AUDITORÍA FORENSE APLICADA LA TECNOLOGÍA

Por: CP Álvaro Fonseca Vivas

RESUMEN

El objetivo de este escrito, es un aporte del resultado de un trabajo realizado con estudiantes de la Universidad San Martín sobre la Auditoría Forense Aplicada a la Tecnología, según los avances de los medios electrónicos de datos en forma virtual y de la globalización de la información, el trabajo que debe realizar el profesional en auditoría y de revisoría fiscal, con el apoyo de otros profesionales de la ingeniería de sistemas u electrónica y que como modo de investigación debe intervenir en el desarrollo de fraudes con las herramientas de la tecnología.

La finalidad del mismo es que se pueda ver el trabajo que desde la profesión de la Contaduría Pública se puede hacer.

Palabras claves: Tecnología, técnico, ingeniería, informática, fraudes informáticos, hacker, cracker, auditoría, forense.

1. CONCEPTOS DE TECNOLOGÍA.

Los diferentes autores lo definen así: *Methere*: Conocimiento aplicado a propósitos prácticos.

Dupree: Define la tecnología como un sistema de información que conecta al homo sapiens con su ambiente.

La finalidad de la tecnología seria la búsqueda de una verdad útil

Falcott. (desde la sociología): Señala que la tecnología es la capacidad socialmente organizada para controlar y alterar activamente objetos del ambiente físico en interés de algún deseo o necesidad humana.

Sabato (desde la economía) conjunto ordenado de conocimientos necesarios para la producción y comercialización de bienes y servicios.

Gallbraith (The new industrial state) La tecnología es la aplicación sistemática del conocimiento científico o de otro tipo de conocimiento organizado, a tareas practicas.

2. CONCEPTO DE TECNOLOGÍA

Resulta impresionante cómo la tecnología evoluciona con cada día que pasa. Y debido a esta evolución, su conceptualización resulta cada vez más rica y variada. Muchos han sido los autores que se han decidido a sentar las bases del término. Amplias y variadas han sido estas definiciones. La gran mayoría la describen y la analizan como un fenómeno científico-social. Otras caen en la disyuntiva de considerarla como una ciencia aplicada o tomarla como un proceso autónomo, más no independiente, respecto a la ciencia. Por otro lado, hay quienes afirman que es necesario diferenciarla muy bien de la técnica. Ésta, posee una connotación más artesanal, común, sin una profunda interrelación con el hecho científico, y que busca solucionar las situaciones concretas e inmediatas a las

cuales se aplica. Mientras que la tecnología no puede obviar este aspecto intrínsecamente científico.

La tecnología no solamente invade toda la actividad industrial, sino que también participa profundamente en cualquier tipo de actividad humana, en todos los campos de actuación. El hombre, moderno utiliza en su comportamiento cotidiano y casi sin percibirlo una inmensa avalancha de contribuciones de la tecnología: el automóvil, el reloj, el teléfono, las comunicaciones, etc. A pesar de que existe conocimiento que no puede ser considerado conocimiento tecnológico

3. INTERRELACIÓN ENTRE CIENCIA Y TECNOLOGÍA

Es interesante ver cómo en nuestros días y a través del tiempo se ha hecho difícil diferenciar la tecnología de la ciencia. Son dos actividades únicas, separadas pero no divorciadas, con naturalezas muy específicas pero con una profunda e íntima interrelación. De manera general, la ciencia sería el "por qué conocer," el "por qué llegar más allá" y el "qué de las cosas y sus circunstancias"; una incansable búsqueda de la verdad. Mientras que la tecnología es el "cómo conocer", el "cómo aplicar" los conocimientos adquiridos para resolver soluciones, crear cosas, con el fin de elevar cada día más la calidad de vida del hombre. La tecnología moderna es predominantemente científica, ya que extrae sus fundamentos teóricos de la ciencia pura o básica.

Los significados de los términos ciencia y tecnología han variado significativamente de una generación a otra. Sin embargo, se encuentran más similitudes que diferencias entre ambos términos.

Tanto la ciencia como la tecnología implican un proceso intelectual, ambas se refieren a relaciones causales dentro del mundo material y emplean una metodología experimental que tiene como resultado demostraciones empíricas que pueden verificarse mediante repetición. La ciencia, al menos en teoría, está menos relacionada con el sentido práctico de sus resultados y se refiere más al desarrollo de leyes generales; pero la ciencia práctica y la tecnología están profundamente. Relacionadas entre sí. La interacción variable de las dos puede observarse en el desarrollo histórico de algunos sectores.

4. EL PAPEL SOCIAL DE LA TECNOLOGÍA

Algunos historiadores científicos argumentan que la tecnología no es sólo una condición esencial para la civilización avanzada y muchas veces industrial, sino que también la velocidad del cambio tecnológico ha desarrollado su propio ímpetu en los últimos siglos. Las innovaciones parecen surgir a un ritmo que se incrementa en progresión geométrica, sin tener en cuenta los límites geográficos ni los sistemas políticos.

Lo siguiente, podría aclarar un poco la diferencia entre la ciencia y la tecnología, en cuanto al medio social en el cual se desarrollan: Las comunidades que las sustentan, tienden a valorar tanto el "conocer" como el "hacer". Es por ello que el auditorio de la ciencia tiende a

constituirse por científicos investigadores, mientras que el auditorio principal de la tecnología no está compuesto por investigadores netos sino por quienes buscan resultados de utilidad práctica.

La producción a gran escala de armas atómicas, capaces de arrasar y acabar en minutos con toda la vida existente en el planeta. En fin, viendo esto y mucho más, es oportuno hacerse esta pregunta: ¿cuál es el fin perseguido por el hombre al crear objetos o productos destinados a su propia aniquilación? En realidad, esto constituye un verdadero acertijo, digno de investigar y resolver.

5. HISTORIA DE LAS ELECOMUNICACIONES

Las telecomunicaciones se encarga del transporte del información a grandes distancias a través de un medio o canal de comunicación por medio de señales.

La misión de las telecomunicaciones es transportar la mayor cantidad de información en el menor tiempo de una manera segura. Eso se logra por medio de varias técnicas tales como la Modulación, codificación**,** Compresión, Formateo, Multicanalización, Esparciendo el espectro, etc.

En el año 5000 a.c. Prehistoria. El hombre prehistórico se comunicaba por medio de gruñidos y otros sonidos (primer forma de comunicación). Además, con señales físicas con las manos y otros movimientos del cuerpo. En el año 3000 a.c. los Egipcios: representaban las ideas mediante símbolos (hieroglyphics) así la información podría se transportada a grandes distancia al ser transcritas en medios como el papel papiro, maderas, piedras.

6. VENTAJAS Y DESVENTAJAS DE LA TECNOLOGÍA

En el siglo XX los logros tecnológicos fueron insuperables, con un ritmo de desarrollo mucho mayor que en periodos anteriores. La invención del automóvil, la radio, la televisión y teléfono revolucionó el modo de vida y de trabajo de muchos millones de personas. Las dos áreas de mayor avance han sido la tecnología médica, que ha proporcionado los medios para diagnosticar y vencer muchas enfermedades mortales, y la exploración del espacio, donde se ha producido el logro tecnológico más espectacular del siglo: por primera vez los hombres consiguieron abandonar y regresar a la biosfera terrestre.

Durante las últimas décadas, algunos observadores han comenzado a advertir sobre algunos resultados de la tecnología que también poseen aspectos destructivos y perjudiciales. De la década de 1970 a la de 1980, el número de estos resultados negativos ha aumentado y sus problemas han alcanzado difusión pública. Los observadores señalaron, entre otros peligros, que los tubos de escape de los automóviles estaban contaminando la atmósfera, que los recursos mundiales se estaban usando por encima de sus posibilidades, que pesticidas como el DDT amenazaban la cadena alimenticia, y que los residuos minerales de una gran variedad de recursos industriales estaban contaminando las reservas de agua subterránea. Los observadores señalaron,

entre otros peligros, que los tubos de escape de los automóviles estaban contaminando la atmósfera, que los recursos mundiales se estaban usando por encima de sus posibilidades, que pesticidas como el DDT amenazaban la cadena alimenticia, y que los residuos minerales de una gran variedad de recursos industriales estaban contaminando las reservas de agua subterránea.

7. CARACTERIZACIÓN DEL DELINCUENTE INFORMÁTICO

Para algunos autores, el sujeto activo de estos delitos se encuentra conformado por un grupo de personas con una inteligencia y educación que superan el común con vastos conocimientos informáticos.

Es cierto que si analizamos los casos más celebres nos encontraremos con personas dotadas de altos conocimientos de informática y tecnología. Valga como ejemplo el caso de Kevin Mitnick, quien ha pasad más de la mitad de su vida defraudando mediante ordenadores. O el caso de Roberto Morris, estudiante de informática de la Universidad de Cornell cuyo Padera era un experto en seguridad del gobierno.

Pero es un mito que el delincuente informático deba forzosamente poseer conocimientos profundos en la materia. A nuestro juicio la computación se halla tan extendida hoy día que cualquier persona que posea conocimientos mínimos de informática y tenga acceso a un ordenador, incluso desde su casa. Puede realizar delito informático.

En esta facilidad de cometer delitos por medio de computadoras han tenido un papel muy importante la expansión del acceso a cualquier sistema informático debido a las redes informáticas.

EN 1994, en su informe al Congreso de los Estados Unidos, la oficina de Asesoramiento Tecnológico del gobierno de ese país opinaba que las redes informáticas hacen de cada usuario básicamente un incidir con el potencia para asestar un golpe letal a lo sistemas de información. D e allí las medidas de seguridad informática que se suelen tomar dentro de la empresa como ser la existencia de passwords, tarjetas magnéticas o con microchips de acceso al sistema e incluso reconocimiento de características físicas de un individuo.

A partir de la experiencia comparada e incluso la nacional, encontramos los siguientes grupos:

Clase de delito	***Sujetos***
Delitos patrimoniales contra bancos y entidades financieras.	Empleados, en especial cajero o personal del área de sistema, ex - empledos.
Delitos de acceso ilegitimo o delitos de daños menores	Hackers, phreakers, usuarios descontentos
Daño o sabotaje informativo	Empleados de la empresa, o espías profesionales o industriales
Violaciones a la	Investigadores

privacidad, tratamiento ilícito de datos personales.	privados, Empresas de marketing, agencias de informes crediticios y de solvencia patrimonial
Violaciones a la propiedad intelectual del software y bancos de datos, con informes o compilaciones de datos.	Piratas informáticos o también usuarios (la copia amigable), empresas que realizan competencia parasitaria.

En definitiva, nos inclinamos por considerar que el delincuente informático no tiene necesariamente profundos conocimientos de computación, sino que es inducido a delinquir por la oportunidad que se le presenta frente al uso diario del ordenador y la impunidad que éste le brinda, o por los conocimientos que éste tiene frente al resto del personal.

8. TIPOS DE FRAUDE EN EL ÁREA TECNOLÓGICA

Suele ser un programa pequeño alojado dentro de una aplicación, una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene. Una vez instalado parece realizar una función útil (aunque cierto tipo de troyanos permanecen ocultos y por tal motivo los antivirus o anti troyanos no los eliminan) pero internamente realiza otras tareas de las que el usuario no es consciente, de igual forma que el Caballo de Troya que los griegos regalaron a los troyanos.

8.1. TROYANOS

Los troyanos de conexión directa son aquellos que el cliente se conecta al servidor. Una bomba lógica es un programa informático que se instala en un ordenador y permanece oculto hasta cumplirse una o más condiciones pre-programadas para entonces ejecutar una acción. A diferencia de un virus, una bomba lógica jamás se reproduce por sí sola.

Ejemplos de condiciones predeterminadas:

- Día de la semana concreto.
- Hora concreta.
- Pulsación de una tecla o una secuencia de teclas concreta.
- Levantamiento de un interfaz de red concreto.

Ejemplos de acciones:

- Borrar la información del disco duro.
- Mostrar un mensaje.
- Reproducir una canción.
- Enviar un correo electrónico.

8.2. PROGRAMAS ESPÍAS O DE CONEXIÓN DIRECTA

Son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a

empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante.

Pueden tener acceso por ejemplo a: el correo electrónico y el password; dirección IP y DNS; teléfono, país; páginas que se visitan, que tiempos se está en ellas y con qué frecuencia se regresa; que software está instalado en el equipo y cual se descarga; que compras se hacen por internet; tarjeta de crédito y cuentas de banco.

Los programas espía pueden ser instalados en un ordenador mediante un virus, un troyano_(informática) que se distribuye por correo electrónico, como el programa Magic Lantern desarrollado por el FBI, o bien puede estar oculto en la instalación de un programa aparentemente inocuo.

Los cookies son un conocido mecanismo que almacena información sobre un usuario de internet en su propio ordenador, y se suelen emplear para asignar a los visitantes de un sitio de internet un número de identificación individual para su reconocimiento subsiguiente. Sin embargo, la existencia de los cookies y su uso generalmente no están ocultos al usuario, quien puede desactivar el acceso a la información de los cookies. Sin embargo, dado que un sitio Web puede emplear un identificador cookie para construir un perfil del usuario y éste no conoce la información que se añade a este perfil, se puede considerar a los cookies una forma de spyware. Por ejemplo, una página con motor de búsqueda puede asignar un número de identificación individual al usuario la primera vez que visita la página, y puede almacenar todos sus términos de búsqueda en una base de datos con su número de identificación como clave en todas sus próximas visitas (hasta que el cookie expira o se borra).

Se trata de un programa que marca un número de tarificación adicional (NTA) usando el módem, estos NTA son números cuyo coste es superior al de una llamada nacional. Estos marcadores se suelen descargar tanto con autorización del usuario (utilizando pop-ups poco claros) como automáticamente. Además pueden ser programas ejecutables o ActiveX (Estos programas sólo funcionan en Internet Explorer).

En principio sus efectos sólo se muestran en usuarios con acceso a la Red Telefónica Básica (RTB) o Red Digital de Servicios Integrados (RDSI) puesto que se establece la comunicación de manera transparente para el usuario con el consiguiente daño económico para el mismo. Aunque la tarificación no funcione con los usuarios de ADSL, PLC, Cable-módem, entre otros. Afecta al comportamiento del ordenador ya que requiere un uso de recursos que se agudiza cuando se está infectada por más de un dialer.

Los marcadores telefónicos son legítimos siempre y cuando no incurran en las malas

artes que los han definido como Malware que son los siguientes trucos:

1. No se avisa de su instalación en la página que lo suministra.
2. Hace una re-conexión a Internet sin previo aviso, o lo intenta.
3. Se instala silenciosamente en el ordenador utilizando vulnerabilidades del navegador, programa de correo electrónico, otros programas de acceso a Internet o el propio sistema operativo.
4. Puede dejar un acceso directo al escritorio sin conocimiento del usuario.
5. Puede instalarse unido a otros programas como barras de mejora para el navegador.
6. No informa de los costes de conexión.

Afortunadamente hay varios programas que pueden detectar y eliminar los dialers, entre ellos la mayoría de los antivirus actuales, sin olvidar los programas gratuitos que podemos encontrar en los enlaces que se pueden encontrar en esta misma página.

Un ***cracker*** es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo.

El término deriva de la expresión "criminal hacker", y fue creado alrededor de 1985 por contraposición al término hacker, en defensa de estos últimos por el uso incorrecto del término.

Se considera que la actividad de esta clase de *cracker* es dañina e ilegal.

También se denomina *cracker* a quien diseña o programa *cracks* informáticos, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo. Esta acepción está más cercana al concepto de *hacker* en cuanto al interés por entender el funcionamiento del programa o hardware, y la adecuación a sus necesidades particulares, generalmente desarrolladas mediante ingeniería inversa.

No puede considerarse que la actividad de esta clase de cracker sea ilegal si ha obtenido el software o hardware legítimamente, aunque la distribución de los *cracks* pudiera serlo.

El cracker también es una persona de amplios conocimientos como el hacker pero éste los utiliza para su bien o el bien de todos, por ejemplo se podría representar como un robbin hood, que altera programas para el uso público y que sean gratis.

Por ello los crackers son temidos y criticados por la mayoría de hackers, por el desprestigio que les supone ante la opinión pública y las empresas, son aquellos que utilizan sus conocimientos técnicos para perturbar procesos informáticos (Haffner y Markoff, 1995). Pueden considerarse un subgrupo marginal de la comunidad de hackers.

Hay muy distintos tipos de crackers, pero no consideramos entre ellos a aquellos que penetran en ordenadores o redes de forma ilegal para robar: éstos son ladrones de guante blanco, una vieja tradición criminal.

Muchos crackers pertenecen a la categoría de script kiddies, es decir, bromistas de mal gusto, muchos de ellos adolescentes, que penetran sin autorización en sistemas o crean y difunden virus informáticos para sentir su poder, para medirse con los otros y para desafiar al mundo de los adultos. La mayoría de ellos tiene conocimientos técnicos limitados y no crea ninguna innovación, por lo que son, en realidad, marginales al mundo hacker.

Otros crackers, más sofisticados, penetran en sistemas informáticos para desafiar personalmente a los poderes establecidos, por ejemplo, a la empresa Microsoft o las grandes empresas. Y algunos utilizan su capacidad tecnológica como forma de protesta social o política, como expresión de su crítica al orden establecido. Ellos son quienes se introducen en sistemas militares, administraciones públicas, bancos o empresas para reprocharles alguna fechoría.Entre los ataques de crackers con motivación política hay que situar los practicados por movimientos políticos o por servicios de inteligencia de los gobiernos, como la guerra informática desarrollada entre los crackers islámicos e israelíes o entre los pro-chechenos y los servicios rusos.

9. FRAUDES EN LA TELECOMUNICACIONES

- Fraude de suscripción
- Clonación de servicios
- Call Back
- By pass

10. TIPOS DE TRANSACCIONES

Son formas de utilización y pago con tarjeta en los cajeros y establecimientos afiliados en donde se acude a la utilización de diferentes dispositivos como Data fono Inteligente, y Maquina Imprinter.

10.1. TRANSACCIONES MANUALES

Aquellas que se realizan haciendo uso de la maquina imprenta del establecimiento y de un comprobante único de venta en donde es necesaria la presencia del plástico.

En este tipo de transacciones es frecuente encontrar las siguientes modalidades de fraude:

- Fraude realizado con tarjeta auténtica.
- Fraude realizado con tarjeta alterada.
- Fraude realizado con tarjeta integralmente falsa.

10.2. TRANSACCIONES ELECTRÓNICAS

En este tipo de transacciones se puede presentar:

- Fraude realizado con tarjeta auténtica
- Fraude realizado con tarjeta alterada.
- Fraude realizado con tarjeta integralmente falsa

10.3. TRANSACCIONES SIN LA PRESENCIA DEL PLÁSTICO

Este tipo de transacciones se puede presentar en:

- Tele-mercadeo
- Por Internet

10.4. TARJETA HURTADA O EXTRAVIADA

El uso de la tarjeta extraviada antes de su bloqueo en el centro de autorizaciones configura el fraude, puede presentarse una cédula autentica o una cédula falsa para la transacción.

10.5. UTILIZACIÓN INDEBIDA (AUTORÍA DEL TARJETA HABIENTE)

Si es el mismo tarjeta habiente quien la utiliza y luego niega la transacción se denomina Autoría del tarjeta habiente o si la presta a un tercero con la intención de cometer el fraude se trata de utilización indebida; generalmente se presenta con cédula autentica.

10.6. TARJETA EMITIDA CON DOCUMENTOS FALSOS

La tarjeta se obtiene mediante el suministro a la entidad emisora de documentos e información de un ciudadano real (suplantación de persona) o inexistente.

En esta modalidad se hacen abonos a la tarjeta para generar saldos favorables; para que se configure el fraude debe existir la reclamación de la entidad financiera.

10.7. SUPLANTACION DEL TARJETA HABIENTE EN EL RETIRO DEL PLÁSTICO

El estafador en ocasiones con complicidad de funcionarios de la entidad, retira una tarjeta suplantando al verdadero tarjeta habiente presentando documentación falsa.

La tarjeta que se presenta al comercio es auténtica y generalmente se allega una cédula falsa al momento de la transacción.

10.8. DOBLE FACTURACIÓN

Se comete directamente en el establecimiento cuando de manera intencional al cancelar un servicio se imprimen otros comprobantes (manual o por data fono) con el desconocimiento del tarjeta habiente. En los comprobantes adicionales se imita la firma del titular, si es comprobante electrónico aparecerán en algunos de ellos los datos del titular como número de cédula, nombres y apellidos.

10.9. FRAUDE CON TARJETA ANTES DE SER ENTREGADA AL TITULAR

Se presenta con complicidad de funcionarios de la entidad financiera o por los proveedores que utilizan la tarjeta antes de ser entregada a quien la solicito. En esta modalidad se puede presentar que la tarjeta autentica sea utilizada directamente en el comercio o que por el contrario se copie la información de la banda magnética para luego ser manipulada.

10.10 FRAUDE CON TARJETA DESPUÉS DE SER DEVUELTA POR EL TITULAR

Si no se siguen los procesos adecuados de control, custodia del plástico, y destrucción del mismo, se facilita la utilización dolosa de la misma por el funcionario que la recibe ya sea de la entidad financiera o del proveedor.

10.11. FRAUDE REALIZADO CON TARJETA ALTERADA

Aquel que se comete con un plástico auténtico, emitido por una entidad financiera y al cual se le modifica alguna de sus partes correspondientes a la información allí contenida bien sea en su alto o bajo relieve, o en la banda magnética.

10.12. TARJETA ALTERADA EN EL REALCE

Generalmente son utilizadas en transacciones manuales, con plásticos originales deteriorando además la banda magnética para obligar al comercio a que se realice con la maquina imprenta..

Cualquier señal de manipulación del plástico como variación en la forma de los dígitos, perdida de brillo del holograma, opacidad son indicios primarios de una tarjeta adulterada.

Se puede presentar acompañada de una cédula Falsa o Auténtica.

10.13. TARJETA ALTERADA EN LA BANDA MAGNÉTICA

Aquellos que se realizan a través de data fonos o de cajeros automáticos utilizando plásticos en cuya banda magnética han grabado información de una tarjeta activa. La información puede ser adicionada en la banda magnética de un plástico, o al borrar y adicionar información en la banda magnética de una tarjeta debito o crédito autentica.

10.14. FRAUDE REALIZADO CON TARJETA INTEGRALMENTE FALSA

Aquel en el que se utiliza un soporte de características similares a los plásticos emitidos por las entidades financieras el cual es impreso, grabado y codificado con información privilegiada, simulando una tarjeta expedida por una entidad financiera. La tarjeta falsa integralmente puede presentarse junto con un documento autentico o uno falso.

11. FRAUDE POR INTERNET Y TELEMERCADEO

Para efectuar una transacción por Internet con cargo a una tarjeta de crédito se necesitan un computador y la información básica de una tarjeta de crédito (nombre del titular y número de tarjeta).

Una vez se cuenta con estos elementos se buscan en Internet la denominadas Tiendas Virtuales, En negocios de café Internet, las cuales ofrecen a través de catálogos una serie de productos para que el usuario escoja y en la misma página aparece el medio de pago, diligenciando las casillas correspondientes a nombre del comprador, número de tarjeta, fecha de vencimiento y dirección de entrega y el comercio virtual se compromete a hacer entrega de la mercancía en un tiempo preestablecido.

12. FORMAS DE OPERAR DE LOS DELINCUENTES

1. Consecución de información privilegiada (mínima) de tarjetas de crédito (nombre del titular y número de tarjeta); la cual puede ser obtenida a través de los comercios, tarjeta habiente, proveedores, entidades financieras o sistemas.

2. Con la utilización de programas de computador utilizan algunos bines de entidades financieras para crear números de tarjetas, las cuales son probadas posteriormente hasta que obtengan una que se encuentra emitida por la entidad la que es afectada con operaciones fraudulentas.

3. Ubicación y acceso a tiendas virtuales.

4. Realización de la compra, suministrando el número de la tarjeta, el nombre de titular, el número de cuotas, la fecha de vencimiento y a dirección de entrega.

5. Recepción de la mercancía:

a. Los delincuentes alquilan un inmueble por espacio de tiempo corto para recibir la mercancía y luego desaparecen.

b. Cuando las compras son hechas en páginas virtuales de comercios ubicados en el exterior, los delincuentes suministran direcciones que no existen, ya que la mercancía no está destinada a salir del país de origen, en este tipo de situaciones se emite una comunicación al comercio en la que se señala que se debe entregar a una persona que se encuentra de visita en ese lugar.

c. La mercancía es recibida por un encargado a la entrada de conjuntos residenciales, edificios de apartamentos, parqueaderos, tiendas de barrio y oficinas de apuestas u otros establecimientos públicos pequeños en los cuales la persona que recibe señala no conocer al destinatario.

d. En algunas ocasiones el receptor de la mercancía es el estafador quien se hace pasar por otra persona y de esta manera intenta evadir su participación en el ilícito argumentado ser un tercero de buena fe.

e. La dirección de entrega no existe sin embargo cuando la empresa que entrega recorre el lugar es abordado por una persona que le indica que el sector sufrió un cambio de nomenclatura y que él es el receptor de los artículos.

f. La entrega de la mercancía se hace directamente en las oficinas de la empresa de mensajería que transporta el artículo y una persona con el número de guía lo reclama en el lugar.

13. CASOS INTERNACIONALES

13.1. TRANSFERENCIA DE FONDOS A OTRAS CUENTAS.

Vladimir Levin, un graduado en matemáticas de la Universidad Tecnológica de San Petesburgo, Rusia, fue acusado de ser la mente maestra de una serie de fraudes tecnológicos que le permitieron a él y la banda que conformaba, substraer más de 10 millones de dólares, de cuentas corporativas del Citibank.

En 1995 fue arrestado por la Interpol, en el aeropuerto de Heathrow, Inglaterra, y luego extraditado a los Estados Unidos.

Las investigaciones establecieron que desde su computadora instalada en la empresa AO Saturn, de San Petersburgo, donde trabajaba, Levin irrumpió en las cuentas del Citibank de New York y transfirió los fondos a cuentas abiertas en Finlandia, Israel y en el Bank of América de San Francisco.

Ante las evidencias y manifestaciones de sus co-inculpados, Vladimir Levin se declaró culpable. Uno de sus cómplices, Alexei

Lashmanov, de 28 años, en Agosto de 1994 había hecho alarde entre sus conocidos, en San Petersburgo, acerca de sus abultadas cuentas bancarias personales en Tel Aviv, Israel.

Estos conspiradores habían obtenido accesos no autorizados al Sistema de Administración de Dinero en Efectivo del Citibank (The Citibank Cash Management System), en Parsipanny, New Jersey, el cual permite a sus clientes acceder a una red de computadoras y transferir fondos a cuentas de otras instituciones financieras, habiendo realizado un total de 40 transferencias ilegales de dinero.

Lashmanov admitió que él y sus cómplices había transferido dinero a cinco cuentas en bancos de Tel Aviv. Incluso trató de retirar en una sola transacción US $ 940,000 en efectivo de estas cuentas.

Otros tres cómplices, entre ellos una mujer, también se declararon culpables. Esta última fue descubierta "in fraganti" cuando intentaba retirar dinero de una cuenta de un banco de San Francisco. Se estima en un total de 10.7 millones de dólares el monto substraído por esta banda.

Las investigaciones y el proceso tuvieron muchas implicancias que no pudieron ser aclaradas ni siquiera por los responsables de la seguridad del sistema de Administración de Dinero en Efectivo, del propio CITIBANK. Jamás se descartó la sospecha de participación de más de un empleado del propio banco.

A pesar de que la banda substrajo más de 10 millones de dólares al CITIBANK, Levin fue sentenciado a 3 años de prisión y a pagar la suma de US $ 240,015 a favor del CITIBANK, ya que las compañías de seguros habían cubierto los montos de las corporaciones agraviadas.

Los técnicos tuvieron que mejorar sus sistemas de seguridad contra "crackers" y Vladimir Levin ahora se encuentra en libertad.

Tim Paterson un ingeniero, de 24 años, que trabajaba para la Seattle Computer Products. Desarrolló un "clone" del sistema operativo CP/M, creado por Kary Kildall de la Digital Research, el cual evidentemente había sido desensamblado y alterado, y al que denominó Quick and Dirty D.O.S o simplemente QDos. En 1981 Microsoft, adquirió a esta compañía los "derechos de autor" de este sistema por US $ 50,000 y contrató al Ing. Tim Paterson, para que trabajase 4 días a la semana, con el objeto de que realizara "algunos cambios" para "transformar" al sistema operativo.

Este mismo producto "mejorado" por Microsoft, fue vendido a la IBM Corporation, bajo el nombre de PC-DOS y Microsoft se reservó el derecho de comercializarlo bajo el nombre de MS-DOS. Tim Paterson recibió además, algunas acciones de Microsoft y hoy está retirado de toda actividad profesional, recuerda con tristeza que alguna vez pudo convertirse en uno de los hombres más ricos del mundo.