La informática forense y los delitos cibernéticos en la sociedad de la información

Autor: Ulises Fernando Ramírez Toledo

Tesina presentada para obtener el título de:
Licenciado en Sistemas Computarizados

Nombre del asesor:
Sergio Francisco Barraza Ibarra

UNIVERSIDAD VASCO DE QUIROGA

ESCUELA DE SISTEMAS COMPUTARIZADOS

" LA INFORMÀTICA FORENSE Y LOS DELITOS CIBERNÈTICOS EN LA SOCIEDAD DE LA INFORMACIÒN "

TESINA

Que para obtener el título de:

LICENCIADO EN SISTEMAS COMPUTARIZADOS

Presenta:

ULISES FERNANDO RAMÌREZ TOLEDO

Asesor:

M. A. ING. SERGIO FRANCISCO BARRAZA IBARRA

No. De acuerdo 952006 CLAVE 16PSU0014Q

Morelia, Michoacàn, Mèxico

Enero de 2005

AGRADECIMIENTOS

Agradezco al ing. Sergio Francisco Barraza Ibarra por su apoyo, colaboración y confianza para la realización de esta tesina.

DEDICATORIAS

A dios por haberme dado salud y fuerzas para lograr esta meta en mi vida.

A mi madre Eva Ramírez Toledo que a sido mi fuerza, mi sostén, mi principal motivo para salir adelante en la vida.

A mi padre Ismael Barriga Reyes por todo el apoyo emocional y espiritual que me brindo durante esta etapa de mi vida.

A mi ti Ma. Elena Ramírez Toledo por haberme brindado incondicionalmente su cariño y su confianza.

A mi hermana Ma. Elena Ramírez Toledo y su familia por quererme y apoyarme.

A mis amigos que siempre recibí un a liento para seguir adelante en este objetivo.

1. INTRODUCCIÓN

La computación forense. En particular, se busca entender con detalle la manera como se generan las posibles fallas de seguridad, donde se pueden encontrar evidencias del hecho y estrategias generales de manejo de las mismas.

En este contexto, el tema ofrece un marco conceptual de análisis que oriente a los participantes ante una situación en la que se encuentre comprometida la seguridad informática de una organización.

La computación forense como ciencia naciente, ofrece una nueva frontera para todos aquellos que reconociendo su formación técnica o experiencia en aspectos de tecnología, avanzan en medio de los estrictos paradigmas forenses de investigación, procedimientos de análisis y formación legal y penal para enfrentar a todos aquellos que desafían los límites de la seguridad y controles de las organizaciones, con el fin de establecer un frente de resistencia e investigación que al igual que los intrusos, continuamente aprenden y buscan nuevas formas de alcanzar nuevas fronteras en el conocimiento técnico y científico.

2. OBJETIVO GENERAL:

Formar a los profesionales en el campo de las nuevas tecnologías de la Información y comunicaciones, y el estudio de la informática forense como objeto para lograr una Sociedad de la Información Justa y Global.

Orientar a los peritos en criminalísticas, abogados, profesionales de seguridad informática corporativa y a los cuerpos de policía de una visión general de la evidencia digital y los crímenes informáticos.

A través de este contexto se establecen las bases de conocimiento así como el manejo de la terminología legal relacionada con los delitos informáticos.

3. OBJETIVOS PERSONALES:

- Comprender y analizar las conductas y perfiles de los atacantes de los sistemas de computación
- Identificar y establecer estrategias para tratar un posible cybercrimen
- Manejo y control de la evidencia en informática
- Consideraciones legales en computación forense.
- Naturaleza de los hechos jurídicos informáticos.
- Aplicaciones de la informática forense.
- Terminología de informática forense.
- Principio de Criminalística aplicado a la informática forense.
- Informática forense en computadoras.

4. INFORMÁTICA FORENSE

4.1. DEFINICION

La Informática Forense se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial.

Es la aplicación de técnicas y herramientas de hardware y software para determinar datos potenciales o relevantes.

También puede servir para informar adecuadamente al cliente acerca de las posibilidades reales de la evidencia existente o supuesta.

Los naturales destinatarios de este servicio son los estudios jurídicos aunque cualquier empresa o persona puede contratarlo.

La necesidad de este servicio se torna evidente desde el momento en que la enorme mayoría de la información generada está almacenada por medios electrónicos.

En la recuperación de información nos enfrentamos con información que no es accesible por medios convencionales, ya sea por problemas de funcionamiento del dispositivo que lo contiene, ya sea porque se borraron o corrompieron las estructuras administrativas de software del sistema de archivos. La información se perdió por un problema de fallo de la tecnología de hardware y/o software o bien por un error humano.

El usuario nos indica su versión de los hechos y a menudo encontramos sobre la falla original otras que el usuario o sus prestadores técnicos agregaron en un intento de recuperación. Así es que debemos figurarnos a partir del análisis del medio qué ocurrió desde el momento en que todo funcionaba bien y la información era accesible.

En informática forense hablamos ya no sólo de recuperación de información sino de descubrimiento de información dado que no hubo necesariamente una falla del dispositivo ni un error humano sino una actividad subrepticia para borrar, adulterar u ocultar información. Es por lo tanto esperable que el mismo hecho de esta adulteración pase desapercibido.

La informática forense apela a nuestra máxima aptitud dado que enfrentamos desde casos en que el dispositivo fue borrado, golpeado y dañado físicamente hasta ligeras alteraciones de información que pueden constituir un crimen.

Este servicio es de utilidad a empresas que llevan adelante juicios laborales con sus empleados, o con sus asociados por conflictos de intereses, a estudios jurídicos que necesitan recabar información ya sea para presentarla frente a un tribunal o bien para negociar con las partes un acuerdo extrajudicial de resarcimiento, renuncia, etc.

Es de utilidad a los organismos judiciales y policiales que buscan evidencias de todo tipo de crímenes. Es un componente indispensable en litigios civiles.

Algunos hechos:

- Se considera que el 75% de los delitos relacionados con sistemas informáticos se producen desde dentro de una organización (hacker dentro del muro de fuego.

- Durante 1999 el 93% de la información se generó en forma electrónica.

- La computación forense tiene aplicación en un amplio rango de crímenes incluido pero no limitado a: mal uso de la computadora que conlleve a pérdida de productividad de empleados (uso personal de correo electrónico, uso de internet para actividades personales o entretenimiento). Robo de secretos comerciales e industriales, robo o destrucción de propiedad intelectual, destrucción de archivos judiciales, de auditoria, etc.

- La evidencia informática es frágil por definición y puede fácilmente ser alterada o modificada y así perder autenticidad frente a una corte. Se deben por lo tanto establecer rígidas normas de preservación y cadena de custodia de la misma.

5. MARCO LEGAL
DE LA INFORMATICA FORENSE

5.1. CÓDIGO PENAL FEDERAL

LIBRO SEGUNDO

TITULO NOVENO REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

CAPITULO II ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

Articulo 211 bis 1

Al que sin autorización modifique, destruya o provoque perdida 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.

Articulo 211 bis 2

Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Articulo 211 bis 3

Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida 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.

Articulo 211 bis 4

Al que sin autorización modifique, destruya o provoque perdida 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.

Articulo 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 perdida 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 articulo se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Articulo 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 articulo 400 bis de este código.

Articulo 211 bis 7

Las penas previstas en este capitulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

6. DELITOS CIBERNÉTICOS

Existen vacíos en los sistemas de seguridad informática, así como en la aplicación y formulación de leyes; dicha situación convierte a Internet en un espacio propicio para la ejecución de delitos cibernéticos.

Según una iniciativa de ley1 propuesta el 22 de marzo de 2000 ante el pleno de la Cámara de Senadores de la Quincuagésima Legislatura, están considerados como delitos informáticos "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen referencia al uso indebido de cualquier medio informático."

El robo o alteración de información, sabotaje, pedofilia, tráfico de menores, fraude, clonación de señales satelitales, de tarjetas de crédito y el ciberterrorismo son actividades consideradas por las autoridades de los tres niveles (federal, estatal y municipal) como una muestra de estos ilícitos, los cuales día con día muestran un incremento en nuestro país, expandiéndose de manera considerablemente rápida.

La Secretaría de Seguridad Pública (SSP), a través de su División de Policía Cibernética, ha detectado a 397 comunidades o sitios Web con pornografía infantil, de las cuales 197 son mexicanas.

Asimismo, esta corporación tiene conocimiento de la existencia de cuatro millones de sitios Web que explotan la pornografía, 60% de ellos son lucrativos, es decir, el sitio exige el pago del "servicio" por medio de la tarjeta de crédito del usuario; el 40% restante son intercambios de fotos y videos persona a persona.

"Se estima que quinientos sitios Web de este tipo son creados diariamente", asegura Hervé Hurtado Ruiz, Director General de Tráficos y Contrabando de la Policía Federal Preventiva.

En relación con el fraude, otro ilícito con alto índice de incidencia, la PFP ha documentado una serie de patrones que son resultado de sus extensos patrullajes en la red.

"Sabemos que los delincuentes actúan entre las 12 del día y las tres de la tarde para subir las 'ofertas'; utilizan cuentas bancarias donde realizan sus depósitos las víctimas, la mayoría de ellas se encuentran en un rango entre los 18 y 30 años, además de que los usuarios afectados son primordialmente hombres.

En el mapa geográfico, el mayor número de delitos se localizan en los estados de Jalisco, Estado de México, Morelos, Yucatán, Sonora y Sinaloa."

Uno de los problemas más importantes para la persecución de estos delitos tiene que ver con la rapidez que ofrece la publicación electrónica para poner y quitar información de cualquier tipo y formato en Web.

Para contrarrestar éstos y otros delitos cibernéticos de creciente expansión, el gobierno mexicano conformó un equipo especializado llamado DC México (Delitos Cibernéticos México).

Este grupo lo integran todas las corporaciones policíacas estatales y federales, así como los proveedores de servicio de Internet, (ISPs) y todas las compañías privadas o públicas que ofrecen seguridad informática en el país.

DC México tiene como tareas fundamentales la identificación, el monitoreo y el rastreo de cualquier manifestación delictiva que se cometa mediante computadoras conectadas en territorio mexicano o fuera de él y que tenga afectaciones en nuestro país.

"La Universidad Nacional Autónoma de México participa en este grupo con UNAM-CERT, que es un organismo importante por las contribuciones que ha realizado en materia de prevención del delito", afirmó el funcionario del gobierno federal.

A su vez, DC México tiene varias divisiones que ejecutan distintas funciones, entre ellas se encuentran el subgrupo de contingencias informáticas, el subgrupo de capacitación y el subgrupo de gobierno.

"Dentro de esta corporación se encuentra la división Nuevas tecnologías e investigación académica y desarrollo, que preside la UNAM, y en la cual este grupo tiene la tarea de ver todo lo relacionado con capacitación y desarrollo de innovaciones tecnológicas."

DC México trabaja conjuntamente con el servicio de aduanas de los Estados Unidos, además de que establece vínculos cercanos con el Servicio Secreto y la Brigada Tecnológica de España.

"Pertenecemos desde hace dos meses a un grupo de tarea internacional que se llama '24 x 7', una alianza de todos los países que tienen policías cibernéticas.

Estamos para rastrear y hacer persecuciones en 'caliente' respecto a cualquier incidencia que acontezca en los países miembros de la organización."

Hay que resaltar que Internet no es un vínculo que desarrolle o propicie la ejecución de actividades delictivas.

En este sentido, las policías cibernéticas son una herramienta innovadora de las corporaciones de procuración de justicia para la seguridad de todos los usuarios que navegan en Internet, sea cual fuere su región geográfica en el mundo.

6.1. DELITOS EN INTERNET.

En México, como en otras partes del mundo, existen delitos cibernéticos o informáticos graves, que, desafortunadamente son desconocidos por una parte importante de la población.

Debido a la trascendencia y magnitud de éstos, el equipo de InfoTICs se ha dado a la tarea de investigar y crear una serie de números en donde se hable abierta y objetivamente sobre el tema.

En ellos te daremos a conocer cada uno de los delitos perseguidos por la Unidad de la Policía Cibernética de nuestro país.

Los riesgos reales para la población de tu comunidad que accedan a Internet desde tu Centro, pero que, por la falta de experiencia informática, son más vulnerables y susceptibles de ser víctimas.

Sin embargo, antes de comenzar queremos decirte que no te alarmes.

Aunque tienden a crecer, los delitos cibernéticos en México son todavía muy pocos, y con la información que te proporcionaremos en éste y los siguientes números estarán mejor capacitado para detectar posibles situaciones de riesgo.

¿Qué son los delitos informáticos?

Según una iniciativa de ley, propuesta el 22 de marzo de 2000 ante el pleno de la Cámara de Senadores, están considerados como delitos informáticos "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen referencia al uso indebido de cualquier medio informáticos".

Es decir, un delito informático es como cualquier otro, sólo que su principal medio de operación es a través de medios digitales

El órgano formalmente encargado de prevenir y combatir los delitos cibernéticos es la Unidad de Policía Cibernética de la Policía Federal Preventiva.

Según esta Unidad, existen nueve grupos de delitos cibernéticos pornografía infantil, tráfico internacional de menores, niños perdidos y sustraídos, fraudes, piratería, ataques a sitios, clonación de señales y tarjetas, snuff y otras amenazas, como virus, correo basura, etc.

Unidad de Policía Cibernética de la PFP.

Los delitos cibernéticos no sólo se han ido incrementando en número, sino que su complejidad ha aumentado conforme se han desarrollado las TIC, e internet se ha convertido en una herramienta básica de uso cotidiano.

Las consecuencias de infectar una computadora con virus en la década de los ochenta y noventa, no son por nada comparables con lo que llega a suceder en la actualidad, en donde todas las redes de comunicación están interconectadas.

En los años ochenta, por ejemplo, los virus cibernéticos se propagaban sólo por disquete y dañaban a una sola computadora. Actualmente, un *hacker* puede hacer que el sistema de toda una compañía se caiga.

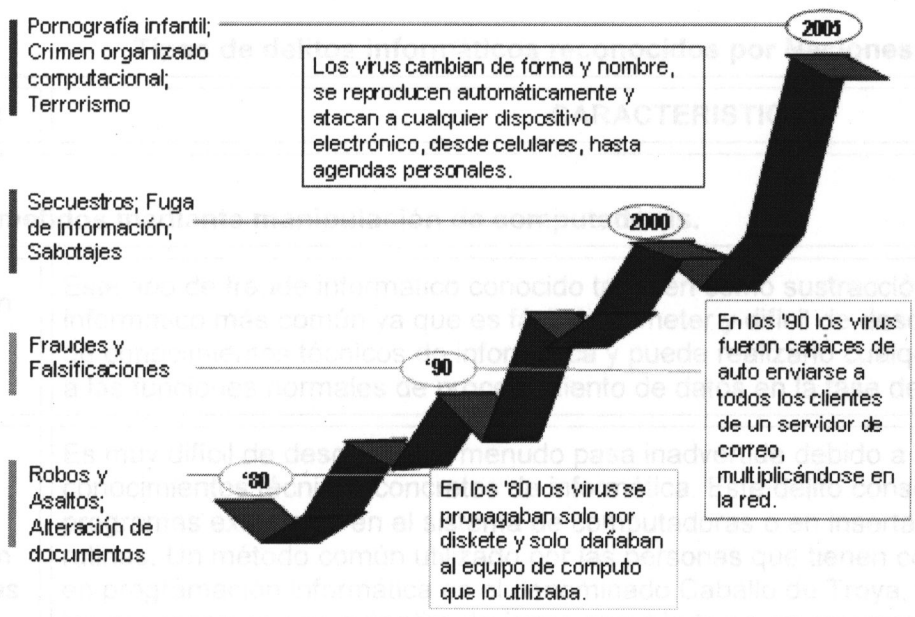
A esto habría que agregar que los delitos actuales son de muchos tipos y más peligrosos.

Anteriormente había asaltos y alteración a documentos, fraudes y falsificaciones, etc.;

Actualmente se les suman delitos como la pornografía infantil, el crimen organizado computacional, y hasta el ciberterrorismo; todos actos ilícitos sumamente difíciles de erradicar y controlar.

Unidad Policía Cibernética, PFP.

Evolución de la Cibernética



Ahora ya conoces un poco más de esta problemática y poco a poco te iremos enterando de cada delito.

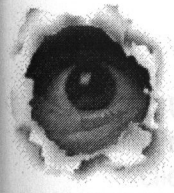
El objetivo es que tú, como líder informático de tu comunidad, hagas conciencia de la importancia de tu papel en la detección y prevención de conductas que pueden arriesgar a las personas.

Trataremos los temas sin tonos de alarma, creando una cultura de seguridad y prevención para todos.

6.2. TIPOS DE DELITOS INFORMATICOS

Tipos de delitos informáticos reconocidos por Naciones Unidas	
DELITO	**CARACTERISTICAS**
Fraudes cometidos mediante manipulación de computadoras.	
Manipulación de los datos de entrada	Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
La manipulación de programas	Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
Manipulación de los datos de salida	Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de c.
Fraude efectuado por manipulación informática	Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.
Falsificaciones informáticas.	
Como objeto	Cuando se alteran datos de los documentos almacenados en forma computarizada.
Como instrumentos	Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Daños o modificaciones de programas o datos computarizados.

Sabotaje informático	Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
 Virus	Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
Gusanos 	Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.
Bomba lógica o cronológica	Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.
Acceso no autorizado a servicios y sistemas informáticos 	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.
Piratas informáticos o hackers	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

7. FRAUDE ELECTRÓNICO

7.1. DEFINICION

Es el uso indebido de los medios informaticos, propios o ajenos, con la finalidad de utilizarlos para apropiarse de los bienes de otra persona, física o moral.

Se da con la desviación de los recursos capitalizables o activos propiedad de otra persona física o moral u organismo público, haciendo uso de prácticas desleales dentro del sistema informático o con un ataque externo a los medios de seguridad informáticos.

La inexistencia de los citados medios no atenúa el delito.

7.2. FRAUDE ELECTRÓNICO

EN GASOLINERAS

Descubre Profeco que gasolineras instalan, con tecnología inalámbrica, dispositivos electrónicos para alterar las bombas de suministro.

CIUDAD DE MÉXICO, México, dic. 29, 2004. - La Procuraduría Federal del Consumidor (Profeco) denunció que gasolineras del país utilizan alta tecnología para defraudar a sus clientes.

Los propietarios instalan dispositivos electrónicos para alterar las bombas de suministro de gasolina.

José Rodrigo Roque, subprocurador de Verificación y Vigilancia de la Profeco, explicó que el cálculo de litros se altera, "y entonces en la pantalla aparece una cantidad distinta a la que en realidad están suministrando, es decir, el fraude ya no es mecánico, sino electrónico".

Los defraudadores cuentan con tecnología inalámbrica para activar los cambios al sistema electrónico de las estaciones de servicio.

"Cuando llegamos, de repente el encargado, como que va a buscar un papel, y desde la computadora, en el despacho, hace los ajustes electrónicos o desde la *palm* o desde el celular", agrega José Rodrigo Roque.

La Norma Oficial Mexicana 005, impide a los verificadores de la Profeco revisar los dispositivos electrónicos de las bombas, donde es general el fraude.

Carlos Arce Macias, procurado federal del Consumidor, señala que "estamos jugando 'al gato y al ratón', y ciertamente no tenemos las trampas necesarias para cazar al ratón, esto únicamente lo podemos tener si hay modificación rápida a la normatividad, a la regulación vigente".

Según un estudio de la Secretaría de Seguridad Pública Federal, cuatro de cada 10 gasolineras del país abastecen en promedio 5% menos gasolina de lo que pagan los clientes.

Una fraude que anualmente deja alrededor de 8 mil millones de pesos en ganancias.

7.3. RECOMIENDAN ACCIONES PARA PROTEGERSE DE FRAUDES ELECTRÓNICOS

Research publicó el documento "Como Evitar el Fraude Electrónico: Buenas Prácticas para Instituciones y Consumidores"

A fin de proporcionar una guía que ayude a combatir este problema creciente. Al respecto, la firma señaló que el esquema de fraude por correo electrónico ha afectado tanto a usuarios corporativos como a consumidores.

México, Marzo 2004 (Notimex) . - McAfee Research publicó el documento "Como Evitar el Fraude Electrónico: Buenas Prácticas para Instituciones y Consumidores" a fin de proporcionar una guía que ayude a combatir este problema creciente.

En un comunicado, Network Associates informó que seguir estas recomendaciones es hoy en día indispensable, toda vez que el esquema reciente de fraude por correo electrónico ha afectado tanto a usuarios corporativos como a consumidores.

Recordó que de acuerdo con el "Informe de Tendencias de los Ataques de Fraude Electrónico" publicado a principios de año por el Anti-Phishing Working Group (APWG), este tipo de agresiones han aumentado al grado de llegar a 5.7 por día en enero pasado.

Ante ello, la firma recomendó a los corporativos establecer políticas corporativas y comunicarlas a los usuarios finales, a fin de que puedan identificar un correo oficial de un mensaje estafador.

Asimismo, sugiere que se trabaje para una autenticación más confiable para sitios web, ya que si las instituciones no solicitan información importante a los usuarios finales cuando ingresan a un sitio, sería más difícil que los estafadores tengan esa información.

Además, propone monitorear internet por posibles sitios web fraudulentos, así como aplicar un antivirus de buena calidad con filtro y soluciones antispam en el punto de enlace de internet.

En cuanto a prácticas para consumidores, Network Associates recomendó bloquear automáticamente los mensajes de correo electrónico maliciosos o fraudulentos, tomando en cuenta que los detectores de spam pueden prevenir que el cliente abra los mensajes sospechosos, pero no son infalibles.

Además, sugirió detectar y borrar automáticamente programas maliciosos, como podrían ser los spyware, y bloquear automáticamente el envío de información importante a terceros con intenciones maliciosas.

Asimismo, ser precavido en todo momento, por lo que si no está seguro de que un mensaje es legítimo es recomendable que el usuario llame a la supuesta institución emisora para verificar la autenticidad.

7.4. REGLAS QUE HAY QUE SEGUIR PARA EVITAR SER VÍCTIMA DE UN FRAUDE ELECTRÓNICO

1. Buscar empresas serias y responsables. Aquellas que en sus políticas mencionen la devolución de su dinero de no estar satisfecho con la compra.

2. Las empresas deben contar con una dirección física donde se pueda contactar, así como con medios tradicionales de contacto: Correo postal, teléfonos, fax, etc.

Hay que tomar muy en cuanta que muchas empresas no tienen dirección física, sino su dirección hace referencia a una casilla postal.

3. No necesariamente la buena reputación de una empresa física se traslada al mundo virtual.

Muchas empresas gracias a sus recursos se han lanzado al web esperando crear un nuevo canal de ventas, pero no relacionan directamente sus procesos físicos con los virtuales, fallando en muchos casos con el usuario.

4. Validar descuentos y promociones especiales.

Si en su supermercado local jamás han existido esos precios, que ventajas tienen esa tienda para ofrecer esos precios y ser rentable.

Muchas empresas al lanzarse al comercio electrónico han reducido costos para ofrecer muy buenos descuentos, pero se han vuelto empresas pasajeras, dejando a muchos clientes inconformes.

5. Verificar el certificado de seguridad y la conexión segura antes de comprometer los datos de la tarjeta de crédito, así como otra información personal.

6. El uso de FAQs (Preguntas Frecuentes) le da una idea del movimiento que tiene cierto negocio en la red, y además muestra la preocupación de la tienda hacia nuevos clientes.

7. Si tiene alguna duda antes de comprar, tómela en cuenta y busque otras opciones para comparar. Podría encontrar mejores opciones.

Con estos consejos, el ser víctima de un fraude en la nueva forma de comercio es muy difícil.

Otra buena recomendación es verificar las políticas de seguridad de la empresa que maneja su tarjeta de créditos, pues han aprendido mucho de los fraudes y podrían asesorarlo antes de realizar alguna compra.

Muchas empresas locales ya se preocupan por consultar vía telefónica al tarjetabiente respecto a la transacción antes de realizar el pago, para verificar que no se hagan cargos extra.

7.5. LA NUEVA LEY DE LOS FRAUDES ELECTRONICOS

No sorprende que la proliferación de estos ataques haya llamado la atención de los legisladores de los Estados Unidos.

Aunque el proyecto de ley de robo de identidad firmado por el presidente Bush a comienzos de julio contempla estipulaciones obligatorias de cárcel para aquellas personas que utilicen una identidad robada para cometer un delito grave, la nueva ley no penaliza el fraude electrónico. El senador norteamericano, Patrick Leahy, quiere cambiar esta situación.

La Ley Anti-Phishing de Leahy de 2004, presentada en julio, abarca el fraude en su totalidad desde el envío de correo electrónico hasta la creación de sitios fraudulentos.

Estos actos se convertirán en delitos graves y estarán sujetos a cinco años en prisión y a una multa máxima de $250.000.

"Algunos estafadores pueden ser procesados de acuerdo a las leyes del Congreso contra el fraude electrónico o robo de identidad, aunque con frecuencia estas acusaciones tienen lugar únicamente después de que alguien ha sido defraudado"

Dijo Leahy cuando presentó el proyecto de ley, según un informe publicado en internetnews.com.

Cuando las personas no pueden confiar en lo que los sitios Web dicen ser, no utilizarán Internet para realizar transacciones seguras.

Por lo tanto, las leyes tradicionales del Congreso antifraude electrónico y antirrobo de identidad no son suficientes para responder a la estafa electrónica.

Esta legislación se encargará de declarar ilegal el envío deliberado de enlaces de correo electrónico suplantados para fingir sitios Web con la intención de cometer un delito.

En segundo lugar, esta ley penaliza los sitios Web falsos que sean un verdadero escenario del delito".

Sin embargo, la resolución de este asunto se pospondrá probablemente hasta que el Congreso vuelva a reunirse después del receso de verano.

8. HACKING

8.1. Antecedentes Históricos y Origen del Hacking

En los últimos 2 años, la intrusión en las computadoras se ha mas que triplicado. Quien está tratando de robar su información. Los hackers no se irán, así que es mejor saber quienes son y porque hacen lo que hacen.

La Internet está llena de sitios y consejos que sirven a los hackers neófitos en sus fechorías, tanto jóvenes, como criminales y terroristas tienen acceso a ella, lo que significa que un mayor número de intrusos está tocando las puertas.

A pesar de una mayor seguridad en la web y de penalidades más estrictas por irrumpir en los sistemas, los ataques de los hackers están por encima del triple en los últimos 2 años.

La mayoría de las compañías rehúsa informar sobre los ataques con el fin de evitar un impacto negativo en la publicidad.

Las estadísticas cubren desde las irrupciones en las redes locales (que le dan acceso al hacker a los archivos con la información), hasta el vandalismo en los sitios web, (los ataques de negación de servicios y el robo de la información).

Los riesgos que se corren aquí son personales y profesionales.

Los hackers se pueden robar las contraseñas y los números de cuentas bancarias de su PC ó pueden apoderarse de los secretos comerciales desde la red local de su compañía.

Este fenómeno también representa un riesgo contra la seguridad nacional, porque los terroristas más conocedores ó los gobiernos más hostiles, pudieran interrumpir los sistemas satelitales, llevar a cabo una guerra económica interfiriendo en las transferencias financieras ó incluso crear problemas en el control de tráfico aéreo.

Pero no todos los hackers tienen malas intenciones.

Algunos se encargan de la seguridad de los sistemas de las compañías y otros contribuyen a la seguridad avisándoles a los fabricantes de software, si encuentran algo vulnerable; sin embargo por cada hacker que cambia su sombrero negro por uno blanco, existen docenas que mantienen en vilo a las compañías y al gobierno.

Antes la piratería informática no tenía nada que ver con la violación de la ley ó el daño a los sistemas.

Los primeros hackers que surgieron en el Instituto Tecnológico de Massachussets en los años 60's estaban impulsados por el deseo de dominar las complejidades de los sistemas computacionales y de empujar la tecnología más allá de sus capacidades conocidas.

La ética del hacker, que es un dictamen aún sin escribir y que gobierna el mundo de la piratería, dice que un hacker no hará daño.

Pero esto no lo podemos comprobar, así que mientras estemos en la red, estamos "a su disposición". Existe por la red un documento llamado "Hacker manifiesto", el cual incluiremos en esta investigación.

Si una persona tiene motivos políticos contra alguna empresa, "X" y decide estropear su página web, solo tiene que entrar en línea y a1prender como hacerlo.

8.2. DEFINICIÓN

Hacker es una expresión idiomática inglesa cuya traducción literal al español tiene varios significados, siendo el más popular el atribuido a "una persona contratada para un trabajo rutinario" y que por la naturaleza del mismo su trabajo es tedioso, entregado, hasta diríase maniático.

El apelativo de hacker se crea a fines del siglo pasado cuando los Estados Unidos de América empieza a recibir un masivo movimiento migratorio de personas de todos los países del mundo que esperaban encontrar en el "país de las oportunidades" un bienestar económico y progreso.

Los hackers eran estibadores informales que se pasaban todos el día bajando las maletas y bultos de las personas y familias completas que llegaban en los barcos a los puertos de New York, Boston, San Francisco, etc.

Estos trabajadores eran infatigables, pues trabajaban muchas veces sin descansar y hasta dormían y comían entre los bultos de los muelles con el objeto de no perderse una oportunidad de ganar dinero.

La palabra "hack" en inglés significa "hacha" en español. Como si fuesen taladores de árboles que usan su hacha, en forma infatigable hasta llegar a tumbarlos, su tesonero propósito les mereció este apelativo.

La palabra hacker aplicada en la computación se refiere a la persona que se dedica a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía.

El hacker es alguien que se apasiona por las computadoras y se dedica a ellas más allá de los límites. Los hackers tienen "un saludable sentido de curiosidad: prueban todas las cerraduras de las puertas para averiguar si están cerradas.

No sueltan un sistema que están investigando hasta que los problemas que se le presenten queden resueltos".

"La revolución de la computación ha sido lograda gracias a los hackers", afirman categóricamente los famosos estudiosos e investigadores pioneros de los virus de computadoras Rob Rosenberg y Ross Greenberg.

"Un Hacker es una persona dedicada a su arte, alguien que sigue el conocimiento hacia donde este se dirija, alguien que se apega a la tecnología para explorarla, observarla, analizarla y modificar su funcionamiento

Es alguien que es capaz de hacer algo raro con cualquier aparato electrónico y lo hace actuar distinto, alguien que no tiene límites para la imaginación y busca información para después compartirla, es alguien al que no le interesa el dinero con lo que hace, solo le importa las bellezas que pueda crear con su cerebro, devorando todo lo que le produzca satisfacción y estimulación mental...

Un hacker es aquel que piensa distinto y hace de ese pensamiento una realidad con diversos métodos. Es aquel que le interesa lo nuevo y que quiere aprender a fondo lo que le interesa."

Hacker, originalmente, un aficionado a los ordenadores o computadoras, un usuario totalmente cautivado por la programación y la tecnología informáticas.

En la década de 1980, con la llegada de las computadoras personales y las redes de acceso remoto, este término adquirió una connotación peyorativa y comenzó a usarse para denominar a quien se conecta a una red para invadir en secreto computadoras, y consultar o alterar los programas o los datos almacenados en las mismas.

También se utiliza para referirse a alguien que, además de programar, disfruta desmenuzando sistemas operativos y programas para ver cómo funcionan.

El Hacking se considera una ofensa o ataque al Derecho de gentes, y no tanto un delito contra un Estado concreto, sino más bien contra la humanidad.

El delito puede ser castigado por los tribunales de cualquier país en el que el agresor se halle. La esencia del Hacking consiste en que el pirata no tiene permiso de ningún Estado soberano o de un Gobierno en hostilidades con otro.

Los HACKERS son considerados delincuentes comunes en toda la humanidad, dado que todas las naciones tienen igual interés en su captura y castigo.

Desde los inicios de la computación electromecánica a base de redes, bobinas y tubos de vidrio al vacío, las tareas de programación eran muy tediosas y el lenguaje de esos años era el críptico lenguaje de máquina y posteriormente se empleó el Assembler Pnemónico.

En la fase inicial de las computadoras, no como las concebimos ahora, hubieron hombres, mujeres, jóvenes y adultos entregados por entero a diversificadas tareas de investigación y experimentación, considerándose su trabajo, rutinario, sumamente perseverante y cuyos resultados sólo se han podido reconocer a través de los años.

Una mujer, la almirante de la armada norteamericana Grace Hooper es considerada el primer hacker de la era de la computación.

Mientras ella trabajaba e investigaba en la computadora Mark I, durante la Segunda Guerra Mundial, fue la primera persona que aseguró que las computadoras no solamente servían para fines bélicos, sino que además podrían ser muy útiles para diversos usos a favor de la humanidad.

Ella creó un lenguaje de programación denominado FlowMatic y años después inventó nada menos que el famoso lenguaje COBOL.

Desde hace algún tiempo el FBI de los Estados Unidos emplea el software "Carnivore" que espía a los usuarios de Internet y recientemente el Senado norteamericano le concedió la facultad de utilizarlo sin autorización judicial.

8.3. EL HACKING DESDE EL PUNTO DE VISTA LEGAL.

La detección de un hacker es bastante difícil. De hecho a no ser que esa persona quiera ser identificada es difícil llegar hasta ella.

En esta ocasión, se conoce que la información se enviaba a un servidor de San Petersburgo.

La policía se ve incapaz de perseguir estos delitos. En cada país la legislación es diferente o incluso inexistente.

Si el caso Microsoft hubiera ocurrido en España no se consideraría delito, ya que la ley española exige que se haga con ánimo de lucro, es decir, que reporte beneficio económico.

En el caso del virus I Love You el hacker conocía las lagunas legales que existían en algunos países.

8.4. ÉTICA

La ética hacker defiende la libertad absoluta de información: libre acceso y libre distribución, por lo que está emparentada estrechamente con la ética open source.

Para muchos defender tanto la libertad es algo muy parecido a defender la rebelión contra el sistema, y es cierto que hay un buen número de hackers que utilizan sus conocimientos para agredir al poder establecido en forma de instituciones o grandes corporaciones, pero el sensacionalismo que han despertado es absolutamente desmedido.

8.5. COMO HACKEAR UNA WEB HECHA EN PHP-NUKE

1º Buscamos alguna web que use php-nuke y que nos podamos registrar en ella (módulo Your_Count activo)

2º Nos vamos a cualquier web de seguridad (securityfocus.com, cyruxnet.org, ...) y buscamos alguna vulnerabilidad en el PHP-Nuke, normalmente de SQL Injection, que explote algún fallo para que nos muestre los hashes de los admin. de la web víctima.

3º Una vez probamos los fallos contra la web victima y encontrado algún hash de algún admin. pasamos a codificarlos a BASE64. Para eso nos vamos a la siguiente web: http://base64-encoder-online.waraxe.us/base64/base64-encoder.php

3.1 - Si vamos a hacer este método modificando una cookie del internet explorer en el cuadro de la web de codificador pondremos "nickadmin:hashadmin:" (sin las comillas) siendo nickadmin el nick de quien hemos sacado el hash y hashadmin su hash xD

3.2- Si vamos a hacer este método modificando una cookie del Mozilla en el cuadro de la web de codificador pondremos "nickadmin:hashadmin" (sin las comillas) siendo nickadmin el nick de quien hemos sacado el hash y hashadmin su hash xD

Aclaración Paso 3:(Localización de las cookies)

Explorer:
Win9x/Me -> C:\windows\cookies
Win2k/Xp -> C:\Documents and Settings\usuario\cookies

Mozilla:
Win9x/Me -> archivo cookies.txt
Win2K/Xp -> C:\Documents and Settings\□usuario□\Datos de programa\Mozilla
Linux -> locate cookies.txt

4º Vamos a la web victima y nos registramos en la misma.

------Recopilación--------

Una vez seguido estos 4 pasos tenemos:
- nickadmin:hashadmin codificados en base64
- una cuenta en la web victima
- su cookie correspondiente.

5º Antes de nada vamos a ver que forma tienen nuestra cookies según el navegador usado:
-> Internet Explorer:

lang
spanish
0
3932635008
29709902
1298043808
29636477
*
user
YWRtaW46MDk4ZjZiY2Q0NjIxZDM3M2NhZGU0ZTgzMjYyN2I0ZjY
0
3258712448
29642512
2770543808
29636477
*

-> Mozilla:

FALSE / FALSE 1092773634 user
YWRtaW46MDk4ZjZiY2Q0NjIxZDM3M2NhZGU0ZTgzMjYyN2I0ZjY

Observamos varias cosas:

a) Aparece la palabra "user"

b) Aparece la siguiente cadena
"YWRtaW46MDk4ZjZiY2Q0NjIxZDM3M2NhZGU0ZTgzMjYyN2I0ZjY" (no siempre es la misma, depende del nick y pass utilizados en el registro de la web)
Esta cadena es nuestro nick:hash convertido a base64

6º Modificación de la cookie

Primero cambiamos la palabra "user" por la palabra "admin"
Segundo cambiamos la cadena, en este ejemplo,

"YWRtaW46MDk4ZjZiY2Q0NjIxZDM3M2NhZGU0ZTgzMjYyN2I0ZjY"
por la que hemos obtenido en la de nickadmin:hashadmin.

7º Guardamos los cambios hechos en la cookie

8º Entramos en la web. En estos momentos entraremos como el admin. de la web al quien le hayamos
cogido el hash y nick

Aclaración

Cuando en la cookie cambiamos "user" por "admin" en realidad estamos cambiando el valor de las cookies de donde estamos identificados, identifican donos como admin en vez de como usuario normal y observaremos el cambio

En este texto observamos la facilidad de "hackear" una pagina web hecha con PHP-Nuke y sin ningún conocimiento. Este texto es PURAMENTE didáctico y no pretende que con la lectura
del mismo se utilice para "hackear" nada.

9. PORNOGRAFIA INFANTIL EN INTERNET

9.1. COMO HACER UN DICTAMEN EN INFORMATICA FORENSE SOBRE PORNOGRAFIA INFANTIL EN INTERNET

UMQ UNIVERSIDAD VASCO DE QUIROGA

Universidad Vasco de Quiroga

01/07/03
01/ExDIPIF/UVAQ

ASUNTO: Se rinde Dictamen en Materia de Informática.

Morelia, Mich. A 22 de Julio del 2003

Ing. Miguel Ángel Álvarez Martínez
Instructor del Diplomado de Informática Forense.
P r e s e n t e.

La Lic. Ulises Fernando Ramírez Toledo egresado de la universidad vasco de Quiroga, cursando el Diplomado de Informática Forense Impartido por el Instituto Nacional de Ciencias Forenses S.C. en coordinación con la Universidad Vasco de Quiroga.

PLANTEAMIENTO DEL PROBLEMA.
Determinar si el sitio de nominado yahoo México existe algún grupo que promueva la pornografía infantil o que la tenga para la disposición de otros usuarios.

METODOLOGÍA.
Para la elaboración del presente dictamen se utilizaron los métodos inductivo, descriptivo y el analítico.

1. De lo general a lo particular.
2. Analizar la información.
3. Hacer conclusiones.

UNIVERSIDAD VASCO DE QUIROGA

Universidad Vasco de Quiroga

01/07/03
01/ExDIPIF/UVAQ

DESCRIPCIÓN DE ELEMENTOS.

Se analizo el portal de Internet "yahoo México" junto con todos sus grupos existentes.

ESTUDIO TÉCNICO PERICIAL.

Se utilizo una computadora personal para la investigación del portal "yahoo México" para accesar a dicho portal se utilizo la aplicación de Internet Explorer

Datos del portal "yahoo México"

DOMINIO: yahoo.com.mx IP 66.218.66.241

FECHA DE CREACION: 06-OCT-97
FECHA DE ULTIMA MODIFICACION: 12-DEC-02

ORGANIZACION: Yahoo! Inc. [yahoo2]
DOMICILIO: Sunnyvale , California, Estados Unidos de América

CONTACTO ADMINISTRATIVO: Yahoo Mail [yahoo]
DOMICILIO: Sunnyvale, California, Estados Unidos de América

CONTACTO TECNICO: Yahoo Mail [yahoo]
DOMICILIO: Sunnyvale, California, Estados Unidos de América

CONTACTO DE PAGO: Domain Billing [dnbil]
DOMICILIO: Walnut Creek, California, Estados Unidos de América

SERVIDOR PRIMARIO: ns1.yahoo.com

SERVIDOR SECUNDARIO: ns2.yahoo.com

SERVIDOR SECUNDARIO: ns3.yahoo.com

SERVIDOR SECUNDARIO: ns4.yahoo.com

SERVIDOR SECUNDARIO: ns5.yahoo.com

UNIVERSIDAD VASCO DE QUIROGA

Universidad Vasco de Quiroga

01/07/03
01/ExDIPIF/UVAQ

Proseguimos a accesar al sitio mencionado, de pues se hizo el registro llenando un formulario con datos personales del investigador una vez registrados accesamos a la opción de grupos continuamos la búsqueda de grupos que promueven la pornografía infantil, encontrando dos grupos.

El primer grupo esta registrado con la dirección:
IP 66.218.66.241
"http://mx.groups.yahoo.com/group/adoraciondepiesdeninos/"

La cual fue fundada el 26 de agosto del 2001 esta integrada por 280 miembros su idioma principal es el español, no se encontró el creador del grupo, pero sí un miembro activo llamado Alejandro J. C. Tlaxcala México 24 años de edad, ing. Civil.

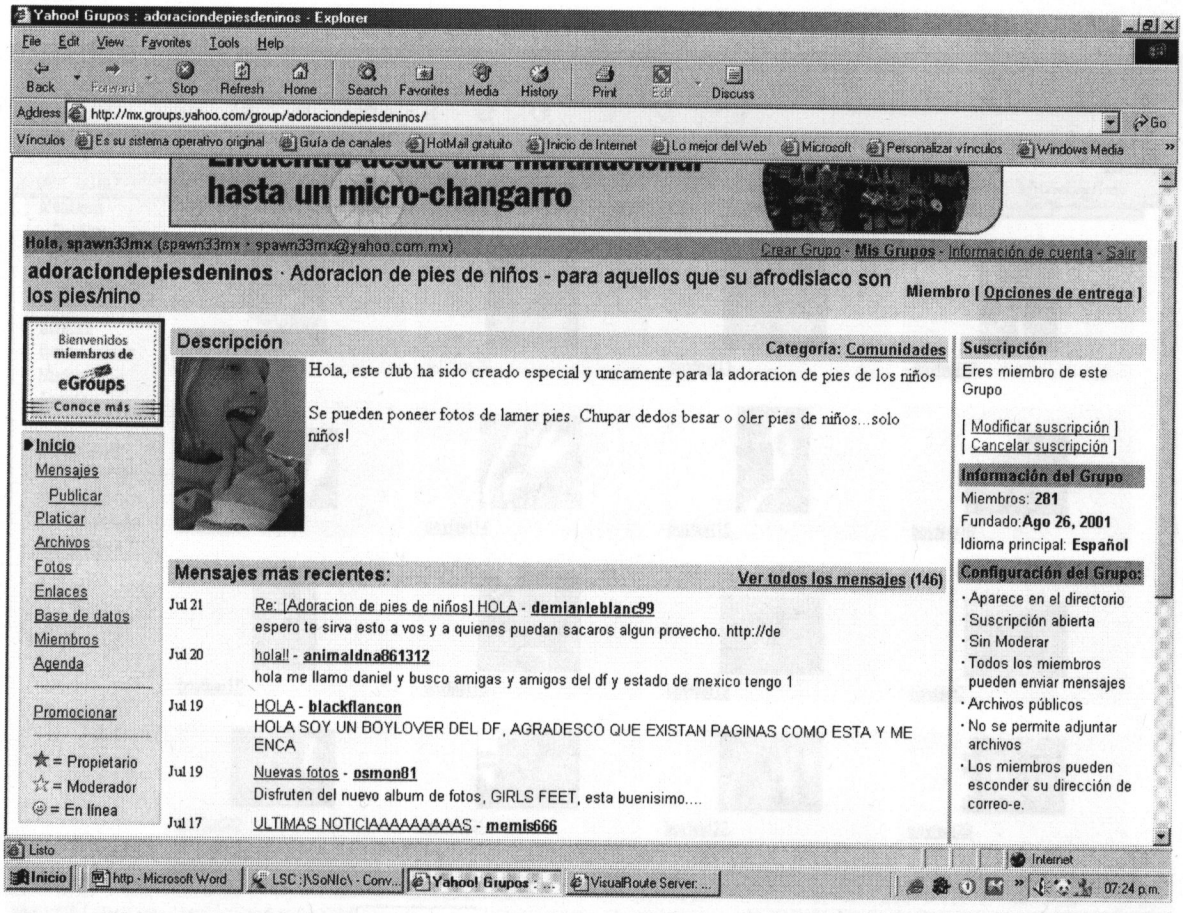
" Su fin de este grupo es promover el morbo hacia los niños", el cual se encontraron imágenes, archivos y links que promovían estos actos.

UNIVERSIDAD VASCO DE QUIROGA

Universidad Vasco de Quiroga

01/07/03
01/ExDIPIF/UVAQ

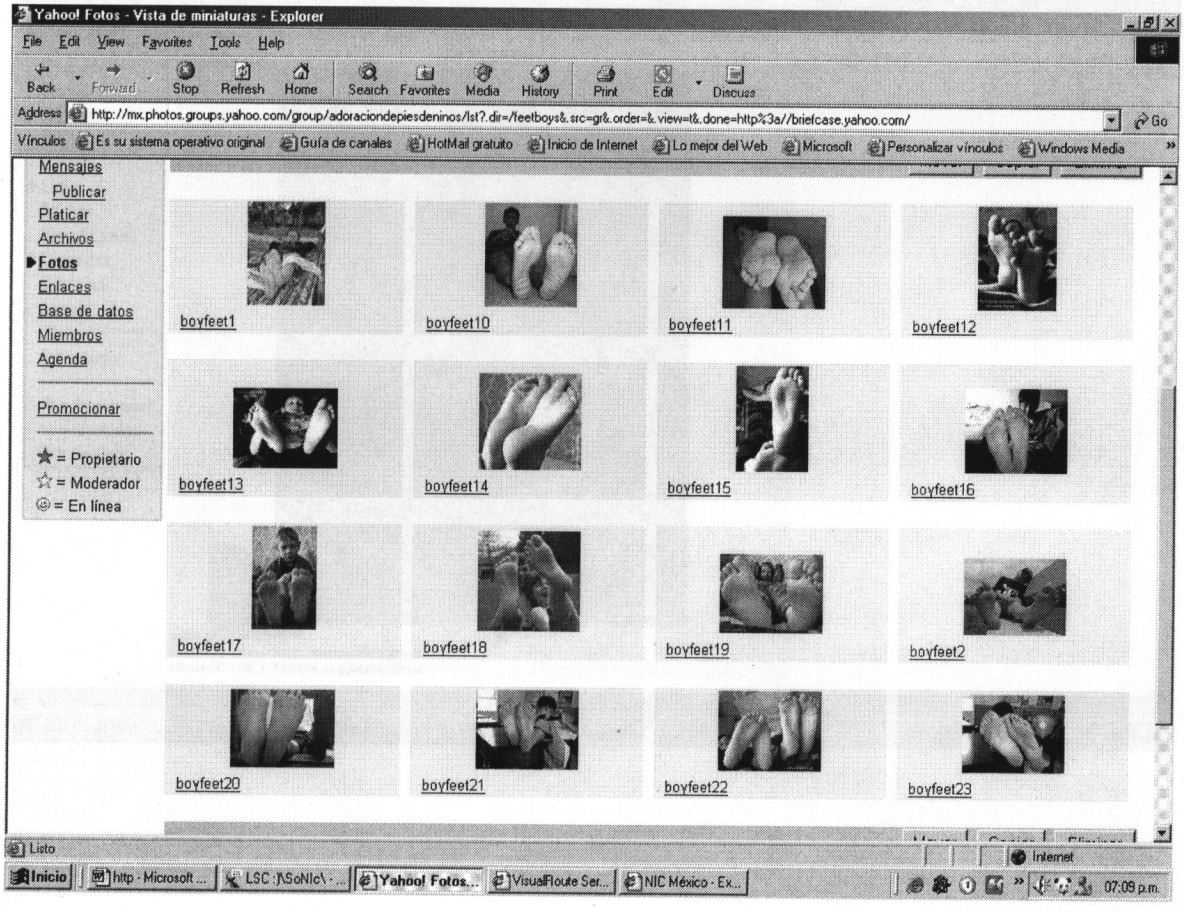
Pagina principal
"http://mx.groups.yahoo.com/group/adoraciondepiesdeninos/"



Universidad Vasco de Quiroga

01/07/03
01/ExDIPIF/UVAQ

Muestra de algunas fotos que se encuentran en este grupo

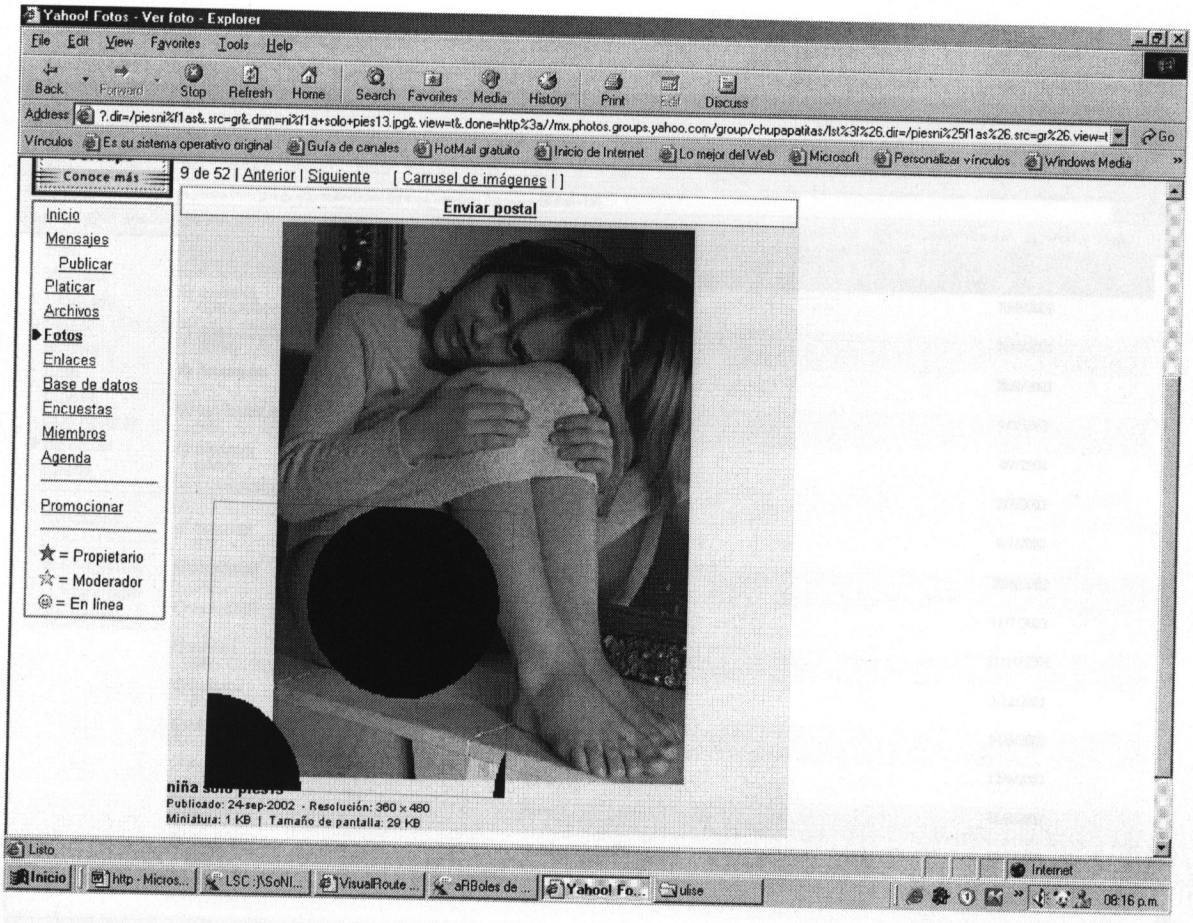


UNIVERSIDAD VASCO DE QUIROGA

Universidad Vasco de Quiroga

01/07/03
01/ExDIPIF/UVAQ

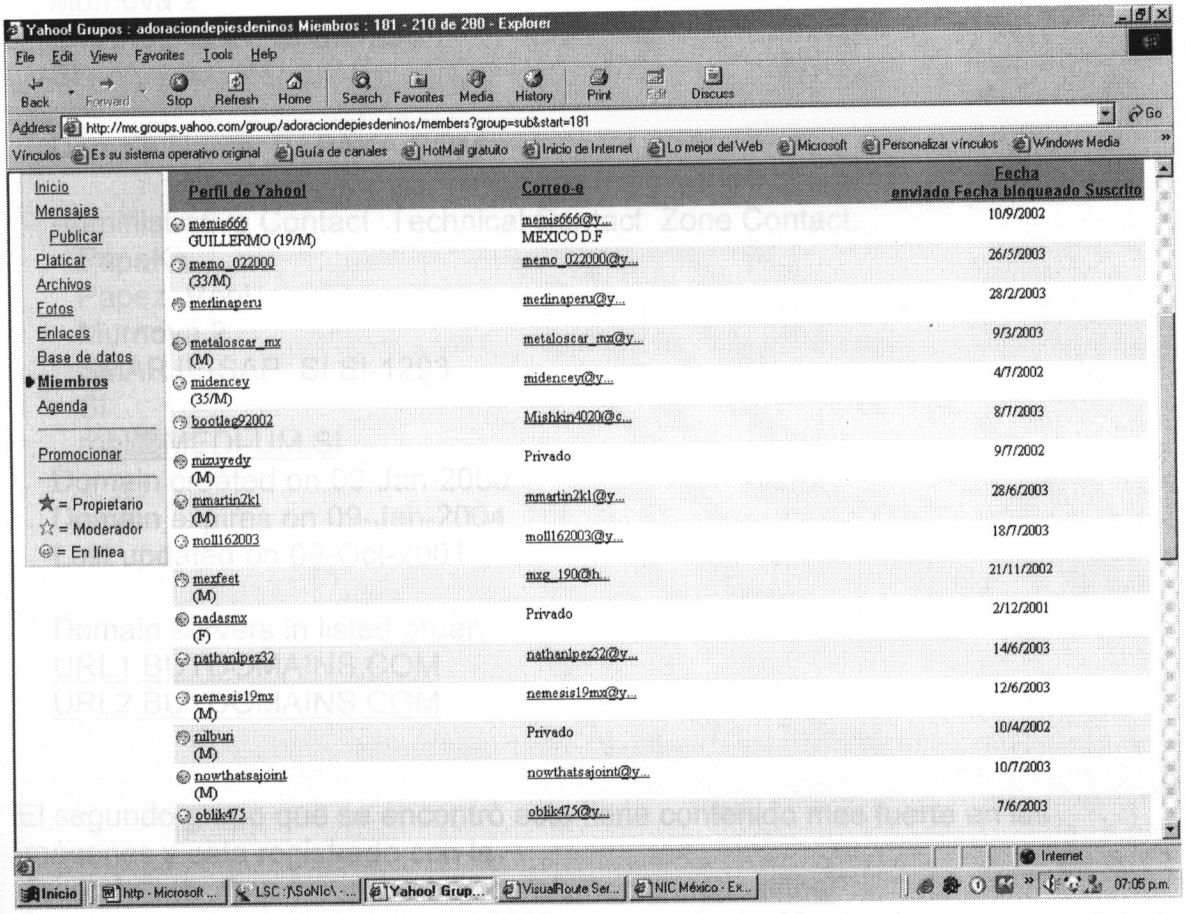
Ejemplo de la pornografía infantil



Universidad Vasco de Quiroga

01/07/03
01/ExDIPIF/UVAQ

Pagina de los miembros activos



UNIVERSIDAD VASCO DE QUIROGA

Universidad Vasco de Quiroga

01/07/03
01/ExDIPIF/UVAQ

link encontrado en el grupo adoración de pies de niños

link de papaka IP 209.62.216.42

Registrant:
PapaKa
Murnova 2
SMARJE-SAP SI SI-1293
SI

Domain Name: PAPAKA.COM

Administrative Contact Technical Contact Zone Contact:
PapaKa
Papez Robi
Murnova 2
SMARJE-SAP SI SI-1293
SI
robi@MEDI-UM.SI
Domain created on 09-Jan-2000
Domain expires on 09-Jan-2004
Last updated on 09-Oct-2001

Domain servers in listed order:
URL1.BUYDOMAINS.COM
URL2.BUYDOMAINS.COM

El segundo grupo que se encontró este tiene contenido mas fuerte en las imágenes y esta registrado con la dirección"http://mx.groups.yahoo.com/group/chupapatitas/"
Que fue creado el 19 de julio del 2002 que consta de 45 miembros y su propietario es chupapatitas, su mail es goquh84@hotmail, su idioma principal es español, en este grupo se encontró pornografía infantil.

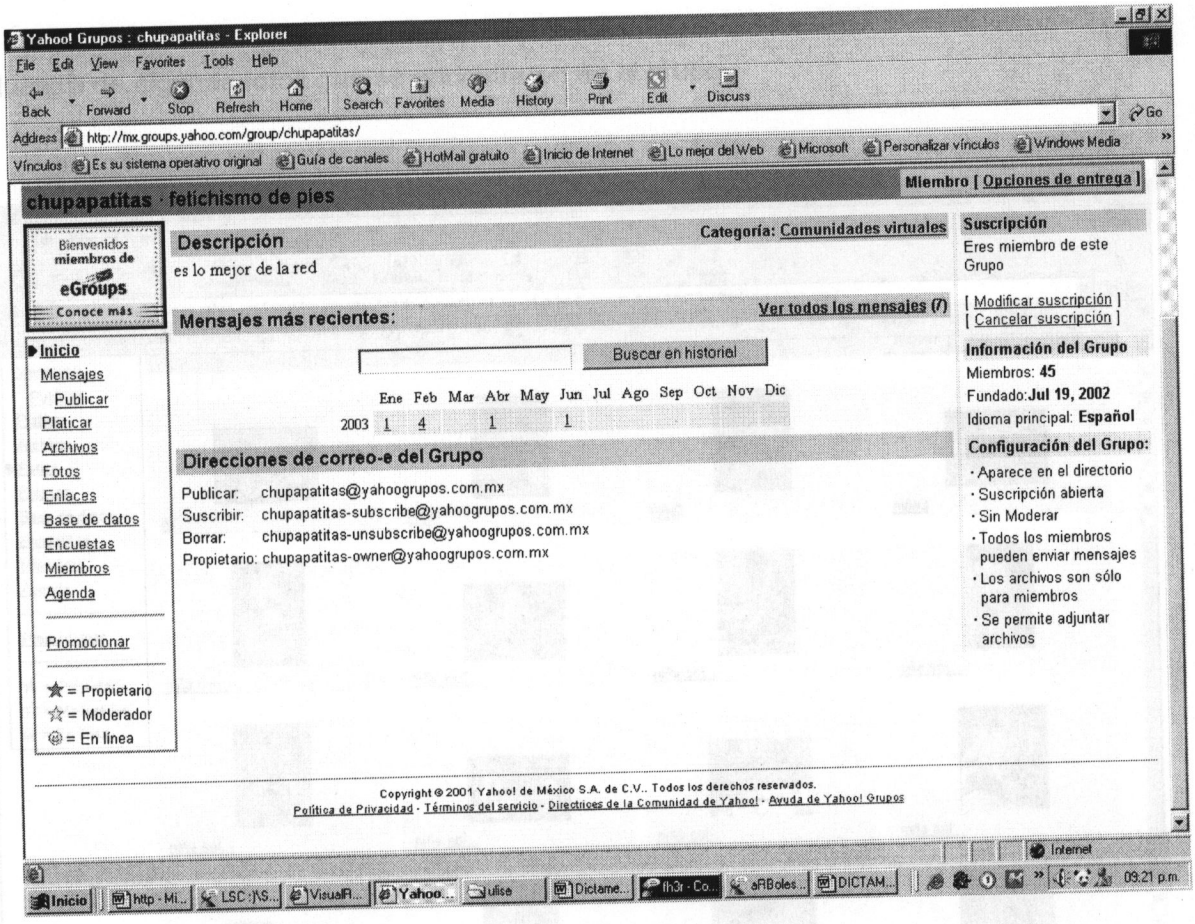
DOMINIO: yahoo.com.mx IP 66.218.66.241

UNIVERSIDAD VASCO DE QUIROGA

Universidad Vasco de Quiroga

01/07/03
01/ExDIPIF/UVAQ

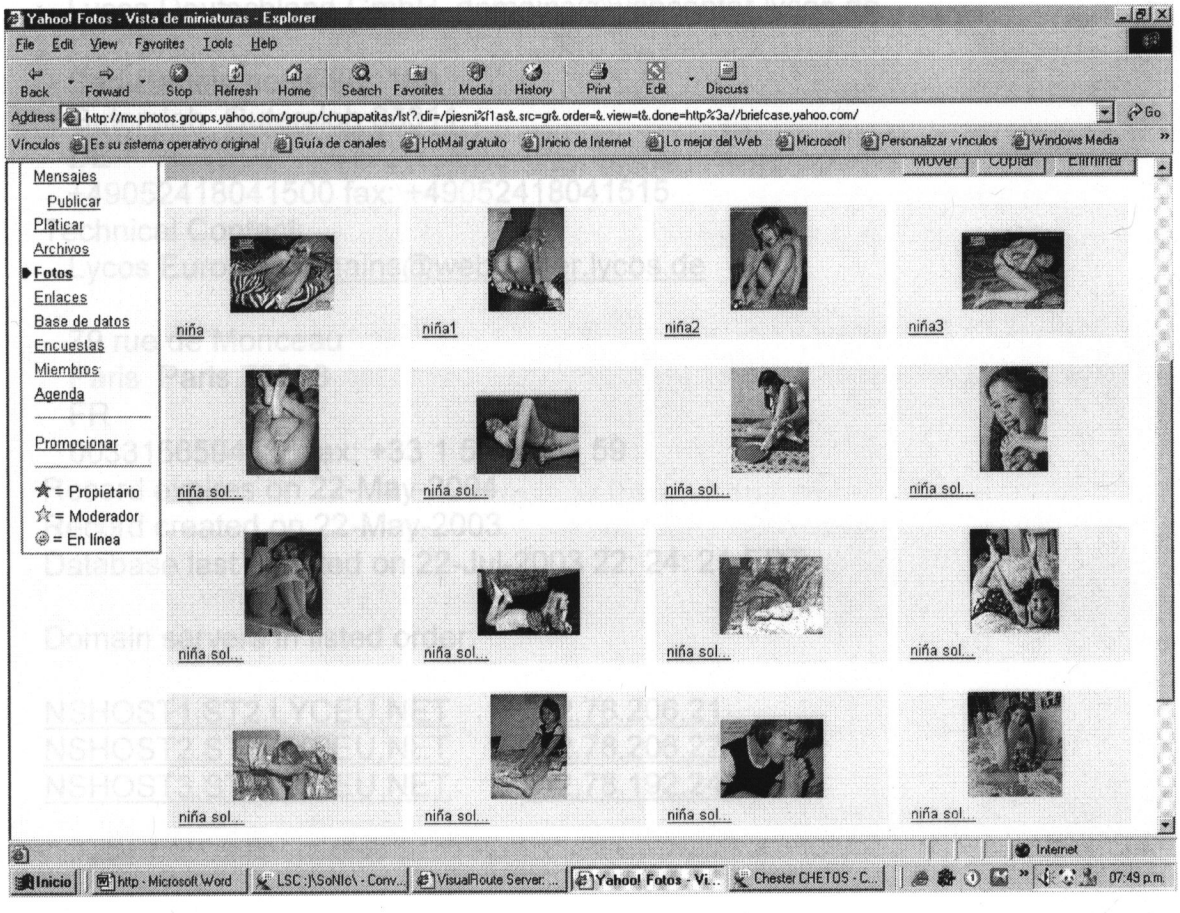
Pagina principal



Universidad Vasco de Quiroga

01/07/03
01/ExDIPIF/UVAQ

Muestra de algunas fotos que se encontraron en el grupo



UNIVERSIDAD VASCO DE QUIROGA

Universidad Vasco de Quiroga

01/07/03
01/ExDIPIF/UVAQ

además se encontró un link
"http://www.worldfeetlinks.com/ " y su IP 212.78.206.150 Sweden

Domain Name: WORLDFEETLINKS.COM

Administrative Contact:
Lycos Deutschland GmbH domains@webcenter.lycos.de

Carl-Bertelsmann-Str. 180
Gutersloh Gutersloh 33311
DE
+49052418041500 fax: +49052418041515
Technical Contact:
Lycos Europe domains@webcenter.lycos.de

79 rue de Monceau
Paris Paris 75008
FR
0033156594508 fax: +33 1 53 96 03 59
Record expires on 22-May-2004.
Record created on 22-May-2003.
Database last updated on 22-Jul-2003 22: 24: 21 EDT.

Domain servers in listed order:

NSHOST1.ST2.LYCEU.NET	212.78.206.21
NSHOST2.ST2.LYCEU.NET	212.78.206.22
NSHOST3.ST2.LYCEU.NET	212.78.192.249

UNIVERSIDAD VASCO DE QUIROGA

Universidad Vasco de Quiroga

01/07/03
01/ExDIPIF/UVAQ

CONSIDERACIONES TÉCNICAS.

Explorer: es una una aplicación que sirve para tener acceso a Internet

Dirección IP: números de 32 bits representados habitualmente *en formato decimal* Para identificar una máquina en Internet.

Link: son enlaces a otra paginas web

CONCLUSIONES.

La pagina investigada "yahoo México" en el área de grupos de la misma fue inspeccionada muy detalladamente, con el fin de encontrar pornografía infantil ya fuera para promoverla o que la contenga y hubo éxito por que fueron halladas dos paginas.

Atentamente,

Ulises Fernando Ramírez Toledo
Licenciado en Sistemas Computacionales

_____
Firma

10. TRAFICO DE DROGAS EN INTERNET

10.1. DROGAS EN INTERNET

La red para bien o para mal, es un reflejo de la vida cotidiana a través de las autopistas de la información.

Una clara muestra de esto es el problema de las drogas, ya que por un lado están aquellos que utilizan Internet para combatirlas, también hay quien la ha convertido en una ayuda para la fabricación y distribución.

El conocimiento de los efectos para la salud de las drogas es esencial para la prevención de dependencias.

La educación es, según los expertos, la única forma de evitar nuevos adictos y la red colabora en esta tarea.

Aunque la red también favorece la venta ilegal de estupefacientes e incluso su fabricación, estos dos últimos problemas son los dos puntos que más de cabeza traen a los países del mundo empeñados en acabar con un mercado tan perjudicial como es el de las drogas.

Páginas contra la adicción

Una buena página en castellano para conocer los entresijos de los estupefacientes es Tardis. El web nació en 1998 como resultado del Plan de Acción sobre Drogas de Barcelona y al amparo de la Comunidad Europea.

Su objetivo es dar respuesta a la demanda social de un plan de acción frente al consumo de drogas y los problemas relacionados con el mismo.

El diseño es muy llamativo y desenfadado, pero sus contenidos son serios y rigurosos. El apartado más interesante es el dedicado a la enumeración de drogas y sus efectos a corto y largo plazo.

Además de visual, es preciso por lo que conecta con el público al que va dirigido: los jóvenes.

El Instituto para el Estudio de las Adicciones (IEA) presenta un portal donde se recogen noticias, novedades, estudios e informes relacionados con la drogadicción.

La librería virtual permite la compra de libros relacionados con este tema desde la web. Además cuenta con foros y chats.

Web of Addictions, es una página creada por dos psicólogos americanos que incluye una útil colección de enlaces, una guía de conferencias, artículos para profesionales y varios grupos de apoyo.

Una de las páginas más completas que existe en castellano es la web personal de Manuel González Rey.

Además de un repaso por la historia de los estupefacientes aporta un interesante recorrido por cada una de las clases de drogas.

Las noticias aparecidas en prensa y varios textos relacionados con el consumo de sustancias y su tratamiento completan este sitio de referencia indispensable.

Los portales dedicados a la psicología en general suelen ser una buena opción para obtener información sobre drogas.

Así por ejemplo Psicología Mundo y Psiquiatria.com disponen de secciones dedicadas a este tema.

Aunque la crudeza del tema es obvia, también se puede tratar de forma más distendida, este es el caso del web de Especialistas contra las Drogas.

Con la intención "de favorecer los aspectos de comprensión y educación acerca de los síntomas principales que presenta el Drogodependiente y su familia" Elsa Hilda Gervasio, Directora de la Comunidad Terapéutica.

El Reparo, y el Diego Alejandro Pares, dibujante humorístico, produjeron una forma gráfica, amena y clara, de acceder al conocimiento de los síntomas de esta dramática enfermedad.

10.2. LA PREPONDERANCIA DE INFORMACIÓN SOBRE DROGAS EN INTERNET

El fomento del uso parece ser la actividad virtual más común en cuanto a las drogas, y los sitios web que se dedican a esto a menudo se dirigen a un público más juvenil. Muchos portales y foros de la red promueven la producción y la venta de drogas ilícitas.

Uso. La información acerca del uso de drogas es fácilmente accesible a través de Internet.

Los jóvenes que tienen curiosidad en saber más sobre una sustancia en particular pueden investigar usando buscadores, entrando en miles de sitios web que alaban los efectos positivos de las drogas, a la vez que intentan minimizar o negar cualquier consecuencia negativa que puedan tener.

Además, normalmente explican y emplean la terminología y jerga de la cultura de drogas, familiarizando así a la persona aún más con este mundo.

Buena parte de los sitios web engañan al cibernauta cuando le explica cómo abusar de las drogas, al insinuar que si se las consumen de forma adecuada (al seguir las instrucciones brindadas), no corre ningún riesgo.

Por otra parte, hay páginas que informan a los internautas acerca del abuso de productos corrientes, tales como los medicamentos contra los resfriados, para que les produzcan efectos eufóricos.

Producción. Internet ofrece cantidades extensas de información sobre la producción de drogas, y cualquier persona que tenga acceso a ella puede conseguir datos sobre los procesos de producción, las recetas, los ingredientes necesarios, y los sucedáneos.

La comercialización del equipo de producción se ha generalizado y los productos químicos que se necesitan en este proceso también se pueden pedir.

Por lo tanto, los fabricantes de droga inexpertos consiguen fácilmente todo lo necesario para producir una variedad de drogas ilegales en laboratorios caseros montados en su cocina, cuarto de baño, o sótano.

La diseminación de información errónea es bastante común, lo que conlleva el riesgo de lesiones graves, enfermedades, y la muerte.

Venta. Los jóvenes no encuentran obstáculos a la hora de buscar en Internet proveedores de droga, sea para comprársela en cantidades aptas para la venta al por mayor o simplemente para el consumo personal.

Se anuncia abiertamente la venta de drogas ilícitas y los proveedores y clientes conciertan las transacciones mediante intercambios por tablones de anuncios.

Hay tiendas virtuales donde se consiguen con facilidad el equipo de producción de drogas, los productos químicos, y otros accesorios.

Es importante subrayar que alguien que ya tenga contactos tendrá menos dificultades a la hora de comprar drogas, así como ocurre en el ámbito tradicional de distribución de drogas.

Por ejemplo, existen numerosos foros en la red que no están clasificados en los buscadores; es decir, no salen en buscadores al escribir terminología relacionada con las drogas, sino que requieren conocimiento previo para tener acceso.

Según la International Criminal Police Organization (Interpol) (la Organización Internacional de Policía Criminal), a principios del 2000 las autoridades de Gran Bretaña e Irlanda del Norte identificaron más de 1.000 sitios web de todo el mundo que anunciaban la venta virtual de drogas ilícitas, sobre todo el cannabis, pero también la MDMA, la cocaína, y la heroína.

Los Países Bajos y Suiza tienen el mayor número de portales de este tipo, aunque en Estados Unidos también hay personas que venden drogas ilícitas por Internet.

10.3. TIPOS DE DROGAS ILÍCITAS MÁS FRECUENTES EN INTERNET

La marihuana parece ser la droga que más se promueve en Internet, y se obtiene con facilidad información acerca de su cultivo, consumo, y venta.

Por otra parte, se divulgan en el ciberespacio datos sobre los accesorios para consumir drogas, sobre todo aquellos relacionados con la marihuana.

Se intercambia información de forma virtual acerca de la MDMA (éxtasis), la LSD, la GHB, y los hongos psilocibios, todos ellos "drogas de club" populares que se consumen en las discotecas o las fiestas raves.

Los jóvenes, los cuales son los que más abusan de las antedichas drogas, son más propensos a caer presos de estos foros de Internet.

Un número creciente de páginas web están orientadas hacia las fiestas juveniles, dando información sobre la próxima rave o macro fiesta en una discoteca donde las drogas de club se venden y se consumen.

Marihuana y los Accesorios Relacionados con las Drogas.

Muchas páginas web venden las semillas de marihuana, además de los instrumentos para su cultivo y consumo--tales como los *kits* de cultivo, los vaporizadores, y las pipas de agua (los narguiles) de buena calidad.

Otras brindan información pormenorizada sobre el cultivo del cannabis y ofrecen hasta muestras gratuitas de semillas. Hay datos virtuales detallados sobre los métodos empleados para fumar e inhalar la marihuana--sea pipa, cigarrillo, o vaporizador--e instrucciones para liar distintos tipos de cigarrillos de marihuana.

La mayoría de los accesorios relacionados con las drogas en Internet son relacionados con la marihuana.

Muchos de estos accesorios se ven como artículos cotidianos, a veces porque están literalmente metidos dentro de la parte exterior de los últimos.

Entre los dispositivos de consumo más populares que se venden en línea están las "pipas ocultas" o las "pipas disfrazadas," las cuales tienen la apariencia de tubería de cobre o fontanería, pero en realidad están diseñadas para ocultar y administrar drogas.

Otras pipas se parecen a recipientes para ungüento de labios, resaltadores, rotuladores, estuches de pintalabios, linternas pequeñas, puros, balas, mecheros, llaveros, paquetes de tabaco, pinceles de maquillaje, y tubos de rimel.

Algunas páginas web brindan instrucciones sobre la producción casera de estos accesorios e incluyen, por ejemplo.

Patrones para pipas de agua, con los cuales los usuarios pueden encontrar toda la información detallada para hacer distintos tipos de pipas de agua empleando artículos cotidianos, tales como botes de cristal, botellas de refrescos de cristal, rollos de papel higiénico, tuberías de PVC, o papel de aluminio.

MDMA. La MDMA (3,4-metilenedioxi-metanfetamina), también llamada éxtasis, E, X, y Adán, es un estimulante que tiene propiedades alucinógenas.

El consumo de esta sustancia tiene más aceptación entre los jóvenes y se suele ingerir en las raves y discotecas. El consumo de la MDMA se promueve y se realza en muchas páginas web y tablones de anuncios en los cuales los usuarios hablan de sus experiencias bajo los efectos de esta droga.

Las páginas web que se dedican a promover las fiestas rave, discotecas, y la legalización de drogas suelen describir MDMA en términos muy benignos, alegando pocos efectos secundarios, a pesar de ser un estimulante peligroso cuyo uso puede provocar la hipertermia aguda (subida de la temperatura corporal), la deshidratación y, a veces, la muerte.

Por otra parte, hay información abundante en Internet que se comparte en los chats y mensajes virtuales con respecto de la producción de la MDMA, información a la cual tienen acceso participantes de la cultura rave.

La MDMA se fabrica a partir de varias sustancias químicas precursoras, la mayoría de las cuales son controladas por las leyes federales.

De forma virtual, los fabricantes pueden identificar proveedores de estos precursores, obtener las recetas e instrucciones para fabricar la MDMA, y conversar sobre este último proceso con otros usuarios.

Por ejemplo, la *Drug Enforcement Administration* (*DEA*) (la Administración para el Control de Drogas) anunció la detención de dos estudiantes que estaban haciendo sus tesis doctorales en química, uno de Georgia y el otro de Arizona, quienes bajaron de Internet las instrucciones para producir la MDMA, la metanfetamina, y precursores químicos y hacían comentarios sobre su progreso mediante correos electrónicos.

Heroína. En muchas zonas del país, heroína de alta pureza está de moda entre los jóvenes de clase media y alta, ya que se la pueden aspirar o fumar, en vez de inyectar.

En la red se venden las semillas para cultivar las amapolas de opio (las cuales dan heroína no procesada) y se brinda información sobre su cultivo y extracción.

La mayoría de la información disponible en Internet relacionada con la heroína tiene que ver con su consumo por vía nasal e intravenosa, aunque este último método es el más recomendado.

La heroína, a pesar de ser peligrosamente adictiva y, en muchos casos, mortífera, se potencia como una sustancia empleada en las raves para bajar de los efectos de la MDMA y aliviar el estrés y dolor físico.

Con toda probabilidad la venta de la heroína se hace en los chats y las redes de páginas web y el consumo de la misma se fomenta mediante el uso de los tablones de anuncios, además de los chats.

Cocaína/Crack. En Internet se consiguen con facilidad datos acerca del uso de la cocaína y tanto los usuarios como los propietarios de la página web suelen presentar el consumo de cocaína como una opción al glamour.

Estas páginas diseminan datos mediante los chats, tablones de anuncios, y grupos de noticias, los cuales debaten específicamente los distintos métodos de consumir la cocaína en polvo y el crack, tales como aspirar, inyectar, fumar, e ingerir.

Hay datos disponibles sobre todo tipo de temas relacionadas con la cocaína, incluyendo las dosis recomendadas, consideraciones jurídicas, la historia del consumo de la misma, los diversos efectos psicológicos y físicos de la cocaína en polvo y el crack, además de los mejores accesorios para aspirar, inyectar, fumar, e ingerir la droga.

Por otra parte, hay instrucciones y "recetas" para transformar la cocaína en polvo en base de cocaína o crack e inclusive existe un directorio virtual que sirve para poder localizar a traficantes de crack, brindando información sobre aquellos que operan en las áreas metropolitanas más importantes.

Por otra parte, se pueden encontrar informes detallando el precio de la cocaína y la pureza de la misma en la mayoría de los estados del país.

11. TRAFICO DE ARMAS DE FUEGO EN INTERNET

11.1. VENTA ILEGAL DE ARMAS VÍA INTERNET

Comercios estadounidenses dedicados a la venta de armas de fuego admiten vía web órdenes ilegales de compra.

En Estados Unidos, país donde poseer un arma de fuego es un derecho ciudadano, el 50% de las empresas del ramo presentes en Internet aceptan órdenes de compra en línea, sin verificar la identidad o edad del comprador.

Con ello, tales empresas incurren en una violación directa de las leyes que regulan la venta de armas a personas naturales.

La irregularidad fue detectada por la publicación Internet Report, que se dirigió a los sitios web de vendedores de armas para encargar un potente revólver 380 Smith & Wesson.

Según se constató, casi la mitad de los vendedores estaban dispuestos a realizar la venta sin siquiera preguntar la edad del comprador.

De igual modo, fue perfectamente posible enviar el arma por correo, en contravención total de las reglas.

En efecto, las ventas de armas a distancia obligan al vendedor a despachar el artículo a otro comercio autorizado, que entonces contacta al comprador, quien debe acudir personalmente a retirarlo.

Antes de poder retirar el arma, el comprador debe cumplir con un plazo de espera y probar su idoneidad para poseer armas de fuego.

Finalmente, la publicación recuerda que el año pasado el propietario de un negocio de venta de armas fue detenido por distribución ilegal, luego que una mujer detectara una pistola semiautomática en un paquete que su hijo recibió por correo.

11.2. COMO COMBATIR EL TRAFICO ILEGAL DE ARMAS DE FUEGO EN INTERNET

La población se sentirá más protegida y no acudirá al mercado negro para comprar armas, ya que la simplificación de los trámites administrativos para obtener licencias ha sido modificada y tan solo bastará con la presentación de una declaración jurada que remplazará a los certificados de antecedentes penales, judiciales y policiales.

"Lo que se busca es combatir el tráfico ilegal de armas de fuego" preciso el ministro del Interior, Fernando Rospigliosi, al ser consultado sobre esta decisión de su despacho.

La modificación se fundamenta también en el artículo 41º de la "Ley de Procedimiento administrativo General", la cual indica que para cumplir con los requisitos para realizar alguna solicitud en una entidad pública.

Estas se encuentran obligadas a recibir "las expresiones escritas" contenidas en declaraciones juradas, mediante las cuales los solicitantes dejan constancia de su situación favorable en relación con los requisitos solicitados.

El titular del sector Interior sostuvo que lo que se busca es simplificar la vida a los ciudadanos. "Muchos recurren al mercado negro por lo engorroso que resulta obtener una licencia. Queremos fomentar la formalidad"

Requisitorias dará antecedentes

En cuanto a la verificación de los antecedentes de las personas que solicitan el permiso para portar armas, el ministro informó que esta labor la realizará la Dirección de General de Control de Servicios de Seguridad, Control de Armas, Munición y Explosivos de Uso Civil (DICSCAMEC).

Para este fin se tendrán que implementar una red computarizada, que permitirá acceder a la base de datos que tiene la División de Requisitorias. "De esta manera una persona con historial delictivo no podrá ser autorizada".

Los Requisitos

Los ciudadanos que deseen tramitar su licencia para portar armas de uso personal ya sea para defensa personal, deporte, caza, seguridad, vigilancia, y colección deberá presentar los siguientes requisitos ante la Discamec.

Solicitud en formulario impreso, Copia del DNI o carné de extranjería, certificado de salud mental, copia de factura o boleta cancelada, carta de la empresa comercializadora para el retiro del arma, y recibo de pago en el Banco de la Nación. Asimismo en la dependencia policial asignada deberá aprobar el examen de manejo de arma y tiro.

Se informó que la PNP se encuentra realizando constantes operativos en diversos puntos del país con la finalidad de requisar pistolas, revólveres o fusiles que se venden ilegalmente.

12. TRAFICO DE ANIMALES EN INTERNET

Querétaro, Qro.- Mediante el internet aprovechándose del anonimato que esta vía permite en México se realiza la venta ilegal de especimenes de animales llamados "exóticos" o en peligro de extinción, incluyendo jaguares, monos titi, iguanas, guacamayas y serpientes, entre otros.

La Procuraduría Federal de Protección al Medio Ambiente (Profepa) investiga el ilícito que a decir del delegado en Querétaro, Enrique Uribarren Castro, se ha convertido en la tercera acción ilícita en el país que reditúa amplias ganancias a quienes la practican, solamente después del tráfico de drogas y de la venta ilegal de armas.

"Enfrentamos un novedoso esquema de venta, muchas veces ilícita, de ejemplares exóticos o en peligro de extinción a través del internet.

Esta vía ha garantizado a quienes se dedican a esta actividad permanecer en el anonimato".

Explicó que varias de estas páginas web ya son investigadas por la Profepa, primeramente para determinar si son instancias que cuentan con la autorización para poder comercializar crías de animales exóticos, aunque ninguna está autorizada para vender animales en peligro de extinción o declarados en veda.

Una de las páginas de internet que ya se investiga originada en el centro de la República Mexicana tiene a la venta ejemplares de jaguar negro y jaguar pinto, así como de titi orejas de algodón, titi manos rojas, mono ardilla y de ardilla voladora, que son especies en veda o en peligro de extinción.

En otras dos páginas de la *web* (una de ellas, del norte del país) se ofertan ejemplares de pitón burmes y pitón burmes albino, de falso coral tricolor, entre otras especies de serpientes.

Las autoridades de la Profepa solicitaron que la identificación de las páginas de internet se mantuviera en reserva hasta en tanto se concluyera la investigación correspondiente.

"En estas páginas de internet, encuentra las características del animal, el precio, las condiciones de tiempo de entrega, modalidad de entrega, costos de envíos, pero en muchas de estas páginas nunca hablan de que cuenten con su certificado de estos animales o con las autorizaciones por parte de la Semarnat para estar constituidos en

Unidad de Manejo Ambiental (UMA) o como un rancho cinegético".

El delegado de la Profepa en Querétaro explicó que las UMA son instancias en donde se cuidan los animales que han sido decomisados por su venta ilegal, y que el gobierno federal, en reconocimiento a la labor que realizan, autoriza a los responsables de dichas instancias a comercializar las crías de estos animales.
La facilidad con la que operan estos negocios ilícitos ha hecho que el comercio de especies animales se constituya en un importante negocio mundial.

13. PIRATERÍA EN INTERNET

La piratería en Internet se refiere al uso del Internet para copiar o distribuir ilegalmente software no autorizado. Los infractores pueden utilizar el Internet para todas o algunas de sus operaciones, incluyendo publicidad, ofertas, compras o distribución de software pirata.

La Business Software Alliance (BSA), una asociación comercial de la industria del software, estima que hay más de 840,000 sitios en Internet que venden software ilegal como auténtico. Muchos clientes que compran software a través de Internet nunca reciben realmente los programas que pagaron.

Otros no pueden obtener la devolución de su dinero cuando descubren que el software que adquirieron es falsificado. Las empresas en Internet de dudosa reputación a menudo desaparecen rápidamente, dejando atrás cientos de clientes insatisfechos.

El Web ha aumentado la piratería de software—es fácil para empresas aparentemente legítimas crear un sitio Web y después anunciarse y distribuir software pirata. Además, el crecimiento explosivo del comercio electrónico, combinado con el anonimato y el volumen ilimitado, han facilitado aún más a los criminales vender software falsificado en línea.

13.1. QUÉ ES LA PIRATERÍA

El término "piratería de software" cubre diferentes actividades: copiar ilegalmente programas, falsificar y distribuir software - incluso compartir un programa con un amigo.

Es importante entender los diferentes canales de piratería de software, no simplemente cumplir con la ley sino también protegerse contra problemas económicos aún mayores como la pérdida de ingresos... y la pérdida de empleos.

OEMs y Resellers
Simplemente porque el disco dice Microsoft o el software venía precargado en su PC, no garantiza que sea legal.

Copiado y falsificación
Se inicia con una copia legítima con licencia de software, y escala a partir de ahí.

Piratería por Internet
La venta de software por medio de sitios Web y sitios de subastas es una práctica común y fácil, lo cual hace que el Internet se convierta en el vehículo perfecto para los falsificadores.

13.2. LA MÚSICA Y EL CINE AMENAZADOS POR LA PIRATERÍA EN INTERNET

La tecnología continúa aplastando paulatinamente los esfuerzos que hacen por mantenerse a flote algunas industrias tradicionales.

De acuerdo con un estudio de la cadena digital Music Choice en nueve países europeos, 50 por ciento de los encuestados bajan música legalmente

La piratería de obras musicales y de cine en internet obligó a las industrias cinematográficas y disquera a buscar alternativas que modificaron profundamente los hábitos de consumo en estos sectores.

Las empresas discográficas subrayan que el sector musical vive la crisis más grave de su historia. En los tres primeros trimestres de 2004, las ventas de CD bajaron 10,7 por ciento en volumen y 12,2 por ciento en valor.

Ellas atribuyen esta caída a las descargas ilegales de internet, a través de las redes de intercambio "peer-to-peer" (de computadora a computadora), que tratan de controlar presentando numerosas querellas contra los internautas.

La situación no es tan catastrófica para el cine, aunque en Francia se efectúan aproximadamente un millón de descargas ilegales de filmes diariamente.

Esta cifra debe ser comparada con las 477 mil entradas vendidas cotidianamente por las salas francesas.

La industria musical reaccionó presentando una oferta de descarga, y en 2004 se crearon numerosas plataformas legales.

Por ahora, el mercado musical en línea sigue siendo marginal (aproximadamente 4,5 por ciento de las ventas en el mundo). Pero según el despacho norteamericano Forrester Research, ese sector crecerá en 2007, cuando podría representar mil millones de euros en Europa (3 mil 500 millones en 2009).

De acuerdo con un estudio de la cadena digital Music Choice en nueve países europeos, 50 por ciento de los encuestados bajan música legalmente.

Ante la amenaza que representa la piratería, los profesionales del cine se movilizan actualmente para concebir una oferta legal, segura y paga de filmes en la web, pues temen que la llegada del acceso a internet de gran velocidad los coloque en una situación comparable a la de la industria disquera.

En Francia ya comenzaron las negociaciones entre los representantes del cine (distribución, producción y explotación), los proveedores de acceso a internet, los editores de vídeos, las cadenas y las pagas.

Sin embargo, las formas tradicionales de consumo no están condenadas.

Según un estudio del gabinete Jupiter Research, aunque las ventas de música en línea y de walkmans digitales aumentarán regularmente para el año 2009, los CD están lejos de ser destronados, gracias paradójicamente a internet. La venta de CD en línea es mejor que nunca en Estados Unidos (+15 por ciento en un año).

En cuanto al cine, las salas francesas registraron ventas sin precedentes en 2004: 174,95 millones de entradas entre el 1 de enero y el 30 de noviembre, 14,7 por ciento más que en el mismo período en 2003

13.3. LEYES Y ACCIONES CONTRA LA PIRATERÍA EN INTERNET

La **OMPI** Organización Mundial de la Propiedad Intelectual, cuenta con 170 miembros, promueve la protección de la propiedad intelectual en el mundo y administra varios tratados de propiedad intelectual.

La OMPI es una agencia de las Naciones Unidas.

Una parte fundamental de las actividades de la OMPI es el desarrollo de normas y estándares internacionales.

La organización administra tratados que establecen acuerdos y estándares comunes acordados internacionalmente para su protección.

Dos tratados—el Tratado Mundial sobre los Derechos de Autor (WCT) y el Tratado de Espectáculos y Fonogramas de la OMPI (WPPT)—están en espera de su ratificación por parte de los estados miembros.

La OMPI también trabaja conjuntamente con la Organización Mundial de Comercio (OMC) para proteger los derechos de la propiedad intelectual.

Contrato TRIPS

El Acuerdo sobre Aspectos Relacionados con el Comercio de los Derechos de la Propiedad Intelectual (TRIPS) es el acuerdo entre todos los miembros de la OMC que requieren protección y hacer cumplir los derechos de propiedad intelectual.

Válido desde enero 1 de 1995, el TRIPS es el acuerdo más completo sobre derechos de propiedad intelectual a la fecha.

El TRIPS cubre derechos de autor y derechos relacionados, como los derechos de artistas, productores de grabaciones de sonido y organizaciones de difusión.

Los países miembro de la OMC continúan implementando el TRIPS al tiempo que consideran nuevas disposiciones que adaptarán mejor el TRIPS a una economía digital.

Microsoft apoya la incorporación del Tratado de Derechos de Autor de la OMPI y el Tratado de Espectáculos y Fonogramas de la OMPI en el TRIPS.

El Gobierno de Estados Unidos está realizando acciones significativas para detener la piratería en todo el mundo.

Específicamente, Microsoft aprueba los esfuerzos del Departamento de Justicia y del Tesoro y sus principales agencias de investigación, el Servicio de Aduanas de Estados Unidos y el F.B.I., en la ejecución de una serie de redadas significativas en todo el mundo contra grupos warez que reproducen, modifican y distribuyen software falsificado a través de Internet.

El Servicio de Aduanas de Estados Unidos combate la piratería y protege los derechos de la propiedad intelectual.

La Sección de Crímenes de Computación y de la Propiedad Intelectual del Departamento de Justicia de Estados Unidos combate la piratería en muchos frentes.

13.4. UNA DE LAS SOLUCIONES PARA DETENER LA PIRATERÍA EN INTERNET

LIMITAR EL ANCHO DE BANDA

Parece que la solución para la piratería en Internet está en cambiar la forma de cobrar los servicios de conexión y las compañías norteamericanas se han dado cuenta de ello.

AT&T Broadband, Charter Communications y Cox Communications, entre otras empresas, se están planteando cambiar su política y poner límites al ancho de banda utilizado por los usuarios

De esta manera, cada internauta tendría un límite de consumo mensual de ancho de banda, y pasaría a pagar más por pasarse de este límite. Bajarse una película o un CD de la Red podría encarecerse hasta el punto de frenar a los usuarios a hacerlo.

El motivo es que los usuarios de este tipo de servicios no sólo se descargan, sino que otros usuarios "tiran" de sus datos, consumiendo un importante ancho de banda.

Las compañías de cable afirman que esto no afectaría a los usuarios de servicios musicales de pago, el motivo es que estos sólo se descargan la música que la compañía ha dejado disponible.

14. COMO SE APLICA LA INFORMATICA FORENSE

Los desarrollos de la tecnología de información han comenzado a plantear nuevos desafíos y la mayoría de las profesiones se han tenido que adaptar a la era digital, particularmente la fuerza policial debe actualizarse, dado que la explotación criminal de las tecnologías digitales hace necesarios nuevos tipos de investigación.

Cada vez más la tecnología informática se ha convertido en un instrumento para cometer crímenes. Investigar estos crímenes sofisticados y recolectar la evidencia necesaria para presentación del caso a la justicia se ha convertido en una significativa responsabilidad de los investigadores asignados.

La aplicación de la tecnología informática en la investigación de un ilícito cometido usando una computadora, ha creado una nueva especialización, la **informática forense**, que es el proceso de identificar, preservar, analizar y presentar la evidencia digital de una manera legalmente aceptable.

Abarca cuatro partes fundamentales.

1. La identificación de evidencia digital.

Es el primer paso en el proceso forense.

Sabiendo qué evidencia está presente, dónde y como se guarda, es vital determinar qué procesos serán empleados para efectuar su recuperación.

Aunque muchas personas piensan que solamente las computadoras personales son el centro de la informática forense, en la realidad el concepto puede extenderse a cualquier dispositivo electrónico que sea capaz de almacenar información, como los teléfonos celulares, las agendas electrónicas y las tarjetas inteligentes.

Además, el examinador forense debe poder identificar el tipo de información almacenada en un dispositivo y el formato en que se guarda para usar la tecnología apropiada para extraerlo.

2. Preservación de la evidencia digital.

Es un elemento crítico en el proceso forense.

Dado que los datos serán analizados minuciosamente en un juzgado, es indispensable que cualquier examen de los datos electrónicamente guardados se lleve cabo de la manera menos intrusiva posible.

Hay circunstancias dónde los cambios de datos son inevitables, pero es importante que se haga en la menor medida posible.

En situaciones dónde el cambio es inevitable, es esencial que la naturaleza y razón del mismo pueda explicarse con detalle.

La alteración en los datos que tengan valor de evidencia debe ser registrada y justificada. Esto no sólo se aplica a cambios hechos a los datos, sino que también incluye cambios físicos que se hagan a un dispositivo electrónico en particular.

3. El análisis de la evidencia digital

La extracción, procesamiento e interpretación de los datos digitales, se consideran generalmente como los elementos principales de la informática forense.

Una vez obtenida, la evidencia digital, normalmente requiere de un proceso, antes que pueda ser comprendida por las personas.

Por ejemplo, cuando se tiene la imagen de un disco, los datos contenidos dentro de la misma requieren un proceso (conversión) para que una persona los pueda interpretar.

4. La presentación de evidencia digital.

Esto incluye la manera formal de la presentación, la especialización y calificaciones del perito y la credibilidad de los procesos que empleó para producir la evidencia que se está presentando ante el juzgado, árbitro o mediador que interviene.

El rasgo distintivo de la informática forense, que la diferencia de cualquier otra área de la tecnología de información, es el requisito que el resultado final debe derivarse de un proceso que sea legalmente aceptable.

Por consiguiente, la aplicación de la tecnología en la investigación de los hechos que poseen estas características específicas debe llevarse a cabo con todos los requisitos que exige la ley.

El no hacerlo puede producir que la evidencia digital sea considerada inadmisible, o al menos dudosa (contaminada).

Esto puede ejemplificarse cuando el examinador forense utiliza un software para leer y reproducir los datos contenidos dentro de un documento electrónico.

Por ejemplo, una hoja de cálculo, que contiene los datos financieros. Si un tercer producto de software es usado para reproducir íntegramente la hoja de cálculo y ese producto no interpreta cada dato con precisión y exactitud, el significado entero del documento puede cambiar.

Esto puede, además de generar dudas con relación a los procesos empleados durante el examen forense, también poner en tela de juicio la habilidad y especialización del examinador que produjo el documento presentado como evidencia.

14.1. ACTIVIDADES DE LA INFORMÁTICA FORENSE.

La informática forense no es una sola actividad, utiliza muchas disciplinas. Involucra la aplicación de tecnología de la información para la búsqueda de la evidencia digital y comprende, entre otras, las siguientes tres actividades:

14.2. ANÁLISIS DE SOPORTES Y DISPOSITIVOS ELECTRÓNICOS.

El análisis de soportes de almacenamiento, como los discos, almacenamientos removibles (por ejemplo disquetes, discos ZIP, CD-ROMs, DVD, etc.), requiere una comprensión completa de la estructura física y del funcionamiento de los medios almacenamiento, así como, la forma y la estructura lógica de cómo se almacenan los datos.

Mucha de la complejidad de esta actividad se ha simplificado gracias a la aplicación de herramientas de recuperación de datos muy eficaces e inteligentes.

Por consiguiente, mucho del conocimiento exigido para realizar la tarea esta integrado en el software de recuperación de datos que se use.

Cuando mencionamos a los "dispositivos electrónicos" nos referimos a cualquier dispositivo capaz de guardar información que posea valor como evidencia, incluyendo teléfonos celulares, agendas y organizadores electrónicos y distintos dispositivos de comunicaciones de red como los routers y hub's.

El análisis de tales dispositivos es algo más complejo que la actividad de recuperar los datos de los soportes y el hardware requerido es generalmente más especializado.

La estandarización de los dispositivos de hardware ha hecho que la extracción de datos de algunos tipos de dispositivos electrónicos sea más fácil y a la vez ha permitido adquirir el conocimiento para realizar la recuperación de los datos en dispositivos específicos.

Dado el amplio alcance de la informática forense, no es para sorprenderse que varias ciencias y disciplinas estén involucradas:

Ingeniería de software, criptografía, ingeniería electrónica, comunicaciones, derecho, son áreas de especialización que, en conjunto hacen posible el análisis de los dispositivos electrónicos y soportes de información.

14.3. EL ANÁLISIS DE LA COMUNICACIÓN DE DATOS.

Este acápite abarca dos actividades separadas:

- Intrusión en una red de computadoras o mal uso de la misma.
- Interceptación de datos.

La intrusión en una red de computadoras o mal uso de la misma es la actividad de la informática forense principal cuando el análisis se hace sobre estructuras de esta naturaleza. Consiste en las funciones siguientes:

- *Detección de la intrusión.*
- Detectar la evidencia, capturarla y preservarla; y
- Reconstrucción de la actividad específica o del hecho en sí.

El descubrimiento de la intrusión generalmente involucra la aplicación de software especializado y en algunos casos hardware, para supervisar la comunicación de los datos y conexiones a fin de identificar y aislar un comportamiento potencialmente ilegal.

Este comportamiento incluye el acceso no autorizado, modificación del sistema en forma remota y el monitoreo no autorizado de paquetes de datos.

La captura de la evidencia y su preservación, generalmente tiene lugar después del descubrimiento de una intrusión o un comportamiento anormal, para que la actividad anormal o sospechosa pueda conservarse para el posterior análisis.

La fase final, la reconstrucción de la intrusión o comportamiento anormal, permite un examen completo de todos los datos recogidos durante la captura de la evidencia.

Para llevar a cabo con éxito estas funciones, el investigador forense debe tener experiencia en comunicación de datos y el apoyo de ingenieros de software.

14.4. INVESTIGACIÓN Y DESARROLLO.

La investigación y desarrollo de nuevas técnicas y herramientas son vitales para estar actualizado frente a cambios en la tecnología.

Deben dedicarse Tiempo y Recursos a la investigación y desarrollo de nuevas técnicas forenses, no sólo desarrollar las soluciones a los problemas existentes, sino también para reconocer problemas futuros y hallar las soluciones más adecuadas.

Desgraciadamente, los recursos y habilidades necesarios para mantener una investigación eficaz y un programa de desarrollo están más allá de la capacidad financiera de muchos grupos forenses.

Y una restricción adicional es que cualquier solución derivada de la investigación debe cumplir con todos los requisitos que marca la ley dentro del marco de trabajo de la informática forense.

14.5. REGLAS DE LA INFORMÁTICA FORENSE.

Dado que el último producto del proceso forense está sujeto al análisis judicial, es importante que las reglas que lo gobiernan se sigan.

Aunque estas reglas son generales para aplicar a cualquier proceso en la informática forense, su cumplimiento es fundamental para asegurar la admisibilidad de cualquier evidencia en un juzgado.

Dado que la metodología que se emplee será determinada por el especialista forense, el proceso escogido debe aplicarse de forma que no se vulneren las reglas básicas de la informática forense.

Esencialmente, las reglas de la informática forense son:

Regla 1—Minimizar el Manejo del Original

La aplicación del proceso de la informática forense durante el examen de los datos originales se deberá reducir al mínimo posible.

Esto puede considerarse como la regla más importante en la informática forense. Cualquier análisis debe dirigirse de manera tal que minimice la probabilidad de alteración.

Cuando sea posible, esto se logra copiando el original y examinando luego los datos duplicados.

La duplicación de evidencia tiene varias ventajas: Primeramente, asegura que el original no será alterado en caso de un uso incorrecto o inapropiado del proceso que se aplique.

Segundo, le permite al examinador aplicar diferentes técnicas en casos dónde el mejor resultado no está claro. Si, durante tales ensayos, los datos se alteran o se destruyen, simplemente se recurre a otra copia.

En tercer lugar, les permite a varios especialistas de informática forense trabajar en los mismos datos, o en partes de los datos, al mismo tiempo.

Esto es especialmente importante si las habilidades de los especialistas (por ejemplo, criptoanálisis) se requiere en distintas etapas de la tarea. Finalmente, asegura que el original se ha preservado en el mejor estado posible para la presentación en un juzgado.

Aunque hay ventajas al duplicar la evidencia, hay también desventajas.

Primeramente, la duplicación de evidencia debe realizarse de forma tal y con herramientas, que aseguren que el duplicado es una copia perfecta del original.

El fracaso para autenticar el duplicado apropiadamente, producirá un cuestionamiento sobre su integridad, lo que lleva inevitablemente a preguntar por la exactitud y fiabilidad del proceso del examen y los resultados logrados.

Segundo, duplicando el original, nosotros estamos agregando un paso adicional en el proceso forense.

Se requieren más recursos y tiempo extra para facilitar el proceso de duplicación.

Más aun, la metodología empleada debe extenderse para incluir el proceso de la duplicación.

Finalmente, la restauración de datos duplicados para recrear el ambiente original puede ser difícil.

En algunos casos para ello serán necesarios dispositivos específicos de hardware o software, más la complejidad y tiempo del proceso forense.

Regla 2—Documentar los cambios.

Cuando ocurren cambios durante un examen forense, la naturaleza, magnitud y razón para ellos debe documentarse apropiadamente, puede ser necesario durante cualquier examen alterar el original o el duplicado.

Esto se aplica para ambos tanto a nivel físico como lógico.

En tales casos es esencial que el examinador entienda la naturaleza del cambio y que es el iniciador de ese cambio.

Adicionalmente, el perito debe ser capaz de identificar correctamente la magnitud de cualquier cambio y dar una explicación detallada de por qué era necesario el mismo.

Esencialmente esto se aplica a cualquier material de evidencia que se obtiene de un proceso forense en el que ha ocurrido un cambio.

Esto no quiere decir que el cambio no ocurrirá sino, que en situaciones dónde es inevitable, el examinador tiene la responsabilidad de identificar correctamente y documentar el cambio, ya que este proceso depende directamente de las habilidades y conocimiento del investigador forense.

Durante el examen forense este punto puede parecer insignificante, pero se vuelve un problema crítico cuando el examinador está presentando sus resultados en un juicio.

Aunque la evidencia puede ser legítima, las preguntas acerca de las habilidades del examinador y conocimiento pueden afectar su credibilidad, así como la confiabilidad del proceso empleado.

Con una duda razonable, los resultados del proceso forense, en el peor de los casos, se consideraran inadmisibles. Aunque la necesidad de alterar los datos ocurre pocas veces, hay casos dónde al examinador se le exige el cambio para facilitar el proceso del examen forense.

Por ejemplo cuando el acceso a los datos se encuentra restringido por alguna forma de control de acceso, el examinador forense se puede ver obligado a cambiar el bit de acceso o una cadena binaria de datos completa (clave de acceso).

Por ello el perito debe dar testimonio que tales cambios no alteraron significativamente los datos a los que se accedió por medio de esta metodología y que luego son presentados como evidencia.

Regla 3—Cumplir con las Reglas de Evidencia

Para la aplicación o el desarrollo de herramientas y técnicas forenses se deben tener en cuenta las reglas pertinentes de evidencia.

Uno de los mandatos fundamentales de informática forense es la necesidad de asegurar que el uso de herramientas y técnicas no disminuye la admisibilidad del producto final.

Por consiguiente es importante asegurar que la manera como son aplicadas las herramientas y técnicas, cumplan con las reglas de evidencia.

Otro factor importante en cuanto a la obediencia de las reglas de evidencia es la manera en que la misma se presenta.

Esencialmente, debe presentarse la información de una manera que sea tan representativa del original como sea posible.

Es decir, el método de presentación no debe alterar el significado de la evidencia.

Regla 4—No exceda su conocimiento

El especialista en informática forense no debe emprender un examen más allá de su nivel de conocimiento y habilidad.

Es esencial que el perito sea consciente del límite de su conocimiento y habilidad. Llegado este punto, tiene varias opciones:

- Detener cualquier examen y buscar la ayuda de personal más experimentado;
- Realizar la investigación necesaria para mejorar su propio conocimiento, para que le permita continuar el examen; o
- Continuar con el examen en la esperanza que...

La última opción es sin la duda la más peligrosa.

Es indispensable que el examinador forense puede describir los procesos empleados durante un examen correctamente y explicar la metodología seguida para ese proceso.

El fracaso para explicar, competentemente y con precisión, la aplicación de un proceso o procesos puede producir cuestionamientos sobre el conocimiento y credibilidad del examinador.

Otro peligro en continuar un examen más allá de las habilidades de uno, es aumentar el riesgo de daño, cambios de los cuales el examinador no es consciente o no entiende y por consiguiente puede ignorar.

Esto probablemente será revelado cuando el examinador está dando la evidencia.

Esencialmente, los análisis complejos deben ser emprendidos por personal calificado y experimentado que posea un apropiado nivel de entrenamiento.

Adicionalmente, dado que la tecnología está avanzando continuamente, es importante que el examinador reciba entrenamiento continuo.

14.6. LOS PROBLEMAS ACTUALES Y FUTUROS PARA LA INFORMÁTICA FORENSE.

Los adelantos en la tecnología dan lugar nuevos y excitantes desafíos, pero también enfrentan al especialista de informática forense con nuevos problemas.

Los adelantos en tecnología también pueden llevar a las soluciones más avanzadas pero desafortunadamente, aunque la tecnología puede cambiar y se puede adaptar, la ley es algo más lenta en su adecuación.

Recordándole al especialista en informática forense que sirve dos amos, la tecnología y la ley, ellos deben encontrar un equilibrio aceptable entre los dos.

No todos los desafíos enfrentados por la informática forense son de naturaleza técnica. Ellos también deben tratar con problemas de procedimiento, política, entrenamiento, cambios organizacionales, presupuesto, etc.

15. CONCLUSIONES

Al haber realizado este proceso de Investigación nos dimos cuenta de que la mayoría de la gente conoce de la existencia de los pitaras informáticos dentro comúnmente de Internet, y que la mayoría trabaja para uso propio y para desbaratar un sistema de computación con fines no lucrativos, la mayoría de las veces, pero sí con el de agraviar a la gente.

También al tener medidas preventivas y aplicándolas en función de combatir agravios de tipo destructor, y por tanto establecer de forma general barreras informáticas y lograr evadir el mal de los hackers.

Aunque hablamos anteriormente que no todos los hackers son malos y utilizan sus herramientas para la obtención de información que les podrá servir para fines de uso común no perjudiciales.

Finalmente corroborar que en una red, siendo un sistema interrelacional de varias conexiones la información viaja a menudo por manos de piratas informáticos y que pueden ocasionar con su "arte" de divulgación, daños, pero también como por medio de publicidad y a la vez darse a conocer ellos y su trabajo, mencionando como mensaje una invitación para que la gente a que utilicé herramientas de Hacking y conforme parte de ellos, formando a la vez la cadena de información más rápida, extensa y muchas veces dañina para el resto de la población, hablando del sistema global de intercomunicación.

16. BIBLIOGRAFÍA

www.unam-cert.unam.mx

(http://www.enterate.unam.mx/).

http://iblnews.com/news/auto/canal.php?c=11

http://html.rincondelvago.com/delitos-informaticos.html

http://www.informatica-juridica.com/legislacion/mexico.asp

http://www.alfa-redi.org/revista/data/57-10.asp

Jeimy J. Cano, Credenciales para investigadores forenses en informática. Certificaciones y entrenamiento, http://www.virusprot.com/Col8.html

Jeimy J. Cano, Informática Forense liderando las investigaciones, http://www.virusprot.com/Col8.html

Aspectos jurídicos del comercio electrónico en Internet. RIBAS, J. Aranzadi Editorial, 1999.

Leyes y negocios en internet. HANCE, O. McGraw Hill, 1996.

Detección de intrusos. Guía avanzada. NORTCUTT y NOVAK. Prentice Hall, 2001.

INDICE