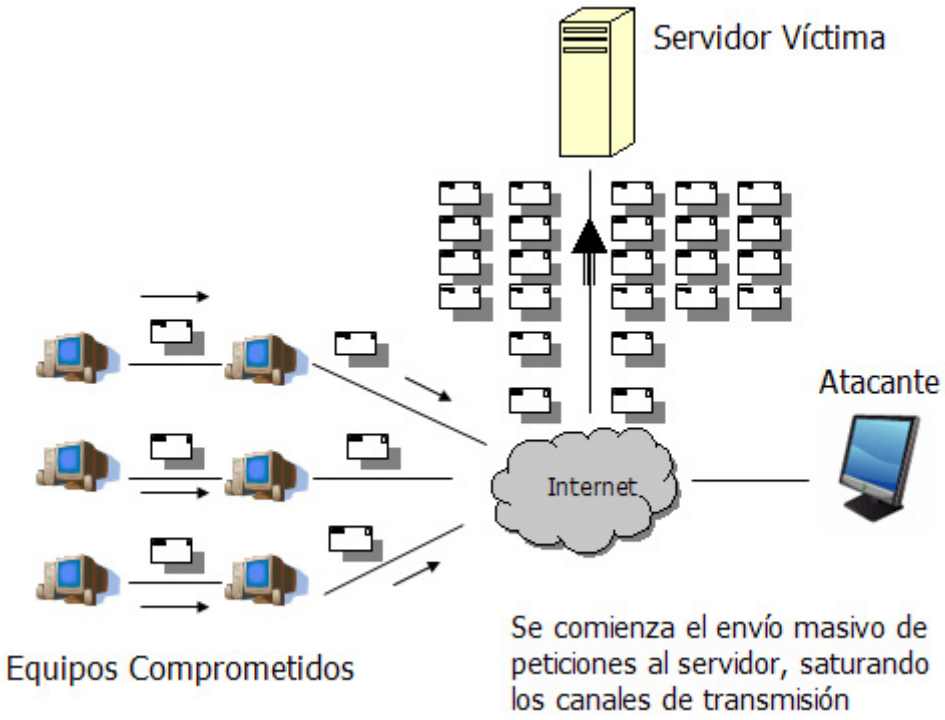

Figura 3.3 Realización de la Denegación de Servicio Distribuida

Se trata de ataques muy efectivos ya que casi siempre logran el objetivo de bloquear la comunicación, prevenir que se realicen es complicado. Lo que se debe tener es un adecuado control en caso de saturar el servidor para poder reestablecer el servicio de la manera más rápida posible.

j) Escaneo de Puertos

Se rastrea la cantidad de puertos abiertos en el equipo víctima con fines de reconocimiento. Para rastrear los puertos activos se utilizan métodos como:

- *Escaneo Vainilla o Vanilla scan:* Consiste en el intento de conexión del atacante a los puertos del 0 al 65,535 mandando paquetes TCP SYN a cada uno de ellos. Cuando se manda la respuesta se indica qué puerto es el que se encuentra *escuchando*.

- *Escaneo de estrobo o strobe scan:* El atacante busca conectarse a puertos comúnmente abiertos para los sistemas Windows o UNIX.

- *Escaneo UDP o UDP scan:* El atacante manda paquetes UDP vacíos a diferentes puertos de un rango de direcciones y espera a la respuesta. Cuando el sistema operativo responde con mensajes de error ICMP se detectan los puertos abiertos.

- *FTP bounce:* El atacante utiliza el protocolo FTP para poder intentar una conexión. Explota una vulnerabilidad en el comando PORT de FTP para poder detectar los puertos abiertos.

- *Barrido de puertos:* El atacante realiza un escaneo de una gran cantidad de direcciones IP en busca de un puerto abierto en específico.

- *Escaneo de FIN o FIN scan:* El atacante manda un paquete TCP FIN a algunos o todos los puertos de varias direcciones

IP. Si el puerto se encuentra cerrado se contesta la petición de FIN con un TCP RST que es un *reset* de la conexión. Si el puerto se encuentra abierto se perderá el mensaje ya que el puerto se encontrará en uso.

- *Escaneo Pasivo:* El atacante monitorea el tráfico de red en busca de puertos abiertos.

El escaneo de puertos puede ser detectado mediante la implementación de controles de detección de intrusos IDS o IPS. Además, un buen firewall puede mantener cerrado el acceso a puertos que no se estén utilizando.

k) Escaneo de Topología o Footprinting

Es otro de los ataques de reconocimiento más utilizados. Consiste en el proceso de recabar la mayor cantidad de información acerca de la red a atacar. El objetivo es obtener un mapa de la red para identificar los sistemas y aplicaciones que pueden ser sujetas a un ataque.

Se puede realizar de varias formas, las más comunes son por medio de envíos de mensaje de *ping*, lo que permite identificar miembros dentro del segmento específico de la red a atacar.

Otra manera de realizar el ataque es por medio de aplicaciones como Nslookup o Nmap, los cuales pueden rastrear e identificar las versiones de los sistemas operativos de los equipos.

Como consecuencia de este tipo de ataques, se realiza un registro de las aplicaciones que se manejan dentro de la red a atacar.

l) *Rootkits*

Son una serie de herramientas que se instalan en el sistema de la víctima con el fin de realizar varias funciones.

- Instalar *puertas traseras* para permitir la entrada al sistema comprometido sin ser detectado.

- Instalar caballos de Troya con el fin de capturar credenciales y *keyloggers,* crear canales de fuga de información, entre otros.

- Utilizar funciones del sistema operativo comprometido, como Mount y Cron.

- Instalar herramientas de administración remota para permitir el control del sistema de manera remota.

- Instalar controladores y filtros de paquetes de tráfico de red.

- Eliminar el contenido de los registros del sistema, para anular cualquier intento de detección. Generalmente éstos se realizan con la alteración o eliminación de programas que permitirían detectar a los intrusos.

Como se puede apreciar, estas herramientas funcionan una vez vulnerado el perímetro de seguridad de la red. El atacante realiza un ataque de reconocimiento con el fin de averiguar las vulnerabilidades del sistema y poder así implantar el *rootkit.*

En fechas recientes, se han detectado *rootkits* que se instalan en el *kernel* del sistema operativo. Se instalan a nivel de procesos del sistema y permanecen ahí ocultos. Generalmente se basan sobre las plataformas UNIX y Linux, añadiendo cualquier cantidad de procesos que realizan las acciones antes mencionadas.

m) Ataques a las contraseñas

Conocido también como *password cracking*, se define como la acción de averiguar las contraseñas de acceso al sistema. Esta actividad ha aumentado en los últimos años. El tratar de obtener una contraseña se puede realizar utilizando dos enfoques:

- *Ataque en línea u online*. Íntimamente relacionado con el *sniffing*, se obtiene la contraseña capturando las sesiones de autenticación. Es un proceso largo y complicado ya que depende del flujo de datos que exista en la red.

- *Ataque desconectado u offline*. Es más utilizado e involucra acciones que atentan contra los sistemas de una manera más activa, es decir, tratando de explotar abiertamente una debilidad en los repósitos de contraseñas para poder capturar la información deseada. Se le conoce como ataque desconectado porque se puede realizar en el equipo víctima.

Básicamente se basan en dos técnicas para obtener las contraseñas:

- *Ataques de Diccionario*. Se basan un compendio de palabras de diversas lenguas, utilizando una a una en el control de acceso.

- *Ataques de fuerza bruta*. Consiste en probar todas las posibles combinaciones de contraseñas del sistema. Es el más tardado ya que la contraseña puede ser robusta, saturando el tiempo de proceso del programa que realiza el ataque.

La mejor forma de evitar el éxito de estos ataques es empleando contraseñas seguras. Las contraseñas seguras son aquellas que no involucran una palabra en cualquier idioma y que contienen además caracteres alfanuméricos y especiales.

Un ejemplo de esto es lo siguiente:

La contraseña *Antonio* es muy vulnerable ya que contiene solamente letras, se encuentra en un idioma específico y puede ser fácilmente detectada por la Ingeniería Social. Si se quisiera utilizar una contraseña segura basada en esa misma palabra se sustituirían algunas letras por números y otras por caracteres especiales, obteniendo así la siguiente contraseña segura.

Contraseña Vulnerable:	Antonio
Contraseña Segura:	@n+0v!()

Por practicidad hacia los usuarios, existen herramientas que generan contraseñas seguras basadas en técnicas de revisión bit a bit. Generan las claves basadas en algoritmos que generan caracteres

pseudos-aleatorios, es decir, caracteres con un patrón específico que permite la máxima protección contra un ataque. Ejemplos de aplicaciones que generan estas claves son el *genpasswd* y *Gorilla Project.*

n) Virus fantasma o Hoax

La definición formal de *hoax* es toda aquella broma pesada o engaño. En el ámbito informático, se les asigna ese nombre a toda aquella amenaza de virus que resulta ser falsa.

Generalmente operan por correo electrónico, generando información acerca de un virus que no existe, alertando a los sistemas de seguridad de la red. El resultado que se obtiene es desviar la atención de los encargados de la seguridad de la red para poder realizar otro tipo de ataques sin ser detectados.

Representa un riesgo considerable a la organización, ya que se realiza un gasto de recursos humanos e informáticos para detectar algo que no existe. Ejemplos claros de ataques de este tipo son las cartas cadena alertando la existencia de un virus nuevo; son fácilmente detectables pero siempre existirá un elemento en la organización que sea engañado por ellos.

o) Ataque del Hombre en Medio o Man in the middle

Consiste en la suplantación del emisor y del receptor de un canal de comunicación. El atacante intercepta una sesión de comunicación segura para obtener información que le permita hacerse pasar por las dos entidades de la comunicación.

Para que un ataque de este tipo se cumpla, el atacante debe acceder al canal de comunicación para poder capturar la información cuando se establezca la comunicación segura entre las partes. Además el atacante debe ser capaz de realizar la intercepción de esos mensajes y reenviarlos a su destino original, con el objeto de no entorpecer la comunicación. Su representación se puede observar en la figura 3.4.

Figura 3.4 Esquematización de un ataque *man in the middle*

Se pueden prevenir los ataques de *hombre en medio* si se emplean métodos criptográficos que aseguren que la información no pueda ser entendida más que por las entidades autorizadas para ello. Mecanismos como las firmas digitales pueden detectar la presencia del atacante ya que las firmas digitales son únicas y dependen de la información del emisor y receptor.

p) Adware

Son programas que se instalan en el equipo víctima de manera involuntaria y despliegan anuncios de publicidad cuando se navega por Internet.

Es un tipo de software que se instala cuando se hace uso de programas gratuitos de Internet o de programas P2P. El mayor problema de este tipo de programas es que no existe un control ni notificación hacia la víctima de que estos programas van a instalarse. Se asocian con el *Spyware* y monitorean los hábitos de navegación de Internet de la víctima.

Troyanos como *Vundo,* instalan aplicaciones adware para desplegar publicidad e información acerca del atacante.

q) Spyware

Consisten en aplicaciones que monitorean la actividad de la computadora. Esto incluye sitios Web visitados, programas utilizados e información confidencial acerca del usuario en sí.

Todo este proceso de envío de información se realiza de manera oculta al usuario, lo que implica la creación de huecos en la seguridad del sistema que pueden ser explotados para generar otros ataques.

Junto con el Adware, forma parte de una de las nuevas plagas de Internet, propagándose a través de la descarga de código gratuito, potencialmente inseguro y por el empleo de programas P2P.

Los ataques aquí mostrados no son los únicos que pueden presentarse, sino que son los más representativos, al mostrar de qué manera se atenta contra la integridad, disponibilidad, confidencialidad o autenticación de la información.

La presencia del elemento humano en la realización de los ataques es algo que siempre se va a hacer presente. Se debe recordar que los diseñadores de software ni los usuarios son perfectos y que los programas creados por ellos tampoco lo serán, lo que debe implicar una sensibilización de los elementos de la organización ante estos posibles ataques.

Ahora bien, no sólo son los miembros de la organización los que deben conocer los riesgos a los que se exponen al conectarse a las redes de datos, en especial la Internet. Datos del primer semestre de 2007 confirman que los usuarios finales fueron el 95% del total de sistemas atacados[31].

Es necesario hacer mención que los ataques generan grandes pérdidas a las organizaciones y a los usuarios finales, no sólo pérdidas financieras, sino de información, ya que los datos comprometidos en muchos de los casos se pierden imposibilitando al miembro de la organización o al usuario final realizar su labor.

Pero, ¿contra quién se realizan éstos ataques? Se ha mencionado a organizaciones y usuarios finales pero es menester hacer mención de los principales blancos de los atacantes. Symantec revela que las

[31] Symantec Internet Security Threat Report, January-June 2007, Symantec, E.E.U.U. 2007 p 5

organizaciones más atacadas son las diez primeras compañías de los Estados Unidos[32].

- Wal-Mart
- Exxon Mobil
- General Motors
- Chevron
- Conoco Phillips
- General Electric
- Ford Motor
- Citigroup
- Bank of America
- American Internacional Group

En su conjunto, representan alrededor del 4% del total de ataques realizados. Un atacante escoge como blanco a este tipo de empresas ya que puede acercarse a víctimas indirectamente explotando entidades de confianza y aprovecha el nivel de seguridad alcanzado al perpetrar en la red para atacar a las verdaderas víctimas.

Es necesario que las organizaciones tomen medidas para proteger la información transferida en sus redes de datos y sobre todo, saber qué protección es la que presenta la ley para castigar a los responsables de los ataques.

Para lograr este objetivo, se abordarán en el siguiente capítulo las directrices del manejo de la información en un nivel técnico jurídico

[32] Idem p 9

con la finalidad de entender cómo es que el marco jurídico protege a la información, ya que debe recordarse que es información personal la que se puede perder en un ataque, o incluso perder la identidad al ser suplantada por otra persona para beneficio de terceros.

Aquí surgen interrogantes, ¿es posible regular la actividad de la red? Si es así, ¿quien debe regularla?, ¿Hasta qué punto se debe regular? Todas estas interrogantes encuentran su fundamento y su razón al conocer los aspectos que señalan la ciencia jurídica. Para ello es imperativo el haber comprendido cómo es que se realiza el intercambio de información en una red de datos, saber qué es lo que podría ponerlo en riesgo y qué se podría hacer para evitarlo.

Capítulo Cuarto

Legislación para el Intercambio de Información en México

4.1 Derecho Informático

El derecho informático es una disciplina en continuo desarrollo, forjada como una rama novedosa dentro del universo jurídico. Se puede considerar como orígenes de esta disciplina la obra de Norbert Wiener, quien expresa la influencia de la cibernética al ámbito jurídico.[33]

Esto se comprueba en los grandes intercambios comerciales, donde ocupa un lugar especial la transacción de bienes y servicios a través de redes de datos, aplicando parte de la teoría de las obligaciones y del derecho mercantil, el derecho internacional el cual es tema de debate actualmente en la Organización de las Naciones Unidas y pretende la codificación del derecho mercantil internacional a través de comisiones como las UNCITRAL. El derecho civil, en materia de derechos personalísimos, en el procesal en el capítulo de valoración de pruebas y ya no se diga sobre los soportes de la información que sirven para acreditar los ilícitos penales.

Todo lo anterior mencionado se puede considerar como la antesala del derecho informático el cual se puede entender por "El conjunto de normas y principios jurídicos que tienen por objetivo estudiar, reglar, definir e interpretar los distintos aspectos en que se relaciona la tecnología informática con una institución jurídica determinada en los diversos ámbitos del derecho"[34]

Es una rama de las ciencias jurídicas que considera al tratamiento lógico de la información como instrumento y objeto de estudio. A la visión de Téllez, se puede conceptualizar en Informática Jurídica y Derecho de la Informática.

4.1.1 Informática Jurídica

Se entiende por tal, a "la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la Informática general, aplicables a la recuperación de información

[33] Téllez Valdés, Julio, Derecho Informático, Tercera Edición, Mc-Graw Hill, 2005, p17
[34] Belmatrone Guillermo, Zavale Esquivel, El Derecho en la Era Digital. Derecho Informático de fin de Siglo, Primera Edición, Iures, México, 1997 p6

jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación"[35]. Visto de una manera mucho más clara, es el empleo de las computadoras en el Derecho.

Se originó por la necesidad de los juristas en emplear técnicas novedosas y vanguardistas de procesamiento de la información manejada, simplificando las labores de archivo y recuperación de toda clase de documentos de índole jurídica.

Ha permitido el desarrollo de un mejor entendimiento de los procesos y fenómenos jurídicos, lo que se traduce en el empleo de las computadoras y las redes de datos para simplificar la tarea del jurista.

4.1.2 Derecho de la Informática

Esta ramificación del derecho informático se emplea como instrumento regulador del fenómeno de la Informática en la sociedad, buscando la interpretación a los posibles daños o perjuicios realizables a través de medios informáticos.

En un sentido estricto, se define como todo aquel conjunto de normas, principios y leyes que pretenden regular la utilización de las tecnologías informáticas (tanto el uso de computadoras como el intercambio de información mismo en las redes de datos).

Por consiguiente, es de particular interés el análisis de las estructuras del Derecho de la Informática, ya que será quien regule los posibles daños o pérdidas a la información sensible de una organización. Provee en teoría, los mecanismos jurídicos imputables a los actos ilícitos perpetrados por elementos informáticos dentro de las redes de datos.

De aquí se desprenden para el análisis tres elementos sustanciales de la definición formal:

[35] Téllez, Ob. Cit., p19.

- *Principios* Refieren a aquellos postulados emitidos por los jueces, magistrados, tratadistas y personas estudiosas del tema.

- *Hechos* Son el resultado de un fenómeno inimputable al hombre y que refiere a la Informática. No intervienen las voluntades de las partes.

- *Actos* Resultado de un fenómeno Informático y que ha sido provocado por el hombre. Refiere a las acciones que realizan las personas a través de medios informáticos. Intervienen las voluntades de las partes para realizarlo y conlleva consecuencias de Derecho.

En específico, la concepción del Derecho de la Informática se desprende de un conjunto de disciplinas, denominadas fuentes del Derecho de la Informática.

A un nivel interdisciplinario, se encuentran en primer lugar las provistas por el Derecho mismo, donde se pueden referir lazos estrechos entre los fenómenos informáticos con el derecho en materia civil, penal, laboral, fiscal, de las obligaciones, comparado, entre otros.

Entre otras fuentes interdisciplinarias se encuentran ciencias y técnicas como la Ingeniería, Filosofía, Sociología, Economía, Estadística, Comunicación y muchas más áreas del conocimiento.

Todo esto lleva al análisis de las definiciones que la legislación misma hace en torno a los delitos informáticos, ya que se basan en esencia en el Derecho de la Informática, tomando a la Ingeniería como base para la definición de los conceptos y elementos técnicos que forman parte de dicho delito.

4.2 Delitos Informáticos

Los ataques contra las redes de datos constituyen una amenaza para la creación de una sociedad de la información más segura y de un espacio de libertad, seguridad y justicia. El hecho de considerar a

los ataques dentro de un marco jurídico referencial conlleva a la enunciación de éstos en la normatividad jurídica.

4.2.1 Definición

Antes de definir a los delitos informáticos, es necesaria la definición formal de delito, la cual, según el Código Penal Federal lo define como "el acto u omisión que sancionan las leyes penales".[36]

Realizar una definición concreta de los delitos informáticos es una tarea compleja; varios son los autores que han generado definiciones concretas para este tipo de delitos. Julio Téllez Valdés los define como "actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto típico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)".[37]

Según María de la Luz Lima, "el delito en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica, ya sea como método, medio o fin y que, en un sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".[38]

Si se analizan con detenimiento estas dos definiciones, se hace notar inmediatamente que se contempla el uso de las computadoras y, en general, los recursos informáticos como un método, medio o fin de la conducta ilícita.

Dentro de las características de este tipo de conductas se encuentran las siguientes:

[36] CFR Código Civil Federal, 16ª Edición, Ed. SISTA, México, 2006
[37] Téllez, Op. Cit., p163.
[38] Lima María de la Luz, Delitos Electrónicos, en Criminalia, México, Academia Mexicana de Ciencias Penales, Porrua, No. 1-6 Año L, Enero-Junio 1984, p100

- Sólo un determinado número de personas, con conocimientos específicos en informática y cómputo pueden llegar a cometerlos.

- Se plantean como acciones ocupacionales, lo que infiere que el atacante se encuentra en un trabajo al momento de realizar el ataque.

- Provocan una gran cantidad de pérdidas económicas a la o las organizaciones afectadas por el ataque.

- Ofrecen facilidades de tiempo y espacio, ya que pueden cometerse en cualquier momento y sin necesidad de estar físicamente en el lugar del ataque.

- Son muchos los casos y muy pocas las denuncias.

- Por su carácter técnico, son difíciles de comprobar ante las instancias jurídicas pertinentes.

- Tienden a ser realizados con mayor frecuencia dados los avances tecnológicos.

Dado a los diferentes usos de los medios informáticos, existen varias formas de clasificar a los delitos Informáticos.

4.2.2 Clasificación

Se puede utilizar la visión de los delitos informáticos, según dos grandes vertientes: como instrumento o medio y como fin u objetivo.

a) Como instrumento o medio

Utilizan los equipos y la infraestructura de red como un medio para alcanzar un fin en específico. Dentro de esta clasificación se encuentran los siguientes actos ilícitos.

- Falsificación de Documentos por medio de la utilización de software y su propagación en las redes de datos.

- Planeación o simulación de delitos *convencionales* como el robo, homicidio, fraude.

- Robo de capacidad de procesamiento de los equipos informáticos.

- Acceso no autorizado de información confidencial almacenada en formato electrónico.

- Aprovechamiento indebido o violación de un código para penetrar a un sistema (por ejemplo en la utilización de *exploits*).

- Penetración a sistemas bancarios con el fin de extraer recursos económicos de las cuentas.

- Uso no autorizado de programas de computadora, comúnmente conocido como piratería.

- Alteración voluntaria o involuntaria del funcionamiento de sistemas y redes (*cracking*).

- Intervención de las líneas de comunicación o los medios de transmisión en redes de datos (ejemplos claros el *sniffing* y el *eavesdropping)*.

b) Como fin u objetivo

Tienen como finalidad efectuar con éxito el ataque hacia los equipos de cómputo o las redes mismas, considerándose como la entidad física víctima.

- Denegación del servicio de un equipo.

- Destrucción de los programas almacenados en los equipos por cualquier medio.

- Atentado físico contra la máquina o red en específico.

- Sabotaje o terrorismo teniendo como objetivo las redes tanto públicas como privadas.

- Secuestro o robo de unidades de almacenaje de información.

De ahí la necesidad de implementar los mecanismos necesarios que lleven a asegurar el cumplimiento de los tres objetivos básicos de la información. Dichos mecanismos se implementan en la organización entendiendo la importancia de éstos ante cualquier posible ataque. Así mismo se deben definir las políticas de seguridad para poder proceder ante las instancias legales en caso de cualquier ataque.

El derecho penal de los estados interesados en combatir este nuevo tipo de conductas ilícitas, presenta grandes vacíos jurídicos y, sobre todo, diferencias sustanciales en la interpretación de cada uno de los ataques. Los autores de estos delitos deben ser identificados y llevados a proceso, con el antecedente de la creación de las penas necesarias que consideren los juristas adecuadas.

4.3 Legislación Mexicana

En nuestro país, se encuentran reguladas las acciones ilícitas referentes a los medios informáticos en el Código Penal Federal. No sólo es este código el que regula el intercambio de información a través de las redes de datos en México, se tiene además las especificaciones en materia de comercio electrónico y de propiedad intelectual, así como el acceso a la información manejada por los sectores públicos.

4.3.1 Constitución Política de los Estados Unidos Mexicanos

Conforme el estado de derecho prevaleciente en los Estados Unidos Mexicanos, se parte del principio rector que inspira y sustenta las normas del país y que es el de **supremacía constitucional.**

La doctrina es coincidente en que la norma de normas es la constitución y que sobre ella no existe ni debe existir poder que se

le oponga. Este principio se desprende del marco constitucional que establece categórico:

> "Artículo 133. Esta Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los Tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión. Los jueces de cada Estado se arreglarán a dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las Constituciones o leyes de los Estados."[39]

A partir de su interpretación se emanan los códigos, leyes y reglamentos que pretenden legislar los aspectos básicos de la conducta en México.

4.3.2 Código Penal Federal

Dentro de su libro segundo, título noveno, capítulo segundo, se plantea la regulación de los delitos informáticos dentro de la jurisdicción mexicana.

A continuación se listan los artículos que expresamente regulan el 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.

[39] Constitución Política de los Estados Unidos Mexicanos, Décima Novena edición, ed. ISEF, México, 2008 p.150

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." [40]

Analizando con detenimiento a estas prescripciones de la vía penal, se observa que en un modo general se encuentran cubiertos los posibles ataques a las redes de datos y a los equipos que los conforman, pero suponiendo que se detectara el ataque no se prevén de forma específica los medios de detección del ataque mismo.

A nivel estatal, se cuenta con una regulación importante de señalar. El estado de Sinaloa contempla dentro de su código penal el concepto de delito informático, concepto que en ninguna otra legislación penal mexicana aparece.

El artículo 217 del título décimo, capítulo quinto lo señala de manera puntual:

> "TITULO DÉCIMO
>
> DELITOS CONTRA EL PATRIMONIO
> …
> CAPÍTULO V
>
> DELITO INFORMÁTICO
>
> **ARTÍCULO 217.** Comete delito informático, la persona que dolosamente y sin derecho:
>
> I. Use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o
>
> II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.
>
> Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa."[41]

[40] CFR Código Civil Federal, 16ª Edición, Ed. SISTA, México, 2006
[41] Código Penal del Estado de Sinaloa, Título Décimo, Capítulo V, Artículo 217

Queda entonces el antecedente de que en México, el delito informático como tal existe sólo en un estado de la República, cuando debiera estar especificado en el código penal federal.

4.3.3 Código Civil Federal

En materia civil se contempla la existencia de los mecanismos informáticos para expresar el consentimiento de una persona, quedando reflejadas en los siguientes artículos.

> "Artículo 1803.- El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:
>
> I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y
>
> II.- El tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente."
>
> "Artículo 1805.- Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata."
>
> "Artículo 1811.- La propuesta y aceptación hechas por telégrafo producen efectos si los contratantes con anterioridad habían estipulado por escrito esta manera de contratar, y si los originales de los respectivos telegramas contienen las firmas de los contratantes y los signos convencionales establecidos entre ellos.
>
> Tratándose de la propuesta y aceptación hechas a través de medios electrónicos, ópticos o de cualquier otra tecnología no se requerirá de estipulación previa entre los contratantes para que produzca efectos." [42]

Como se hace notar, la utilización de medios informáticos aparece como un medio para el consentimiento de las partes, lo cual provee a la informática de una naturaleza meramente de medio o instrumento.

[42] Código Civil Federal, 17ª Edición, Ed. SISTA, México, 2008, pp 252-254

4.3.4 Ley Federal del Derecho de Autor

En esta ley se regulan de manera específica la protección de los programas y bases de datos, utilizando un certificado autoral expedido por el Instituto Nacional del Derecho de Autor.

A continuación se enuncian los artículos 101 a 114, que regulan dichas protecciones.

> "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 contenida 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." [43]

Aquí se ahonda de una manera más profunda el supuesto de la protección a la información de un programa de cómputo; recuérdese que los programas de cómputo pueden trabajar a nivel de red o a nivel de usuario, en cualquiera de los casos se presentan las regulaciones específicas.

4.3.5 Código de Comercio

[43] CFR Ley Federal del Derecho de Autor, Edición 2008, Ed. ISEF, 2008

Es probablemente la ley que más regulación y modificaciones ha recibido para poder contemplar lo referente al comercio electrónico. Desde el *boom* de la Internet se han realizado transacciones de manera electrónica, generando la necesidad de una regulación tanto internacional como nacional. El fin máximo de este tipo de legislación es proveer el marco jurídico necesario para proveer una protección al intercambio de bienes y servicios a través de las redes de datos.

Contempla principalmente lo referente a la *firma electrónica,* la cual describe Andrés Cámpoli como "aquella que a través de la utilización de procesos electrónicos permite la identificación positiva del emisor de un documento y aseguran su integridad y conformidad".[44]

Su principal utilización es en los *contratos electrónicos,* los cuales fungen como medidas reguladoras entre las partes que realizan un intercambio de bienes o servicios. Representa al elemento que garantiza que las partes se han identificado plenamente, garantizando uno de los aspectos fundamentales de la información, la confidencialidad.

En la medida que se automatizan los procesos de intercambio de bienes y servicios a través de las redes de datos, el contrato mismo entre las partes se realiza sin siquiera un conocimiento previo de éstas. Aquí es donde se vuelve fundamental el lograr que el documento probatorio o *contrato,* presente un mecanismo que garantice la autenticidad del mismo.

Haciendo referencia a las modificaciones realizadas al Código Federal de Comercio, se presentan varios artículos que describen las modificaciones hechas para dar entendimiento al comercio por medios electrónicos.

En el título segundo de esta ley se especifican tanto las disposiciones oficiales de los mensajes de datos, como los mecanismos de protección (firmas) y la regulación de las entidades encargadas de certificar dichos procedimientos de validación.

[44] Cámpoli Andrés, La Firma Electrónica en el Régimen Comercial Mexicano, Primera Edición, Editorial Porrua, México, 2004, p.8

El artículo 89 de este código refleja los principios por los que se rigen los mensajes de datos:

> "Artículo 89.- Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.
>
> Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa.
>
> En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, se deberán tomar en cuenta las siguientes definiciones:
>
> Certificado: Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.
>
> Datos de Creación de Firma Electrónica: Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, ~~a~~ con el fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.
>
> Destinatario: La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje.
>
> Emisor: Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.
>
> Firma Electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Firma Electrónica Avanzada o Fiable: Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97.

En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.

Firmante: La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.

Intermediario: En relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él.

Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

Parte que Confía: La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.

Prestador de Servicios de Certificación: La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.

Secretaría: Se entenderá la Secretaría de Economía.

Sistema de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos.

Titular del Certificado: Se entenderá a la persona a cuyo favor fue expedido el Certificado." [45]

Teniendo entonces definida por la legislación mexicana la percepción del mensaje, se genera el reconocimiento del mensaje de datos como elemento válido para todo proceso jurídico, tal como lo muestra el Artículo 89 BIS.

"Artículo 89 bis.- No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos."[46]

[45] Legislación de Comercio, Código de Comercio, 37ª Edición, Ed. SISTA, 2008, pp. 39 y ss.
[46] CFR Legislación de Comercio, Código de Comercio, 37ª Edición, Ed. SISTA, 2008

Como se ha podido observar a lo largo de este apartado, la legislación mexicana no es ajena al uso y regulación de la tecnología informática. Ahora bien, lo interesante es comparar la normatividad mexicana con las principales normatividades a nivel mundial ya que se vive en un mundo globalizado en constante cambio y cualquier régimen jurídico debe apegarse a estos cambios que cada vez son más frecuentes, especialmente en el ámbito informático.

4.3.6 Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

Si bien esta ley se considera como instrumento con que cuentan los ciudadanos para el acceso a la información que manejan las entidades gubernamentales, representa la base para la formalización y optimización de los mecanismos de protección de dicha información.

Los distintos numerales que integran la legislación en comento, demuestran el avance que México ha tenido frente a los demás países, lo que permite aseverar que tiene la intención de incorporarse al mundo informático global.

Esto invita a reproducir, aspectos relevantes de las disposiciones de la ley, y así enriquecer la materia substancial de la investigación que es la fusión de las tecnologías informáticas, como las redes de datos, con la ciencia jurídica.

> "TÍTULO PRIMERO
> DISPOSICIONES COMUNES PARA LOS SUJETOS OBLIGADOS
> ...
> Artículo 3. Para los efectos de esta Ley se entenderá por:
> …
> II. Datos personales: La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad;

III. Documentos: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico;"[47]

Determinada entonces la especificación de estos dos elementos, se plantea entonces la definición de información reservada y confidencial, dentro del Capítulo Tercero, comprendiendo los artículos 13 al 19. A continuación se reproducen los artículos trece y catorce:

"Capítulo III

Información reservada y confidencial
Artículo 13. Como información reservada podrá clasificarse aquélla cuya difusión pueda:

I. Comprometer la seguridad nacional, la seguridad pública o la defensa nacional;

II. Menoscabar la conducción de las negociaciones o bien, de las relaciones internacionales, incluida aquella información que otros estados u organismos internacionales entreguen con carácter de confidencial al Estado Mexicano;

III. Dañar la estabilidad financiera, económica o monetaria del país;"

IV. Poner en riesgo la vida, la seguridad o la salud de cualquier persona, o

V. Causar un serio perjuicio a las actividades de verificación del cumplimiento de las leyes, prevención o persecución de los delitos, la impartición de la justicia, la recaudación de las contribuciones, las operaciones de control migratorio, las estrategias procesales en procesos judiciales o administrativos mientras las resoluciones no causen estado."

"Artículo 14. También se considerará como información reservada:

[47] CFR. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Reglamento y decreto, Agenda de la Administración Pública Federal, 18° Edición, Ed. ISEF, apartado XXVIII, México, 2007.

> I. La que por disposición expresa de una Ley sea considerada confidencial, reservada, comercial reservada o gubernamental confidencial;
>
> II. Los secretos comercial, industrial, fiscal, bancario, fiduciario u otro considerado como tal por una disposición legal;
>
> III. Las averiguaciones previas;
>
> IV. Los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio en tanto no hayan causado estado;
>
> V. Los procedimientos de responsabilidad de los servidores públicos, en tanto no se haya dictado la resolución administrativa o la jurisdiccional definitiva, o
>
> VI. La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada.
>
> Cuando concluya el periodo de reserva o las causas que hayan dado origen a la reserva de la información a que se refieren las fracciones III y IV de este Artículo, dicha información podrá ser pública, protegiendo la información confidencial que en ella se contenga.
>
> No podrá invocarse el carácter de reservado cuando se trate de la investigación de violaciones graves de derechos fundamentales o delitos de lesa humanidad."[48]

Es de gran valor hacer notar las especificaciones que implica la confidencialidad de la información. Basándose en los principios discutidos sobre las características de la seguridad, el estado mexicano cuenta con las disposiciones necesarias para permitir el acceso a información sensible, sólo a personal autorizado y no a cualquier persona, como debe ser el manejo de esta materia, en donde se busca y se recomienda seguridad en las redes de datos.

[48] CFR. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Reglamento y decreto, Agenda de la Administración Pública Federal, 18° Edición, Ed. ISEF, apartado XXVIII, México, 2007.

Ahora bien, la información recopilada por el estado, a través de sus entidades gubernamentales, se debe manejar de una forma especial, para poder garantizar la confidencialidad de la misma. Dentro de esta ley se establece en el capítulo IV las especificaciones generales de la protección de datos personales.

Los mecanismos más generales se describen en los artículos 20 y 21, los cuales detallan a las entidades encargadas del manejo de los datos personales:

> "Capítulo IV
> Protección de datos personales
>
> Artículo 20. Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:
>
> I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61;
>
> II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
>
> III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61;
>
> IV. Procurar que los datos personales sean exactos y actualizados;
>
> V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y
>
> VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado."
>
> "Artículo 21. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo

> que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información."[49]

En síntesis, lo que esta ley provee, es de una base muy sólida con respecto al manejo de la información por parte del sector público. No sólo especifica la disposición de las entidades de gobierno a abrir cierta información a los ciudadanos que la necesiten, sino que también plantea los mecanismos y las adecuaciones necesarias para lograr discriminar a la información confidencial de la de libre acceso.

Pero, ¿de dónde surge la idea de regular la información almacenada en medios electrónicos y propagados por redes de datos? Surge de la imperante necesidad de un sistema de intercomunicación entre entidades. En algunos casos, las entidades no pertenecen a un solo país, sino que pactan entre ellos la manera de compartir la información que consideran *no sensible* , esto se debe en gran forma a que México no se encuentra aislado, se encuentra en una situación donde los países se interrelacionan con otros países, la llamada **globalización**.

4.4 México ante el mundo Globalizado

Un aspecto importante a analizar dentro de los grandes avances de la computación en su conjunto es la globalización, que se impulsa en el concierto internacional, por un sistema que propende entre otras cosas, al logro de la utilidad, sea cual fuera el medio; dentro de éste se encuentra el neoliberalismo el cual puede describirse como "un movimiento ideológico internacional, que enarbola la restauración de los valores originales del liberalismo: el individualismo, la propiedad privada como base de la libertad, el mercado que impone sus reglas en beneficio de todos, una visión del progreso que excluye los cambios estructurales bruscos."[50]

Ante esta visión del panorama global, la informática en general, se ha visto afectada de una manera positiva. Ninguno de los

[49] CFR. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Reglamento y decreto, Agenda de la Administración Pública Federal, 18° Edición, Ed. ISEF, apartado XXVIII, México, 2007.

[50] Semo Enrique, La Búsqueda, Primera Reimpresión, Océano, 2003, p.15

desarrollos en tecnologías de intercambio de información hubiera sido posible sin la cooperación e interrelación de expertos de todas las latitudes del mundo. Se experimenta una nueva revolución tecnológica, aquella que busca liberar a las personas de los trabajos y rutinas de orden físico para dar pie a la creación de elementos que simplifiquen la vida al máximo posible.

Es dentro de este contexto que México necesita realizar un estudio concienzudo de los mecanismos y regulaciones a implementar, con los mecanismos implementados en los países más avanzados en la materia informática. No debe aislarse en sus propias interpretaciones, debe basarse en modelos que pudieran funcionar y que han sido probados con éxito en otros países.

4.4.1 Legislaciones a nivel mundial

Dentro de las figuras legislativas, en el mundo se han estudiado dos perspectivas acerca de la seguridad de la información con mucho más detalle, los delitos informáticos y la protección de la información de los usuarios.

No es de extrañarse que se observen países denominados de *primer mundo* entre los pioneros en legislar estos aspectos informáticos, se puede observar con gran facilidad que por diversos motivos impulsarán siempre el desarrollo de tecnologías y de regulación en el uso de las mismas. A continuación se abordará en forma sucinta, los aspectos que regulan algunos países en esta materia, de lo que pueden apreciarse avances y retrocesos en la legislación mexicana, en relación al derecho comparado.[51]

a) Estados Unidos

Se adoptó en el año de 1994 el Acta Federal de Abuso Computacional. Dentro de esta acta se encuentran las especificaciones inherentes a la transmisión de programas, información, códigos maliciosos, redes, información, datos o programas. Representa un acercamiento más responsable, utilizando la descripción del acto de un virus en vez de su definición

[51] Téllez Valdés, Ob. Cit, pp 64-73, 171-180

formal, con el fin de obtener un antecedente para regular los ataques futuros por ese medio.

Existe una legislación muy concreta acerca de las estafas electrónicas por *phishing*, fraudes y otros actos dolosos perpetrados con ataques como los vistos en capítulos anteriores.

En lo referente a la protección de los datos personales, existe la Ley sobre la Protección de las Libertades Individuales de la Administración Federal de 1974[52], la cual enumera una serie de principios que garantizan la protección a la información privada de los ciudadanos de EE.UU. y representa la base para muchas legislaciones en el mundo.

b) Alemania

La Ley contra la Criminalidad Económica de 1986, contempla lo referente al espionaje de los datos, el fraude informático, la alteración de los propios datos y el sabotaje informático. Para la protección de los datos personales, la ley Federal del 21 de enero de 1977 para la protección contra el empleo abusivo de datos de identificación provee de la metodología necesaria para proteger a la información personal de los ciudadanos alemanes, además de contar con las legislaciones para cada uno los territorios federales.

c) Austria

Se sanciona a través del código penal federal modificado el 22 de diciembre de 1987 a todos aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de la elaboración automática de datos, a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso de procesamiento de datos. Además contempla las sanciones correspondientes para todo aquel que ejerciendo profesionalmente cause un daño a un tercero.

d) Canadá

[52] Fair Information Practice Principles

Dentro de la ley federal sobre la protección de las Informaciones Personales se muestran las características y procedimientos de sanción en caso de no respetar a la información personal.[53]

Impone obligaciones en alrededor de 150 departamentos federales de gobierno y a las agencias a respetar los derechos de privacidad al limitar la recolección, uso y permisión de información personal.

Otra ley federal canadiense que permite la protección no sólo a las personas, sino también a los documentos electrónicos es el Acta de Protección a la Información Personal y de Documentos electrónicos[54], documento en el cual se fijan las reglas que deben seguir las empresas privadas para el manejo correcto de la información personal para actividades comerciales.

Además de la legislación federal, cada una de las provincias canadienses mantiene su propio código de manejo de información personal, siendo las provincias de Alberta, Saskatchewan, Manitoba y Ontario las que cuentan con las regulaciones más claras y aprobadas tanto a nivel local como internacional.

Por considerar que esta legislación define avances substanciales en la materia de estudio, se considera pertinente incorporar un anexo donde aparece íntegramente la legislación.

e) Gran Bretaña

Tiene como base la Ley de Abusos Informáticos[55], la cual señala penas de hasta cinco años de prisión a aquel o aquellas personas que intenten con éxito o no, alterar datos informáticos. Posee una tipificación de los virus y sus sanciones, las cuales dependen del daño que causen dichos virus.

Fue originado en 1990 a raíz de un caso de acceso no autorizado. Robert Schifreen y Stephen Gold lograron acceder a los servicios de datos de la agencia de telecomunicaciones de Reino Unido a través de un ataque de *shoulder surfing,* obteniendo los nombres de usuario y contraseñas para poder entrar al sistema.

[53] Personal Information Protection and Electronic Documents Act 2000, c. 5
[54] Privacy Act for Canada
[55] Computer Misuse Act for the Great Britain

f) Holanda

Los *hackers, phreackers,* ingenieros sociales y los distribuidores de virus son sancionados mediante la Ley de Delitos Informáticos de 1993. También se encuentra definido dentro del código penal federal de Holanda.

Existe una ley de protección de la información aprobada el 23 de Noviembre de 1999, en la cual se señalan los principios en los que se debe regir el procesamiento, almacenaje y acceso a la información registrada por medios electrónicos en aquel país.

g) Francia

Se dictó la Ley relativa al Fraude Informático, en la cual se prevén penas de dos meses a dos años de prisión para toda aquella intrusión que genere pérdida o modificación no autorizada de los datos.

Establece también un tipo doloso y pena al mero acceso, agravando la pena si es que se modifican los datos de un sistema o equipo. Maneja el castigo o sanción para todo aquel intento de intrusión a una red de datos.

h) España

El Nuevo Código Civil de España establece la aplicación de uno a tres años de prisión a todo aquel que por cualquier medio destruya, altere, inutilice o dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos. A continuación se muestra el artículo 264 íntegro, el caso que se debe analizar está en la fracción segunda.

> "Artículo 264.
>
> 1. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriere alguno de los supuestos siguientes:

1. Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o puedan contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2. Que se cause por cualquier medio infección o contagio de ganado.

3. Que se empleen sustancias venenosas o corrosivas.

4. Que afecten a bienes de dominio o uso público o comunal.

5. Que arruinen al perjudicado o se le coloque en grave situación económica.

2. La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos." [56]

i) Leyes en América Latina

Existe un anteproyecto de ley en Argentina que plantea las penas y sanciones contra los delitos informáticos, mientras que en Venezuela se encuentran en discusiones las modificaciones al proyecto de Ley Especial Contra los Delitos Informáticos.

Dado el interés que despiertan estas tres legislaciones en específico, se han incluido en el Anexo II de este trabajo.

Dentro de estos esquemas globales existe una serie de acuerdos entre los gobiernos de la Unión Europea y los Estados Unidos, los cuales fijan una serie de procedimientos estándar para la protección de la información sensible de las personas. Este acuerdo se conoce como el **Safe – Harbor** o Puerto Seguro.[57]

Se plantea el asegurar el cumplimiento de esas normas en territorio de los Estados Unidos y de la Unión Europea, utilizando la

[56] Nuevo Código Penal Español
[57] Safe Harbor Privacy Principles

legislación específica para cada país en el que se desarrolle el intercambio de información.

Habiendo analizado estas legislaciones, se puede entender entonces que la seguridad de la información es un asunto de índole internacional, las instancias penales deberían de homologarse con el fin de mantener un balance entre las soberanías de las naciones. Si bien es cierto que la soberanía de los estados es un factor primordial, también es cierto que la cooperación internacional en materia de legislación es fundamental para comprender el fenómeno mismo de la globalización.

4.4.2 Comparativa entre la legislación mexicana y las más representativas a nivel mundial

Con relación al tema y para su enriquecimiento, se maneja para dar una panorámica de conjunto, un cuadro que refleja el qué, cómo y cuándo se manejan los mecanismos de acceso a la información de carácter electrónico, como los delitos informáticos a nivel mundial, en los países que al efecto se señalan (Tabla 4.1).

Tabla 4.1 Comparativa referente a la Protección de la Información[58]

	México	**Canadá**	**Holanda**	**Venezuela**
Legislación Base	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Reglamento y decreto (LFTAIPG) Ley Federal del Derecho de Autor (LFDA)	Acta de Privacidad (R.S., 1985, c P21)	Acta de protección de Datos Personales, 2000	Proyecto de Ley de los Delitos Informáticos de Venezuela

[58] Las legislaciones internacionales contenidas en este comparativo se encuentran en los Anexos I, II y III de este trabajo

Definición de Datos Personales	Artículo 2 Fracción II (LFTAIPG)	Artículo 3 Referente a la Información Personal	Artículo 1 Inciso A	Artículo 2 Inciso D
Definición de Documento o Archivo	Artículo 3 Fracción III (LFTAIPG)	No contiene definición	Artículo 1 Inciso C	Artículo 2 Inciso E
Información Reservada o Confidencial	Capítulo III Artículos 13 y 14 (LFTAIPG)	Artículos 21, 22 y 26	Artículo 43	Artículo 22
Protección de Datos Personales	Capítulo IV Artículo 20 Fracción IV (LFTAIPG)	Artículo 11 Referente a la Información Personal	Artículos 11, 12, 13 y 14	No contiene definición
Sujetos con Acceso a la Información	Capítulo I Artículo 2 (LFTAIPG) Artículo 101 (LFDA)	Artículo 12 Referente al Derecho de Acceso	Artículo 4°	No contiene definición
Procesado y Manejo de la Información	Artículo 9 (LFTAIPG)	Artículo 10°	Artículo 9	No contiene definición

A nivel de Delitos Informáticos, se ha elegido realizar la comparativa entre legislaciones de Latinoamérica. La razón es simple, las legislaciones latinoamericanas se basan en el Derecho Comparado y llegan a compartir preceptos y conceptos entre las mismas.

Tabla 4.2 Comparativa referente a los Delitos Informáticos[59]

[59] Las legislaciones internacionales contenidas en este comparativo se encuentran en los Anexos 1, 2 y 3 de este trabajo

	México	Argentina	Venezuela	Chile
Legislación Base	Código Penal Federal	Anteproyecto de Ley de Delitos Informáticos, Resolución 476/2001	Proyecto de Ley de los Delitos Informáticos de Venezuela	Ley Relativa a Delitos Informáticos No:19223
Modificación, Alteración o Destrucción de datos	Artículo 211 bis 1, bis 2, bis 3, bis 4, bis 5, bis 6 y bis 7	Artículo 2 y 3	Artículo 2	Artículo 3
Intercepción y Acceso No Autorizado	Inferido tácitamente en el Artículo 211	Artículo 1	Artículo 6	Artículo 2
Difusión Ilegal de Datos	Artículo 211 bis 2	Artículo 1	Artículo 11	Artículo 4
Sabotaje Informático	No especificado	Artículo 2	Artículos 7, 8, 9 y 10	Inferido tácitamente en el Artículo 3
Robo de Información	Artículo 211 bis 1, bis 2, bis 3, bis 4, bis 5, bis 6 y bis 7	Articulo 5	Articulo 13	Articulo 2

La mayor diferencia que salta a la vista del análisis de ambos cuadros, es la representación de la legislación mexicana en varias leyes. A nivel técnico, se podría considerar poco práctico, ya que la legislación se encuentra *dispersa* en una gran cantidad de leyes y disposiciones legales. Pero si se analiza a nivel jurídico, se puede observar que la legislación es eficiente en comparación a sus contrapartes extranjeras, sobre todo tomando en consideración la estructura jurídica, política y administrativa del estado mexicano.

Lo anterior, se puede explicar partiendo del análisis de la conformación del poder de la Federación; precisa la norma

fundamental: "Artículo 49. El Supremo Poder de la Federación se divide para su ejercicio en Legislativo, Ejecutivo y Judicial."[60]

Quiere esto decir, que los tres poderes se sirven del manejo de redes y de los avances de la tecnología, fundamentalmente de la informática, para lograr la eficiencia en el manejo de las funciones a su cargo.

Un simple asomo a la estructura de estos poderes, corroboraría lo que se está señalando; si se toma por ejemplo al poder Legislativo, se observará que las funciones a su cargo se manejan a través de la Ley Orgánica del Congreso de la Unión y de ésta se derivan diversas disposiciones que permiten la orientación adecuada del quehacer parlamentario, así como también de la función administrativa que tiene encomendada.

Aquí juega un papel importante la utilización de los sistemas de cómputo basados en redes de datos y por tanto el avance en este rubro, no deja dudas, sin dejar de un lado la Ley de Acceso a la Información Pública Gubernamental, que es prioritaria para el manejo de la estructura burocrática.

Esto no le es ajeno al poder Ejecutivo Federal, bastaría ojear la Ley Orgánica de la Administración Pública federal, para comprobar el sinfín de disposiciones, funciones y atribuciones que corresponden a la administración pública centralizada, paraestatal, que se complementa con la desconcentración a que alude al artículo 17 de la propia ley.

Bajo este tenor, se puede analizar la Ley Orgánica del Poder Judicial de la Federación, que sigue los senderos de la informática y de los avances de la ciencia y la técnica en la búsqueda de la seguridad y de la certeza jurídica que debe imperar en una adecuada administración de justicia.

Cabe advertir, que en cada poder de la Federación, de los estados que la integran y de los municipios, que son la base jurídica, política y administrativa del estado mexicano, cuenta con un sistema

[60] Constitución Política de los Estados Unidos Mexicanos, Décima Novena edición, ed. ISEF, México, 2008 p.54

integral de Informática, esto para poner a tono a la administración en el manejo de las redes, sin dejar también de lado a los avances sustanciales que sobre este rubro se encuentran en la alianza para el mejoramiento de la educación del pueblo.

Conclusiones

Ante la inminente incorporación de los órdenes jurídicos mundiales a la globalización, México no puede darse el lujo de pasar por alto los mecanismos reguladores a nivel mundial, de las redes de datos y de la información que se intercambia a través de ellas.

La apertura de las comunicaciones hacia todos los rincones del orbe, plantea la necesidad de contar con mecanismos jurídicos homologados internacionalmente, con el fin de mantener una claridad en las acciones reguladoras a aplicar en caso de cualquier ataque a las redes o a la información misma.

Es claro el hecho de que los avances de la informática a nivel técnico van ligados con los cambios a nivel jurídico entre los países, es evidente que el impacto de las tecnologías de cómputo en el ámbito comercial, social y jurídico es mayor en tanto avanza el tiempo.

Las redes de datos se encuentran en una constante evolución, todo ha cambiado a partir de aquellos Mainframes que controlaban todas las acciones de los clientes, los cuales trabajaban en estaciones *tontas.* Ahora las telecomunicaciones permiten una interoperabilidad e independencia de las plataformas a un nivel tal, que permiten la incorporación de tecnologías de todas las latitudes del planeta en cualquier momento.

El futuro de las conexiones de redes de datos tienden a un procesamiento distribuido, basando sus conexiones en servidores auxiliares, generando una gran *nube de información* en donde se permitirá compartir información entre cada vez más redes y equipos.

Debido a este desarrollo inimaginable de las tecnologías de las redes de datos, es necesario replantear en las organizaciones cuáles son las verdaderas amenazas que pudieran afectar a los activos de la misma. El mantener una actualización concreta de los conceptos teóricos de seguridad con los sistemas manejados a nivel mundial, marcarán la pauta para el planteamiento de

seguridad dentro de las organizaciones privadas y las entidades gubernamentales.

Ante esto, es menester mantener además la actualización constante de los procesos informáticos, así como la documentación de los ataques informáticos que se vayan desarrollando con el paso del tiempo. Es esencial decir que los atacantes se mantienen actualizados en cuestiones técnicas, por lo que las organizaciones públicas y privadas deben centrar sus esfuerzos de seguridad no sólo a proteger la información de sus redes con base en lo que conocen, sino explorar y documentarse tanto a nivel técnico como administrativo.

Bajo esta óptica, los cambios en el intercambio de información, surge la necesidad inherente de regular dichas tecnologías con el fin de lograr preservar las tres características principales de la información, la integridad, confidencialidad y disponibilidad.

Así, la legislación mexicana debe afrontar los retos que presenta la incorporación de la información en el ámbito global, de manera que pueda ser lo suficientemente capaz de responder ante cualquier eventualidad suscitada dentro de una organización en México.

En este contexto, el primer paso dentro de esta incorporación al mundo globalizado del intercambio de información, debería ser que se reconozca propiamente, en las instancias correspondientes, la necesidad de mantener actualizado el control normativo, para el manejo adecuado de la información, en todas sus aristas.

Se puede advertir, que la legislación actual dista mucho de ser perfecta, constituye el primer paso mencionado anteriormente para lograr un ambiente sano y seguro para los negocios y comunicaciones electrónicas en México.

Es un camino largo y sinuoso que debe recorrerse para poder colocar a México a la vanguardia de los países con tecnología de punta, para ser capaz de afrontar los problemas informáticos actuales.

La legislación mexicana, es prioridad en las políticas que se debaten en los cambios vertiginosos del mundo globalizado, por ello, en forma diseminada aunque incipiente y perfectible, se encuentra en las diversas ramas que inciden en los avances de la técnica y la ciencia, pero que hablan bien del quehacer del legislador.

La legislación mexicana, en la forma que se ha regulado por el poder Legislativo, para adecuar la normativa jurídica a los avances que se observan en el Derecho Comparado, responde a la pregunta que hacen los teóricos respecto al manejo de las redes que son el referente para que se califique al mundo en el siglo XXI, como una nueva era de globalización, que es la del *aplanamiento* de la tierra.

Glosario de Términos

Administrador Persona que supervisa y controla el correcto funcionamiento de un sistema informático.

ARP (Address Resolution Protocol) Es un protocolo utilizado para realizar un mapeo de direcciones IP con las direcciones físicas de un equipo.

ASCII Código (American Standard Code for Information Exchange) Estándar utilizado para representar la codificación de números, letras, dígitos y caracteres especiales.

Certificado Digital Estructura de datos creada y emitida por una autoridad certificadora, con el propósito primordial de identificar a un suscriptor de sus servicios.

Código Cuerpo de leyes ordenadas metódicamente.

Computadora Personal Tipo de computadora que se emplea para oficina, casa y diversos propósitos. Tiene una capacidad de procesamiento media y permite al usuario acceder a Internet y demás programas.

Copyhackers Falsificadores que obtienen lo que les interesa y se lo venden a alguien sin escrúpulos de tal manera que éste comercializa el sistema o programas posteriormente.

Criptografía Es el estudio de las técnicas para convertir información a una forma que no se puede entender sin conocimiento del método de transformación empleado.

Cron Es un servicio de programación de tareas en ambientes UNIX, empleado para especificar la ejecución de tareas en un momento determinado.

Delito	Es el acto u omisión que sanciona la ley penal.
Derecho	Conjunto de normas jurídicas que regulan la vida del hombre en sociedad.
Derecho Civil	Conjunto de normas jurídicas y principios que regulan las relaciones personales o patrimoniales entre personas privadas.
Derecho Penal	Es el conjunto de normas que regulan la potestad punitiva del estado, asociando hechos con sanciones, estrictamente determinados por la ley.
Derecho Procesal	Conjunto de normas jurídicas que regula la organización y atribuciones de los tribunales de justicia y la actuación de las distintas personas que intervienen en los procesos judiciales.
DNS	(Domain Name Server) Conjunto de protocolos y mecanismos que permiten la traducción de las URL en una dirección del Protocolo de Internet (IP- *Internet Protocol).* Por ejemplo, la URL www.sitiocualquiera.com se traduce en 192.168.92.45 en una red local.
EAP	(Extensible Autentication Protocol) Es una extensión del protocolo PPP definido en el RFC 2284. Es un protocolo de autenticación que soporta diversos tipos, incluyendo las contraseñas habituales, tarjetas de acceso, Kerberos, Certificados Digitales, entre otros.
Entorno de Seguridad	Conjunto de elementos importantes a los que se quiere brindar seguridad dentro de una organización.
Estación de	Es una computadora conectada a una red, la

Trabajo	cual interactúa con el *software* disponible en la propia red.
Firewall o Cortafuegos	Sistema que funciona como una *frontera* entre dos redes, el cual regula la entrada y salida de información hacia la red que se desea asegurar.
Firma Electrónica	Método de autenticación por medio de datos anexos o transformación criptográfica de una unidad de datos, que permite probar a emisor y receptor de la unidad de datos, la fuente y la integridad misma, protegiendo de posibles fraudes.
Gurú Informático	Atacante del mayor grado jerárquico. Generalmente es el autor intelectual de los ataques informáticos y se encarga de reclutar y entrenar *hackers* y *crackers.*
Hardware	Conjunto de elementos físicos materiales de los que se compone una computadora y, en general, un equipo informático.
HTML	(Hypertext Markup Language) Es un lenguaje diseñado para la creación de documentos de hipertexto, es la base de la creación de todas las páginas Web actuales.
IDS	(Intruder Detection System) Conjunto de programas y dispositivos que permiten la detección de actividades inusuales, incorrectas o anómalas en una red o equipo en particular.
Internet	Es un conjunto de redes públicas interconectadas entre sí, que utilizan los protocolos estandarizados para la transmisión de información a nivel global.
IP	(Internet Protocol) Parte de la suite de

	protocolos TCP/IP que es responsable de la transferencia de los paquetes de información en la red.
IPS	(Intruder Protection System) Conjunto de programas y dispositivos que detectan y toman acciones contra las posibles intrusiones no autorizadas en la red o equipo específico.
ISP	(Internet Service Provider) Empresa que provee al usuario final el acceso a la Internet a través de servidores de acceso remoto.
Ley	Es una norma jurídica positiva, de carácter coercitivo, general, obligatoria, abstracta y de vigencia indeterminada.
Linux	Estrictamente, es el centro o *kernel* de un sistema operativo basado en UNIX creado por Linus Torvalds en 1992. Actualmente se maneja como aquel sistema operativo que maneja al *kernel* desarrollado por Torvalds, existiendo una gran cantidad de sistemas desarrollados bajo esa plataforma, como por ejemplo Ubuntu, SuSE, RedHat, Fedora.
Macro	Conjunto de comandos que simplifican la ejecución de tareas en sistemas, a través de la automatización de las mismas.
Microsoft	Acrónimo de Microcomputer Software. Empresa estadounidense fundada en 1975 por Bill Gates y Paul Allen; dueña y productora de los sistemas operativos MS-DOS y Microsoft Windows, que son utilizados en la mayoría de las computadoras del mundo. De hecho es la proveedora del 50% de las aplicaciones de software a nivel mundial.
Microsoft IIS	(Internet Information Services) Suite

	desarrollada por Microsoft capaz de proveer servicio Web y de transferencia de archivos.
Mount	Comando UNIX que permite la preparación de un sistema de archivos para que sea reconocido por el sistema operativo.
Newbies	Atacante que no tiene mucho conocimiento en materia informática. Generalmente realiza ataques debido a la ignorancia, ya que descarga paquetes y los ejecuta sin saber su correcto funcionamiento con la intención de un fin específico.
Ping	(Packet Internet Groper) Es una utilizad de los sistemas operativos que permite el envío de paquetes de información para verificar la calidad o la existencia de la conexión de una red.
Piratas	Persona que comercializa y distribuye productos ilegales de software. No necesariamente conoce de informática.
Puerto Lógico	Son representaciones lógicas conformadas por un número de 16 bits que definen los puntos finales de una conexión dentro del protocolo TCP/IP.
Red	Sistema de comunicaciones de datos que permite a un número de dispositivos independientes comunicarse entre sí.
Red Centralizada	Topología de red la cual tiene uno o varios elementos como sistemas principales y de control.
Red de Datos	Conjunto de dispositivos conectados entre sí mediante un medio de transmisión para permitir la transferencia de información o

	compartir recursos de una manera confiable y eficiente.
Red Distribuida	Topología de red que se caracteriza por la ausencia de un centro de control en particular.
Registro del Sistema	Base de datos donde se almacenan las configuraciones y opciones de los sistemas Windows.
RFC	(Request for Comments) Son documentos donde se hacen las especificaciones referentes a un protocolo de Internet. Contienen las descripciones y los mecanismos de los que se conforman los protocolos liberados.
Script	Una serie de comandos escritos en un lenguaje para la automatización de ciertas aplicaciones en un sistema.
Software	Consiste en un código en un lenguaje máquina específico para un procesador individual. El código es una secuencia de instrucciones ordenadas que cambian el estado del hardware de una computadora.
Spammer	Persona o entidad que se dedica a enviar una gran cantidad de correo basura o *spam*. El spam es todo aquel correo que no es solicitado pero que de cualquier forma llega al usuario.
Suma Hash	Es un valor único calculado por un algoritmo bien conocido para crear un compendio del contenido de un archivo. Este valor es único y se calcula con base en la criptografía de clave pública.
TCP	(Transmision Control Protocol) Conjunto de protocolos que aseguran la transferencia

correcta de los mensajes de datos a su destino. Fue definido por el RFC 793.

Thrasher Atacantes que obtienen información sensible a través de analizar la basura y los desechos de una organización. Existe una variante que revisa las localidades de memoria en busca de código.

TKIP (Temporal Key Integrity Protocol) Es un Protocolo de seguridad utilizado en WPA. Consiste en un algoritmo mucho más robusto que WEP.

UNIX Grupo genérico de sistemas operativos que comparten determinados criterios en su diseño y por lo tanto son llamados de la familia (o tipo) UNIX. Son más de 100 sistemas operativos que se consideran de su familia. Sistema operativo multiplataforma, multitarea y multiusuario desarrollado originalmente por empleados de Bell de AT&T.

Usuario Individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático. Por lo general es una única persona.

WEP (Wired Equivalent Privacy) Es un protocolo de seguridad para medios inalámbricos, especificado en el estándar IEEE 802.11. diseñado para proveer un nivel de seguridad comparable a una red cableada. Actualmente no es tan seguro y se está remplazando por el WPA.

WPA (WiFi Protected Access) Especificación que plantea los mecanismos de cifrado y de autenticación para redes inalámbricas. Mucho más robusto que WEP.

Bibliografía Consultada

Belmatrone Guillermo, Zavale Esquivel, El Derecho en la Era Digital. Derecho Informático de fin de Siglo, Primera Edición, Iures, México, 1997

Canavan John, Fundamentals of Network Security, Primera Edición, Artech House, E.E.U.U., 2001

Cámpoli Andrés, La Firma Electrónica en el Régimen Comercial Mexicano, Primera Edición, Editorial Porrúa, México, 2004

Cole Eric, Krutz Donald, Conley James, Network Security Bible, Wiley Publishing Inc., E.E.U.U., 2005

Correa Carlos, Derecho Informático, Ediciones Depalma, Buenos Aires, Argentina, 1987

Daswani Neil, Kern Christoph, Kesavan Anita, Foundations of Security: What every Programmer needs to know, Apress, E.E.U.U., 2007

Dulaney, E., Edwards, M., Mar-Elia, D., McIntosh, R., Savil, J., Smith, R., A Guide to Group Policy, Primera Edición, Prenton Media, E.E.U.U., 2004

Elías Azar Edgar, La Contratación por Medios Electrónicos, Primera Edición, Editorial Porrua, México, 2005

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

López B., Jaquelina y Quezada R., Cintia, Fundamentos de Seguridad Informática, Primera Edición, U.N.A.M. Facultad de Ingeniería, 2006

Loosley Chris, Douglas Frank, High-Performance Client/Server, John Wiley & Sons, E.E.U.U., 1998

Molina Salgado Jesús, Delitos y Otros Ilícitos Informáticos en el Derecho de la Propiedad Industrial, Primera Edición, Editorial Porrua, Colección Breviarios Jurídicos, México, 2003

Muñoz Machado Santiago, La regulación de la red, Poder y Derecho en Internet, Primera Edición, Editorial Taurus, México, 2002

Nava Garcés Alberto, Análisis de los Delitos Informáticos, Primera Edición, Editorial Porrua, México, 2005

Olguín Romo Heriberto, Dirección, Organización y Administración de Centros de Tecnología de Información, Primera Edición, U.N.A.M. Facultad de Ingeniería, 2005.

Oram Andy, Peer to Peer: Harnessing the Power of Disruptive Technologies, Primera Edición, Oreilly & Associates, E.E.U.U., 2001

Paquet Catherine, Saxe Warren, The Business Case For Network Security: Advocacy, Governance, And ROI, Primera Edición, Cisco Press, E.E.U.U., 2004

Semo Enrique, La Búsqueda, Primera Reimpresión, Océano, 2003

Strebe Matthew, Network Security Foundations: Technology Fundamentals for IT Success, Primera Edición, Sybex, E.E.U.U., 2004

Sutherland Keith, Understanding the Internet: A clear guide to Internet Technologies, Primera Edición, Butterworth-Heinemann, Reino Unido, 2000

Téllez Valdés, Julio, Derecho Informático, Tercera Edición, Mc-Graw Hill, 2005

Tulloch Mitch, Microsoft Encyclopedia of Security, Primera Edición, Microsoft Press, E.E.U.U., 2003

Wang, Wallace, Steal this File Sharing Book, No Starch Press, E.E.U.U., 2004

Legislación Mexicana Consultada

Constitución Política de los Estados Unidos Mexicanos, Décima Novena edición, ed. ISEF, México, 2008

Código Penal Federal, Agenda Penal del Distrito Federal, 16ª Edición, Ed. ISEF, 2008

Código Penal para el Estado de Sinaloa, 2008

Código Civil Federal, 16ª Edición, Ed. SISTA, México, 2006

Legislación de Comercio, Código de Comercio, 37ª Edición, Ed. SISTA, 2008

Ley Federal del Derecho de Autor, Edición 2008, Ed. ISEF, 2008

Ley del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, 2008

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Reglamento y decreto, Agenda de la Administración Pública Federal, 18ª Edición, Ed. ISEF, apartado XXVIII, México, 2007

Legislación Internacional Consultada

Anteproyecto de Ley de Delitos Informáticos, Resolución 476/2001, Argentina
http://delitosinformaticos.com/legislacion/argentina.shtml

Computer Misuse Act, Gran Bretaña
http://www.opsi.gov.uk/acts/acts1990/plain/ukpga_19900018_en

Fair Information Practice Principles
http://www.oispp.ca.gov/consumer_privacy/laws/fairinfo.asp

Legislación Sobre Delitos Informáticos en Chile, Ley Relativa a Delitos Informáticos, Ley 19223
http://delitosinformaticos.com/legislacion/chile.shtml

Nuevo Código Penal Español
http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html

Personal Information Protection and Electronic Documents Act 2000, c. 5
http://laws.justice.gc.ca/en/P-8.6/text.html

Personal Data Protection act, Holanda, Abril, 2008
http://www.legislationline.org//legislation.php?tid=219&lid=7107&less=false
http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp_wbp.shtml

Privacy Act of Canada (R.S., 1985, c. P-21), Department of Justice of Canada, Abril, 2008

Proyecto de Ley de Delitos Informáticos de Venezuela
http://delitosinformaticos.com/legislacion/venezuela.shtml

Safe Harbor Privacy Principles, E.E.U.U. – Unión Europea
http://www.export.gov/safeharbor/SH_Privacy.asp

Medios Electrónicos

Breve Historia de la escritura
http://centros5.pntic.mec.es/ies.arzobispo.valdes.salas/alumnos/escri/civili.html

CERT Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL
http://www.cert.org/advisories/CA-2001-19.html

Cliente – Servidor: Tecnología, potencial y futuro
http://www.inei.gob.pe/biblioineipub/bancopub/inf/Lib5038/defi.HTM

Dausin, Mike, Remote file inclusion
http://dvlabs.tippingpoint.com/blog/2008/02/04/php-file-include-attacks-part-1-of-4

Dissecting the Linux Worm
http://www.firenze.linux.it/~sash/worm/dissect_worm.html

Huracán Katrina: la información continúa gracias a la Red
http://www.elmundo.es/navegante/2005/08/31/esociedad/1125478323.html

RFC 15 Definición de Telnet
http://tools.ietf.org/html/rfc15

RFC 821 Definición de Simple Mail Transfer Protocol
http://www.faqs.org/rfcs/rfc821.html

RFC 959 Definición de FTP en español
http://www.rfc-es.org/rfc/rfc0959-es.txt

RFC 2616 Definición de HTTP 1.1
http://www.w3.org/Protocols/rfc2616/rfc2616.html

Symantec Internet Security Threat Report, January-June 2007, Symantec, E.E.U.U. 2007
http://www.symantec.com/business/theme.jsp?themeid=threatreport

Winer, Dave, Bill Gates vs The Internet, 1994
http://www.scripting.com/davenet/1994/10/18/billgatesvstheinternet.html

Anexo I

Legislaciones Latinoamericanas

(ARGENTINA)
ANTEPROYECTO DE LEY DE DELITOS INFORMÁTICOS SOMETIDO A CONSULTA PÚBLICA POR LA SECRETARÍA DE COMUNICACIONES POR RESOLUCIÓN No. 476/2001 DEL 21.11.2001

Acceso Ilegítimo Informático:

Artículo 1.- Será reprimido con pena de multa de mil quinientos a treinta mil pesos, si no resultare un delito más severamente penado, el que ilegítimamente y a sabiendas accediere, por cualquier medio, a un sistema o dato informático de carácter privado o público de acceso restringido.

La pena será de un mes a dos años de prisión si el autor revelare, divulgare o comercializare la información accedida ilegítimamente.

En el caso de los dos párrafos anteriores, si las conductas se dirigen a sistemas o datos informáticos concernientes a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos, la pena de prisión será de seis meses a seis años.

Daño Informático

Artículo 2.- Será reprimido con prisión de un mes a tres años, siempre que el hecho no constituya un delito más severamente penado, el que ilegítimamente y a sabiendas, alterare de cualquier forma, destruyere, inutilizare, suprimiere o hiciere inaccesible, o de cualquier modo y por cualquier medio, dañare un sistema o dato informático.

Artículo 3.- En el caso del artículo 2º, la pena será de dos a ocho años de prisión, si mediara cualquiera de las circunstancias siguientes:

1) Ejecutarse el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;

2) Si fuera cometido contra un sistema o dato informático de valor científico, artístico, cultural o financiero de cualquier administración pública, establecimiento público o de uso público de todo género;

3) Si fuera cometido contra un sistema o dato informático concerniente a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos. Sí del hecho resultaren, además, lesiones de las descritas en los artículos 90 o 91 del Código Penal, la pena será de tres a quince años de prisión, y si resultare la muerte se elevará hasta veinte años de prisión.

Fraude Informático

Artículo 5.- Será reprimido con prisión de un mes a seis años, el que con ánimo de lucro, para sí o para un tercero, mediante cualquier manipulación o artificio tecnológico semejante de un sistema o dato informático, procure la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

En el caso del párrafo anterior, si el perjuicio recae en alguna administración pública, o entidad financiera, la pena será de dos a ocho años de prisión.

Disposiciones Comunes

Artículo 6.-

1) A los fines de la presente ley se entenderá por sistema informático todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio.

2) A los fines de la presente ley se entenderá por dato informático o información, toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático.

3) En todos los casos de los artículos anteriores, si el autor de la conducta se tratare del responsable de la custodia, operación, mantenimiento o seguridad de un sistema o dato informático, la pena se elevará un tercio del máximo y la mitad del mínimo, no pudiendo superar, en ninguno de los casos, los veinticinco años de prisión.

(CHILE)
LEY RELATIVA A DELITOS INFORMÁTICOS
Ley No.:19223

Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

Santiago, 28 de Mayo de 1993.- ENRIQUE KRAUSS RUSQUE, Vicepresidente de la República.- Francisco Cumplido Cereceda, Ministro de Justicia.

(Venezuela)

Ley Especial Contra los Delitos Informáticos

Título I

Disposiciones Generales

Artículo 1- Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Artículo 2.-Definiciones. A los efectos de la presente ley y cumpliendo con lo previsto en el art. 9 de la Constitución de la República Bolivariana de Venezuela, se entiende por:

a. Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data.

b. Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

c. Data: hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado.

d. Información: significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

e. Documento: registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o

información acerca de un hecho o acto capaces de causar efectos jurídicos.

f. Computador: dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

g. Hardware: equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes.

h. Firmware: programa o segmento de programa incorporado de manera permanente en algún componente de hardware.

i. Software: información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas.

j. Programa: plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador.

k. Procesamiento de data o de información: realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.

l. Seguridad: Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación.

m. Virus: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema.

n. Tarjeta inteligente: rótulo, cédula o carnet que se utiliza como instrumento de identificación, de acceso a un sistema, de pago o de

crédito y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.

o. Contraseña (password): secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.

p. Mensaje de datos: cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.

Artículo 3. Extraterritorialidad. Cuando alguno de los delitos previstos en la presente ley se cometa fuera del territorio de la República, el sujeto activo quedará sujeto a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

Artículo 4. -Sanciones. Las sanciones por los delitos previstos en esta ley serán principales y accesorias.

Las sanciones principales concurrirán con las accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente ley.

Artículo 5. Responsabilidad de las personas jurídicas. Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable.

La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente

Título II

De los delitos

Capítulo I

De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información

Artículo 6.- Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

Artículo 7.- Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

Artículo 8.- Sabotaje o daño culposos. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

Artículo 9.- Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas

Artículo 10.- Posesión de equipos o prestación de servicios de sabotaje. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Artículo 11.- Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado.

Artículo 12.- Falsificación de documentos. El que, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad. El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

Capítulo II

De los Delitos Contra la Propiedad

Artículo 13.- Hurto. El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 14.- Fraude. El que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Artículo 15.- Obtención indebida de bienes o servicios. El que, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 16.- Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. El que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o el que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penado con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias. En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o

instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

Artículo 17.-Apropiación de tarjetas inteligentes o instrumentos análogos. El que se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se hayan perdido, extraviado o hayan sido entregados por equivocación, con el fin de retenerlos, usarlos, venderlos o transferirlos a persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias. La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Artículo 18- Provisión indebida de bienes o servicios. El que a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado, se haya indebidamente obtenido, retenido, falsificado, alterado, provea a quien los presente de dinero, efectos, bienes o servicios o cualquier otra cosa de valor económico, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 19.- Posesión de equipo para falsificaciones. El que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Capítulo III

De los delitos contra la privacidad de las personas y de las comunicaciones

Artículo 20.- Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que

utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 21.- Violación de la privacidad de las comunicaciones. El que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 22.- Revelación indebida de data o información de carácter personal. El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Capítulo IV

De los delitos contra niños, niñas o adolescentes

Artículo 23.-

Difusión o exhibición de material pornográfico. El que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 24.- Exhibición pornográfica de niños o adolescentes. El que

por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Capítulo V

De los delitos contra el orden económico

Artículo 25.- Apropiación de propiedad intelectual. El que sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

Artículo 26.- Oferta engañosa. El que ofrezca, comercialice o provea de bienes o servicios mediante el uso de tecnologías de información y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta de modo que pueda resultar algún perjuicio para los consumidores, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

Título III

Disposiciones comunes

Artículo 27.- Agravantes. La pena correspondiente a los delitos previstos en la presente Ley se incrementará entre un tercio y la mitad:

1º Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido.

2º Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función.

Artículo 28.- Agravante especial. La sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el

artículo 5 de esta Ley, será únicamente de multa, pero por el doble del monto establecido para el referido delito.

Artículo 29.- Penas accesorias. Además de las penas principales previstas en los capítulos anteriores, se impondrán, necesariamente sin perjuicio de las establecidas en el Código Penal, las accesorias siguientes:

1º El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos previstos en los artículos 10 y 19 de la presente ley.

2º El trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos en los artículos 6 y 8 de esta Ley.

3º La inhabilitación para el ejercicio de funciones o empleos públicos, para el ejercicio de la profesión, arte o industria, o para laborar en instituciones o empresas del ramo por un período de hasta tres (3) años después de cumplida o conmutada la sanción principal cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función públicos, del ejercicio privado de una profesión u oficio o del desempeño en una institución o empresa privadas, respectivamente.

4º La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica.

Artículo 30.- Divulgación de la sentencia condenatoria. El Tribunal podrá disponer, además, la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

Artículo 31.- Indemnización Civil. En los casos de condena por cualquiera de los delitos previstos en los Capítulos II y V de esta

Ley, el Juez impondrá en la sentencia una indemnización en favor de la víctima por un monto equivalente al daño causado.

Para la determinación del monto de la indemnización acordada, el Juez requerirá del auxilio de expertos.

Título IV

Disposiciones Finales

Artículo 32.-Vigencia. La presente Ley entrará en vigencia, treinta días después de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela

Artículo 33. -Derogatoria. Se deroga cualquier disposición que colida con la presente Ley.

Dada, firmada y sellada en el Palacio Federal Legislativo, sede de la Asamblea Nacional, en Caracas a los seis días del mes de septiembre de dos mil uno. Año 191° de la Independencia y 142° de la Federación.

Willian lara
Presidente

Gerardo Saer Pérez
Segundo Vicepresidente

Leopoldo Puchi
Primer Vicepresidente

Eustoquio Contreras Vladimir Villegas
Secretario Subsecretario

Anexo II

Privacy Act of Canada (R.S., 1985, c. P-21)

A continuación se presentan los fragmentos de dicha acta, en la cual se encuentran contenidos los artículos empleados para el análisis en el capítulo 4.

El siguiente, es un extracto tomado de la Oficina del Comisionado de Privacidad de Canadá (*Office of the Privacy Commissioner of Canada*)[61], cuya misión es proteger y promover los derechos de privacidad de los individuos de ese país. Se presenta en su lenguaje original para mostrar lo expresamente convenido en dicha acta.

"Privacy Act

P-21

An Act to extend the present laws of Canada that protect the privacy of individuals and that provide individuals with a right of access to personal information about themselves
SHORT TITLE

Short title

1. This Act may be cited as the Privacy Act.

1980-81-82-83, c. 111, Sch. II "1".
PURPOSE OF ACT

Purpose

2. The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information.

1980-81-82-83, c. 111, Sch. II "2".
INTERPRETATION

Definitions

[61]Sitio oficial http://www.privcom.gc.ca/aboutUs/index_e.asp

3. In this Act,
"administrative purpose"
«fins administratives »

"administrative purpose" , in relation to the use of personal information about an individual, means the use of that information in a decision making process that directly affects that individual;
"alternative format"
«support de substitution »

"alternative format" , with respect to personal information, means a format that allows a person with a sensory disability to read or listen to the personal information;
"Court"
«Cour »

"Court" means the Federal Court;
"designated Minister"
«ministre désigné »

"designated Minister" means a person who is designated as the Minister under subsection 3.1(1);
"government institution"
«institution fédérale »

"government institution" means

(a) any department or ministry of state of the Government of Canada, or any body or office, listed in the schedule, and

(b) any parent Crown corporation, and any wholly-owned subsidiary of such a corporation, within the meaning of section 83 of the Financial Administration Act;
"head"
«responsable d'institution fédérale »

"head" , in respect of a government institution, means

(a) in the case of a department or ministry of state, the member of the Queen's Privy Council for Canada who presides over the department or ministry, or

(b) in any other case, either the person designated under subsection 3.1(2) to be the head of the institution for the purposes of this Act or, if no such person is designated, the chief executive officer of the institution, whatever their title;
"personal information"
«renseignements personnels »

"personal information" means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,

(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,

(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual,

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but, for the purposes of sections 7, 8 and 26 and section 19 of the Access to Information Act, does not include

(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

(i) the fact that the individual is or was an officer or employee of the government institution,

(ii) the title, business address and telephone number of the individual,

(iii) the classification, salary range and responsibilities of the position held by the individual,

(iv) the name of the individual on a document prepared by the individual in the course of employment, and

(v) the personal opinions or views of the individual given in the course of employment,

(k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,

(l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on

an individual, including the name of the individual and the exact nature of the benefit, and

(m) information about an individual who has been dead for more than twenty years;
"personal information bank"
«fichier de renseignements personnels »

"personal information bank" means a collection or grouping of personal information described in section 10;
"Privacy Commissioner"
«Commissaire à la protection de la vie privée »

"Privacy Commissioner" means the Commissioner appointed under section 53;
"sensory disability"
«déficience sensorielle »

"sensory disability" means a disability that relates to sight or hearing.

R.S., 1985, c. P-21, s. 3; 1992, c. 1, s. 144(F), c. 21, s. 34; 2002, c. 8, s. 183; 2006, c. 9, s. 181.

For greater certainty

3.01 (1) For greater certainty, any provision of this Act that applies to a government institution that is a parent Crown corporation applies to any of its wholly-owned subsidiaries within the meaning of section 83 of the Financial Administration Act.

For greater certainty
(2) For greater certainty, the Canadian Race Relations Foundation and the Public Sector Pension Investment Board are parent Crown corporations for the purposes of this Act.

2006, c. 9, s. 182.
DESIGNATION

Power to designate Minister

3.1 (1) The Governor in Council may designate a member of the Queen's Privy Council for Canada to be the Minister for the purposes of any provision of this Act.

Power to designate head
(2) The Governor in Council may, by order, designate a person to be the head of a government institution, other than a department or ministry of state, for the purposes of this Act.

2006, c. 9, s. 182.
COLLECTION, RETENTION AND DISPOSAL OF PERSONAL INFORMATION

Collection of personal information

4. No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.

1980-81-82-83, c. 111, Sch. II "4".

Personal information to be collected directly

5. (1) A government institution shall, wherever possible, collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates except where the individual authorizes otherwise or where personal information may be disclosed to the institution under subsection 8(2).

Individual to be informed of purpose
(2) A government institution shall inform any individual from whom the institution collects personal information about the individual of the purpose for which the information is being collected.

Exception
(3) Subsections (1) and (2) do not apply where compliance therewith might

(a) result in the collection of inaccurate information; or

(b) defeat the purpose or prejudice the use for which information is collected.

1980-81-82-83, c. 111, Sch. II "5".

Retention of personal information used for an administrative purpose

6. (1) Personal information that has been used by a government institution for an administrative purpose shall be retained by the institution for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information.

Accuracy of personal information
(2) A government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible.

Disposal of personal information
(3) A government institution shall dispose of personal information under the control of the institution in accordance with the regulations and in accordance with any directives or guidelines issued by the designated minister in relation to the disposal of that information.

1980-81-82-83, c. 111, Sch. II "6".
PROTECTION OF PERSONAL INFORMATION

Use of personal information

7. Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or

(b) for a purpose for which the information may be disclosed to the institution under subsection 8(2).

1980-81-82-83, c. 111, Sch. II "7".

Disclosure of personal information

8. (1) Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

Where personal information may be disclosed
(2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;

(b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;

(c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;

(d) to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada;

(e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;

(f) under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a province, the council of the Westbank First Nation, the council of a participating First Nation — as defined in subsection 2(1) of the First Nations Jurisdiction over Education in British Columbia Act —, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation;

(g) to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem;

(h) to officers or employees of the institution for internal audit purposes, or to the office of the Comptroller General or any other person or body specified in the regulations for audit purposes;

(i) to the Library and Archives of Canada for archival purposes;

(j) to any person or body for research or statistical purposes if the head of the government institution

(i) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and

(ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates;

(k) to any aboriginal government, association of aboriginal people, Indian band, government institution or part thereof, or to any person acting on behalf of such government, association, band, institution or part thereof, for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada;

(l) to any government institution for the purpose of locating an individual in order to collect a debt owing to Her Majesty in right of Canada by that individual or make a payment owing to that individual by Her Majesty in right of Canada; and

(m) for any purpose where, in the opinion of the head of the institution,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates.

Personal information disclosed by Library and Archives of Canada
(3) Subject to any other Act of Parliament, personal information under the custody or control of the Library and Archives of Canada that has been transferred there by a government institution for historical or archival purposes may be disclosed in accordance with the regulations to any person or body for research or statistical purposes.

Copies of requests under paragraph (2)(e) to be retained
(4) The head of a government institution shall retain a copy of every request received by the government institution under paragraph (2)(e) for such period of time as may be prescribed by regulation, shall keep a record of any information disclosed pursuant to the request for such period of time as may be prescribed by regulation and shall, on the request of the Privacy Commissioner, make those copies and records available to the Privacy Commissioner.

Notice of disclosure under paragraph (2)(m)
(5) The head of a government institution shall notify the Privacy Commissioner in writing of any disclosure of personal information under paragraph (2)(m) prior to the disclosure where reasonably practicable or in any other case forthwith on the disclosure, and the Privacy Commissioner may, if the Commissioner deems it appropriate, notify the individual to whom the information relates of the disclosure.

Definition of “Indian band”
(6) In paragraph (2)(k), "Indian band" means

(a) a band, as defined in the Indian Act;

(b) a band, as defined in the Cree-Naskapi (of Quebec) Act, chapter 18 of the Statutes of Canada, 1984;

(c) the Band, as defined in the Sechelt Indian Band Self-Government Act, chapter 27 of the Statutes of Canada, 1986; or

(d) a first nation named in Schedule II to the Yukon First Nations Self-Government Act.

Definition of "aboriginal government"
(7) The expression "aboriginal government" in paragraph (2)(k) means

(a) Nisga’a Government, as defined in the Nisga’a Final Agreement given effect by the Nisga’a Final Agreement Act;

(b) the council of the Westbank First Nation;

(c) the Tlicho Government, as defined in section 2 of the Tlicho Land Claims and Self-Government Act;

(d) the Nunatsiavut Government, as defined in section 2 of the Labrador Inuit Land Claims Agreement Act; or

(e) the council of a participating First Nation as defined in subsection 2(1) of the First Nations Jurisdiction over Education in British Columbia Act.

Definition of "council of the Westbank First Nation"
(8) The expression "council of the Westbank First Nation" in paragraphs (2)(f) and (7)(b) means the council, as defined in the Westbank First Nation Self-Government Agreement given effect by the Westbank First Nation Self-Government Act.

R.S., 1985, c. P-21, s. 8; R.S., 1985, c. 20 (2nd Supp.), s. 13, c. 1 (3rd Supp.), s. 12; 1994, c. 35, s. 39; 2000, c. 7, s. 26; 2004, c. 11, s. 37, c. 17, s. 18; 2005, c. 1, ss. 106, 109, c. 27, ss. 21, 25; 2006, c. 10, s. 33.

Record of disclosures to be retained

9. (1) The head of a government institution shall retain a record of any use by the institution of personal information contained in a personal information bank or any use or purpose for which that information is disclosed by the institution where the use or purpose is not included in the statements of uses and purposes set forth pursuant to subparagraph 11(1)(a)(iv) and subsection 11(2) in the index referred to in section 11, and shall attach the record to the personal information.

Limitation
(2) Subsection (1) does not apply in respect of information disclosed pursuant to paragraph 8(2)(e).

Record forms part of personal information
(3) For the purposes of this Act, a record retained under subsection (1) shall be deemed to form part of the personal information to which it is attached.

Consistent uses
(4) Where personal information in a personal information bank under the control of a government institution is used or disclosed for a use consistent with the purpose for which the information was obtained or compiled by the institution but the use is not included in the statement of consistent uses set forth pursuant to subparagraph 11(1)(a)(iv) in the index referred to in section 11, the head of the government institution shall

(a) forthwith notify the Privacy Commissioner of the use for which the information was used or disclosed; and

(b) ensure that the use is included in the next statement of consistent uses set forth in the index.

1980-81-82-83, c. 111, Sch. II "9"; 1984, c. 21, s. 89.
PERSONAL INFORMATION BANKS

Personal information to be included in personal information banks

10. (1) The head of a government institution shall cause to be included in personal information banks all personal information under the control of the government institution that

(a) has been used, is being used or is available for use for an administrative purpose; or

(b) is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

Exception for Library and Archives of Canada
(2) Subsection (1) does not apply in respect of personal information under the custody or control of the Library and Archives of Canada that has been transferred there by a government institution for historical or archival purposes.

R.S., 1985, c. P-21, s. 10; R.S., 1985, c. 1 (3rd Supp.), s. 12; 2004, c. 11, s. 38.
PERSONAL INFORMATION INDEX

Index of personal information

11. (1) The designated Minister shall cause to be published on a periodic basis not less frequently than once each year, an index of

(a) all personal information banks setting forth, in respect of each bank,

(i) the identification and a description of the bank, the registration number assigned to it by the designated Minister pursuant to paragraph 71(1)(b) and a description of the class of individuals to whom personal information contained in the bank relates,

(ii) the name of the government institution that has control of the bank,

(iii) the title and address of the appropriate officer to whom requests relating to personal information contained in the bank should be sent,

(iv) a statement of the purposes for which personal information in the bank was obtained or compiled and a statement of the uses consistent with those purposes for which the information is used or disclosed,

(v) a statement of the retention and disposal standards applied to personal information in the bank, and

(vi) an indication, where applicable, that the bank was designated as an exempt bank by an order under section 18 and the provision of section 21 or 22 on the basis of which the order was made; and

(b) all classes of personal information under the control of a government institution that are not contained in personal information banks, setting forth in respect of each class

(i) a description of the class in sufficient detail to facilitate the right of access under this Act, and

(ii) the title and address of the appropriate officer for each government institution to whom requests relating to personal information within the class should be sent.

Statement of uses and purposes
(2) The designated Minister may set forth in the index referred to in subsection (1) a statement of any of the uses and purposes, not included in the statements made pursuant to subparagraph (1)(a)(iv), for which personal information contained in any of the personal information banks referred to in the index is used or disclosed on a regular basis.

Index to be made available

(3) The designated Minister shall cause the index referred to in subsection (1) to be made available throughout Canada in conformity with the principle that every person is entitled to reasonable access to the index.

1980-81-82-83, c. 111, Sch. II "11".
ACCESS TO PERSONAL INFORMATION
Right of Access

Right of access

12. (1) Subject to this Act, every individual who is a Canadian citizen or a permanent resident within the meaning of subsection 2(1) of the Immigration and Refugee Protection Act has a right to and shall, on request, be given access to

(a) any personal information about the individual contained in a personal information bank; and

(b) any other personal information about the individual under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution.

Other rights relating to personal information
(2) Every individual who is given access under paragraph (1)(a) to personal information that has been used, is being used or is available for use for an administrative purpose is entitled to

(a) request correction of the personal information where the individual believes there is an error or omission therein;

(b) require that a notation be attached to the information reflecting any correction requested but not made; and

(c) require that any person or body to whom that information has been disclosed for use for an administrative purpose within two years prior to the time a correction is requested or a notation is required under this subsection in respect of that information

(i) be notified of the correction or notation, and

(ii) where the disclosure is to a government institution, the institution make the correction or notation on any copy of the information under its control.

Extension of right of access by order
(3) The Governor in Council may, by order, extend the right to be given access to personal information under subsection (1) to include individuals not referred to in that subsection and may set such conditions as the Governor in Council deems appropriate.

R.S., 1985, c. P-21, s. 12; 2001, c. 27, s. 269.
Requests for Access

Request for access under paragraph 12(1)(a)

13. (1) A request for access to personal information under paragraph 12(1)(a) shall be made in writing to the government institution that has control of the personal information bank that contains the information and shall identify the bank.

Request for access under 12(1)(b)
(2) A request for access to personal information under paragraph 12(1)(b) shall be made in writing to the government institution that has control of the information and shall provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution.

1980-81-82-83, c. 111, Sch. II "13".

Notice where access requested

14. Where access to personal information is requested under subsection 12(1), the head of the government institution to which the request is made shall, subject to section 15, within thirty days after the request is received,

(a) give written notice to the individual who made the request as to whether or not access to the information or a part thereof will be given; and

(b) if access is to be given, give the individual who made the request access to the information or the part thereof.

1980-81-82-83, c. 111, Sch. II "14".

Extension of time limits

15. The head of a government institution may extend the time limit set out in section 14 in respect of a request for

(a) a maximum of thirty days if

(i) meeting the original time limit would unreasonably interfere with the operations of the government institution, or

(ii) consultations are necessary to comply with the request that cannot reasonably be completed within the original time limit, or

(b) such period of time as is reasonable, if additional time is necessary for translation purposes or for the purposes of converting the personal information into an alternative format,

by giving notice of the extension and the length of the extension to the individual who made the request within thirty days after the request is received, which notice shall contain a statement that the individual has a right to make a complaint to the Privacy Commissioner about the extension.

R.S., 1985, c. P-21, s. 15; 1992, c. 21, s. 35.

Where access is refused

16. (1) Where the head of a government institution refuses to give access to any personal information requested under subsection 12(1), the head of the institution shall state in the notice given under paragraph 14(a)

(a) that the personal information does not exist, or

(b) the specific provision of this Act on which the refusal was based or the provision on which a refusal could reasonably be expected to be based if the information existed,

and shall state in the notice that the individual who made the request has a right to make a complaint to the Privacy Commissioner about the refusal.

Existence not required to be disclosed
(2) The head of a government institution may but is not required to indicate under subsection (1) whether personal information exists.

Deemed refusal to give access
(3) Where the head of a government institution fails to give access to any personal information requested under subsection 12(1) within the time limits set out in this Act, the head of the institution shall, for the purposes of this Act, be deemed to have refused to give access.

1980-81-82-83, c. 111, Sch. II "16".
Access

Form of access

17. (1) Subject to any regulations made under paragraph 77(1)(o), where an individual is to be given access to personal information requested under subsection 12(1), the government institution shall

(a) permit the individual to examine the information in accordance with the regulations; or

(b) provide the individual with a copy thereof.

Language of access
(2) Where access to personal information is to be given under this Act and the individual to whom access is to be given requests that

access be given in a particular one of the official languages of Canada,

(a) access shall be given in that language, if the personal information already exists under the control of a government institution in that language; and

(b) where the personal information does not exist in that language, the head of the government institution that has control of the personal information shall cause it to be translated or interpreted for the individual if the head of the institution considers a translation or interpretation to be necessary to enable the individual to understand the information.

Access to personal information in alternative format
(3) Where access to personal information is to be given under this Act and the individual to whom access is to be given has a sensory disability and requests that access be given in an alternative format, access shall be given in an alternative format if

(a) the personal information already exists under the control of a government institution in an alternative format that is acceptable to the individual; or

(b) the head of the government institution that has control of the personal information considers the giving of access in an alternative format to be necessary to enable the individual to exercise the individual's right of access under this Act and considers it reasonable to cause the personal information to be converted.

R.S., 1985, c. P-21, s. 17; 1992, c. 21, s. 36.
EXEMPTIONS
Exempt Banks

Governor in Council may designate exempt banks

18. (1) The Governor in Council may, by order, designate as exempt banks certain personal information banks that contain files all of which consist predominantly of personal information described in section 2l or 22.

Disclosure may be refused
(2) The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) that is contained in a personal information bank designated as an exempt bank under subsection (1).

Contents of order
(3) An order made under subsection (1) shall specify

(a) the section on the basis of which the order is made; and

(b) where a personal information bank is designated that contains files that consist predominantly of personal information described in subparagraph 22(1)(a)(ii), the law concerned.

1980-81-82-83, c. 111, Sch. II "18".
Responsibilities of Government

Personal information obtained in confidence

19. (1) Subject to subsection (2), the head of a government institution shall refuse to disclose any personal information requested under subsection 12(1) that was obtained in confidence from

(a) the government of a foreign state or an institution thereof;

(b) an international organization of states or an institution thereof;

(c) the government of a province or an institution thereof;

(d) a municipal or regional government established by or pursuant to an Act of the legislature of a province or an institution of such a government;

(e) the council, as defined in the Westbank First Nation Self-Government Agreement given effect by the Westbank First Nation Self-Government Act; or

(f) the council of a participating First Nation as defined in subsection 2(1) of the First Nations Jurisdiction over Education in British Columbia Act.

Where disclosure authorized
(2) The head of a government institution may disclose any personal information requested under subsection 12(1) that was obtained from any government, organization or institution described in subsection (1) if the government, organization or institution from which the information was obtained

(a) consents to the disclosure; or

(b) makes the information public.

R.S., 1985, c. P-21, s. 19; 2004, c. 17, s. 19; 2006, c. 10, s. 34.

Federal-provincial affairs

20. The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) the disclosure of which could reasonably be expected to be injurious to the conduct by the Government of Canada of federal-provincial affairs.

1980-81-82-83, c. 111, Sch. II "20".

International affairs and defence

21. The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada, as defined in subsection 15(2) of the Access to Information Act, or the efforts of Canada toward detecting, preventing or suppressing subversive or hostile activities, as defined in subsection 15(2) of the Access to Information Act, including, without restricting the generality of the foregoing, any such information listed in paragraphs 15(1)(a) to (i) of the Access to Information Act.

1980-81-82-83, c. 111, Sch. II "21".

..."

Anexo III

Personal Data Protection Act of the Netherlands

A continuación se presentan los fragmentos de dicha acta, en la cual se encuentran contenidos los artículos empleados para el análisis en el capítulo 4.

Esta acta pertenece a la Autoridad Holandesa de Protección a la Información (*Dutch Data Protection Authority),* encargada de supervisar y regular el uso de la información personal con el fin de asegurar la privacidad de la información. Se presenta la traducción al inglés de su original en holandés.[62]

"Personal Data Protection Act

UPPER HOUSE OF THE DUTCH PARLIAMENT

Session 1999-2000 Nr. 92

25 892 - Rules for the protection of personal data (Personal Data Protection Act) (Wet bescherming persoonsgegevens)

REVISED BILL (as approved by the Lower House on 23 November 1999)

We, Beatrix, by the grace of God, Queen of the Netherlands, Princess of Orange-Nassau, etc. etc. etc.

To all those who read or hear this, We greet you and hereby proclaim as follows:

Whereas it is necessary to implement Directive 95/46/EC of the European Parliament and of the Council of the European Union of 23 November 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of that data (OJ L 28 1);

Having regard to Article 10(2) and (3) of the Constitution;

[62] http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp.shtml

We, having consulted the State Council, and in joint consultation with Parliament, have approved and understood, as We approve and understand, the following:

CHAPTER 1. GENERAL PROVISIONS

Article 1

For the purposes of this Act and the provisions based upon it:

a. "personal data" shall mean: any information relating to an identified or identifiable natural person;

b. "processing of personal data" shall mean: any operation or any set of operations concerning personal data, including in any case the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as blocking, erasure or destruction of data;

c. "file" shall mean: any structured set of personal data, regardless of whether or not this data set is centralized or dispersed along functional or geographical lines, that is accessible according to specific criteria and relates to different persons;

d. "responsible party" shall mean: the natural person, legal person, administrative body or any other entity which, alone or in conjunction with others, determines the purpose of and means for processing personal data;

e. "processor" shall mean: the person or body which processes personal data for the responsible party, without coming under the direct authority of that party;

f. "data subject" shall mean: the person to whom personal data relate;

g. "third party" shall mean: any party other than the data subject, the responsible party, the processor, or any person under the direct authority of the responsible party or the processor, who is authorized to process personal data;

h. "recipient" shall mean: the party to whom the personal data are provided;

i. consent of the data subject: any freely-given, specific and informed expression of will whereby data subjects agree to the processing of personal data relating to them;

j. "Our Minister" shall mean: Our Minister of Justice;

k. "Data Protection Commission" or "Commission" shall mean: the body referred to in Article 51;

1. "officer" shall mean: the data protection officer referred to in Article 62;

m. "prior investigation" shall mean: an investigation as referred to in Article 31;

n. "provision of personal data" shall mean: the disclosure or making available of personal data;

o. "collection of personal data" shall mean: the obtaining of personal data.

Article 2

1 . This Act applies to the fully or partly automated processing of personal data, and the non-automated processing of personal data entered in a file or intended to be entered therein.

2. This Act does not apply to the processing of personal data:

a. in the course of a purely personal or household activity;

b. by or on behalf of the intelligence or security services referred to in the Intelligence and Security Services Act (Wet op de inlichtingen- en veiligheidsdiensten);

c. for the purposes of implementing the police tasks defined in Article 2 of the Police Act 1993 (Politiewet 1993);

d. governed by or under the Municipal Database (Personal Records) Act (Wet gemeentelijke basisadministratie persoonsgegevens);

e. for the purposes of implementing the Judicial Documentation Act (Wet justitiële documentatie) and

f. for the purposes of implementing the Electoral Provisions Act (Kieswet).

3. This Act does not apply to the processing of personal data by the armed forces where Our Defense Minister so decides with a view to deploying or making available the armed forces to maintain or promote the international legal order. Such a decision shall be communicated to the Data Protection Commission as quickly as possible.

Article 3

1. This Act does not apply to the processing of personal data for exclusively journalistic, artistic or literary purposes, except where otherwise provided in this Chapter and in Articles 6 to 11, 13 to 15, 25 and 49.

2. The prohibition on processing personal data referred to in Article 16 does not apply where this is necessary for the purposes referred to under (1).

Article 4

1. This Act applies to the processing of personal data carried out in the context of the activities of an establishment of a responsible party in the Netherlands.

2. This Act applies to the processing of personal data by or for responsible parties who are not established in the European Union, whereby use is made of automated or non-automated means situated in the Netherlands, unless these means are used only for forwarding personal data.

3. The responsible parties referred to under (2) are prohibited from processing personal data, unless they designate a person or body in the Netherlands to act on their behalf in accordance with the provisions of this Act. For the purposes of application of this Act and the provisions based upon it, the said person or body shall be deemed to be the responsible party.

Article 5

1. In the case that the data subjects are minors and have not yet reached the age of sixteen, or have been placed under legal restraint or the care of a mentor, instead of the consent of the data subjects, that of their legal representative is required.

The data subjects or their legal representative may withdraw consent at any time.

CHAPTER 2. CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL DATA

Section 1. Processing of personal data in general

Article 6

Personal data shall be processed in accordance with the law and in a proper and careful manner.

Article 7

Personal data shall be collected for specific, explicitly defined and legitimate purposes.

Article 8

Personal data may only be processed where:

a. the data subject has unambiguously given his consent for the processing;

b. the processing is necessary for the performance of a contract to which the data subject is party, or for actions to be carried out at the request of the data subject and which are necessary for the conclusion of a contract;

c. the processing is necessary in order to comply with a legal obligation to which the responsible party is subject;

d. the processing is necessary in order to protect a vital interest of the data subject;

e. the processing is necessary for the proper performance of a public law duty by the administrative body concerned or by the administrative body to which the data are provided, or

f. the processing is necessary for upholding the legitimate interests of the responsible party or of a third party to whom the data are supplied, except where the interests or fundamental rights and freedoms of the data subject, in particular the right to protection of individual privacy, prevail.

Article 9

1. Personal data shall not be further processed in a way incompatible with the purposes for which they have been obtained.

2. For the purposes of assessing whether processing is incompatible, as referred to under (1), the responsible party shall in any case take account of the following:

a. the relationship between the purpose of the intended processing and the purpose for which the data have been obtained;

b. the nature of the data concerned;

c. the consequences of the intended processing for the data subject;

d. the manner in which the data have been obtained, and

e. the extent to which appropriate guarantees have been put in place with respect to the data subject.

3. The further processing of personal data for historical, statistical or scientific purposes shall not be regarded as incompatible where the responsible party has made the necessary arrangements to ensure that the further processing is carried out solely for these specific purposes.

4. The processing of personal data shall not take place where this is precluded by an obligation of confidentiality by virtue of office, profession or legal provision.

Article 10

1. Personal data shall not be kept in a form which allows the data subject to be identified for any longer than is necessary for achieving the purposes for which they were collected or subsequently processed.

2. Personal data may be kept for longer than provided under (1), where this is for historical, statistical or scientific purposes, and where the responsible party has made the necessary arrangements to ensure that the data concerned are used solely for these specific purposes.

Article 11

1. Personal data shall only be processed where, given the purposes for which they are collected or subsequently processed, they are adequate, relevant and not excessive.

2. The responsible party shall take the necessary steps to ensure that personal data, given the purposes for which they are collected or subsequently processed, are correct and accurate.

Article 12

1. Anyone acting under the authority of the responsible party or the processor, as well as the processor himself, where they have access to personal data, shall only process such data on the orders of the responsible party, except where otherwise required by law.

2. The persons referred to under (1), who are not subject to an obligation of confidentiality by virtue of office, profession or legal provision, are required to treat as confidential the personal data which comes to their knowledge, except where the communication of such data is required by a legal provision or the proper performance of their duties. Article 272(2) of the Penal Code is not applicable.

Article 13

The responsible party shall implement appropriate technical and organizational measures to secure personal data against loss or against any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected. These measures shall also aim at preventing unnecessary collection and further processing of personal data.

Article 14

1. Where responsible parties have personal data processed for their purposes by a processor, these responsible parties shall make sure that the processor provides adequate guarantees concerning the technical and organizational security measures for the processing to be carried out. The responsible parties shall make sure that these measures are complied with.

2. The carrying out of processing by a processor shall be governed by an agreement or another legal act whereby an obligation is created between the processor and the responsible party.

3. The responsible party shall make sure that the processor:

a. processes the personal data in accordance with Article 12(l) and

b. complies with the obligations incumbent upon the responsible party under Article 13.

4. Where the processor is established in another country of the European Union, the responsible party shall make sure that the processor complies with the laws of that other country, notwithstanding the provisions of (3)(b).

5. With a view to the keeping of proof, the parts of the agreement or legal act relating to personal data protection and the security measures referred to in Article 13, shall be set down in writing or in another equivalent form.

…

CHAPTER 7. EXCEPTIONS AND RESTRICTIONS

Article 43

Responsible parties are not required to apply Articles 9(1), 30(3), 33, 34 and 35, where this is necessary in the interests of:

a. State security;

b. the prevention, detection and prosecution of criminal offences;

c. important economic and financial interests of the State and other public bodies;

d. supervising compliance with legal provisions established in the interests referred to under (b) and (c), or

e. protecting the data subject or the rights and freedoms of other persons.

…

It is hereby ordered that this Act shall be published in the Official Gazette and that all ministries, authorities, bodies and officials whom it may concern shall ensure that it is implemented scrupulously.

Done

The Minister of Justice,

The Minister for the Major Cities and Integration Policy

Updated 15.12.2005”