LA INVESTIGACIÓN
QUE REALIZA EL CRIMINÓLOGO-CRIMINALISTA EN LA CLONACIÓN DE TARJETAS BANCARIAS

COLECTIVO ARCION

Surge en el año 2008, equipo interdisciplinario de investigadores en el campo de lo Criminológico-criminalistico, su actividad científica coadyuva al desarrollo y consolidación del modelo educativo CLEU. "Investigar para la libertad". Representa su filosofía de batalla.

RESUMEN

El presente trabajo se tomara en cuenta la participación del Criminólogo-criminalista en una conducta antisocial denominada clonación de tarjetas bancarias, donde se hará una investigación de cómo es que se comete esta conducta, quienes participan y la realizan, así mismo como se debe de iniciar la investigación usando una metodología aplicada a la recolección de indicios del tipo electrónico-tecnológicos.

> "Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología."
>
> *Bruce Schneier experto en seguridad informática.*

INTRODUCCIÓN

Uno de los primeros delitos que empezó a cometer el ser humano en contra de la sociedad fue el robo, y de alguna manera los que tuvieron mayor importancia es el robo a los bancos, en donde los delincuentes se disponían a robar todo el dinero posible y tomar un rumbo desconocido.

Pero a medida que las tecnologías han avanzado, y se han descubierto nuevos medios para hacer más fácil la rutina del individuo, los delincuentes han buscado la utilización de estas tecnologías y de estos sistemas informáticos para hacer más fácil la tarea de delinquir.

En la actualidad todas las instituciones bancarias utilizan sistemas de seguridad complejos basados en informática, así como tecnologías que permitan la protección de datos, tanto de la Institución como la de los clientes.

Estas tecnologías y sistemas informáticos son utilizados por los delincuentes que ven un mayor aprovechamiento en la clonación de tarjetas bancarias y el robo de datos confidenciales como pueden ser base de datos, contraseñas, códigos, etcétera, que robar dinero, pues al obtener estos datos, es más fácil poder realizar un robo o algún otro delito, sin la necesidad de ir al lugar, utilizar la violencia y exponer su integridad para lograr dicho objetivo.

Es aquí donde tiene participación el profesionista Criminólogo-criminalista, en esta conducta antisocial, que si ciertamente aun no está tipificada como delito pero por las características que tiene, atenta contra el bienestar social de los individuos y de las dependencias encargadas de la protección de nuestros bienes.

La importancia del Criminólogo-criminalista en esta conducta antisocial es significativo, pues con las bases de su formación, analiza cómo el individuo tiende a cometer conductas antisociales y que instrumentos utiliza, así del como maneja los artefactos para obtener su objetivo final, con esto se precisa la necesidad de contar con un profesionista que anticipe la conducta y que tenga una metodología para poder llegar al hecho y así poder iniciar la investigación observando y describiendo.

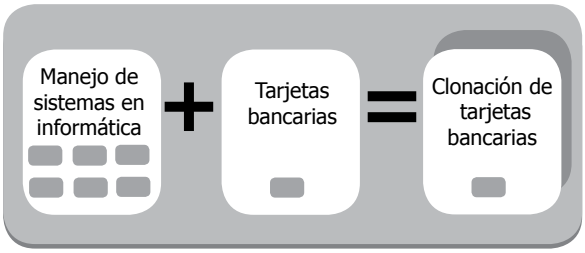
También es importante que las instituciones de gobierno nos puedan brindar recomendaciones que sirvan a la sociedad en el manejo de tarjetas bancarias, con la finalidad de no ser víctimas de alguna conducta, por el mal manejo de cuentas bancarias.

CONCEPTOS DE LA CLONACIÓN DE TARJETAS BANCARIAS

La clonación de tarjetas bancarias es una conducta la cual no es nueva, simplemente no se ha podido encuadrar como delito en alguna ley o código, representa un serio problema, no solo para la persona sobre la cual recae el daño, sino también para las dependencias bancarias y por su puesto al Estado.

La clonación de tarjetas representa una nueva forma de robo en la cual no se necesita el uso de la fuerza y la violencia para obtener dinero, basta con tener un poco de conocimientos sobre sistemas informáticos, manejo de *software* que permitan la decodificación de códigos, y el uso de aparatos tecnológicos para cometer la conducta (ver cuadro número 1).

CUADRO NÚMERO 1
CLONACIÓN DE TARJETAS DE CRÉDITO



Colectivo ARCION, Puebla, Puebla, 13 de enero de 2012. En la actualidad se han desarrollado nuevos sistemas informáticos y tecnológicos, en donde se pueden descifrar los códigos de seguridad de algunas tarjetas bancarias, y con esto se pueden cometer nuevas conductas antisociales como la clonación de tarjetas bancarias.

A partir de este punto es donde entra el profesionista Criminólogo-criminalista en el desarrollo de la investigación de esta conducta antisocial, en donde no es necesario que tenga conocimientos en informática, solo basta con identificar la conducta y ver cómo afecta a la sociedad para poder darle solución y tratar de evitar que se siga cometiendo.

El Criminólogo-criminalista es un profesionista multidisciplinario y para la investigación que realiza requiere de un gripo de profesionistas que posean conocimientos sobre sistemas de informática para obtener datos y tratar de comprender como se desarrolla esta conducta.

Durante la investigación el Criminólogo-criminalista debe de ver que indicios son los que se dejan en el lugar del hecho, también es necesario que haga de su conocimiento sobre el origen de estos indicios y como obtener los datos necesarios para que se lleve a cabo la clonación de los datos bancarios.

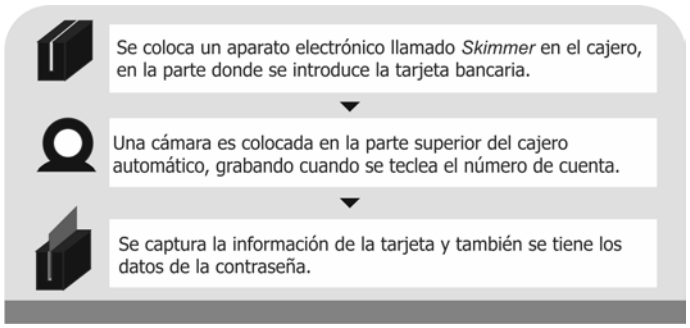
El '*Skimming*'[1], también conocido como clonación de tarjetas de crédito o débito, consiste en la duplicación de tarjetas de crédito o débito sin el consentimiento del dueño de la tarjeta. Los delincuentes que se dedican a esto utilizan diferentes tipos de dispositivos electrónicos que los ayudan a clonar las tarjetas.

El problema suele presentarse cuando los dueños de las tarjetas de crédito o débito no se dan cuenta de que son víctimas de la clonación de tarjetas hasta que les llega el estado de cuenta o cuando van a comprar algo en una tienda o por internet con su tarjeta y le dicen que su tarjeta está al límite o se la rechazan.

Clonar una tarjeta de crédito o débito a través de un cajero automático es un proceso sencillo, por eso es necesario tener mucho cuidado al realizar las transacciones en estas terminales.

El dispositivo más utilizado es un aparato diminuto cuyo nombre es '*Skimmer*'[2], se trata de un aditamento que se inserta en la ranura para la tarjeta en el cajero, tiene una cámara para captar en video cuando se teclea el Número de Identificación Personal (NIP) y al deslizar la tarjeta al interior, se captura la información de la banda magnética (ver cuadro número 2).

CUADRO NÚMERO 2
MÉTODO PARA LA CLONACIÓN DE TARJETAS BANCARIAS



Colectivo ARCION, Puebla, Puebla, 13 de enero de 2012. La obtención de los datos de una tarjeta bancaria es un proceso que a simple vista es muy fácil, pero en verdad es un complejo sistema de informática en la decodificación de códigos y en la clonación de datos.

Este tipo de aparatos no sólo es utilizado para clonar tarjetas en los cajeros, sino también se puede emplear en terminales bancarias, por tal motivo es necesario que cada vez que se realiza un pago no se pierda de vista el plástico y se conserven los comprobantes o

1 Data Security. Skimming: Clonaciòn de tarjetas bancarias. 'skimming'. [En línea]. [Consultado: 06 de enero de 2012]. Disponible en la web: http://www.wisedatasecurity.com/clonacion-tarjetas-credito.html

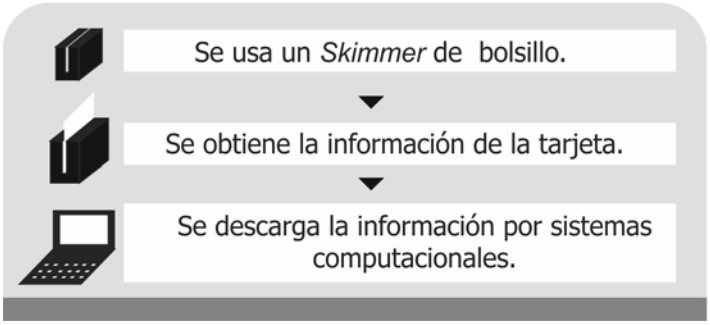
2 CNN expansión. ¿Cómo clonan tus tarjetas bancarias? 'skimmer'. [En línea]. [Consultado: 06 de enero de 2012]. Disponible en la web: http://www.cnnexpansion.com/mi-dinero/2011/09/12/como-clonan-tus-tarjetas-bancarias

recibos, para poder hacer la reclamación si aparecen cargos que no se realizaron, con esta forma el usuario pueda tener el control de los lugares en que has utilizado la tarjeta.

Pero no solamente en los cajeros automáticos se puede presentar esta conducta, en las terminales bancarias, en donde bajo el mismo procedimiento se puede llevar a cabo la clonación de tarjetas bancarias:

- El delincuente tiene en su poder un *skimmer* de bolsillo, usado para leer y guardar la información de la tarjeta.
- Luego el delincuente que trabaja en una tienda o restaurante espera a que alguien vaya a pagar y pasa la tarjeta del cliente por la maquina original de la tienda y por su *skimmer* para guardar la información de la tarjeta.
- Prosigue en su casa y conecta el *skimmer* a una computadora y pasa la información desde el *skimmer* hacia la computadora.
- Por último, el delincuente utiliza una tarjeta en blanco con cinta magnética y la pasa por otra máquina llamada codificador de tarjetas de crédito para pasar la información de la computadora hacia la tarjeta en blanco (ver cuadro número 3).

CUADRO NÚMERO 3
DESCARGA DE INFORMACIÓN A PARTIR DEL USO DEL *SKIMMER*



Colectivo ARCION, Puebla, Puebla, 13 de enero de 2012. Para la clonación de tarjetas bancarias en terminales bancarias, es un proceso muy similar al de los cajeros automáticos, los mismos instrumentos la diferencia es que aquí el trato victima-victimario es más directo y se puede reconocer al victimario.

"Durante el 2011, el problema de la clonación de tarjetas de crédito y de débito se incrementó, lo que para el 2012 continuará siendo uno de los principales temas de atención de parte de las Instituciones bancarias en México"[3].

Según información de la Asociación de Bancos de México (ABM)[4], en los últimos dos años la clonación de tarjetas de crédito se incrementó 30%, lo cual cada año deja pérdidas cercanas a los 700 millones de pesos en promedio, por lo que los bancos tuvieron que acelerar el proceso de cambio de los plásticos de débito con chip, al igual que los cajeros automáticos lectores de este tipo de productos.

De acuerdo con las disposiciones de la Comisión Nacional Bancaria y de Valores, los bancos tendrán que cambiar 100% de los cajeros automáticos a lectores de tarjetas con chip, con lo que espera controlar el fraude en este tipo de aparatos.

3 El Economista. Clonación de tarjetas, dolor para la banca. 'cifras'. [En línea]. [Consultado: 06 de enero de 2012]. Disponible en la web: http://eleconomista.com.mx/sistema-financiero/2011/12/29/clonacion-tarjetas-dolor-banca

4 Ibíd. Fecha de revisión 06 de enero de 2012.

Metodología del Criminólogo-criminalista en el lugar del hecho y la relación con en el material sensible significativo informático o electrónico

"Los intrusos y delincuentes encuentran en las tecnologías emergentes una estrategia confiable para materializar sus acciones, con una alta probabilidad de evitar cualquier tipo de proceso o de investigación que logre asociarlos con los hechos"[5].

En la actualidad, los avances informáticos y tecnológicos han sido de gran apoyo en la sociedad pues nos facilitan algunas cosas y hacen más prácticas otras. También para hacer uso del manejos de estas tecnologías no es difícil, pues hoy en día no es necesario que alguna persona tenga conocimientos en informática, con el simple hecho de conocer y explorar estos sistemas se puede tener la práctica necesaria para realizar conductas, buenas o malas.

Es por esta razón cuando se tiene como actividad la clonación de tarjetas bancarias, es difícil precisar quiénes están detrás de esta conducta, pues puede ser un experto en sistemas informáticos –*hacker*- o alguna persona que a través de la práctica y de la experiencia, obtiene los conocimientos necesarios para cometer esta conducta.

El profesionista Criminólogo-criminalista tal vez, en algunos casos, no tenga el conocimiento sobre programas de informática, pero el objeto sobre el cual va a recaer la investigación de la clonación de tarjetas son objetos materiales, como son por ejemplo las computadoras.

Al tener todo indicio relacionado con sistemas informáticos el Criminólogo-criminalista debe de tomar ciertas características para evitar la contaminación de estos indicios como lo es:

- "Alteración: por estar soportadas en medios electrónicos esta puede llegar a ser manipulada o alterada.
- Destrucción: de igual manera el 'indicio informático'[6] podrá ser eliminada, trayendo consigo problemas en el caso que se está investigando.
- Daño: puede ser modificada de tal manera que no se elimine pero la misma no puede ser recuperada o de cierta manera no posee ningún valor o presente algún aporte significativo en una investigación digital"[7].

Para poder iniciar la investigación el Criminólogo-criminalista debe de conocer ciertos pasos a seguir, así mismo premisas que no debe dejar pasar como lo son:

- "El elemento tecnológico es el objeto del ilícito.

5 Cano M. Jeimy J. Computación Forense; Descubriendo los rastros informáticos. México, DF. Alfaomega. 2009. Pág. 143.

6 Evidencia digital: en algunos países de Sudamérica se maneja el término evidencia digital, en México se mantendrá el término indicio informático.

7 Enciclopedia Criminalística, Criminología e Investigación, tomo III. Colombia. Sigma editores. 2010. Pág. 1207.

- El componente tecnológico es el instrumento para cometer el ilícito.
- El componente tecnológico facilita la consumación del ilícito"[8].

En el lugar del hecho, donde este de por medio el uso de tecnologías, sistemas informáticos, el Criminólogo-criminalista deberá siempre tener el apoyo de una persona especializada en sistemas informáticos, de programación o aquellos donde este de por medio bases de datos.

Como primera medida lo que se debe de hacer al llegar al lugar es no alterarlo, es decir, que todo material que se encuentre no sea movido de su lugar de origen, así este en el suelo, o esté en condiciones ajenas al investigador, no se debe de alterar; esto tiene por finalidad relacionar el objeto con la persona que pudo haberlo utilizado, es decir el probable responsable del hecho.

Por ello siempre se deben de tomar las precauciones habituales en cualquier lugar del hecho, tener el material idóneo para la observación, descripción, recolección, embalaje, etiquetamiento y traslado del indicio a estudiar, por todo eso se necesita de:

- Guantes de hule.
- Bolsas de plástico de diferentes tamaños.
- Cinta adhesiva.
- Etiquetas.
- Discos o dispositivos electrónicos de datos en estado virgen.
- Bolsas Faraday[9].

Teniendo el material para poder trabajar, el Criminólogo-criminalista debe de tener una metodología para iniciar con la investigación en un lugar del hecho donde se tienen materiales del tipo informático, es decir, para la clonación de tarjetas bancarias, se necesitan de dispositivos electrónicos e informáticos que permitan almacenar la información bancaria, así mismo para utilizarlos en nuevos dispositivos y cometer la conducta antisocial.

A todo este proceso desde que el Criminólogo-criminalista llega al lugar del hecho e inicia con la investigación, llevándose los indicios informáticos para su estudio en laboratorio, y dar una conclusión de la relación que existe indicio-conducta antisocial, se le llamara análisis forense[10] informático-electrónico.

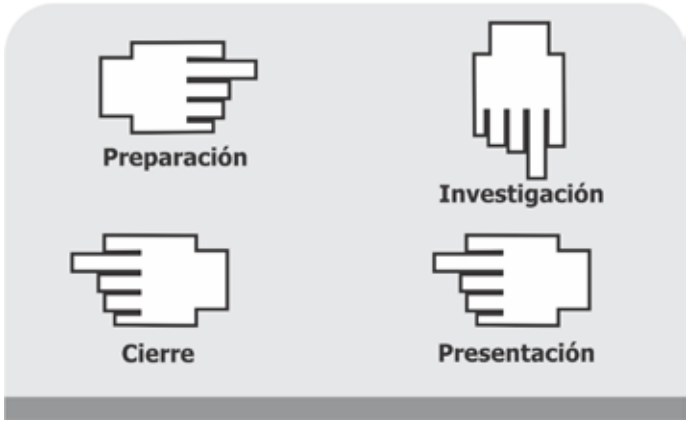
Las etapas de este proceso que el profesionista Criminólogo-criminalista debe de llevar a cabo durante la observación y descripción de un lugar del hecho donde existan indicios electrónicos o informáticos son las siguientes (ver cuadro número 4):

8 Ibídem., pág. 1207.

9 Bolsas Faraday: bolsa especial para aislamiento de emisiones electromagnéticas.

10 Análisis forense: proceso formal que se encarga de recoger, analizar, preservar y presentar a través de técnicas y herramientas la información, de tal forma que el investigador forense digital pueda entregar un informe en donde presente los hallazgos de manera lógica y con un sustento claro de lo que desea mostrar.

CUADRO NÚMERO 4
ANÁLISIS FORENSE INFORMÁTICO-ELECTRÓNICO PARA LLEVAR A CABO LA INVESTIGACIÓN



Colectivo ARCION, Puebla, Puebla, 28 de febrero de 2012. Las etapas que se deben de seguir para iniciar la investigación son preparación, investigación, presentación y cierre; en cada etapa el Criminólogo-criminalista debe de estar preparado para comprender la relación entre los indicios con el tipo de lugar del hecho y determinar una posible personalidad del individuo que comete la acción.

Preparación

Es la primera etapa, consiste en tener todo preparado antes de ir al lugar del hecho. Esto quiere decir que el Criminólogo-criminalista debe de tener todo preparado antes de ir a un lugar del hecho donde exista la posibilidad que haya indicios del tipo informativo o electrónico.

Siendo también estas actividades durante esta etapa:

1. "Establecer lo que se necesita para realizar la investigación tanto a nivel operacional como técnico.
2. Es necesario que los protocolos de la primera persona que llega al hecho estén claramente definidos, de tal manera que aseguren el lugar que está bajo investigación.
3. Definir de manera clara la estrategia con la que se debe identificar, recolectar, etiquetar, analizar y transportar todo indicio.
4. Definir claramente los perfiles que van a ser involucrados en la investigación, tanto a nivel operacional, analistas forenses y líder o líderes de los casos"[11].

Investigación

Esta etapa es la más compleja para el Criminólogo-criminalista, es donde interviene directamente con el lugar del hecho, involucrando un gran número de actividades.

"Esta etapa de investigación debe de tener clara la premisa de que es importante, desde el principio hasta el fin, mantener la cadena de custodia; por consiguiente, la documentación será la pieza fundamental del proceso"[12].

En el lugar del hecho es donde se van a encontrar la gran mayoría de indicios, por tal motivo se tiene que tener cuidado al

11 Enciclopedia Criminalística, Criminología e Investigación, tomo III. Colombia. Sigma editores. 2010. Pág. 1209.

12 Enciclopedia Criminalística, Criminología e Investigación, tomo III. Colombia. Sigma editores. 2010. Pág. 1209.

observarlo y describirlo; en un lugar del hecho donde intervienen aparatos electrónicos o informáticos el manejo de estos aparatos es importante, pues pueden tener información valiosa durante la investigación (ver cuadro número 5).

CUADRO NÚMERO 5
APARATOS ELECTRÓNICOS Y/O INFORMÁTICOS QUE SE ENCUENTRAN EN UN LUGAR DEL HECHO

Aparato electrónico o informático	Función	Relación con el fenómeno o hecho delictivo
Unidad Central de Procesamiento (CPU).	Interpreta las instrucciones contenidas en los programas y procesa los datos.	Puede contener toda la información relacionada con las actividades del individuo, desde programas que utiliza, hasta documentos personales.
Dispositivos de almacenamiento (memorias USB, Discos Compactos (cd), *Digital Versatile Disc* (dvd) o tarjetas 3 1/2).	Estos dispositivos realizan las operaciones de lectura o escritura de los medios o soportes donde se almacenan o guardan, lógica y físicamente, los archivos de un sistema informático.	Estos dispositivos pueden tener información de primera mano es decir actualizada, así como documentos que pueden transportarse de un lugar a otro.
Computadora portátil.	Son capaces de realizar la mayor parte de las tareas que realizan los ordenadores de escritorio, con similar capacidad y con la ventaja de su peso y tamaño reducidos; sumado también a que tienen la capacidad de operar por un período determinado sin estar conectadas a una corriente eléctrica.	Al igual que el CPU, tiene toda la información del individuo, tiene todos sus documentos y programas, por tal motivo en un lugar del hecho, estos aparatos pueden ser de gran importancia para determinar la actividad del individuo.
Dispositivos electrónicos (celulares, *Iphone*, *Ipad*, agendas electrónicas).	Son todos aquellos que tienen información personal del individuo, esta información puede tener datos personales de otras personas	Al tener estos dispositivos se pueden ver los movimientos que hace el individuo, como lo son amistades, lugares e inclusive eventos en donde participará.

Colectivo ARCION, Puebla, Puebla, 29 de febrero de 2012. La importancia de los indicios que se pueden encontrar en el lugar del hecho es significativa, por tal motivo se debe de conocer la relación indicio-lugar-sujeto.

Una vez que se tiene el tipo de indicios que se puede encontrar en un lugar del hecho, se tiene que emplear una metodología para hacer su estudio, es decir recurrir a la observación y descripción.

La finalidad de emplear esta metodología tiene que ver con el aseguramiento del lugar, evitando posible contaminación así como la perdida de indicios que pueden tener una relación estrecha con el hecho a estudiar. Para que se lleve a cabo esto se empleara el siguiente procedimiento:

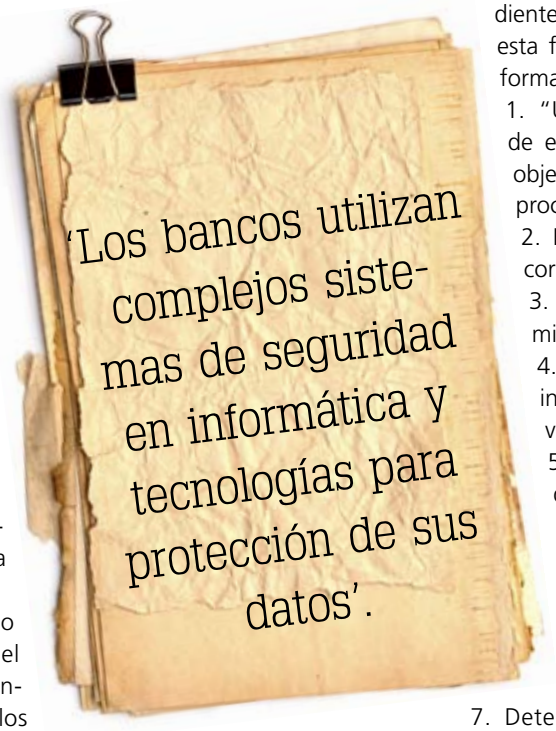
1. "No tomar los objetos sin guantes de hule, pues se podría altera, encubrir o desaparecer las huellas dactilares o adeníticas existentes en el equipo o en el área donde se encuentra residiendo el sistema informático.
2. Proteger en la medida de lo posible la zona de posibles interacciones humanas o animales.
3. Tener extrema precaución de no tropezar, jalar o cortar cables de conexión de equipos, periféricos o conexiones de entrada o salida de datos.
4. Asegurar la zona y los equipos de acceso remoto, lo cual debe hacerse con extremo cuidado si se trata de servidores que deben ser intervenidos, ya que estos, por su propia naturaleza, están especialmente preparados para ser accesados en forma remota.
5. Controlar los presuntos responsables o la persona que estaba a cargo de los equipos no tenga en su poder un control remoto o cualquier otro dispositivo electrónico que pueda alterar el contenido o el estado de los equipos o periféricos, ya estén estos conectados o no al servidor o sistema central.
6. Retirar los teléfonos celulares o dispositivos tipo *blue berry* o similares –dispositivos que conjuntan las PDA[13] con teléfonos celulares-, ya que con ellos pueden realizarse en ciertos casos modificaciones sobre los equipos en distancias cortas.
7. Asegurar el acceso y control de los suministros de luz, ya que existen muchos equipos que sin son apagados de manera incorrecta pueden dañarse o bien pueden perder información, como por ejemplo la de inicio de sesión.
8. Una vez garantizado el cierre del área, debe procederse a tomar fotografías del estado y posición de los equipos, así como de sus

13 PDA: del inglés personal digital assistant (asistente digital personal), también denominado ordenador de bolsillo u organizador personal, es una computadora de mano originalmente diseñado como agenda electrónica.

puertos –conectores de cables, lectores de CD, lectores de disquete y cualquier otro punto de contacto del equipo con el exterior- y de igual manera de la pantalla en el estado en que se encuentre, incluyéndose los cables, conectores externos e, incluso, los dos los periféricos que se hallan en el área o los que pudieran estar conectados de forma remota si ello es posible, con las debidas identificaciones, ya sea de marca o cualquier otra que pueda dar certeza sobre el equipo. Es ideal tomar fotografías de los números de serie de todos ellos"[14].

Una vez que se llega al lugar del hecho se observa y describe todo lo que se encuentra en ese momento, iniciando la recolección de los posibles indicios, etapa de mucho cuidado en la que el Criminólogo-criminalista debe de prestar mucha atención a la forma como los indicios son recolectados, de tal manera que no afecten la integridad de la información que es almacenada a través de un medio digital o fuente donde se encuentra la información. Por tal motivo es necesario:

1. "Se documente el estado en el que se encuentra el medio tecnológico, indispensable documentar si se encuentra apagado o encendido el medio tecnológico, puesto que cada uno de estos estados se debe realizar una acción particular.
2. Tomar en caso de ser necesario la información más volátil del sistema, entre ellas están la información de la memoria y los procesos que están ejecutando en caso de estar prendida la maquina y en operación normal"[15].



Para que se pueda recolectar el indicio informático o electrónico es necesario tomar en cuenta las condiciones necesarias para el almacenamiento y transporte de estos indicios, dado que condiciones como la humedad, la temperatura, las corrientes eléctricas y los campos magnéticos pueden alterar los medios de almacenamiento y por lo tanto la información que se encuentra almacenada. Por ello es necesario garantizar:

1. "Etiquetado de los indicios identificados con el objetivo de poder replicar en un ambiente controlado para su posterior análisis.
2. Guardar los medios tecnológicos en embalajes que eviten los problemas con estática.
3. No transportar los indicios por largos periodos, en este aspecto que salga del lugar directo para el laboratorio donde se realizara su posterior análisis.
4. Se debe de almacenar en un ambiente adecuado para ello, como son los laboratorios que se dispongan para investigar y analizar los componentes tecnológicos definidos"[16].

Una vez que se tienen los indicios recolectados, se envían al laboratorio donde viene la parte más importante de la investigación: el análisis de los indicios. En esta fase fundamentalmente se busca extraer la información de los medios digitales identificados de tal forma que se pueda realizar la correspondiente reconstrucción de los hechos. En esta fase se busca la extracción de información:

1. "Utilizar más de una herramienta de extracción de información, con el objetivo de dar mayores garantías al proceso.
2. Extraer la información acerca del correo electrónico.
3. *Logs*[17] del sistema, ingresados al mismo.
4. Identificación de volatilidad de la información más volátil a la menos volátil.
5. Extracción de los datos y filtrado de los mismos.
6. Identificar y recuperar datos y filtrado de los mismos:
   a. Eliminados.
   b. Escondidos.
   c. Cifrados.
   d. Corruptos.
7. Determinar líneas del tiempo o secuencia en que los eventos se presentaron.
8. Evaluación del perfil atacante.
9. Construir un marco del caso en donde, de manera lógica y secuencial, se relaten los hechos identificados basados en los hallazgos"[18].

Presentación

Esta fase permite entregar un informe donde se presenta de manera ordenada los hallazgos encontrados o los indicios necesarios para concluir la investigación que se esté realizando.

El informe que presentara el Criminólogo-criminalista será un dictamen, en donde se escriba todo lo relacionado con el hecho, los indicios y la probable responsabilidad del sujeto en el hecho.

14 Andrés Cámpoli, Gabriel. Manual básico de cateo y aseguramiento de evidencia digital. México. Instituto Nacional de Ciencias Penales. 2006. Pág. 18.

15 Enciclopedia Criminalística, Criminología e Investigación, tomo III. Colombia. Sigma editores. 2010. Pág. 1210.

16 Enciclopedia Criminalística, Criminología e Investigación, tomo III. Colombia. Sigma editores. 2010. Pág. 1211.

17 Logs: Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where and why) un evento ocurre para un dispositivo en particular o aplicación.

18 Enciclopedia Criminalística, Criminología e Investigación, tomo III. Colombia. Sigma editores. 2010. Pág. 1212.

Este dictamen deberá de ser concreto, preciso y entendible para el juzgador, porque de esto se determinara la intervención de uno o varios sujetos en la comisión de algún delito.

Cierre

Esta etapa consiste en el cierre total de la investigación donde una vez que se resolvió el caso y se obtuvieron los resultados necesarios para determinar la intervención de uno o varios sujetos en la comisión de un hecho delictivo, el Criminólogo-criminalista debe de dar por terminada la investigación, una vez que se hayan utilizado y desahogado todas las pruebas, para demostrar la relación lugar del hechos-indicios-sujeto(s).

Intervención del Criminólogo-criminalista en la actividad de la clonación de tarjetas bancarias

El Criminólogo-criminalista interviene en esta actividad desde el momento en que se fabrica el denominado *skimmer*, hasta que se obtienen los datos de la tarjeta bancaria y son utilizados para obtener el dinero de manera ilícita.

Una cosa si es cierta, en estos casos los procedimientos que se utilizan tienen que ver con sistemas informáticos, computacionales y el manejo de tecnologías, cosas que el Criminólogo-criminalista no tiene conocimientos, pero si sabe como poder llevar la investigación, o que tipo de metodología es la que se tiene que llevar para que no se pierda información.

Para que se lleve a cabo esto, necesita primeramente el apoyo de un especialista en sistemas informáticos, pues el si conoce los instrumentos y los *software* que se utilizan para la clonación de tarjetas bancarias.

En el Criminólogo-criminalista recae la investigación, es la persona idónea, pues el va a ser quien intervenga en los indicios que se encuentren en el lugar del hecho –puede ser un *skimmer* en el cajero automático o uno portátil- dando una posible mecánica de los hechos (ver cuadro número 6).

CUADRO NÚMERO 6
INTERVENCIÓN DEL CRIMINÓLOGO-CRIMINALISTA

Nombre de la conducta antisocial	Medio que se utiliza para cometer la conducta	Finalidad de la conducta	Relación Criminólogo-criminalista
Clonación de tarjetas bancarias.	Mediante la utilización de sistemas informáticos y electrónicos.	Obtener dinero, usando la información bancaria de otro individuo –robo-.	Determinar cómo se lleva a cabo la conducta, quienes son los probables responsables, cual es su finalidad y que instrumentos son los que utilizan para finalizar su actividad.

Colectivo ARCION, Puebla, Puebla, 25 de enero de 2012. En el presente cuadro se analiza la posible intervención en un hecho donde está el uso de tarjetas clonadas, desde el medio que utiliza, su finalidad y la relación que tiene con este profesionista.

Las personas idóneas que intervienen en todos estos tipos de actividades son los *hackers*.

Hackers[19], una palabra que aún no se encuentra en los diccionarios pero que las personas en la actualidad empiezan a manejar haciendo relación con el internet y sistemas informáticos.

Los *crackers* 'crack´ -destruir- son aquellas personas que siempre buscan molestar a otros, piratear *software* protegido por leyes, destruir sistemas muy complejos mediante la transmisión de poderosos virus, etc. Se diferencian con los Hackers porque no poseen ningún tipo de ideología cuando realizan sus trabajos. En cambio, el principal objetivo de los Hackers no es convertirse en delincuentes sino pelear contra un sistema injusto utilizando como arma al propio sistema.

El avance de la era informática ha introducido nuevos términos en el vocabulario de cada día. Una de estas palabras *hacker,* que tiene relación con los delitos informáticos.

Los Criminólogos, por otra parte, describen a los *hackers* en términos menos halagadores. Donn Parker los denomina violadores electrónicos y August Bequai los describe como vándalos electrónicos. Ambos, aunque aseveran que las actividades de los *hackers* son ilegales, evitan hábilmente llamarlos criminales informáticos. Hacen una clara distinción entre el *hacker* que realiza sus actividades por diversión y el empleado que de repente decide hacer algo malo.

Por tanto, parece que se tiene una definición en la que caben dos extremos: por un lado, la persona que roba a bancos y por otro lado la persona inquieta. Ambas actividades son calificadas con el mismo término. Difícilmente se podría considerar esto como un ejemplo de conceptualización precisa.

El término comenzó a usarse aplicándolo a un grupo de pioneros de la informática, a principios de la década de 1960. Desde entonces, y casi hasta finales de la década de 1970, un *hacker* era una persona obsesionada por conocer lo más posible sobre los sistemas informáticos.

Pero a principios de la década de 1980, los *hackers* pasaron a ser considerados como chicos jóvenes capaces de vulnerar sistemas informáticos de grandes empresas y del gobierno. Infortunadamente, los medios de información y la comunidad científica social no han puesto mucho esfuerzo por variar esta definición. El problema para llegar a una definición más precisa radica, tanto en la poca información que hay sobre sus actividades diarias, como en el hecho de que lo que se conoce de ellos no siempre cabe bajo las etiquetas de los delitos conocidos.

19 Seguridad informática: hackers. Seguridad informática. 'Hacker'. [En línea]. [Consultado: 27 de enero de 2012]. Disponible en la web: http://www.monografias.com/trabajos/hackers/hackers.shtml

Es decir, no hay una definición legal que sea aplicable a los *hackers*, ni todas sus actividades conllevan la transgresión de las leyes. Esto lleva a que la aplicación del término varié según los casos, dependiendo de los cargos que se puedan imputar y no a raíz de un claro entendimiento de lo que el término significa.

Este problema, y la falta de entendimiento de lo que significa ser un hacker, convierten a esta en una etiqueta excesivamente utilizada para aplicar a muchos tipos de intrusiones informáticas.

El *hacker*, en algunos casos puede emplear una metodología para obtener lo que quiere, las cuales se clasificaran como fases:

Fase 1. Reconocimiento; El reconocimiento se refiere a la fase preparatoria donde el atacante obtiene toda la información necesaria de su objetivo o victima antes de lanzar el ataque. Esta fase también puede incluir el escaneo de la red que el *hacker* quiere atacar no importa si el ataque va a ser interno o externo. Esta fase le permite al atacante crear una estrategia para su ataque.

Fase 2. Escaneo; Esta es la fase en el atacante realiza antes de lanzar un ataque a la red. En el escaneo el atacante utiliza toda la información que obtuvo en la Fase del Reconocimiento, para identificar vulnerabilidades específicas

Fase 3. Ganar Acceso; Esta es una de las fases más importantes para el *hacker* porque es la fase de penetración al sistema, en esta fase el *hacker* explota las vulnerabilidades que encontró en la fase 2. La explotación puede ocurrir localmente, *off line*, sobre el *Local Área Network* (Red de Área Local), o sobre el internet.

Fase 4. Mantener el Acceso; Una vez que el *hacker* gana acceso al sistema objetivo. Su prioridad es mantener el acceso que gano en el sistema. En esta fase el *hacker* usa sus recursos y recursos del sistema, y usa el sistema objetivo como plataforma de lanzamiento de ataques para escanear y explotar a otros sistemas que quiere atacar.

Fase 5. Cubrir las huellas; En esta fase es donde el *hacker* trata de destruir toda la evidencia de sus actividades ilícitas y lo hace por varias razones entre ellas seguir manteniendo el acceso al sistema comprometido ya que si borra sus huellas los administradores de redes no tendrán pistas claras del atacante y el *hacker* podrá seguir penetrando el sistema cuando quiera, además borrando sus huellas evita ser detectado y ser atrapado por la policía.

Ahora que se tiene un concepto más amplio acerca de que es un *hacker*, que puede hacer, ahora hay que relacionarlo con la actividad de la clonación (ver cuadro número 7).

CUADRO NÚMERO 7
RELACIÓN DEL *HACKER* CON LA CLONACIÓN DE TARJETAS

Hacker	Relación
Interceptan códigos de tarjetas de crédito.	Estos códigos son la llave para obtener datos de la tarjeta.
Vulnerar sistemas informáticos de grandes empresas y del gobierno.	Al vulnerar estos sistemas acceden a información confidencial y por lo tanto a la obtención de esos datos.
Realizan transacciones de una cuenta bancaria a otra.	Al hacer esto pueden transferir cantidades de dinero a diferentes cuentas de distintos bancos, para no ser rastreados.

Colectivo ARCION, Puebla, Puebla, 31 de enero de 2012. En el presentecuadro se muestra la relación que existe en la actividad de un hacker relacionado con la clonación de tarjetas, cual es acción que ejerce para que se lleve a cabo esta conducta.

Existen personas que conocen de los sistemas informáticos pues estudiaron una licenciatura, pero también existen personas que no precisamente tienen conocimiento en sistemas informáticos y pueden descifrar todo un sistema complejo de programación, o utilizar aplicaciones informáticas para decodificar contraseñas y poder entrar a sitios seguros e inclusive robar información de otras personas.

Esto sucede con la clonación de tarjetas bancarias, donde en algunas ocasiones los *hacker* pueden estar presentes en esta conducta con la creación de programas encargados de robar los datos de la tarjeta bancaria, así mismo para interpretarlos y usarlos de nuevo.

Pero el *hacker* es solo una pieza, principal y significativa de esta actividad ilícita pero no la única, su especialidad es interpretar los datos que obtenga de una tarjeta o en su caso de un *skimmer*, necesitando de otras personas que pongan el *skimmer,* para conseguir el instrumento requerido y llevar a cabo la clonación (ver cuadro número 8).

CUADRO NÚMERO 8
PERSONAS QUE INTERVIENEN EN EL HECHO

Hacker	Es la persona que va descifrar los datos obtenidos de las tarjetas de crédito, y quien va a efectuar la clonación. No necesariamente tiene que ser un ingeniero en sistemas informáticos, basta con conocer estos sistemas e interpretarlos.
Transportador	Es la persona que transporta el skimmer –en algunos caso la cámara- al cajero donde se va a instalar, también es el responsable de recogerlo.
Halcón	Es la persona encargada de la vigilancia del transportador.
Negociador	Esta persona puede estar o no, es la encargada de hacer negocios, es decir, vender las tarjetas clonadas.

Colectivo ARCION, Puebla, Puebla, 01 de febrero de 2012. Algo importante en la clonación de tarjetas, es saber que personas son las que intervienen, no solo es un hacker o alguien con conocimientos en sistemas computacionales, sino otras personas que se encargan de ejecutar la acción.

En este cuadro se habla de la clonación de tarjetas cuando intervienen varias personas, y como en el último recuadro esta marcado, cuando se tiene fines de lucro. Pero no es así en los casos donde la finalidad es personal, o sea, clonar la tarjeta para hacer un uso propio del dinero que se obtenga.

Ahora que sabemos las personas que intervienen en esta actividad, nos daremos a la tarea de ver qué tipo de material es el se emplea para la clonación (ver cuadro número 9).

CUADRO NÚMERO 9
MATERIAL QUE SE EMPLEA PARA LA CLONACIÓN

Aparato	Función
Skimmer	Es un lector de bandas magnéticas de las tarjetas o plásticos que utilizan algunas personas para conocer el saldo del usuario y los movimientos que realiza.
Programas	Es el componente de software que se encarga de administrar los recursos de hardware como la memoria, el disco duro, los dispositivos periféricos.
Decodificador	Necesita leer y decodificar la información almacenada en las cintas magnéticas de las tarjetas de crédito.
Tarjetas blancas	Son aquellas en la cual se va a descargar la información obtenida a través del skimmer.

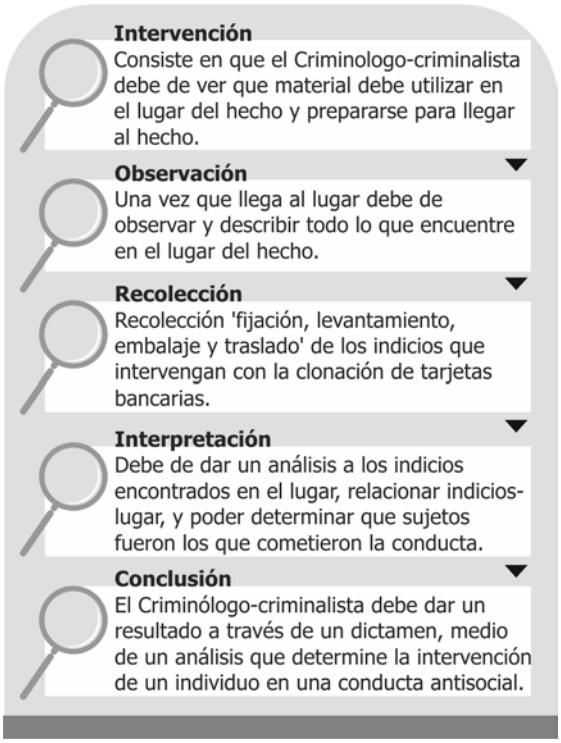
Colectivo ARCION, Puebla, Puebla, 02 de febrero de 2012. Otra de las cosas que se debe de ver dentro de la clonación de tarjetas es el material que se va a utilizar, como un skimmer, pasando por una computadora hasta las tarjetas blancas.

Estos aparatos tecnológicos se pueden encontrar en internet, lo que es un factor que favorece a que se cometa esta conducta.

Sabemos que indicios se pueden encontrar en el lugar del hecho, y los tipos de personas que pueden cometer la conducta de la clonación de las tarjetas, siendo su finalidad obtener el dinero de otra persona. En algunos casos se han llegado a vender tarjetas de crédito que han obtenido sus datos a partir de otras que han clonado, incluso de manera sarcástica se burlan de sus acciones.

Por esta razón se necesita de un profesionista encargado de seguir las líneas de investigación como el Criminólogo-criminalista, quien en un lugar del hecho debe de ser la persona indicada para llevar el caso, utilizando todos los métodos de observación y descripción del lugar, los indicios que intervengan para que se realice la conducta de la clonación de tarjetas, no conforme con eso debe de determinar qué tipo de persona es la que comete la conducta, cual es su finalidad y tratar de dar un esclarecimiento del hecho (ver cuadro número 10).

CUADRO NÚMERO 10
LÍNEA DE INVESTIGACIÓN DEL CRIMINÓLOGO-CRIMINALISTA



Colectivo ARCION, Puebla, Puebla, 01 de marzo de 2012. La línea de investigación del Criminólogo-criminalista es todo el proceso que tiene que llevar a cabo para que realizar la observación y descripción del lugar del hecho.

Mesa de trabajo con el Delegado Estatal de Puebla de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), con el tema 'Clonación de tarjetas y suplantación de identidad'

Fotografía número 1. Colectivo ARCION, Condusef, Delegación Puebla. 16 de febrero de 2012. Se encuentra de izquierda a derecha el Ingeniero Bernardo Arrubarrena García (Delegado Estatal de la Condusef), el Licenciado Rafael Gerardo Vallejo Minuti (Subdelegado Estatal de la Condusef) y la Licenciada Victoria Elizondo Cruz (Área de Oficialía de la Condusef).

El día jueves 16 de febrero siendo las 9:15 horas, se realizo una entrevista ante la Comisión Nacional para la Protección y Defensa (Condusef) en donde se tuvo una mesa de trabajo con el Delegado Estatal de Puebla y sus dos principales funcionarios (ver fotografía número 01). A continuación se pone parte de la conversación que se tuvo durante la reunión:

La Condusef es la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, es una Institución financiera que tiene 13 años de existencia, atiende solamente quejas y asuntos de carácter financiero, no tienen relaciones con asuntos comerciales, para ese tipo de asuntos comerciales esta la Procuraduría Federal del Consumidor (Profeco).

Los tipos de asuntos que atiende la Condusef tienen relación con Bancos, Sofoles[20], Sofomes[21], figuras financieras alternativas, Seguros, Fianzas y Afores.

Cabe hacer mención que la Condusef tampoco es una Institución donde se procure o administre justicia, su labor radica principalmente en la conciliación entre ambas partes –Institución financiera/cliente- a través de un esquema de negociación, en donde a partir de una denuncia ciudadana contra una Institución financiera, la Condusef da una asesoría a la persona afectada para abrir los vínculos con la Institución financiera y llegar a los primeros acuerdos, si la respuesta es negativa por parte de la Institución financiera, la Condusef llevara a cabo una Audiencia de Conciliación con la institución.

De las 20,000 quejas y asuntos relacionados con instituciones financieras, 7 de cada 10 se resolvieron, es decir se llego a un acuerdo y se demostró la inocencia del usuario de algún servicio financiero. Para llevar a cabo estas quejas y asuntos la Condusef tiene abogados que ejercen de manera gratuita

Para tener más informes acerca de las atribuciones la Condusef, esta institución tiene una página web, la cual es la segunda más visitada después del Servicio de Administración Tributaria (SAT), en donde se registro en el año 2011 aproximadamente 21 millones de consultas, siendo los temas más solicitados los relacionados con comparativos de seguro, rendimiento de inversiones.

Las acciones de atención registradas ante Condusef en un estudio a nivel nacional, Puebla representa el 4% de datos económicos a nivel nacional.

En cuanto a la relación con la clonación de tarjetas, la Condusef tiene relación con dependencias de gobierno como la Secretaria de Seguridad del Municipio, donde interviene en delitos como robo de cajeros automáticos, clonación de tarjetas, así mismo con el Consejo Ciudadano de Seguridad Pública, en donde para iniciar con una investigación es necesario la instancia judicial, es decir que la persona afectada de estas conductas levante una denuncia.

La Condusef reconoce la diferencia entre la suplantación de identidad y la clonación de tarjetas bancarias como dos asuntos distintos. Esta comisión ha tenido casos de clonación de tarjetas en la ciudad de Puebla, en donde está involucrada la suplantación de identidad en algunos casos.

En la clonación de tarjetas bancarias las personas que cometen este hecho forman bandas especializadas, en donde por ejemplo, en un restaurante o bar, se paga con la tarjeta de crédito, el mesero la lleva y con ayuda incluso del mismo gerente o de la persona que atiende alguna caja, pasan la tarjeta por un escáner, vacían los datos de la tarjeta de crédito a una tarjeta virgen clonando la tarjeta de crédito.

Lamentablemente los equipos para la clonación se venden por internet, desde tarjetas vírgenes hasta el *skimmer*, incluso se venden tarjetas clonadas. También existen videos que representan el cómo se lleva a cabo la clonación de la tarjeta bancaria.

En cuanto a la suplantación de identidad, una de estas formas se lleva a cabo cuando se quiere hacer un trámite en una institución, dependencia o agencia, se dejan los datos personales, como pueden ser comprobante domiciliario o copia del IFE por ejemplo, y las personas encargadas de recabar estos datos hacen un mal uso de estos, en donde se tramitan créditos a nombre del afectado sin que este se dé por enterado.

20 Sofoles: Sociedades Financieras de Objeto Limitado, son sociedades anónimas especializadas en el otorgamiento de créditos a una determinada actividad o sector.
21 Sofomes: Sociedades Financieras de Objeto Múltiple, son sociedades anónimas cuyo objeto social principal es el otorgamiento de crédito, y/o la celebración de arrendamiento financiero.

En cuanto a investigación de estos hechos, la Condusef no lleva líneas de investigación, se hace allegar de información a través de un informe que por ley tiene la facultad de solicitar a la Institución financiera; la Institución rinde un informe, en donde se hace investigación a nivel técnico y operación para detectar elementos y presumir que hubo alteración en la solicitud de dinero, movimientos irregulares –por ejemplo-, pero como tal investigación propiamente dicha la Condusef no hace, no interviene, ni cuestiona; toda las prueba que se obtienen de las instituciones y los usuarios, son solamente elementos de convicción, porque no se tiene la facultad de juzgar el asunto, se puede valorar y percibir que el cliente tiene o no la razón en el hecho pero no emite juicio.

El asunto de la clonación de tarjeta y suplantación de identidad también tiene que ver con el marco legal, aun no existe una legislación adecuada, útil y practica, por ejemplo: una persona que le aparece en su muro de crédito una tarjeta y un coche, así como créditos que no le corresponde, en este caso existe una suplantación de identidad, porque alguien falsifica pasaporte, comprobante domiciliario, comprobantes de ingresos, que aunque se hable de falsificación de documentos se abren dos vías, por un lado, se le informa al banco, que la persona afectada no corresponde a la de los datos que se presentaron, pues aunque se tengan los documentos de la persona, simplemente no son los originales, esto quiere decir que fueron falsificados –inclusive su firma-, entonces no se le puede cobrar los créditos, el afectado levanta la denuncia penal, con la finalidad de exonerar culpas del mal usos de los datos personales. Es aquí donde entran dos procesos, por un lado la vía de la conciliación y por otro lado la vía legal-judicial.

Por lo regular este tipo de hechos pasa cuando la víctima deja sus datos confidenciales a promotores, quien a su vez intercambia información con otro promotor, el problema radica en la salvedad de confidencialidad de datos personales. Es aquí donde existen las denominadas redes de complicidad.

En el caso de la clonación de tarjetas hoy en día no se acaba de identificar muy bien, porque en algunos casos puede ser clonación o en otros puede ser compra no reconocida -compra vía electrónica, cuando se obtienen los datos de la tarjeta y conociendo el domicilio de la persona, se hace una compra vía internet- siendo este un robo más simple.

De las 20,000 quejas recibidas a la Condusef, un poco más de las 10,000 tienen que ver con Instituciones financieras, siendo alrededor 5,000 tiene que ver con clonaciones de tarjetas, robo de identidad, cargos no reconocidos, representando un 25% de estas modalidades.

En cuanto a las instituciones financieras que han sido víctimas de clonación de tarjetas, estas han sido de forma proporcionada, algunos bancos han migrado todas sus tarjetas a chip como el caso de Santander, pero aun así han sido clonadas. No se puede saber que Institución presenta más casos de clonación de tarjetas, pues eso va a depender del número de cuentahabientes que tenga el banco, el número de quejas de un banco que maneja una cartera mayor se va a ver aumentado.

Los bancos que están en instituciones comerciales también son objeto de estudio de la Condusef si son víctimas de una clonación de tarjetas, pues son banca múltiple, reúne los requisitos de Institución financiera, pese a que se encuentre en una tienda comercial, son dos personas morales distintas.

Las Instituciones financieras donde la Condusef interviene son los siguientes:

Bancomer, Banamex, HSBC, Santander, Banorte, IXE Banco, Scotiabank, Grupo financiero Inbursa; BanCoppel, Compartamos Banco, Banco Amigo, Grupo financiero Multiva, Banco Walmart, Volkswagen Bank, Banco del Bajío, por mencionar algunos Bancos.

La Condusef es identificada o reconocida por tres medios:

1. Medios masivos de comunicación.
2. La misma sociedad, es la que recomienda este consejo.
3. Los bancos son los que recomiendan ir a la Condusef.

Medidas de seguridad que da la Condusef para no ser víctimas de suplantación de identidad o clonación de tarjetas bancarias:

1. No traer credenciales de identificación en la cartera, pues al perderse o extraviarse se pueden utilizar en contra de uno mismo.
2. No llevar las credenciales de identificación junto con las tarjetas bancarias en la cartera.
3. No contestar ninguna pregunta vía correo electrónico.
4. No dar datos personales vía telefónica.
5. En la búsqueda de créditos en los pasillos de centros comerciales, no dar datos personales a estas personas.
6. Si se va a pagar con tarjeta en un restaurante o bar, no perder de vista la tarjeta bancaria, de preferencia usar la terminal portátil.
7. Tratar de no pagar en gasolineras con la tarjeta de crédito.
8. Usar los cajeros de las sucursales bancarias nunca en los que están en la calle o en centros de conveniencia, pues estos no están vigilados con sistemas de seguridad.

Qué hacer si se es víctima de una clonación de tarjeta:

1. Si se detecta que es víctima de una posible clonación se debe de notificar al banco, para que se inicie el proceso de investigación del banco.
2. Cuando el banco ya agoto todos sus dictámenes, y no se llega a un resultado, se puede ir a la Condusef. Todo esto tiene un periodo de investigación.
3. Deben de recordar todos sus movimientos financieros, es decir, si utilizaron la tarjeta para hacer un pago, no lo deben de pasar desapercibido, puede ser haber una confusión.
4. Seguir los pasos que le indique la Institución bancaria para que se lleve a cabo la investigación de una manera más eficiente.
5. La Condusef tiene 2 años a partir de que surge la controversia para conocer del caso de clonación de tarjeta y de 15 a 20 días se dará audiencia para resolver el caso.
6. El usuario tiene 90 días para objetar los cargos a la institución bancaria.
7. No confundir la clonación de tarjetas con el robo familiar, el delincuente se va a robar todo el dinero de la tarjeta, no se robara

solo una modesta cantidad ni mucho menos de manera repetitiva, es decir que algún familiar se robe la tarjeta y sustraiga el dinero sin el consentimiento del titular.

La Condusef tiene la facultad de pedir todo tipo de documentación a las Instituciones financieras, en este caso con los cajeros automáticos, las secuencias fotográficas de las cámaras de seguridad. Así mismo todo el tipo de información necesaria para el desahogo de cualquier problema, desde un contrato de apertura, una firma de misión de tarjeta, videos o secuencia fotográficas de cajeros y demás, y si lo requiere documentación auditiva que tenga relación directa con el caso.

Después de esto se da por terminada la mesa de trabajo, agradeciendo al delegado Estatal y a su equipo de trabajo la oportunidad de trabajar juntos, pudiendo observar con más claridad y precisión esta nueva conducta antisocial y así evitar que personas caigan victimas en esta nueva forma de conductas.

Conclusión

En el presente ensayo se observo el actuar del profesionista Criminólogo-criminalista en una conducta delictiva denominada clonación de tarjetas bancarias, en donde también se relaciona este hecho con la suplantación de identidad.

Es por esta razón, que al conocerse una nueva conducta que puede ser delictiva y se está manifestando en la sociedad de una manera repetitiva, afectando no solo a la institución bancaria, y a sus usuarios, sino también representando una amenaza al Estado y a sus órganos encargados de procurar y administrar justicia, púes esta conducta delictiva se hace presente con modalidades nuevas, usando tecnologías electrónicas e informáticas en donde realizar una investigación y recabar la suficiente información para probar su existencia es una tarea un poco difícil para el investigador, ya que no existe una metodología encaminada a estos hechos delictivos.

En este tipo de hechos es donde interviene el Criminólogo-criminalista, siendo la persona investigadora que utilizando una metodología encaminada a la resolución del hecho antisocial. No se dice, que sea una conducta delictiva, ya que aún no ha sido sancionada por el Derecho Penal, existiendo algunas iniciativas de ley para tipificar dicha conducta.

En el hecho de la clonación de tarjetas, nos podemos encontrar con indicios como el *skimmer*, tarjetas virgenes o blancas, programas de informática o *software* que se utilicen para el robo de información bancaria, inclusive cámaras de video; ya que al manipular y utilizar este tipo de indicios, y no tener un buen cuidado durante la cadena de custodia esta se puede perder, desperdiciando los datos útiles en la resolución del hecho delictivo.

No solo se van a encontrar indicios físicos para determinar la existencia de la conducta antisocial, también pueden existir otros elementos que de igual manera nos pueden servir para comprobar la existencia de este hecho, tales como pueden ser por ejemplo declaraciones de la partes afectadas, la declaración del victimario y de los testigos o cómplices del acto los cuales al estar en polos opuestos de la conducta nos pueden arrojar datos para esclarecer el hecho delictivo.

Para determinar qué papel tiene el Criminólogo-criminalista en un hecho donde existan indicios informáticos o electrónicos, se hizo una investigación relacionando el lugar del hecho, con los indicios que pueda presentar y los sujetos que los utilizan para obtener un producto. Proponiendo una metodología que reúna los requisitos necesarios para involucrar a estos tres personajes que intervienen en el hecho –lugar, indicios, sujeto- para no perder la información que pueda abarcar estos personajes del hecho y así poder terminar con la investigación llegando a las conclusiones resolviendo el hecho delictivo.

FUENTES DE INFORMACIÓN

Bibliográficas

Andrés Cámpoli, Gabriel. Manual básico de cateo y aseguramiento de evidencia digital. México. Instituto Nacional de Ciencias Penales. 2006.

Cano M. Jeimy J. Computación Forense; Descubriendo los rastros informáticos. México DF. Alfaomega. 2009.

Enciclopedia Criminalística, Criminología e Investigación, tomos I y III. Colombia. Sigma editores. 2010.

Orts Berenguer, Enrique. Delitos informáticos y delitos comunes cometidos a través de la informática. Valencia. Tirant lo Blanch. 2001.

Electrónicas

CNN expansión. ¿Cómo clonan tus tarjetas bancarias?. [En línea]. [Consultado: 06 de enero de 2012]. Disponible en la web: http://www.cnnexpansion.com/mi-dinero/2011/09/12/como-clonan-tus-tarjetas-bancarias

Comisión Nacional para la Protección y Defensa. Clonación de tarjetas bancarias. [En línea]. [Consultado: 09 de febrero de 2012]. Disponible en la web: http://www.condusef.gob.mx/

Data Security. Skimming: Clonación de tarjetas bancarias. [En línea]. [Consultado: 06 de enero de 2012]. Disponible en la web:http://www.wisedatasecurity.com/clonacion-tarjetas-credito.html

Diccionario del Hacking. Definición de Hacker. [En línea]. [Consultado: 17 de febrero de 2012]. Disponible en la web: http://www.biografica.info/redei/diccionario-de-hacking

Real Academia Española. Diccionario de la Lengua Española. [En línea]. [Consultado: 09 de febrero de 2012]. Disponible en la web: http://www.rae.es/rael.html

Seguridad informática: hackers. Seguridad informática. 'Hacker'. [En línea]. [Consultado: 27 de enero de 2012]. Disponible en la web: http://www.monografias.com/trabajos/hackers/hackers.shtml

Fuentes externas (mesa de trabajo)

Comisión Nacional para la Protección y Defensa (Condusef); mesa trabajo con el tema Clonación de tarjetas y suplantación de identidad. Oficina del Delegado Estatal de Condusef. 16 de febrero de 2012.

Et pro blaborum, cusae. Nequam, quodi id utem dollit utemquia pore landuntiis enduntiis eiuntibus, soles re opturepreм fugiamet ea sequo