

VISIÓN CRIMINOLÓGICA CRIMINALÍSTICA

• AÑO 1 • NÚMERO 1 • ENERO-MARZO 2013 • REVISTA DIGITAL TRIMESTRAL



*El Criminólogo-criminalista
ante el fenómeno delictivo*

DIRECTORIO GENERAL

Visión Criminológica-criminalística
Año 1 / Número 1 / Enero-Marzo 2013

CONSEJO EDITORIAL

Lic. Elia Moreno Martínez
Dr. José Luis Pérez Angeles
Arq. Juan Manuel Pérez Angeles

DIRECTOR DE LA REVISTA

Arq. Juan Manuel Pérez Angeles

CONSEJO DE REDACCIÓN

Dra. María Elena Sánchez Gutiérrez
Dr. Salvador Felipe Espinet Vázquez
Dr. Ricardo Pérez Avilés
Mtro. Miguel Angel Pérez Angeles
Urb. Delfino López Vázquez

COLECTIVO ARCION

LCCTP. Alejandro Arévalo Ponce
LCCTP. Irma Nayeli Ramírez Balderas
Urb. Miguel Angel Pérez Cuautle
Urb. Delfino López Vázquez
Mtro. en Criminología Miguel Angel
Pérez Angeles
Arq. Juan Manuel Pérez Angeles

DISEÑO EDITORIAL

Mtro. Obed Meza Romero



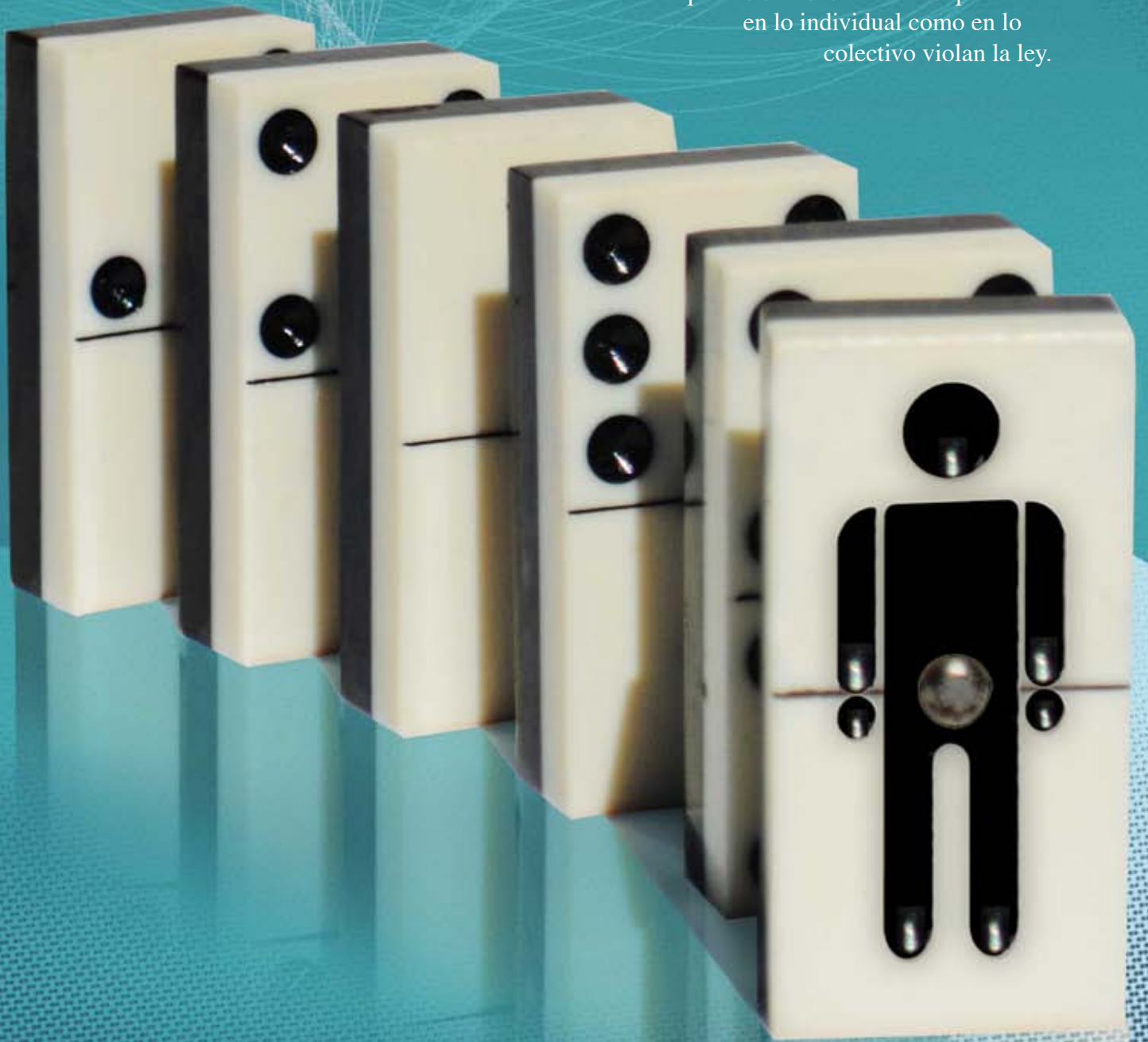
PLANTEL CLEU MÉRIDA

VISIÓN CRIMINOLÓGICA-CRIMINALÍSTICA, Año 1, No. 1, enero-marzo 2013, es una publicación trimestral editada por Grupo Universitario de Puebla, A.C., con domicilio en la 2da. de Vicente Suárez no. 2520, colonia Bella Vista, C.P. 72500, Puebla, Puebla, México. Teléfono (01 222) 2110048, <http://revista.cleu.edu.mx>, investigacion@revista.cleu.edu.mx. Editor responsable: Arq. Juan Manuel Pérez Angeles. Reservas de Derechos al Uso Exclusivo No. 04-2012-10241333800, ISSN: en trámite, ambos otorgados por el Instituto Nacional del Derecho de Autor. Responsable de la última actualización de este Número, Dirección General de Investigación, Urb. Miguel Angel Pérez Cuautle, 2da. de Vicente Suárez no. 2520, colonia Bella Vista, C.P. 72500, Puebla, Puebla, México, fecha última de modificación, 31 de marzo de 2013.

La ortografía, el estilo y gráficos, son responsabilidad de cada autor, así mismo las opiniones expresadas, no reflejan la postura del editor de la publicación.

Ninguna parte de esta publicación, incluyendo el diseño de la cubierta, puede ser reproducida, almacenada o transmitida de manera alguna, ni por ningún medio ya sea: electrónico, químico, mecánico, óptico, de grabación, de fotocopia sin permiso previo de la editorial.

Para la portada de este número titulado “El Criminólogo-criminalista ante el fenómeno delictivo”, se acudió a una fotografía del juego de destreza llamado dominó como imagen principal, con la cual se creó una metáfora visual que tuviera relación con la temática. En dicha fotografía se colocaron una serie de fichas rectangulares en hilera, la metáfora se aplicó en la primera ficha cuando se sustituyó la cara de frente de la numeración por un pictograma de la figura humana; ya que al dar un leve empujón a esta ficha provocará un suceso llamado comúnmente “efecto dominó” al que progresivamente se irán cayendo las fichas que le anteceden, de esto se desprende originar un nuevo significado a este juego, es decir que un delito deriva otro delito asociando a aquellos sucesos delictivos que tanto en lo individual como en lo colectivo violan la ley.



EDITORIAL

El primer ensayo explica el fenómeno de la suplantación de identidad como una conducta antisocial que no es prevista ni sancionada por las legislaciones penales, actualmente las cifras se han incrementado, razón suficiente para realizar estudios que permitan entender la problemática y clarificar la intervención del Criminólogo-criminalista.

El segundo ensayo explica la intervención del Criminólogo-criminalista, profesionalista que investiga cuales son las conductas e indicios que determinan la suplantación de identidad, formulando las evidencias y pruebas requeridas por la autoridad en los procesos de aplicación de la ley.

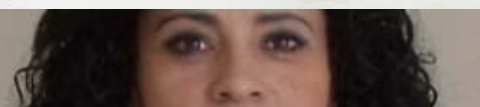
En el tercer ensayo explica la clonación de tarjetas bancarias, donde, el Criminólogo-criminalista debe conocer métodos, técnicas, materiales y una metodología que desmadeje el hecho delictivo y presente como inteligible el desarrollo del mismo.

El cuarto ensayo explica el campo de trabajo del Criminólogo-criminalista y su actividad profesional en las instituciones públicas, privadas y en las organizaciones no gubernamentales.

El quinto ensayo explica como el internet ha conseguido modificar las formas de interactuar de los individuos, espacio de comunicación por excelencia de nuestros días, sin embargo, a pesar de sus beneficios existen a la par riesgos en los que todo cibernauta puede ser victimizado, pues hay quienes han sacado partida de los conocimientos informáticos y de programación para innovar en la forma de delinquir, haciendo de este medio un espacio más de incursión para los delincuentes.

El sexto ensayo da una reflexión sobre la conciencia, la imitación y la percatación, expone argumentos concernientes al concepto del meme, invita a analizar los aspectos del comportamiento criminal, por medio de los resultados de los avances sobre el problema de la conciencia.





SECCIÓN CRIMINOLÓGICA-CRIMINALÍSTICA

- 6 La suplantación de identidad de tipo físico, informático y de telecomunicaciones como nueva manifestación de las conductas antisociales
Colectivo ARCION
- 23 La falsificación y alteración de documentos oficiales y su importancia en la suplantación de identidad de tipo físico
Colectivo ARCION
- 45 La investigación que realiza el Criminólogo-criminalista en la clonación de tarjetas bancarias
Colectivo ARCION
- 57 Otras áreas laborales para el Criminólogo-criminalista
Wael Hikal

SECCIÓN TÓPICOS

- 66 Delito.com
Algunas notas de la delincuencia *online*
Colectivo ARCION
- 74 El problema de la explicación de la criminalidad y sus causas, desde teorías socio-cognitivas y epistemológicas
Edgardo Noé Rubio Montalvo

PERSONAJES CLEU

- 81 Beatriz Yarce Alfaro

RECOMENDACIONES

- 83 Universidad Virtual CLEU

SECCIÓN

Criminológica-criminalística

La suplantación de identidad de tipo físico, informático y de telecomunicaciones como nueva manifestación de las conductas antisociales

COLECTIVO ARCION

Surge en el año 2008, equipo interdisciplinario de investigadores en el campo de lo Criminológico-criminalístico, su actividad científica coadyuva al desarrollo y consolidación del modelo educativo CLEU.

"Investigar para la libertad".
Representa su filosofía de batalla.

6 “La mayoría de los países no cuentan con una clara definición respecto del delito de robo de identidad, ilícito del que se valen algunos grupos de la delincuencia organizada y de terroristas para facilitar y financiar sus actividades ”

Donald Piragoff

RESUMEN

La inevitable revolución tecnológica modifica el *modus vivendi* de millones de personas, que manifiestan una manía al uso de telefonía móvil, ordenadores, tabletas electrónicas, *ipods*, entre otros, donde el uso del internet es casi indispensable, pero muy cerca de ellos y a la par de la tecnología se encuentra el sujeto que se aprovecha de la vulnerabilidad de la víctima, y es entonces el momento justo donde se desarrolla la suplantación de identidad.

INTRODUCCIÓN

El ser humano está dotado de derechos y obligaciones, todo ello por el simple hecho de nacer dentro de un territorio nacional, dichos beneficios son otorgados por el Estado y es responsabilidad del ciudadano corresponder al beneficio.

La identidad es un beneficio otorgado por el Estado para la ciudadanía, ya que corresponde a éste otorgar los recursos necesarios para generar documentos oficiales que acrediten los datos personales de los solicitantes, por ello es que cada integrante de las poblaciones cuentan con documentaciones que demuestren su nacionalidad, lugar de nacimiento, fecha de nacimiento, y número de control dentro de los registros de cada entida.

Hoy en día, la delincuencia busca diversas situaciones que pueden ser bien aprovechadas para cometer delitos o simplemente para perjudicar a sus semejantes, como muestra de este acontecimiento, la suplantación de identidad, fenómeno que retoma fuerza por la vulnerabilidad y confianza de la población, este procedimiento sucede cuando simplemente a través de la telefonía la víctima acepta brindar cualquier información que le solicita el moderador, sin razonar plenamente que se puede tratar de un sujeto que utilice dicha confidencialidad para obtener beneficios económicos o patrimoniales que son fruto del esfuerzo del trabajo de la ciudadanía.

Los malhechores tienen gran ingenio para cometer sus fechorías y recibir enormes cantidades de dinero sin la necesidad de enfrentar a sus víctimas o utilizar la violencia para obtener lo que desean, tan solo basta con robar

los bolsillos o carteras para conseguir tarjetas de crédito, débito, identificaciones personales, claves bancarias entre otras más, o simplemente sentarse detrás un ordenador para conseguir claves o interferir en la intimidad de millones de personas que descuidan su información confidencial.

Con base a las denuncias y quejas realizadas por la ciudadanía, es como se llegó a obtener las diversas modalidades de la suplantación de identidad, y éstas son:

- Físico.
- Informático.
- De telecomunicación.

Actividades como la clonación de tarjeta, alteración y falsificación de documentos oficiales de identidad, envío de mensajes vía internet o celular anunciando supuestos sorteos o concursos, o *hackeo* de cuentas, son tan solo algunas de las actividades derivadas de la suplantación de identidad.

Esta conducta antisocial permite favorecer ciertos delitos como el caso del tráfico de personas, terrorismo, usurpación de funciones, falsificación y alteración de documentos en general, lavado de dinero, entre otros, por ello debe atenderse con prontitud la problemática que afectó de manera indirecta gracias a la tecnología o de algunas artimañas de la delincuencia.

ROBO DE IDENTIDAD

Una de las actividades ilícitas que ha trascendido de manera considerable en algunos países, es el llamado robo de identidad o mejor conocido como *identity theft* (voz inglesa). Apropiación ilegal de identidad. Este fenómeno delictivo afecta en algunos casos de manera inmediata a las víctimas que lo padecen, y en otros casos las repercusiones se manifiestan a largo plazo, ejemplo de ello, cuando una persona utiliza la identidad de otra para realizar una solicitud de crédito, procedimiento que es desconocido por la víctima, pero a mediano plazo ésta empieza a recibir notificaciones de la deuda existente por un crédito que jamás solicitó, o en casos extremos le es comunicada que es perseguida por la justicia.

La parte afectada en esta problemática sin lugar a duda es la víctima, quien pierde de manera específica, su identidad legal, su estabilidad económica, en casos extremos su libertad, y principalmente se encuentra ante un inevitable daño moral, donde su prestigio o su imagen se ven completamente dañadas ante los ojos de la sociedad o de la justicia.

Para dar prioridad a la demanda de la ciudadanía que ha sido víctima de robo de identidad y por la magnitud de éste, así como la amenaza que representa para la población, algunos países han puesto su atención y conciben de manera específica a esta conducta como "un crimen federal que ocurre cuando la identi-

ficación de la persona es utilizada o transferida por otra persona para actividades ilegales"¹.

Entre las actividades más destacadas por este delito se encuentra las siguientes:

- Quejas relacionadas con el robo de identidad.
- "Fraude con Tarjetas de Pago.
- Servicios no Autorizados de Servicios Públicos o Teléfono.
- Fraude Bancario.
- Préstamos Fraudulentos.
- Documentos o Beneficios Gubernamentales.

Estafas de robo de identidad más utilizadas:

- Sorteos falsos u obras de beneficencia falsificadas.
- Trabajos en el hogar que ofrecen ganar dinero fácil.
- Tarjeta de pago, protección de crédito u ofertas de reparación de créditos falsos.
- Ofertas de viajes a tarifa reducida u ofertas con descuento en revistas.
- Estafas de Becas"².

Otra forma de delinquir realizada a nivel mundial, derivada de la obtención de datos personales para actividades ilegales, es el delito informático, definido como "Cualquier comportamiento criminal en que la computadora u otros periféricos o dispositivos informáticos, estén involucrados como material, objeto o símbolo para perpetuar un fraude, engaño, o delito informático tipificado"³.

Por su parte Estados Unidos, Canadá, y la mayoría de los países Europeos, han determinado que existen tres tipos de comportamiento ilícito relacionado con los delitos informáticos:

- Acceso no autorizado.
- Actos dañinos o circulación de material dañino.
- Intercepción no autorizada.

Estos tres tipos fueron tipificados y penalizados por los sistemas legales de aquellas naciones, pero desde el punto de vista criminológico algunos autores clasifican a los delitos informáticos desde dos variantes:

- Como instrumento o medio.
- Como fin u objetivo.

Estas dos apreciaciones se entienden de la siguiente manera:

Como instrumento o medio: se tiene como manifiesto aquellas conductas criminógenas que utilizan la tecnología para utilizarla como artificio para ejecutar actividades ilícitas.

Como fin u objetivo: En esta etapa las conductas criminógenas rechazan la presencia de la computadora o programa entendido como entidad física, mientras que por su parte otros conciben a esta como una clasificación *sui generis*, como los llamados -delitos electrónicos-, mismos que se dividen en tres categorías:

1. Individuos que a beneficio utilizan la tecnología electrónica como un método, es decir, esta vía es un medio cuyo objetivo es llegar a consumir una actividad ilícita.

1 Slideshare present yourself 'Robo de identidad/ identity theft/ Apropiación ilegal de identidad Rivera Suárez, Waleska'. [En línea]. [Consultado: 12 de enero de 2012]. Disponible en la web: <http://www.slideshare.net/waleska123/robo-de-identidad-5323179>

2 Master card 'Robo de identidad'. [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: <http://www.mastercard.com/us/personal/es/basicosdeseguridad/robodeidentidad/>

3 Scribd. 'Unidad III. Seguridad informática. [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: <http://es.scribd.com/doc/20781206/Delitos-Informaticos>

2. De aquellas personas que a través innovación de la tecnología electrónica usan la computadora como herramienta principal para cometer sus fechorías.
3. Los que se valen del avance tecnológico para cometer un solo fin: dañar el medio electrónico.

La seguridad internacional se ha visto amenazada por intrusos del internet, que se introducen en los sistemas para robar información confidencial y vulnerar al país, como el tan famoso gusano de internet proyectado en Estados Unidos de América en el año de 1988 por Robert Morris Jr., mismo que fue detenido y sancionado gracias a la existencia del acta fraude y abuso informático que circulaba durante esa época.

Los delitos informáticos han atormentado la economía de diferentes países, como el caso de Estados Unidos de América, que su pérdida económica alcanza los 10,000 millones de dólares, esta información es brindada por las compañías de seguros contratadas por estas potencias mundiales, mismas que registran que es tan grande el daño y perjuicio económico que se propone crear grupos exclusivos de investigadores especializados en delitos informáticos.

Tan solo el *Federal Bureau of Investigation* (FBI). Oficina Federal de Investigaciones, ha atendido tan solo el 90% de los delitos informáticos perpetrados en los Estados Unidos de América vía internet.

Las redes de comunicación hoy en día, se han vuelto una necesidad, y no un lujo, como se creía en épocas pasadas, ahora acceder a internet significa fuente de empleo, comunicación, transacciones, desarrollo, publicidad, imagen, entre otras cosas.

Una de las herramientas indispensables en ésta época es la llamada red de comunicación mejor conocida como internet, el cual no estaba diseñado para las inferencias criminales de los últimos años, los protocolos con los que se cuenta no se encuentran protegidos, por ello es que en la actualidad, se puede observar ataques contra la seguridad por parte de *hackers*.

Otro tema de seguridad es el uso inapropiado de la "criptología"⁴ a favor de la delincuencia para ocultar mensajes que pueden ser ininteligibles para los demás así como para ocultar movimientos realizados en un sistema informático, e inclusive se puede ocultar exactamente lo que se estaba realizando ya que dicha información se encuentra encriptado. Otra forma de realizar un ataque informático es mediante los llamados "cripto-virus"⁵.

Ante esta problemática las legislaciones internacionales han integrado dentro de sus ordenamientos incluir la suplantación de identidad de tipo electrónico mismo que a la letra dice:

Nuevo Código Penal Español (aprobado por Ley-Organica 10/1995, de 23 de noviembre / BOE número 281, de 24 de noviembre de 1995):

1.- El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Con base a ello la Organización de las Naciones Unidas a través de un manual denominado la prevención y control de los delitos informáticos número 43 y 44 informa que el 90% de los casos detectados por delito informático fueron realizados por los propios empleados de las empresas denunciadas, mientras que dentro de América Latina y Europa el 73% de los delitos consumados por esta modalidad fueron realizados por fuentes internas a empresas y tan solo el 23% de los hechos fueron señalados por personas ajenas a las empresas.

Convenios internacionales para prevenir el robo de identidad por internet

El mal uso de los ordenadores han producido en el ámbito internacional realizar una correcta valoración político-jurídico donde se ha admitido modificar el derecho penal nacional.

Para ello se cuentan con ciertos convenios internacionales realizados para combatir la suplantación de identidad vía internet:

- El Convenio de Berna.
- La Convención sobre la Propiedad Intelectual de Estocolmo.
- La Convención para la Protección y Producción de Fonogramas de 1971.
- La Convención Relativa a la Distribución de Programas y Señales.

En el año de 1983 la Organización de Cooperación y Desarrollo Económico (OCDE), comenzó a realizar un estudio para reordenar las leyes penales a fin de tipificar aquellas actividades donde se realice un mal uso de programas de computación.

Esta problemática determina ampliamente una implicación económica que deja la delincuencia por el mal uso de un ordenador, su daño no queda únicamente dentro de las naciones, sino que es un problema de carácter internacional e incluso transnacional, motivo que incita a las autoridades a unificar las legislaciones para combatir este problema.

En el año de 1986 la OCDE realizó un informe que fue publicado bajo el nombre de –Delitos de informática: análisis de la norma jurídica-, mismo que indicaba las normas legislativas vigentes así como las nuevas propuestas a reformas que debe adoptar los Estados, así como algunas actividades. Durante el año de 1992 esta organización realizó un conjunto de normas dirigidas hacia la protección de la información con la finalidad de ofrecer las bases para que los Estados y empresas del sector privado tengan alguna opción para realizar un marco legal que permita proteger la base de datos confidenciales.

Para 1990 la Organización de las Naciones Unidas (ONU), dentro de su octavo congreso celebrado en la Habana, Cuba, titulado

4 Criptología (del griego krypto: 'oculto' y logos: 'discurso') es, tradicionalmente, la disciplina científica que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas, Wikipedia, la enciclopedia libre 'Criptología'. [En línea]. [Consultado: 29 de enero de 2012]. Disponible en la web: Criptología <http://es.wikipedia.org/wiki/Criptologia%C3%ADa>

5 Cripto-virus. Programas con código virico encriptados.

prevención del delito y justicia penal, se concluyó que la delincuencia relacionada con la informática simplemente es consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países, por ello se había difundido la comisión de actos delictivos.

En Wurzburg durante 1992, la Asociación Internacional de Derecho Penal emitió recomendaciones con respecto a los delitos de tipo informático, entre ellas destaca la iniciativa de reformar el contenido penal y definir las nuevas conductas antisociales para ser tipificadas como delitos.

En Mérida España se celebró la II Jornada Internacional sobre –delitos cibernéticos- realizado en noviembre de 1997 donde se reveló lo siguiente.

- Aplicaciones en la Administración de las Tecnologías Informáticas/cibernéticas.
- Blanqueo de capitales, contrabando y narcotráfico.
- Hacia una policía Europea en la persecución del delito Cibernético.
- Internet: a la búsqueda de un entorno seguro.
- Marco legal y Deontológico de la Informática.

Las legislaciones mundiales contra el delito de robo de identidad

Las actividades ilícitas derivadas de la informática son un punto en concreto que debe estudiarse paso a paso y con su debida precaución implementando medidas de carácter legislativo y penal, por ello para países desarrollados del occidente se tuvo a bien realizar una valoración que incluye entre sus líneas una reforma legal que ha imperado durante los últimos diez años.

Este problema que ha generado cuantiosas pérdidas millonarias, sólo es vislumbrado por algunos países entre los más destacados:

Alemania

Alemania también fue perpetrada por la delincuencia informática, por ello contempló implementar una segunda ley dedicada a tipificar la criminalidad económica, todo ello ocurrido dentro del año de 1986 donde expresa lo siguiente:

- Espionaje de datos (202 a).
- Estafa informática (263 a).
- Falsificación de datos probatorios junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos. (269, 270, 271 y 273).
- Alteración de datos es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible. (303 a).
- Sabotaje informático. Destrucción de elaboración de datos de especial significado por medio de hecatombe, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa (303 b).

- Utilización abusiva de cheques o tarjetas de crédito (266 b).

Las autoridades alemanas detectaron una modalidad que se determinó como estafa informática y que fue incluido como un nuevo tipo penal, que en sus inicios tuvo algunas incongruencias, pero para demostrar su existencia debía cumplir con lo siguiente:

- Acción engañosa.
- Causa del error.
- Disposición patrimonial en el engaño del computador.

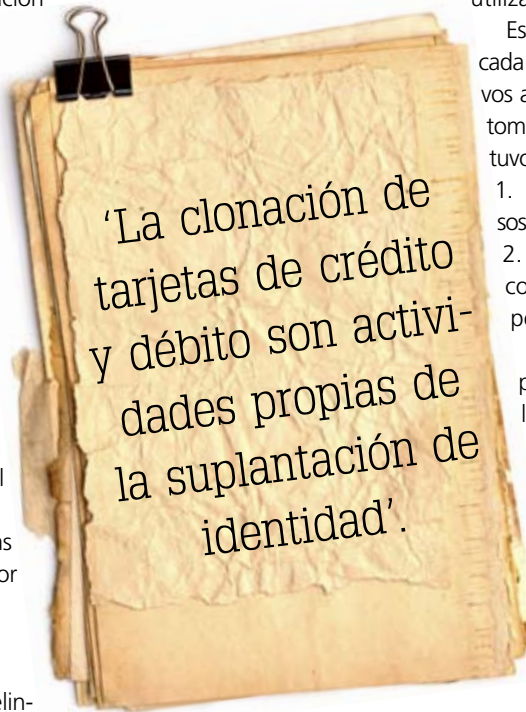
El resultado de este fenómeno es el daño directo que sufre la víctima en su patrimonio, por ello las autoridades elaboraron un programa contemplado la administración de datos por medio de un acto incorrecto del programa, esto con ayuda del uso de datos incorrectos e incompletos que han sido utilizados de manera ilegal

Esta expresión penal fue adjudicada también por países Escandinavos así como en Austria. Para poder tomarse en cuenta este delito se tuvo que estudiar:

1. Los comportamientos dañosos vía electrónica.
2. Analizar los bienes jurídicos merecedores de protección penal que eran dañados.

Con base a ello, se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero en realidad tan sólo constituyen un nuevo *modus operandi*,

que no ofrece problemas para la aplicación de determinados tipos. Por otra parte, en cambio, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas. En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos. El tipo de daños protege cosas corporales contra menoscabos de sus sustancias o función de alteraciones de su forma de aparición.



Austria

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

Esta ley contempla los siguientes delitos:

- Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
- Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

Francia

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

- Acceso fraudulento a un sistema de elaboración de datos (462-2). En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje informático (462-3). En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos (462-4). En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
 - Falsificación de documentos informatizados (462-5). En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.
 - Uso de documentos informatizados falsos (462-6). En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

Estados Unidos de América

Es importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya, etcétera y en que difieren de los virus, la nueva acta proscribió la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programas (18 U.S.C.:

Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus. El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de

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

El Acta de 1994 aclara que el creador de un virus no escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje. En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley. Se considera importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de \$10,000 por cada persona afectada y hasta \$50,000 el acceso imprudente a una base de datos, etcétera.

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos. Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (*computer contaminant*) conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

Holanda

El primero de marzo de 1993 entró en vigor la Ley de los Delitos Informáticos, en la cual se penaliza el *hacking*, el *preancking* (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

Reino Unido de la Gran Bretaña e Irlanda del Norte

Debido al caso de *hacking* en 1991, comenzó a regir la *Computer Misuse Act*, Ley de los abusos informáticos. Mediante esta ley el intento, exitoso o no de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Pena además la modificación de datos sin autorización donde se incluyen los virus.

Venezuela

En el año 2001 se promulgó la Ley Especial contra los delitos Informáticos por Asamblea Nacional de la República Bolivariana de Venezuela.

De los delitos contra los sistemas que utilizan tecnologías de información, de los delitos contra la propiedad, de los delitos contra la privacidad de las personas y de las comunicaciones, de los delitos contra niños, niñas o adolescentes, de los delitos contra el orden económico, argumentados en cinco capítulos respectivamente. En las disposiciones comunes se abordan elementos importantes como las agravantes, las penas accesorias, la divulgación de la sentencia condenatoria etcétera.

Los Estados miembros de la Unión Europea acordaron castigar con penas de uno a tres años de prisión a los responsables de delitos informáticos. Cuando quede comprobado que los ataques cibernéticos están relacionados con el crimen organizado, la pena ascenderá hasta los cinco años. Esta decisión marco se convierte en un gran avance dentro de la armonización de las legislaciones europeas para luchar contra los delitos informáticos. Estos delitos se han convertido en un quebradero de cabeza para los cuerpos de policía de los Estados miembros y, sobre todo, para los perjudicados por estos crímenes. El principio de territorialidad del derecho provoca que sea muy complicado perseguir a delincuentes informáticos que actúan desde otros países.

Con este intento de unificar la legislación, las autoridades europeas podrán perseguir con una mayor efectividad a delincuentes que, hasta ahora, podían cometer sus delitos con casi total impunidad. Además, el acuerdo del Consejo de Ministros de Justicia de los quince, establece otro aspecto importante, como es la definición de los delitos que se consideran –informáticos–.

Los Estados miembros distinguen tres tipos de ataques cibernéticos: el acceso ilegal a sistemas informáticos, la ocupación de sistemas a través de ejemplos como el envío de mensajes que ocupan un espacio considerable, y la difusión de virus informáticos. La intención de la Unión Europea es doble: por un lado se trata de definir el delito; por otro pretende unificar las penas, ya que el lugar de la comisión del delito es fundamental para saber el derecho aplicable, se trata además de una medida muy sensata que evita la desprotección absoluta que presentan hoy en día las empresas del Viejo Continente. Los Quince Estados Europeos disponen ahora de un plazo de más de dos años para la adaptación de esta medida a sus textos legislativos.

El daño colateral para México

Los efectos que se desarrollaron en países como Estados Unidos, Argentina, Reino Unido, Alemania, entre otros, repercutieron de manera indirecta para México y vulneró la seguridad tanto del país como de los ciudadanos que habitan dentro de ella.

La tecnología que llega a manos de países tercermundistas son la fortuna que va llegando a México de manera gradual, lo más importante de ello son las herramientas como las computadoras de nueva generación, las *iPad* o tabletas electrónicas, entre otros, donde fácilmente se tiene acceso a internet, punto que es accesible para cualquier individuo que tenga conocimiento de ello, y tan solo basta con algunos dominios para hacer que las víctimas se vean vulneradas en sus datos personales, o en su estabilidad económica.

La era de la informática llega a manos de la sociedad, donde cualquier persona tiene acceso a un ordenador y al internet, y de manera virtual explora mundos desconocidos. Esta innovación se encuentra versada dentro de dos vertientes:

1. De beneficio social.
2. De acciones ilegales.

La primera de ellas resulta placentera y necesaria, ya que gracias al uso de un ordenador y del acceso a internet se facilita la socialización y la actividad laboral, este beneficio hoy en día, no está considerado como un lujo, si no como una herramienta de primera necesidad.

La segunda se encuentra encaminada hacia el acercamiento de la tecnología y las comunicaciones, misma que permite descubrir el talento de miles de hombres o mujeres jóvenes con gran capacidad para crear más que una simple escritura, tan solo basta con que se pueda manipular un programa de comunicación, un navegador o un gestor de correo para poder vincularlo en ocasiones con malas intenciones.

Esta actividad se encuentra prevista por muchos pensadores como -fuga de cerebros-, donde jóvenes con gran talento e inteligencia son guiados por personas malintencionadas hacia la comisión de conductas delictivas, y existe otra parte de la población joven que se inspira en los vicios de la red de internet, donde a través de ello se forman los grandes “*hackers*”⁶.

6 Hacker es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etcétera. Se suele llamar *hackeo* y *hackear* a las obras propias de un hacker.

El término *hackers* trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.

Mirrorlinux.net, 'hacker'. [En línea]. [Consultado: 9 de enero de 2012]. Disponible en la web: http://mirrorlinux.net/index.php?option=com_content&view=article&id=93:hacker&catid=37:hack&Itemid=80

Los efectos en materia de informática que afectan a México son realmente considerables, y se clasifican de la siguiente manera:
"De impacto

Esta primera clasificación afecta directamente a la base de datos del gobierno sea éste municipal, estatal o federal, donde toda aquella información confidencial se encuentra expuesta ante los ojos de los genios informáticos mejor conocidos como *hackers*.

De afectación social

Este procedimiento tiene como repercusión el daño moral y patrimonial de la víctima a la cual le es suplantada su identidad, en muchas ocasiones el perjuicio se puede manifestar a largo plazo, donde la víctima pasa años sin saber que ha sido afectada, y en otras ocasiones puede observarse el daño de manera inmediata"⁷.

México se encuentra vulnerable ante esta conducta antisocial, a la cual se le ha denominado -suplantación de identidad de tipo informático- y únicamente los argumentos jurídico-penales toma como referencia el delito de -Acceso ilícito a sistemas y equipos de informática-, donde entre algunas líneas principales se expresa lo siguiente:

"Artículo 211 bis 1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa"⁸.

Como se puede observar este delito bajo el nombre de -Acceso ilícito a sistemas y equipos de informática- solo resguardan la información confidencial del Estado y de las Instituciones financieras, pero deja desprotegido la información con la que cuentan empresas y las demás personas del país.

Queda claro que la protección de los datos y de la identidad de las personas en medios informáticos se encuentra vulnerable ante la presente situación que se encuentra viviendo México, por ello es fácil realizar esta actividad que se realiza sin temor alguno.

La naciente legislación penal para la suplantación de identidad en México

Para México, la actividad de suplantación de identidad surgió de manera gradual, empezando por falsificación y alteración de documentos, como una forma de ocupar el lugar de otra, para posteriormente generar una crisis informática. Los factores físicos como la modificación y reproducción ilícita de documentos generó al hombre la gran idea de tener otra personalidad y mantener la propia, la que le fue legal y socialmente proporcionada, éste era una modalidad que no había sido tomada en cuenta y que progresivamente tendría la tendencia en convertirse en un fenómeno delictivo, las leyes Mexicanas hasta hace poco solo contemplaban como único hecho punitivo el fraude pero condicionalmente en las siguientes circunstancias:

"Artículo 387 fracciones:

II.- Al que por título oneroso enajene alguna cosa con conocimiento de que no tiene derecho para disponer de ella, o la arriende, hipoteque, empeñe o grave de cualquier otro modo, si ha recibido el precio, el alquiler, la cantidad en que la gravó, parte de ellos o un lucro equivalente;

III.- Al que obtenga de otro una cantidad de dinero o cualquiera otro lucro, otorgándole o endosándole a nombre propio o de otro, un documento nominativo, a la orden o al portador contra una persona supuesta o que el otorgante sabe que no ha de pagarle;

VII.- Al que vende a dos personas una misma cosa, sea mueble o raíz y recibe el precio de la primera o de la segunda enajenación, de ambas o parte de él, o cualquier otro lucro con perjuicio del primero o del segundo comprador.

VIII.- Al que valiéndose de la ignorancia o de las malas condiciones económicas de una persona, obtenga de ésta ventajas usuarias por medio de contratos o convenios en los cuales se estipulen réditos o lucros superiores a los usuales en el mercado.

IX.- Al que para obtener un lucro indebido, ponga en circulación fichas, tarjetas, planchuelas u otros objetos de cualquier materia como signos convencionales en sustitución de la moneda legal;

X.- Al que simulare un contrato, un acto o escrito judicial, con perjuicio de otro o para obtener cualquier beneficio indebido.

XXI.- Al que libre un cheque contra una cuenta bancaria, que sea rechazado por la institución o sociedad nacional de crédito correspondiente, en los términos de la legislación aplicable, por no tener el librador cuenta en la institución o sociedad respectiva o por carecer éste de fondos suficientes para el pago. La certificación relativa a la inexistencia de la cuenta o a la falta de fondos suficientes para el pago, deberá realizarse exclusivamente por personal específicamente autorizado para tal efecto por la institución o sociedad nacional de crédito de que se trate"⁹.

Las anteriores concepciones obtenidas del ordenamiento jurídico penal, son las que encuadran a la conducta antisocial a estudiar en este momento, ya que se habla de la utilización de un soporte y de un útil inscriptor, donde se deja en un -pseudo convenio- datos personales, cantidades de dinero y firmas, mismas que son utilizados por personas con intenciones engañosas para obtener un beneficio sea este económico, mueble o inmueble, donde para llevar a cabo esto se realiza una alteración ya sea en una cifra, un grama o una firma.

El delito de falsificación de documentos en general y oficiales, está relacionado con la suplantación de iden-

7 Colectivo Arcion. Dirección General de Investigación 2012.

8 Código penal federal, Publicado en el Diario Oficial de la Federación el 14 de agosto de 1931, última reforma publicada en el Diario Oficial de la Federación el 24-10-2011, 'capítulo II Acceso ilícito a los sistemas y equipos de informática, artículo 211 bis' 1. [En línea]. [Consultado: 9 de enero de 2012]. Disponible en la web: <http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf>

9 Código Penal Federal, Última Reforma DOF 24-10-2011. 'Capítulo III Fraude' [En línea]. [Consultado: 12 de diciembre de 2011]. Disponible en la web: <http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf>

idad, ya que si en algún documento se puede alterar el nombre, la edad, folio entre otros, se podrá obtener otra identidad social y legal.

Otro rubro que no debe pasar por desapercibido es el acceso ilícito a sistemas y equipos de informática, modalidad que también se encuentra relacionada con la suplantación de identidad, por ello es necesario realizar la siguiente apreciación legal respecto a dicha modalidad, objeto que se puede estudiar dentro del Código Penal Federal dentro de los artículos 211 bis 1, 211 bis 2, 211 bis 3, 211 bis 4, 211 bis 5, 211 bis 6, 211 bis 7 mismos que a la letra dicen:

“Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

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

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad

pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que

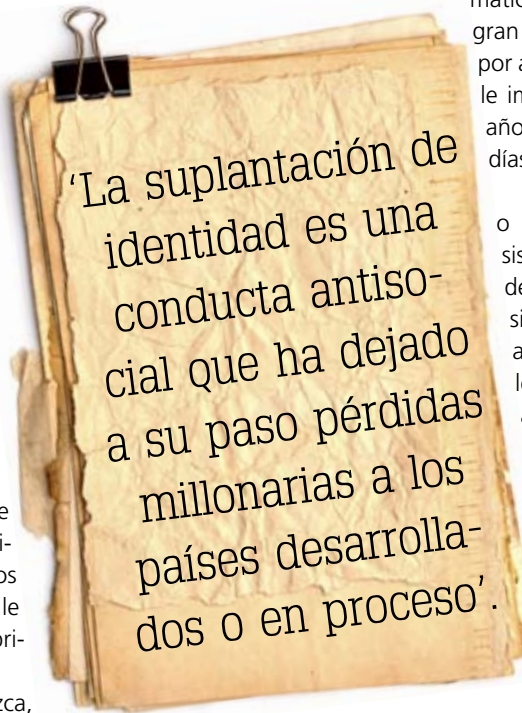
contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando



la información obtenida se utilice en provecho propio o ajeno"¹⁰.

Este es un indicio de lo que sería un delito informático, pero que dentro de esta legislación penal Mexicana se conoce bajo el nombre de Acceso ilícito a sistemas y equipos de informática, donde como se puede observar no se encuentra contemplada la figura de suplantación de identidad, motivo por el cual es necesario reajustar los preceptos jurídicos que se quedan bajo las líneas mientras en la realidad la tecnología facilita la labor del delincuente.

Otro elemento que debe considerarse para introducir dentro de las leyes penales mexicanas la conducta antisocial denominada como suplantación de identidad, es la actual iniciativa que se realizó con base en lo siguiente:

- 300 mil denuncias por robo de identidad con intenciones fraudulentas a bancos y otras instituciones, cifra que ubicó a México en el octavo lugar a nivel mundial en la práctica de esta conducta antisocial.

De éstos argumentos se obtuvo lo siguiente: aprobó en el reciente "periodo ordinario de sesiones"¹¹ una reforma al artículo 387 del Código Penal Federal, a fin de tipificar el robo de identidad dentro de las figuras de fraude específico, además de que penaliza hasta con 12 años de prisión a quien utilice indebidamente cualquier tipo de identificación, clave de identificación personal bancaria, u otro documento identificatorio que sea de otra persona"¹².

Este proceso se reconoce debido a la falta de conocimiento sobre conductas y su prevención, aunque se tenía conocimiento de que se empezaban a cometer actos ilícitos, por ello "Esta conducta hasta el día de hoy no se había sancionado porque los tipos penales no contemplaban nuevas conductas en las que interviene, inclusive, la delincuencia organizada; es una conducta que anteriormente, por el avance de las tecnologías, no existía"¹³.

Existe una falta de análisis desde la óptica de la Criminología-criminalística por parte de las autoridades, ya

que no contemplaron la amenaza que otros países manifestaron ante el delito de suplantación de identidad, mismo que iba a vulnerar al gobierno y sociedad mexicana, por ello se hace hincapié en la necesidad de un profesionista que prevea ciertas conductas antisociales que en un futuro generen un problema de mayor consideración.

Suplantación de identidad

La evolución es un proceso que se desarrolla en diferentes circunstancias, una de ellas es la conducta del hombre y la colectividad, este asunto alcanza en ocasiones a crear nuevos delitos, y esto sucede cuando el individuo se da cuenta que ha madurado emocionalmente y ha pasado la línea de superación y de superioridad, luego entonces se da cuenta que es necesario adquirir nuevos conocimientos y artimañas para sobrepasar los límites de lo moral y legalmente permitidos. "La evolución de la criminalidad se presenta en nuevas características para llevar a cabo cierta conducta, dichas características serán aprendidas por unos y mejoradas por otros"¹⁴.

Otro ejemplo de evolución es el despliegue de la tecnología que llega a revolucionar las herramientas de trabajo, es un mecanismo progresivo que perfecciona cualquier actividad, inclusive la seguridad, pero a la par de esta maravilla se encuentran los delincuentes que burlan los sistemas de seguridad de muchas instituciones tanto públicas como privadas, así como la privacidad y confidencialidad de civiles.

Las generaciones de estos años y las futuras, prometen ser muy avanzadas en conocimientos, especialmente dentro de la informática, donde es fácil observar que la población joven manipula a la perfección las tecnologías, todo ello mediante el uso del sistema binario y mediante la exploración, por ello que se ha identificado a sujetos con un coeficiente intelectual promedio que le permite tomar una computadora y llegar demasiado lejos, inclusive hasta ingresar a la base de datos de una institución.

Existen diversas modalidades de efectuar una conducta antisocial, las más comunes van desde el uso de la violencia, hasta idear situaciones que crean engaño, en la primera de ellas, su procedimiento se desarrolla mediante un enfrentamiento a mano armada o usando la fuerza física para dirigirse a la víctima, y cuyo resultado es de manera visible lesiones o en casos extremos causar la muerte, en el segundo de los casos el victimario decide emplear algunas de sus artimañas para obtener algún beneficio ya sea financiero, mueble o inmueble, esto mediante el trato físico frente a frente, donde la víctima es engañada.

A nivel mundial se detectó una problemática de carácter delictivo, donde no necesariamente se violentaba a la víctima, y cuyo ejercicio se desarrollaba únicamente con el empleo de *software* y el uso del internet, su actuación fue desde simples bromas hasta robo de identidad e identidad financiera.

Este fenómeno delictivo se conoce como '*impersonation*' (voz inglesa). Suplantación de identidad. Este término se define de la siguiente manera: "suplantación o identidad a que finge ser una

10 Código Penal Federal, Última Reforma DOF 24-10-2011. "Título noveno Revelación de secretos y acceso ilícito a sistemas y equipos de informática Capítulo I Revelación de secretos". [En línea]. [Consultado: 27 de Febrero de 2012]. Disponible en la web: <http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf>

11 Existen dos tipos de periodos: desiciones ordinarias y desiciones extraordinarias. los primeros son aquellos que se desarrollan en fechas establecidas formalmente. En dichos periodos las Cámaras se ocupan del estudio, discusión y votación de las iniciativas que se les presenten y de la resolución de los demás asuntos que le correspondan.

12 Cámara de Diputados, Congreso de la Unión, "Boletín número 4520". [En línea]. [Consultado: 3 de enero de 2012]. Disponible en la web: http://www3.diputados.gob.mx/english/005_comunicacion/a_boletines/2011_2011/012_diciembre/18_18/4520_el_robo_de_identidad_origina_en_mexico_perdidas_anuales_por_9_millones_de_dolares_favor_de_utilizar_de_domingo_para_lunes.

13 Cámara de Diputados, Congreso de la Unión, "Boletín número 4520". [En línea]. [Consultado: 3 de Enero de 2012]. Disponible en la web: http://www3.diputados.gob.mx/english/005_comunicacion/a_boletines/2011_2011/012_diciembre/18_18/4520_el_robo_de_identidad_origina_en_mexico_perdidas_anuales_por_9_millones_de_dolares_favor_de_utilizar_de_domingo_para_lunes.

14 Hikal, Wael. Introducción al estudio de la Criminología, México, Editorial Porrúa, 2011, pág.148.

persona que no es"¹⁵, por solo nombrar algunos casos se conoce la utilización de documentos personales o las tarjetas de crédito y débito.

Tan sólo en América Latina la suplantación de identidad se vislumbra en las siguientes cifras, como se puede observar en la tabla número 1.

TABLA NÚMERO 1
CIFRAS DE ROBO DE IDENTIDAD EN AMÉRICA LATINA

País	Cifra
Ecuador	891 denuncias asociadas al robo de identidad.
Argentina	1700 denuncias de identidades robadas.
Estados Unidos de América	8.4 a 11.1 millones de denuncias de identidades robadas.
México	300 mil denuncias por robo de identidad.

Colectivo ARCIÓN, 12 de enero de 2012. Como se puede observar los países que persiguen esta problemática de manera alarmante son: Ecuador, Argentina, México y Estados Unidos de América, donde éste último es el que presenta cifras más impresionantes.

Es tanta la magnitud de este problema que la Organización de las Naciones Unidas (ONU) ha determinado que esta situación puede llegar a ser una amenaza contra la seguridad de las Naciones.

El robo de identidad, "se ha convertido en la forma más común de fraude al consumidor en Internet, y la manera más corriente es mediante el abuso de información de tarjetas de crédito, esta actividad puede causar efectos depresivos en la economía, elevar los costes del crédito y reducir la confianza en el comercio electrónico"¹⁶.

Este fenómeno creciente es considerado por la misma ONU como una amenaza para la sociedad y que particularmente se perpetra más en países desarrollados con grandes bancos de información y patrimonio financiero.

Para México este tipo de delitos tipificados internacionalmente como robo de identidad es totalmente ajeno, ya que se desconoce la conducta, la magnitud del problema, las dimensiones y las causas que podría tener si no se realiza un estudio a profundidad así como programas donde todo ciudadano de población rural y urbana conozcan el fenómeno y las medidas de prevención que pueden realizar para evitar ser víctima de suplantación de identidad.

Es necesario realizar una apreciación sobre el uso de términos como robo o suplantación de identidad, ya que algunas legislaciones consideran emplear el término de robo al apoderamiento de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley, es decir se habla de una cosa material, siendo esto que puede ser dinero, vehículos, equipos de cómputo, entre otras.

El ser humano no es un objeto material del que se puede disponer, ya que no es una propiedad, o un artículo, por ello se recomienda utilizar una terminología que comprenda no únicamente la modalidad física para apoderarse de una identidad, sino las diferentes formas de expresión delictiva que de ésta se pueda desprender.

Luego de realizar un análisis minucioso sobre la concepción de esta conducta antisocial se llegó a la conclusión de que debiera de utilizarse el término de suplantación, ya que estructuralmente concuerda más con lo que se encuentra desarrollando en la presente investigación.

Por ello se define suplantación como "Acción y efecto de suplantar"¹⁷, y éste último se precisa de la siguiente manera: "Expresión que se define como ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba"¹⁸.

El término -suplantar- contempla dentro de su expresión -al individuo- como dueño de su propia idiosincracia, donde de manera atinada se vislumbra la pérdida de uno de los derechos fundamentales como ciudadano, misma que ha sido disfrutada por alguien más que ocupa los rasgos distintivos ajenos para realizar actividades ilícitas.

Ahora bien la suplantación de identidad se define como "uso indebido de identificaciones personales e información confidencial y privada por medio de vías físicas, informáticas, electrónicas y de telecomunicaciones para ejecutar actividades ilícitas perjudiciales"¹⁹, aspecto que contempla diversas modalidades de la conducta antisocial y no parte únicamente de lo posiblemente tangible.

Es conveniente considerar que muchos de los delincuentes que realizan dicha actividad, mantienen una o varias intenciones delictivas detrás de la obtención de datos personales de sus víctimas, ya que se pueden cometer delitos tales como los que se puede observar dentro del esquema número 1.

15 Cabinas net. 'Robo de identidad'. [En línea]. [Consultado: 12 de enero de 2012]. Disponible en la web: <http://www.cabinas.net/informatica/robo-de-identidad.asp>

16 ONU 'alerta del robo de la identidad online y el tráfico con pornografía infantil' [En línea]. [Consultado: 13 de enero de 2012]. Disponible en la web: <http://www.elmundo.es/elmundo/2010/06/17/navegante/1276776963.html>

17 Real Academia Española. Diccionario de la Lengua Española. 'suplantación'. [En línea]. [consultado: 27 de enero de 2012]. Disponible en la web: <http://www.rae.es/rae.html>

18 Real Academia Española. Diccionario de la Lengua Española. 'suplantar'. [En línea]. [consultado: 27 de enero de 2012]. Disponible en la web: <http://www.rae.es/rae.html>

19 Colectivo ARCIÓN, Dirección General de Investigación, 07 de febrero 2012.

ESQUEMA NÚMERO 1
ACTIVIDADES ILÍCITAS DETRÁS DE LA SUPLANTACIÓN DE IDENTIDAD



16

Colectivo ARCIÓN, 22 de febrero de 2012. Estos son tan solo algunos de los delitos que pueden ser derivados de la suplantación de identidad, dicha analogía es tomada con referencia en las legislaciones nacionales e internacionales.

Estos fenómenos se desarrollan ilegalmente de la ayuda de la suplantación de identidad, como ejemplo lo siguiente:

1. Marcos es empleado de una tienda departamental y adquiere un *skimmer* para clonar tarjetas de clientes.
2. Con el dinero obtenido de manera ilícita Marcos adquiere actas de nacimiento falsas donde se observan diferentes nombres de mujeres, hombres y niños.
3. Marcos compra a personas de diferentes partes de la República Mexicana así como de otros países, a las cuales les asigna un nombre y les da un acta de nacimiento que había adquirido.
4. Marcos engaña a las personas que acabo de comprar-, diciéndoles que van a trabajar en un lugar serio y que les van a pagar muy bien, por lo cual les realiza unos contratos donde estipula algunas condiciones, mismo que es firmado por éstas víctimas, posteriormente Marcos altera cantidades de dinero que eran fruto del trabajo de sus víctimas.
5. Marcos adquiere un pasaporte falso para salir del país y evadir a la justicia.

Suplantación de identidad de tipo físico, informático, y de telecomunicaciones

La suplantación de identidad tiene un sin número de modalidades que son poco perceptibles o desconocidas por

la autoridad competente, así como por víctimas, por ello es necesario realizar una clasificación de las modalidades derivadas de ésta conducta antisocial.

De acuerdo a las actividades realizadas por los autores de las conductas antisociales, se conocen tres modalidades y éstas son:

- Físicas. Esta forma se realiza cuando el delincuente realiza actividades mediante el uso de ciertos artificios, con el fin de ocupar el lugar de otra persona.
- Informáticos. Actividad que utiliza métodos, procesos, técnicas y "desarrollos"²⁰ mediante el uso de ordenadores, con el fin de realizar actividades ilícitas, como el caso de uso de un *software* para modificar la originalidad de un documento de identificación oficial o privada.
- Telecomunicaciones. Uso de otra identidad mediante la utilización de internet o teléfono, para cometer una actividad delictiva.

Dentro de la suplantación de identidad en su modalidad de tipo físico se encuentran las siguientes manifestaciones:

- a) Alteración y falsificación de documentos Oficiales y privados, mediante el uso de técnicas como, raspado, borrado, remarcado y anexos. Esta forma es una de las más comunes para su-

²⁰ Desarrollos. Es el conjunto de técnicas y procedimientos que permiten conocer los elementos necesarios para definir un proyecto de software. monografias.com 'Proceso de desarrollo de software'. En línea.[consultado: 27 de enero de 2012]. Disponible en la web: <http://www.monografias.com/trabajos5/desof/desof.shtml>

plantar a una persona y no necesita de tecnologías o mucho esfuerzo para modificar la originalidad de un documento.

- b) Invencción de personalidad. Esta es la forma en que una persona pueda crear una carta o constancia de identidad falsa para obtener algún trámite.
- c) Robo de documentos a instituciones privadas, o personas. La primera manifestación del robo se empieza a convertir en una situación recurrente, ya que empleados o delincuentes se introducen en la base de datos de instituciones públicas o privadas para obtener información confidencial de ciertas personas, para así poder suplantarla, mientras que la segunda es una forma más cotidiana que es realizada por carteristas que asaltan en camiones del transporte público o transeúntes para obtener información confidencial, ya que toda persona acostumbra a traer entre sus objetos identificaciones personales o claves que muchas veces pueden ser de su cuenta bancaria.
- d) Medio de comunicación impresos, como un instrumento para obtener datos personales y suplantar la identidad. Los medios de comunicación impresos suelen ser un instrumento recurrente de los delincuentes, ya que anuncian u ofertan sorteos, premios o trabajos falsos, mismos que logran obtener la atención del lector o víctima, y éstos a su vez realizan acto de presencia al lugar marcado y brindan toda información que se les solicita a tal grado de dejar copias u originales de documentos oficiales.
- e) Peparar documentos que se encuentren dentro de la basura. Esta es una actividad que resulta del descuido de la ciudadanía al dejar todo tipo de información de identificación personal dentro de los botes de basura, acto que es aprovechado por la delincuencia.
- f) Suplantación de identidad moral. Esta es una actividad que es realizada por individuos que se hacen pasar por representantes de empresas privadas, para obtener documentos o firmas de víctimas que desconocen la verdadera identidad de los supuestos –funcionarios-, por este medio los delincuentes obtienen información confidencial misma que también puede servir para realizar fraudes.
- g) Suplantación de identidad de cadáveres y presos. Esta actividad puede ser completada mediante la información que brindan funcionarios públicos adscritos dentro de un registro civil, Instituto Federal Electoral o Centros de Reinserción Social, ya que son ellos los encargados de realizar un control sobre las defunciones o de ingreso de delincuentes.

Otra forma fácil de realizar es mediante una visita a las tumbas de los cementerios, donde se obtiene el nombre de la persona fallecida que va a ser utilizado para realizar una actividad ilícita.

Delitos Electorales. Esta actividad también está inscrita dentro del código penal federal, donde se prevé que dentro de los artículos 403 y 409.

“Artículo 403 fracción V. Recoja en cualquier tiempo, sin causa prevista por la ley, credenciales para votar de los ciudadanos”²¹. Esta actividad es comúnmente conocida como –“efecto carrusel”²²–, donde muchas personas con condiciones precarias aceptan –prestar sus credenciales para votar– y recibir a cambio el beneficio que cubra su necesidad momentánea.

“Artículo 409 fracciones:

I.- Proporcione documentos o información falsa al Registro Nacional de Ciudadanos para obtener el documento que acredite la ciudadanía; y

II.- Altere en cualquier forma, sustituya, destruya o haga un uso indebido del documento que acredita

- a) la ciudadanía, que en los términos de la ley de la materia, expida el Registro Nacional de Ciudadanos”²³.

Actividad que también se considera como suplantación de identidad, ya que se proporciona información que pueda ser de otra persona o de un finado.

Formas de suplantación de identidad en su modalidad de tipo informático:

- a) Clonación de tarjetas. Esta actividad consiste en la “duplicación de tarjetas de crédito o debito 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”²⁴.
- b) Alteración y falsificación de documentos mediante el uso de *software*. Es muy común que personas con dominio en la informática utilicen la tecnología para realizar actividades ilícitas, ejemplo de ello la alteración y falsificación de documentos, donde se emplee un *software* que facilite la labor ilícita, como ejemplo de ello el *spy ware*, “programa utilizado dentro de los ordenadores que permite registrar los golpes de las teclas que tocan las víctimas cuando usan su computadora”²⁵.

Formas de suplantación de identidad en su modalidad de telecomunicación.

Primero se debe definir que es una telecomunicación, y ésta se precisa como toda forma de “comunicación a distancia. La palabra

21 Procuraduría General de la República ‘de los delitos electorales’ [En línea]. [consultado: 28 de febrero de 2012]. Disponible en la web: <http://www.pgr.gob.mx/fepade/cuales%20son%20los%20delitos%20electorales/cuales%20son%20los%20delitos%20electorales.asp>

22 Efecto carrusel. Es un sobrenombre que se utiliza para denominar un acto de fraude electoral que algunos ciudadanos realizan, donde organizaciones políticas convencen a la ciudadanía para realizar un voto a favor del candidato político que se encuentran representando a cambio de darles un –beneficio– ya sea éste económico o alimenticio.

23 Código Penal Federal, Última Reforma DOF 24-10-2011, ‘Titulo vigesimocuarto, Delitos electorales y en materia de registro nacional de ciudadanos, Capítulo único’. [En línea]. [Consultado: 27 de febrero de 2012]. Disponible en la web: <http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf>

24 Data security.com ‘clonación de tarjetas’. [En línea]. [Consultado: 28 de febrero de 2012]. Disponible en la web: <http://www.wisedatasecurity.com/clonacion-tarjetas-credito.html>

25 Cabeza de Vaca, Daniel F. et al. Intercriminis número 13 segunda época, México, INACIPE, 2005, pág. 311.

incluye el prefijo griego *tele*, que significa -distancia o lejos-. Por lo tanto, la telecomunicación es una técnica que consiste en la transmisión de un mensaje desde un punto hacia otro, usualmente con la característica adicional de ser bidireccional. La telefonía, la radio, la televisión y la transmisión de datos a través de computadoras son parte del sector de las telecomunicaciones”²⁶.

Cabe mencionar que explícitamente se reconoce el uso de computadoras que permitan la comunicación a distancia, y para ello se requiere del uso del internet, ya que con las redes de comunicación el hombre puede intercambiar conversaciones con gente de otras naciones, o simplemente comunicarse con amigos a través de redes sociales, correo electrónico, o mediante el programa de mensajería instantánea.

La tecnología parecía tan perfecta hasta que el ser humano decidió utilizarla en contra de sus semejantes, por ello que a través de estas herramientas se pueden desarrollar otras actividades que no precisamente son consideradas como benéficas.

Dentro de la magia del internet se pueden realizar actividades de socialización como es el caso de las redes sociales, donde con facilidad hombres y mujeres de cualquier edad entablan conversaciones con gente de cualquier otro lugar del mundo o del país, y en muchas ocasiones el usuario deja al alcance de todos su información confidencial o en situaciones más profundas dentro de la propia conversación acceden a brindar cualquier tipo de datos privados que en muchas de las ocasiones es utilizado por delincuentes que se dedican a suplantar la identidad o contactar a sus víctimas para cometer otros delitos.

Existe una actividad que está relacionada con el tema que se está desarrollando, y es la simulación de identidad, esta actividad consiste en usar una terminal de un sistema en nombre de otro usuario, y esto resulta por el conocimiento de claves, servirse del abandono de terminales que no han sido desconectadas por el usuario, “El término también es aplicable al uso de tarjetas de crédito o documentos falsos a nombre de otra persona”²⁷, y esto solo funciona a través de los ordenadores conectados a redes de comunicación.

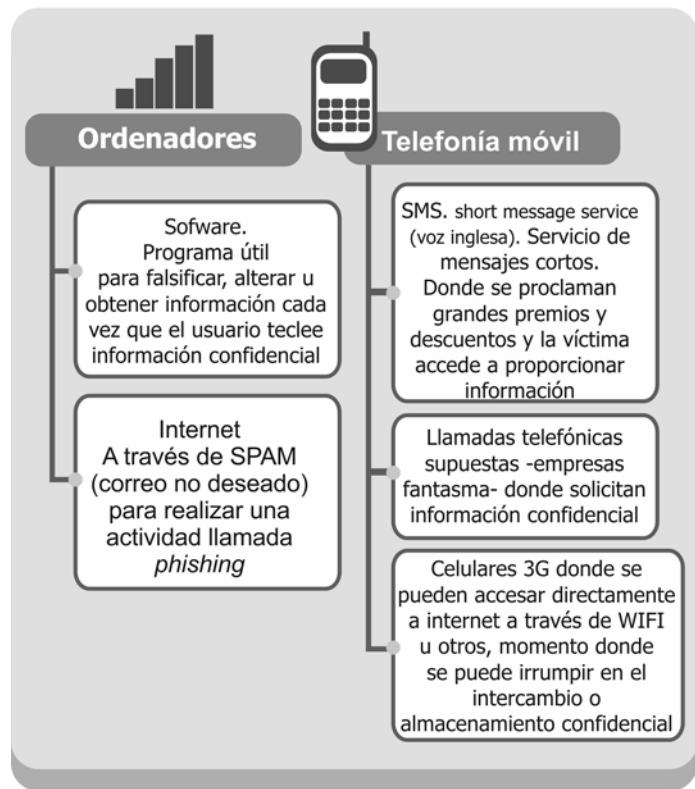
Otro medio que facilita la labor del delincuente es el llamado *-wifi- wireless lan* (voz inglesa). Red inalámbrica. Esta útil tecnología también sirve al delincuente que realiza un *“hackeo”*²⁸ a los códigos de los sistemas utilizados por usuarios, ya que dentro de este proceso se pueden realizar intercambios de información, transacciones bancarias entre otras, y es qué gracias a ello, puede ponerse

en riesgo la seguridad de la base de datos de las instituciones, con ello se consigue información que puede utilizarse para cometer delitos, y de esta manera suplantar la identidad de quien aún no lo ha descubierto.

Otro fenómeno importante que se desarrolla dentro de ésta modalidad es el llamado *-phishing-* (voz inglesa), pescando. Actividad que se realiza para “obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima”²⁹.

Esta manifestación vía internet se presenta en las páginas web que son duplicadas, y que muchas veces hacen acto de presencia en los correos electrónicos, donde se encuentran enlaces a sitios web falsos con una apariencia casi idéntica a los sitios legítimos, una vez logrado engaño, la víctima accede ingresar y es justo ahí cuando ingresa sus datos confidenciales como contraseñas, tarjetas de crédito o datos financieros y bancarios, por ello a continuación se muestra el esquema número 2, mismo que describe las desventajas del uso del internet.

**ESQUEMA NÚMERO 2
LA DESVENTAJA DE LA TECNOLOGÍA**



Colectivo ARCION, 25 de febrero de 2012. Sin lugar a duda la tecnología facilitó la comunicación y la tarea de muchos, pero ésta también es aprovechada al máximo por la delincuencia para lograr obtener la privacidad e identidad de aquellos descuidados y confiados ciudadanos.

26 Definición. de 'Definición de telecomunicación'. [En línea]. [consultado: 29 de Febrero de 2012]. Disponible en la web: <http://definicion.de/telecomunicacion/>
 27 Redel, red de entretenimiento e información. 'Simulación de identidad'. [En línea]. [consultado: 1 de marzo de 2012]. Disponible en la web:<http://www.biografica.info/redei/diccionario-de-hacking-25.php>
 28 Hackeo. Actividad que se realiza mediante la exploración y búsqueda de las limitantes de un código o una máquina.

29 Segu-info seguridad de la información. 'Phishing' [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: <http://www.segu-info.com.ar/malware/phishing.htm>

Los grandes problemas de las redes no terminan únicamente ahí, existe una aplicación dispuesta para cualquier dispositivo que utiliza la fuente del internet y es el llamado *-pul wifi-*, este dispositivo obtiene las claves de las conexiones protegidas asignadas por los "routers"³⁰, esta actividad pone en riesgo la seguridad de las contraseñas de correos electrónicos, tarjetas de crédito, redes sociales y demás que actividades que contemplen información confidencial. Esta es una cara más de la suplantación de identidad en su modalidad de telecomunicación.

Las células criminales y su relación con la suplantación de identidad

Esta conducta antisocial que se desarrolla con potencialidad en la era moderna, toma mayor fuerza cuando grupos perfectamente organizados se dan a la tarea de realizar actividades ilícitas para conseguir grandes beneficios económicos, donde los integrantes pueden llegar a ser profesionistas o gente que sabe manipular los ordenadores, o cualquier otra técnica inmersa para llevar a cabo la suplantación de identidad.

Las actividades que realiza una "célula criminal"³¹ están perfectamente coordinadas, se establecen medios, métodos y técnicas para cometer el delito y no verse vulnerado ante las autoridades, es por ello que se convierten en profesionales del delito, por ello dentro del esquema número 3 se muestran las principales actividades.

**ESQUEMA NÚMERO 3
PRINCIPALES ACTIVIDADES DE UNA
CÉLULA DELICTIVA**



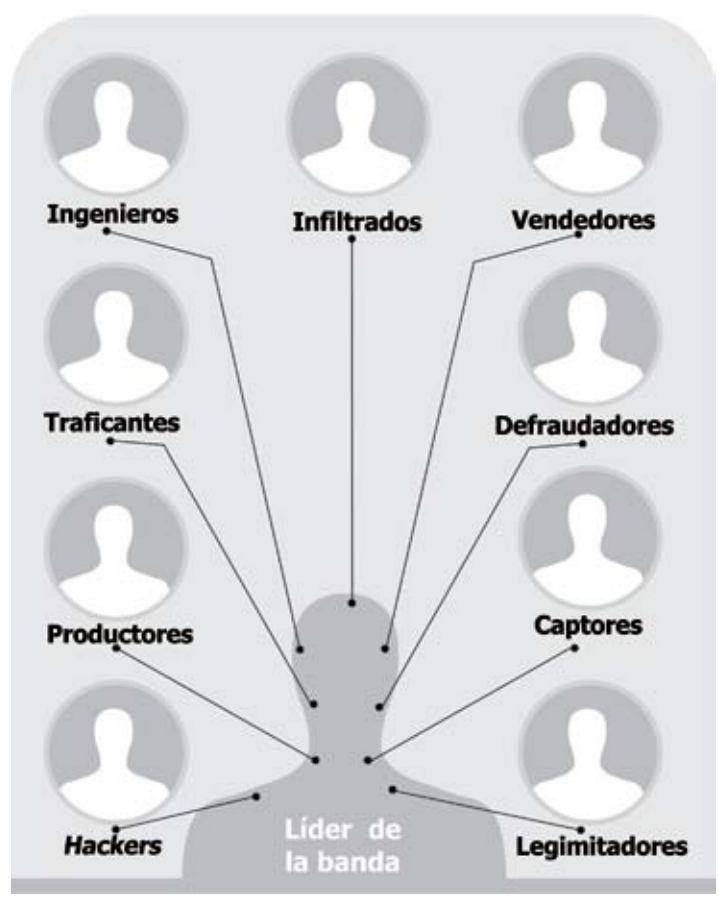
Colectivo ARCION. 26 de febrero de 2012. Para formar una célula delictiva profesional se requieren de ciertas actividades que la delincuencia requiere para obtener satisfactoriamente sus objetivos.

30 Un router, (voz inglesa) encaminador, enrutador, direccionador o ruteador. Es un dispositivo de hardware usado para la interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar. Router, Wikipedia, la enciclopedia libre, 'router' [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: <http://es.wikipedia.org/wiki/Router>

31 Célula criminal. Grupo de personas que funcionan dentro de organizaciones delictivas.

Estas actividades se encuentran relacionadas con el perfil del delincuente o delincuentes, que son reclutados con base a sus conocimientos o aptitudes, muchos de ellos son profesionistas como contadores, ingenieros, abogados, químicos, administradores, entre otros. De manera paralela también se encuentran aquellos que son contratados por la delincuencia y que solo cubren ciertos requisitos básicos o aptitudes y pueden ser menores de edad, obreros, albañiles, mecánicos, o gente llamada vulgarmente dentro del argot Mexicano como *-"ni-ni"*³², por ello a continuación se muestra el esquema número 4.

**ESQUEMA NÚMERO 4
LOGÍSTICA DENTRO DE LA SUPLANTACIÓN DE IDENTIDAD**



Colectivo ARCION, 29 de febrero de 2012. Esquema que muestra la integración de una célula delictiva dedicada a la suplantación de identidad al alimón con algunos delitos.

"Hackers. Grupo de personas que penetran dentro de los sistemas informáticos de manera virtual para obtener información confidencial y privada.

32 Ni-ni. El término de 'ni-ni' hace referencia al sector de la población que en la actualidad no está trabajando ni estudiando (Ni estudia, ni trabaja), siendo la mayoría jóvenes en edad escolar. Los principales detonantes de este problema son la falta de empleo, la deserción escolar y la baja calidad educativa. En Estados Unidos se le conoce a este fenómeno social como NEET (voz inglesa) No employment, no education and no training. Sin empleo, sin educación y sin capacidad. Wikipedia, la enciclopedia libre 'ni-ni' [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: <http://es.wikipedia.org/wiki/Ni-Ni>

Productores. Grupo de personas dedicadas producir documentos de identificaciones fraudulentas para los traficantes de personas o para realizar otras actividades delictivas derivadas de las identidades de clientes.

Traficantes. Grupo de personas encargadas de "traficar a personas"³³, y tienen completa relación con los falsificadores, ingenieros e infiltrados para obtener documentos oficiales apócrifos y darles una identidad falsa a aquellos inmigrantes, mujeres o niños dentro del territorio nacional.

Ingenieros. Profesionistas en informática encargados de realizar actividades como la falsificación de documentos, realizar actividades como *phishing*, simulación de identidad, clonación de tarjetas, o diseñar programas como *pul wifi* para obtener información confidencial y privada de usuarios del internet.

Infiltrados. Grupo de personas inmiscuidas dentro de instituciones de gobierno o privadas, que se dedican a entrar a la base de datos y obtener información confidencial y personal de trabajadores o usuarios.

Vendedores. Son un conjunto de individuos encargadas de vender datos de información personal o documentos oficiales apócrifos a otras personas que se encuentren en territorio Mexicano que sean indocumentados, que deseen salir del país por evadir a la autoridad, o simplemente para vender dicha información a personas de otros países.

Defraudadores. Son aquellas personas encargadas de engañar a una o varias personas y hacerse pasar por empresas –fantasma- para obtener información confidencial y dinero, otra actividad relacionada con estas personas es la de realizar llamadas telefónicas para engañar a las víctimas y obtener claves bancarias o información personal.

Captos. Grupo de personas encargadas de –echarse un clavado en la basura- para obtener información privada es decir estados de cuenta, copias de identificaciones, claves bancarias, *tickets* de saldos obtenidos de los cajeros automáticos, y demás información que revele la identidad, otra actividad realizada por esta gente es el proceso llamado –búsqueda de tumbas- y ésta consiste en recolectar información sobre personas fallecidas misma que será utilizada posteriormente para hacer creer que él es la persona finada, o simplemente emitir un voto durante el proceso de electoral, es decir la persona que ha fallecido tiene pleno goce de su democracia, procedimiento que se reconoce como una suplantación de identidad de tipo físico.

Legitimadores. Se trata de un conjunto de personas encargadas de realizar una actividad ilícita denominada –lavado de dinero-, su actividad consiste básicamente en canalizar los montos encubriendo los fondos que se hayan generado mediante alguna actividad ilícita como el tráfico de personas"³⁴.

La necesidad de implementar medidas de seguridad eficaces en el combate contra la suplantación de identidad

En la actualidad, México se encuentra desprotegido ante la conducta antisocial denominada suplantación de identidad, no existe una ley que penalice esta actividad.

Esta forma de expresión criminal es desconocida por las autoridades que día a día se encuentran incapaces ante las demandas que la sociedad exige, ejemplo de ello las tres mil denuncias impuestas ante las autoridades bancarias por clonación de tarjeta, acontecimiento que puso en caos a la ciudadanía y autoridades poblanas, otro caso parecido son los 105 casos detectados por suplantación de identidad dentro de la zona metropolitana y municipios del Estado de Puebla, lo mismo puede estar sucediendo en los demás Estados de la República Mexicana, donde de igual manera queda impune el hecho que se comete directamente sobre la apariencia y patrimonio de la víctima que padece este fenómeno delictivo.

México no se encuentra preparado para combatir la conducta antisocial denominada suplantación de identidad, ya que no cuenta con estudios ni análisis que demuestren la existencia y manifestaciones constantes de este fenómeno, por ello es necesario que los legisladores pongan atención en las denuncias y quejas realizadas por la ciudadanía.

Este procedimiento debe ser analizado y estudiado satisfactoriamente por un Criminólogo-criminalista que identifique las modalidades y los indicios que deja él o los probables responsables y realizar un análisis que muestre:

- Análisis del fenómeno mundial denominado suplantación de identidad.
- Las modalidades de la suplantación de identidad.
- La magnitud del problema.
- El daño ocasionado a las víctimas.
- Probable incremento de la suplantación de identidad.
- Vulnerabilidad de la población.
- Análisis de las zonas donde la población utilice de manera frecuente ordenadores.
- Análisis de los clonadores de tarjetas colocados en los cajeros automáticos de los bancos.
- Análisis de los *skimmer* localizados en tiendas departamentales y negocios.
- Mapeo de la zona para ubicar las zonas donde se hayan reportado clonadores de tarjetas de los cajeros automáticos.
- Mapeo de la zona para ubicar las zonas donde se hayan encontrado *skimmer*.
- Y realizar un programa preventivo que debe darse a conocer a la población en general para evitar ser víctimas de la suplantación de identidad.

Es muy importante resaltar que debe ser cuidadosamente es-

33 La convención de la ONU contra la Delincuencia Organizada y sus Protocolos, definió el Tráfico de Personas, como -el reclutamiento, transporte, encubrimiento o recepción de personas, por medio del uso de amenazas o el uso de la fuerza u otra forma de coacción. Los traficantes son aquellos que transportan emigrantes y se benefician económicamente o de alguna otra manera del de personas-, Un lugar.com "Tráfico de personas, La tercera actividad ilegal más lucrativa del mundo". [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: <http://www.iuspenalismo.com.ar/doctrina/felipe.htm>

34 Colectivo ARCION. Dirección General de Investigación, febrero de 2012.

tudiado el fenómeno de suplantación de identidad a nivel mundial, ya que de manera indirecta la creación de la tecnología pueden afectar a la seguridad pública e informática de México.

Una vez realizado un análisis profundo sobre la suplantación de identidad por el Criminólogo-criminalista, las autoridades competentes deberán tomar en consideración las demostraciones técnicas y científicas expuestas por el profesionalista en cuestión para poder tipificar y sancionar esta conducta antisocial.

Otro factor importante es la prevención terciaria, que se debe desarrollar mediante la implementación de un tratamiento penitenciario adecuado para aquellos sujetos que cometen la actividad conocida como -suplantación de identidad-, ya que si no se atiende al sujeto o sujetos, éstos pueden reincidir en la conducta y hasta mejorar la forma de realizarlo, por ello se debe garantizar el esfuerzo del consejo interdisciplinario para que realicen favorablemente una reinserción social, pero específicamente destacar la labor titánica que deberá de realizar el Criminólogo clínico.

Otro estudio que favorece a la prevención del fenómeno denominado suplantación de identidad es el contacto con la víctima, misma que arrojará datos importantes que ayuden a complementar el análisis realizado por el Criminólogo-criminalista, y finalmente realizar un tratamiento especial de atención víctimas, con todo este trabajo se podrá difundir a la ciudadanía un programa preventivo que indique las acciones que debe tomar para evitar una suplantación de identidad.

CONCLUSIÓN

A través de esta investigación se pudo detectar que el fenómeno delictivo reconocido por otros países como suplantación de identidad tuvo gran impacto, en la sociedad Mexicana, debido a que miles de personas manifestaron sus quejas ante autoridades para pedir justicia ante el hecho de que alguna persona se hizo pasar por ella para dejarlos en banca rota o para conseguir créditos que nunca habían pedido.

Resulta interesante poner atención a los casos de clonación de tarjetas, donde la víctima que padece este fenómeno detecta que le han sido vaciadas sus cuentas bancarias, sin haber hecho ni siquiera un retiro, denuncia que es atendido por algunas autoridades

que se quedan incapaces de proceder ante la suplantación de identidad, ya que dentro de los argumentos legales, levemente se consideran iniciativas de ley que contemplan la introducción de dichas conductas en los ordenamientos.

La suplantación de identidad es una nueva conducta antisocial que debe ser estudiada debidamente por un Criminólogo-criminalista, ya que se están pasando por desapercibido muchos factores que son de confort para la delincuencia, y que si no es atendido en estos momentos se puede convertir en un verdadero problema de seguridad que no solo afectaría a la ciudadanía, sino que a la base de datos de las instituciones públicas y privadas.

Esta conducta antisocial que se describe dentro de esta investigación no se manifiesta únicamente de manera física, sino que el delincuente aprovecha la tecnología para cometer sus actividades ilícitas, ejemplo de ello los llamados *hackers* que irrumpen dentro de la base de datos de grandes instituciones de gobierno élite, o simplemente se introduce dentro de las cuentas de correo electrónico de millones de personas que no toman alternativas eficaces para evitar ser víctima de este acontecimiento, dicho fenómeno indica que México no se encuentra preparado para afrontar esta situación que a nivel mundial genera millones de pérdidas económicas.

No solo se trata de identificar el problema o la magnitud de éste, por el contrario se requiere de realizar una opción que favorezca la prevención para disminuirlo, y sobre todo que sea contemplado por los legisladores, para que ellos viertan una sanción oportuna que permita ser aprovechada por el consejo interdisciplinario y especialmente por el Criminólogo clínico que adecuará un tratamiento completo y favorable que facilite la prevención terciaria y evitar reincidencias.

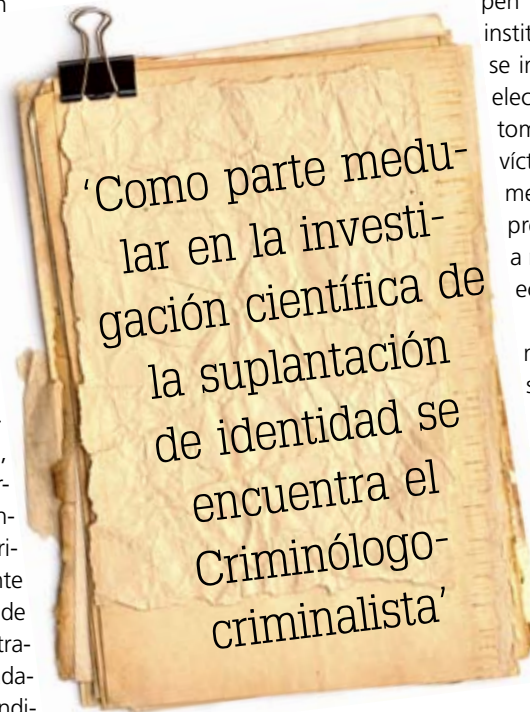
La labor del Criminólogo-criminalista dentro de la llamada suplantación de identidad se encuentra en la detección de nuevas conductas que se ponen de manifiesto mediante el uso material de objetos tales como ordenadores, telefonía celular o *software*, es decir mediante el estudio y análisis de la tecnología.

Dichas conductas sirven al investigador científico como base para formular hipótesis que orienten el origen del o de los probables responsables, así como de su conocimiento tecnológico y manejo del mismo, utilizado en contra de la sociedad, todo ello mediante la búsqueda incanzable de indicios materiales que sirvan como orientativos, así como de lo expuesto por la víctima.

FUENTES DE INFORMACIÓN

Bibliográficas

Aboso, Gustavo Eduardo, et al. Cibercriminalidad y derecho penal, Buenos Aires Argentina, Editorial B de F Montevideo- Buenos Aires, 2006.



Cabeza de Vaca, Daniel F. et al. Intercriminis número 13 segunda época, México, INACIPE, 2005.

Cámpoli, Gabriel Andrés. Delitos informáticos en la legislación mexicana, México. INACIPE, 2007.

Hikal, Wael. Introducción al estudio de la Criminología, México, Editorial Porrúa, 2011.

Téllez Valdés, Julio. Derecho informático, México, MacGraw-hill, 2009.

Electrónicas

Cabinas net. 'Robo de identidad'. [En línea]. [Consultado: 12 de enero de 2012]. Disponible en la web: <http://www.cabinas.net>

Cámara de Diputados, Congreso de la Unión. 'Boletín número 4520', [En línea]. [Consultado: 3 de enero de 2012]. Disponible en la web: <http://www3.diputados.gob.mx>

Código Penal Federal, Publicado en el Diario Oficial de la Federación el 14 de agosto de 1931, última reforma publicada en el Diario Oficial de la Federación el 24-10-2011, 'capítulo II Acceso ilícito a los sistemas y equipos de informática, artículo 211 bis, Título noveno Revelación de secretos y acceso ilícito a sistemas y equipos de informática Capítulo I Revelación de secretos, Capítulo III Fraude, Título vigesimocuarto, Delitos electorales y en materia de registro nacional de ciudadanos, Capítulo único' 1. [En línea]. [Consultado: 9 de enero de 2012]. Disponible en la web: <http://www.diputados.gob.mx>

Data security.com 'clonación de tarjetas'. [En línea]. [Consultado: 28 de febrero de 2012]. Disponible en la web: <http://www.wisedatasecurity.com>

Definición.DE 'Definición de telecomunicación'. [En línea]. [Consultado: 29 de febrero de 2012]. Disponible en la web: <http://definicion.de>

Master card 'Robo de identidad'. [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: <http://www.mastercard.com>

Mirrorlinux.net 'hacker'. [En línea]. [Consultado: 09 de enero de 2012]. Disponible en la web: <http://mirrorlinux.net>

ONU 'alerta del robo de la identidad online y el tráfico con pornografía infantil' [En línea]. [Consultado: 13 de enero de 2012]. Disponible en la web: <http://www.elmundo.es>

Procuraduría General de la República 'de los delitos electorales' [En línea]. [Consultado: 28 de febrero de 2012]. Disponible en la web: <http://www.pgr.gob.mx>

Real Academia Española. Diccionario de la Lengua Española. 'suplantación, suplantar'. [En línea]. [Consultado: 27 de enero de 2012]. Disponible en la web: <http://www.rae.es/rae.html>

Redel, red de entretenimiento e información. 'Simulación de identidad'. [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: <http://www.biografica.info>

Router, Wikipedia, la enciclopedia libre, 'router' [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: <http://es.wikipedia.org>

Scribd. 'Unidad III. Seguridad informática. [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: <http://es.scribd.com>

Segu-info seguridad de la información. 'Phishing' [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: <http://www.segu-info.com>

Slideshare present yourself 'Robo de identidad/ identity theft/ Apropiación ilegal de identidad Rivera Suárez, Waleska'. [En línea]. [Consultado: 12 de enero de 2012]. Disponible en la web: <http://www.slideshare.net>

Un lugar.com 'Tráfico de personas, La tercera actividad ilegal más lucrativa del mundo'. [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: <http://www.iuspenalismo.com>

Wikipedia, la enciclopedia libre 'Criptología, nini'. [En línea]. [Consultado: 29 de enero de 2012]. Disponible en la web: Criptología <http://es.wikipedia.org>

La falsificación y alteración de documentos oficiales y su importancia en la suplantación de identidad de tipo físico

COLECTIVO ARCION

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

Colectivo Arcion
DGLCLEU

“ La identificación es un derecho que otorga el Estado a cualquier persona nacida dentro de un país, y ésta se puede representar en documentos oficiales. ”

RESUMEN

La delincuencia hoy en día, realiza sus actividades ilegales utilizando artimañas que le permitan dañar la esfera jurídica de las víctimas dejando de lado el uso de la fuerza excesiva para evitar enfrentamientos directos y utilizar el beneficio de la tecnología, ya que el beneficio de ésta permite perpetrar en la intimidad de cualquier persona, conducta que se puede convertir en una suplantación de identidad.

INTRODUCCIÓN

Dentro de la presente investigación se podrá conocer la importancia de la intervención del Criminólogo-criminalista en la investigación de la suplantación de identidad de tipo físico, específicamente dentro de la alteración y falsificación de actas de nacimiento, puesto que éste, es el documento principal que se brinda a cualquier ciudadano nacido en tierras Mexicanas.

Cabe mencionar que cualquier ciudadano nacido como mexicano adquiere derechos y obligaciones dentro del país, y uno de los derechos otorgados por el gobierno es la de identificarlo legalmente, y para ello se le otorga una acta de nacimiento expedida por un Registro del Estado Civil de cualquier Estado donde haya nacido, es por ello que dicho reconocimiento natural se otorga sin distinción alguna.

La identidad y la identificación son términos que tienen diferente o igual significado, estas apreciaciones se realizan con base a las ciencias o disciplinas que intervienen para darle construcción teórica, como el caso muy específico de la Medicina, la Psicología, el Derecho o lo Forense.

Para muestra de la identificación se tiene como presente la expedición de documentos oficiales o privados, donde se aprecian datos principales que corroboran los testimonios rendidos ante autoridad, como ejemplo de ello se tiene la licencia para conducir expedida por la Secretaría de Comunicaciones y Transportes (SCT), la credencial para votar expedida por el Instituto Federal Electoral (IFE), mientras que por documento de identificación privada se tienen las credenciales escolares particulares o las credenciales laborales.

Como parte fundamental de la suplantación de identidad se encuentra la falsificación y alteración de documentos de tipo físico, donde se detectan algunas anomalías en los documentos, siendo estos raspados de impresiones, lavado de documentos mediante la utilización de solventes químicos o elementos como gomas que desprenden el trazo, la impresión de tintas o la mecanografía.

Finalmente se hará mención de la necesidad del Criminólogo-criminalista dentro de la investigación de suplantación de identidad de tipo físico, así como la recomendación de que este profesionista debe participar dentro de los juzgados, municipios y juntas auxiliares donde se expiden o corrigen actas de nacimiento para poder así identificar el delito llamado falsificación de documentos y la reciente conducta antisocial denominada –suplantación de identidad–.

LA IDENTIDAD E IDENTIFICACIÓN

Todo ser humano al nacer cuenta con derechos y obligaciones, ya que por el simple hecho de nacer es acreedor de ser reconocido en sociedad y ante el gobierno, por tal motivo para ser identificado e individualizado, las instituciones de gobierno idearon la forma de registrar a cada nuevo ser humano, para así gozar de los atributos de la personalidad, y una de esas es la nacionalidad siendo en este caso la Mexicana.

Todo Mexicano que tenga su residencia en cualquier Estado de la República debe de identificarse con cualquier documento oficial, pero ¿Qué es la identidad y la identificación? Por ello a continuación se realiza la siguiente reflexión.

Algunas ciencias admiten que la identidad y la identificación son términos diferentes, mientras que otras determinan que significan lo mismo, de manera general la Real Academia de la Lengua Española define: “Del b. lat. *identitas*, -*ātis*. Conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás”¹.

Para el término identificación se puede observar lo siguiente: “Acción y efecto de identificar o identificarse”².

Finalmente la Real Academia de la Lengua Española define identificar como: “Dar los datos personales necesarios para ser reconocido”³.

La Medicina por su parte realiza la siguiente analogía y define identidad de la siguiente manera: “Conjunto de características que hacen a una persona distinta de las demás y sólo igual a sí misma”⁴.

Mientras que para el término de identificación la ciencia médica lo define como: “Métodos para establecer la identidad”⁵.

Otra ciencia disciplinaria de la Criminología-criminalística en la que se apoya es la Psicología, misma que define los términos en cuestión de la siguiente forma:

Identidad: “Parte del Autoconcepto que implica la identificación de una persona”⁶.

Identificación: “Mecanismo psíquico inconsciente que induce a un sujeto a comportarse, pensar y sentir como otro que actúa con su modelo”⁷.

Para las Ciencias Forenses identidad e identificación se precisan como:

Identidad: “Del latín *identitas*. Conjunto de rasgos y características físicos de una persona, haciéndola única a sí misma y distinta de todas las demás”⁸.

Identificación: “Acción de identificar, reconocer a una persona, objeto, animal o cosa, la cual se busca y está relacionada con situación jurídica”⁹.

Finalmente dentro del tema en cuestión, estas ciencias disciplinares definen también el término de identificar, y este es: “Determinar de manera inequívoca la verdadera personalidad de un individuo, un lugar o una cosa, sin existir confusión”¹⁰.

Legalmente se concibe una apreciación terminológica sobre el derecho a la identidad, por ello el “Dr. Hugo Daniel D’Antonio, disertante de la Asociación de Magistrados y funcionarios de la Justicia de Menores y Familia, define al derecho de la identidad como el presupuesto de la persona que se refiere a sus orígenes como ser humano y a su pertenencia abarcando: su nombre, filiación, nacionalidad, idioma, costumbres, cultura propia y demás elementos componentes de su propio ser”¹¹.

La identidad legal es una valoración que implica que los Estados reconozcan la existencia de individuos que integran la población. Como prueba fiel de este procedimiento se tiene el registro de nacimientos, la expedición de un certificado o acta de nacimiento y de un documento de identidad, puesto que éstos forman parte de la comprobación más visible del reconocimiento legal por parte de un Estado, con ello se conoce la existencia de un niño o niña y/o la continuidad de un

‘identificación’. [En línea]. [Consultado: 05 de enero de 2012]. Disponible en la web: <http://www.rae.es/rae.html>

3 Real Academia Española. Diccionario de la Lengua Española. ‘identificar’. [En línea]. [Consultado: 05 de enero de 2012]. Disponible en la web: <http://www.rae.es/rae.html>

4 Vargas Alvarado, Eduardo. Medicina Legal, México, Editorial Trillas, 2008, pág. 58.

5 Ibid., pág. 58.

6 Dzib Aguilar, José Paulino. Glosario Psicológico- Jurídico, México, Editorial de Península, S.A. de C.V., primera edición 2010, pág. 101.

7 Ibid., pág. 101.

8 Nando Lefort, Víctor, et al. Diccionario terminológico de Ciencias Forenses, México, Editorial Trillas, 1998, pág. 57.

9 Ibid., pág. 57.

10 Ibid., pág. 57.

11 Instituto José Manuel Estrada-Doblas, La Palma, Una pregunta sin respuesta, ‘Derecho a la identidad’. [En línea]. [consultado: 05 de enero de 2012]. Disponible en la web: http://www.oni.esuelas.edu.ar/2006/LA_PAMPA/1118/Pagina%20Segunda.htm

1 Real Academia Española. Diccionario de la Lengua Española. ‘identidad’. [En línea]. [Consultado: 05 de enero de 2012]. Disponible en la web: <http://www.rae.es/rae.html>

2 Real Academia Española. Diccionario de la Lengua Española.

adulto como miembro de la sociedad. Sin lugar a duda la identidad legal concede la ciudadanía, formándose en un derecho que habilita otros beneficios, como la educación, la salud, el trabajo, la vivienda o la participación durante las elecciones.

La identidad no pertenece únicamente a una sola expresión, sino que pueden encontrarse diversas formas, como identidad sexual, identidad social, identidad cultural, identidad jurídica, éste es un derecho reconocido para todo ser humano que hace diferente uno de otro, el reconocimiento de una identidad, nombre y nacionalidad es otorgado por la Ley.

Los documentos de identidad públicos y privados

La forma más certera de comprobar la identidad es a través de un documento, que desde el punto de vista jurídico se concibe como la representación material idónea para poner de manifiesto la existencia de un hecho o acto jurídico, dentro de ésta misma concepción se encuentra una clasificación de documentos, como se puede observar en las imágenes A,B,C y D.

- Cédula profesional expedida por la Secretaría de Educación Pública (SEP).
- Cartilla del Servicio Militar Nacional, expedida por la Secretaría de Defensa Nacional (SEDENA).
- Clave Única de Registro de Población (CURP) expedida por la Secretaría de Gobernación (SG).
- Cartilla de Salud expedida por la Secretaría de Salud (SSA).
- Licencia de Conducir expedida por la Secretaría de Comunicación y Transportes (SCT).
- Acta de Defunción expedida por un Registro Civil.
- Carta de Antecedentes no Penales expedida por la Procuraduría General de Justicia (PGJ).
- Cédula de Identidad Personal expedida por el Registro Nacional de Población e Identificación Personal (RENAPO).

Existen otros medios de identificación personal, que son tramitados ante instituciones privadas, ejemplo de ellas:

- Tarjeta de crédito y débito, expedida por Instituciones bancarias.
- Credenciales de estudiante, expedida por instituciones educativas.
- CárDEX o tarjetón de pago, expedidos por instituciones de enseñanza privadas o públicas.
- Credenciales de club, expedidos por instituciones deportivas privadas.
- Credenciales de trabajadores, expedidas por empresas privadas o dependencias gubernamentales.
- Otros.

Dentro del argot utilizado por las ciencias forenses y por el Criminólogo-criminalista, existe otra clasificación de documentos y ésta se presenta a continuación dentro de las imágenes E, F y G.

**IMÁGENES A, B, C y D
TIPOS DE DOCUMENTOS**

Documento público

Son aquellos expedidos por funcionarios públicos competentes, por profesionistas dotados de Fé Pública, que estén en el desempeño de sus funciones.



Imagen A



Imagen B



Imagen C



Imagen D

Imagen. A y B. Colectivo ARCION, Dirección General de Investigación. 05 de enero de 2012. Licencia de manejo expedida por la Secretaría de Comunicaciones y Transportes (SCT).

Documento Privado

Son todos aquellos documentos expedidos por cualquier persona que no tenga Fé Pública, por ejemplo notas, cartas, contratos de arrendamiento, etcétera.

Imagen. C y D. Colectivo ARCION, Dirección General de Investigación. 05 de enero de 2012. Credencial de estudiante, expedida por el Colegio Libre de Estudios Universitarios (CLEU).

Colectivo ARCION, 05 de enero de 2012. Se puede observar ejemplos de identificación público y privado.

La identidad Mexicana consiste en poseer documentos oficiales, como:

- Acta de Nacimiento expedida por un Registro Civil.
- Pasaporte vigente expedido por la Secretaría de Relaciones Exteriores (SRE).
- Credencial para votar expedida por el Instituto Federal Electoral (IFE).

**IMÁGENES E, F y G
DOCUMENTOS DUBITABLES E INDUBITABLES**

Documentos dubitables

Aquellos que de alguna manera son auténticos, y pueden ir desde documentos oficiales, hasta documentos privados.



Imagen F

Documentos indubitables

Son aquellos documentos los cuales se tiene alguna duda de su autenticidad, es decir, que su contenido haya sido alterado de manera física.



Imagen G

Imagen. G. Colectivo ARCION. Dirección General de Investigación. 05 de enero de 2012. Pagaré.

Colectivo ARCION, 05 de enero de 2012. Se puede observar documentos dubitables e indubitables.

La falsificación de documentos

Una de las actividades más comunes por los delincuentes, es la falsificación de documentos, misma que se desarrolla sin mayor complejidad, esta acción es definida por la Real Academia de la Lengua Española como "acción y efecto de falsificar"¹², haciendo uso nuevamente de esta consagración, falsificar se define del siguiente modo "falsear o adulterar algo"¹³.

Una segunda concepción del término de falsificación es precisamente la siguiente: "Copia o imitación de una cosa que se quiere hacer pasar por verdadera o auténtica"¹⁴, específicamente realizar una falsificación es contrario a la ley, por lo tanto está considerada como un delito.

De manera específica esta actividad está relacionada con los documentos en general, y por falsificación de documentos se entiende como "el proceso a través del cual una o varias personas alteran y/o transforman la información original que posea un documento de cualquier índole. La falsificación puede ser material como también ideológica, en esta última podemos encontrarnos con un documento cuyo soporte corresponde a la fórmula virgen y por ende auténtica. Pero, en cambio, sus datos y/o contenidos son fraudulentos"¹⁵, esta actividad se proclama en contra de las normas sociales así como de la misma ley.

Un acontecimiento extraordinario que se manifiesta de manera creciente no solo en México sino que a nivel mundial, es la falsificación de documentos en general, ésta actividad se va a definir como "El proceso a través del cual una o varias personas alteran y/o transforman la información original que posea un documento de cualquier índole. La falsificación puede ser material como también ideológica, en esta íntima podemos encontrar un documento cuyo soporte corresponde a la fórmula virgen y por ende auténtica. Pero, en cambio, sus datos y/o contenidos son fraudulentos"¹⁶.

Antecedentes históricos de la falsificación de documentos y su análisis

El primer antecedente que se tiene con respecto a la falsificación de documentos, es Atenas, Grecia durante el siglo V a.C., ya que fue aquí donde se realizó esta actividad sobre un documento público.

Otro gran imperio que formó parte en las filas de la delincuencia en cuanto a este delito se refiere, fue Roma, donde era común utilizar ardid con fines ilícitos, los artefactos que eran falseados eran las monedas y testamentos. Debido a la gravedad del problema en el año 78 a.C. "fue promulgada por Lucio Cornelio Sila la *-Lex*

Cornelia de Falsis-"¹⁷, esta actividad consistía en realizar una comparación entre escrituras, esto se realizaba siempre que se tuviera alguna duda en cuanto a la procedencia de los documentos expuestos, este procedimiento se considera como un antecedente arcaico, precario y poco confiable de lo que sería un peritaje caligráfico.

Es momento de trasladar la historia y remontarla hacia la Edad Media, donde tras la caída del imperio Romano aproximadamente hacia el siglo IV d.C., donde las ciencias jurídicas perdieron terreno y tuvieron un inesperado estancamiento, ya que fue aquí donde se sustituye la prueba de testimonio y de comparación por el uso de la confesión del inculpado, misma que de manera reprochable consistía en torturar a quien era delincuente. "Durante este período, proliferaron los títulos nobiliarios falsos o adulterados, como así también, los privilegios reales y las bulas papales que, al no existir un método para diferenciar lo falso de lo verdadero, circulaban con total impunidad"¹⁸.

En el año 1200, fue elaborado un libro llamado *-El libro de las Leyes-*, esta obra fue elaborada por el rey de León y Castilla, Alfonso X el Sabio, pero años más tarde pasaría a ser conocido como *-cuerpo legal-*, cuya función era única y exclusivamente implementar justicia en todo el reino, pero debía mantener la cualidad de ser equitativo. Se refiere que dentro de este documento se hayan modificaciones de la escritura sin fines criminales o sin la intención de engañar, esto sin lugar a duda se obtenía ya que según el rey las personas no mantienen la misma escritura al paso de los años, es decir cuando se posee la juventud, la rapidez, la energía, se refleja en los trazos ejecutados durante la escritura, mientras que al paso de los años, cuando se hace presente vejez y la velocidad así como la agilidad se van perdiendo, se logra percibir en la escritura un cambio notable, aunque se trate de la misma persona.

Dentro de esta obra ejemplar también se puede apreciar el primer antecedente de la función de un profesionalista como el Criminólogo-criminalista, ante el estudio y análisis de la escritura y documentos dubitables, ya que era necesario evaluar los escritos impugnados presentes en ese momento.

En el siglo XV, el avance tecnológico tuvo grandes aportaciones, como el perfeccionamiento de la imprenta de tipos móviles elaborado por Johann Gutenberg, ya que con esto se pudo incrementar la distribución de libros, movimiento que produjo la divulgación del idioma de manera escrita, pero ante todo beneficio sus

12 Real Academia Española. Diccionario de la Lengua Española. 'identidad'. [En línea]. [Consultado: 05 de enero de 2012]. Disponible en la web: <http://www.rae.es/rae.html>

13 Real Academia Española. Diccionario de la Lengua Española. 'falsificar'. [En línea]. [Consultado: 05 de enero de 2012]. Disponible en la web: <http://www.rae.es/rae.html>

14 The free Dictionary, by farflex. 'Falsificación'. [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: <http://es.thefreedictionary.com/falsificaci%C3%B3n>

15 Todo vLex México, concepto falsificación de documentos [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: <http://vlex.com.mx/tags/concepto-falsificacion-documentos-411056>

16 Scribd. 'Falsificación de documentos'. [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: <http://es.scribd.com/doc/8223726/Falsificacion-de-Documentos>.

17 Wikipedia, La enciclopedia libre. 'Documentología'. [En línea]. [Consultado: 26 de enero de 2012]. Disponible en la web: http://es.wikipedia.org/wiki/Documentolog%C3%ADa#Breve_evoluci.C3.B3n_hist.C3.B3rica

18 Wikipedia, La enciclopedia libre. 'Documentología'. [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: http://es.wikipedia.org/wiki/Documentolog%C3%ADa#Breve_evoluci.C3.B3n_hist.C3.B3rica

consecuencias, y estas consistían en conocer también las nuevas técnicas de falsificación y alteración de documentos, que evolucionaban con los pasos agigantados de la tecnología.

Michón, Crépieux-Jamin, Solange Pellat, Locard, son solo algunos de los investigadores franceses con mayor prestigio, y reconocidos por su gran aportación en el estudio y análisis documental. Cabe recordar que la escuela francesa fue un ejemplo a seguir para los demás países y colegios europeos, como lo fue el caso de la inglesa representada por Subier y Saudek, o la alemana que fue identificada por Preyer, Meyer, Klages y Scheneickert, y la italiana, con Morelli, Andreani, Ottolenghi y Marchesan.

Wilhem Preyer determinó que la escritura estaba considerada como una manifestación de la actividad cerebral, ya que presenta características similares del órgano que la realiza, esta versión o aportación sería afirmada años más tarde por Edmond Solange Pellat, como -ley de la escritura-.

Dentro de la obra titulada – *Traité de incryptations en faux* de Jacques Revenau, se puede encontrar un procedimiento que consiste en el análisis comparativo de escrituras, donde se ponía demasiada atención a los trazos que la integran, y se dejaba pasar por alto las semejanzas morfológicas que la integraban, mismas que podían ser imitadas y llevaban al investigador por rumbos diferentes a las metas que se proponían.

La tecnología para el perfeccionamiento de las técnicas fotográficas, informática y documentología llegó a la luz del siglo XX, donde los profesionales mejoraron la forma de analizar un documento

En México el análisis de documentos no fue la excepción, los primeros inicios se encuentran en el año de 1519, con el *Amatl* (voz Náhuatl) *āmatl*, Español: amate o amate del papel, es una forma de papel que fue fabricado durante el periodo pre-Colombino Mesoamérica.

Sobre esta textura se plasmaron los libros del país, y contemplaban los pictogramas doblados en castilla, hoy en día, conocida como -a caballo-, su cualidad única era la de estar impresa por ambos lados, de esta obra se ponía en tela de juicio el hecho que la técnica de impresión y armado eran modernas y no podía corresponder a la época.

En el año de 1539 con la llegada a México de Juan Pablos y de la imprenta Sevillana de Juan Cromberg,

se logró capacitar a los más reconocidos impresores, pero de manera indirecta también se logró dar todas las facilidades para los primeros falsificadores en México.

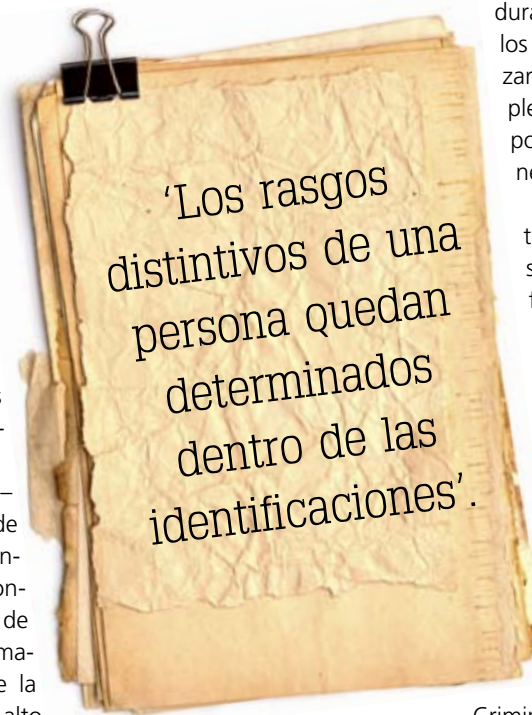
En México se detectaron muchos casos de falsificación de documentos, y ejemplo de ello fue en el año de 1823, cuando se empezaron a imprimir los primeros documentos en "papel fiduciario"¹⁹ cuya base se sustentaba en la "bula papel"²⁰, este antecedente formó parte de la historia de la falsificación de documentos, actividad que permitió la formación de los primeros especialistas en el análisis de documentos.

Hay que recordar que la figura de perito durante esa época no era aún descubierta, y los únicos que tenían la facultad para analizar un documento o moneda eran los empleados del banco o los impresores, ya que poseían cierta experiencia en las falsificaciones de billetes.

Durante el año de 1837 en Tacubaya se tenían detectados algunos talleres de falsificación de monedas, y se volvieron tan famosos ya que eran personalidades las que se dedicaban a realizar esta actividad ilícita, por estas filas circulaban impresores, políticos y militares de ese momento.

Al paso del tiempo esta actividad se fue perfeccionando a tal grado de ser operada por la delincuencia organizada, misma que recobra fuerza gracias a los patrocinios financieros, recursos humanos, técnicos y de información, y al mismo tiempo el estudio de análisis de documentos se hace presente para surgir como una disciplina más de la

Criminología-criminalística.



La falsificación de documentos y su apreciación legal

La falsificación de documentos, está considerada en México como un delito, y se encuentra previsto dentro del Código Penal Federal en su artículo 244, mismo que indica los medios empleados para realizar dicha actividad, y se puede observar desde la fracción primera hasta la décima.

I.- Poniendo una firma o rúbrica falsa, aunque sea imaginaria, o alterando una verdadera;

II.- Aprovechando indebidamente una firma o rúbrica en blanco ajena, extendiendo una obligación, liberación o cualquier otro documento que pueda comprometer los bienes, la honra, la persona o la reputación de otro, o causar un perjuicio a la sociedad, al Estado o a un tercero;

III.- Alterando el contexto de un documento verdadero, después de concluido y firmado, si esto cambiare su sentido sobre alguna circuns-

19 Papel fiduciario. Es un contrato realizado durante un negocio donde sus condiciones se basan principalmente en la confianza entre las partes que realizan dicho convenio.

20 Bula Papel. Es un documento oficial político o religioso sellado, y si éste contaba con la cualidad de ser auténtico y contar con el sello papal, recibía el nombre de bula papel o bula pontificia.

tancia o punto substancial, ya se haga añadiendo, enmendando o borrando, en todo o en parte, una o más palabras o cláusulas, o ya variando la puntuación;

IV.- Variando la fecha o cualquiera otra circunstancia relativa al tiempo de la ejecución del acto que se exprese en el documento;

V.- Atribuyéndose el que extiende el documento, o atribuyendo a la persona en cuyo nombre lo hace: un nombre o una investidura, calidad o circunstancia que no tenga y que sea necesaria para la validez del acto;

VI.- Redactando un documento en términos que cambien la convención celebrada en otra diversa en que varíen la declaración o disposición del otorgante, las obligaciones que se propuso contraer, o los derechos que debió adquirir;

VII.- Añadiendo o alterando cláusulas o declaraciones, o asentando como ciertos hechos falsos, o como confesados los que no lo están, si el documento en que se asientan, se extendiere para hacerlos constar y como prueba de ellos;

VIII.- Expidiendo un testimonio supuesto de documentos que no existen; dándolo de otro existente que carece de los requisitos legales, suponiendo falsamente que los tiene; o de otro que no carece de ellos, pero agregando o suprimiendo en la copia algo que importe una variación substancial, y

IX.- Alterando un perito traductor o paleógrafo el contenido de un documento, al traducirlo o descifrarlo.

X.- Elaborando placas, gafetes, distintivos, documentos o cualquier otra identificación oficial, sin contar con la autorización de la autoridad correspondiente"²¹.

Elementos documentales

Los documentos han estado en circulación a través de la historia, por tal motivo en manos del ciudadano, algunos de ellos tienen la gran utilidad de ser oficiales, mientras que otros simplemente llevan impreso un lenguaje de comunicación escrita, pero todos se encuentran palpables ante la luz de la humanidad.

La palabra documento proviene del latín *documentum*, que significa "Diploma, carta, relación u otro escrito que ilustra acerca de algún hecho, principalmente de los históricos"²².

El documento tiene una serie de elementos que integran su contenido, y que se encuentra presente en casi todos ellos, como primer punto se encuentra el soporte o papel, que se encuentra constituido por fibra celulosa polipropileno o polietileno.

Se pueden encontrar varios tipos de papel, por ejemplo:

- Papel biblia.
- Papel carbónico.

- Papel cristal.
- Papel manifold.
- Papel calco.
- Papel manteca.
- Papel pergamino vegetal.
- Papel para diarios.
- Papel obra.
- Papel rotograbado.
- Papel afiche.
- Papel tapa.
- Papel manila.
- Papel embalaje.
- Papel sulfito.
- Papel para cigarrillos.
- Papel de estraza.
- Papel libre de ácido.
- Papel kraft.
- Papel liner.
- Papel (cartón) multicapa.
- Papel pergamino vegetal.
- Papel similpergamino.
- Papel similsulfurizado.
- Papel sulfurizado.
- Papel tisúe.
- Papel permanente.
- Papel fluting.
- Papel de piedra.

El papel es fabricado a partir de una pasta o solución acuosa donde es suprimida el agua debido al procedimiento que se realiza para obtener el soporte, también está constituida por las fibras, mismas que pueden ser vegetal, animal o mineral, la primera clasificación está integrada por material celuloso que debe tener las siguientes cualidades:

- Flexibilidad.
- Finura.
- Resistencia.

Por su parte la fibra mineral posee la cualidad de ser inorgánica, y se puede observar en el papel como hilo o polvo metálico, mientras que la fibra animal deriva de las proteínas de la mayoría de los ácidos orgánicos, y pueden ser visibles en el soporte como hilo de lana.

Para poder obtener el papel es necesario que sus elementos sean procesados, a tal grado de obtener una pasta triturada en agua trapos de hilos o algodón, o diversas materias fibrosas como madera, cáñamo, esparto, paja, etcétera, añadiéndose encolantes para mejorar su consistencia, así como otros aditivos según el tipo de papel que se desee fabricar. Antiguamente la celulosa no se extraía en forma directa de los vegetales, sino que se aprovechaban los trapos e hilos de origen no animal, sobre todo el algodón.

Las materias primas que son utilizadas para la fabricación del 'soporte' mejor conocido como papel, y éstas son:

1. Fibras de lino.
2. Fibras de cáñamo.
3. Fibras de algodón.
4. Celulosa.
5. Almidón.

21 Código Penal Federal, Última Reforma DOF 24-10-2011, 'capítulo IV, artículo 244 Falsificación de documentos en general'. [En línea]. [Consultado: 27 de febrero de 2012]. Disponible en la web: <http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf>

22 Real Academia Española. Diccionario de la Lengua Española. 'documento'. [En línea]. [Consultado: 05 de enero de 2012]. Disponible en la web: <http://www.rae.es/rae.html>

6. Madera.
7. Residuos.
 - 7.1 Bagazo.
 - 7.2 Paja de trigo.
 - 7.3 Linter.
8. Pasta mecánica.
9. Pasta química.

Otro elemento presente en el papel es la tinta, misma que se define de la siguiente manera: "tinta del latín *tinctoria*, part. pas. de *tingere*. Teñir. f. Líquido coloreado que se emplea para escribir o dibujar, mediante un instrumento apropiado"²³, cabe mencionar que las tintas se encuentran plasmadas dentro de las hojas de papel.

Las tintas se encuentran constituidas por líquidos con cola que se impregnan dentro de las fibras del papel de manera evaporada dejando huella de su existencia. Las tintas pueden estar presentes de manera líquida fluida, con elementos grasos, o como anilina, a tal grado de estar siempre dispuestas para cualquier impresión.

Como dato importante se tiene que las tintas que se conocen hoy en día, como tinta china o tinta india fueron conocidas inicialmente bajo el nombre de carbonosas ya que se encontraban elaboradas por material sólida denominado carbón mismo que era realizada por la combustión incompleta de sustancias orgánicas.

A continuación se presentan algunas de los tipos de tinta que existen, mismo que se puede apreciar dentro de la tabla número 1.

**TABLA NÚMERO 1
TIPOS DE TINTAS**

Elementos	Concepto
Tinta hectográfica.	Esta tinta tiene gran concentración de tinte en solución de glicerina o en su caso de alcohol.
Tinta mimeográfica.	Es una tinta elaborada a base de negro de humo o carbono con adhesivo oleoso.
Tinta de las cintas mecanográficas y de los sellos de caucho.	Esta tinta está realizada mediante agua, mezclada con glicerina para evitar que se seque.
Tintas indelebles.	Entre sus compuestos se encuentra el nitrato de plata. Cuando esta es expuesta a la luz, al calor o a una reacción química, se logra observar las marcas de los sedimentos de plata de un color negro metálico. Si son expuestas al calor o a la luz, o a la acción química, dejan marcados en los tejidos unos sedimentos de plata de un color negro metálico.

23 Real Academia Española. Diccionario de la Lengua Española. 'Tinta'. [En línea]. [Consultado: 05 de enero de 2012]. Disponible en la web: <http://www.rae.es/rae.html>

Tinta invisible.	Las tintas invisibles también reciben el nombre de simpáticas, y ejemplo de ellas son los jugos vegetales como: mucílago, albúmina o azúcar como el zumo de cebolla, de pera, de limón, de naranja, de manzana, etcétera. Estas sustancias pueden servir como tintas simpáticas, porque la huella incolora que dejan al principio, se revela cuando se calienta el papel. A simple vista no pueden ser observadas porque no deja algún rastro, pero se puede percibir con la presencia del calor, mientras que otras se pueden hacer manifiestas a través del uso de la radiación ultra violeta o mediante una reacción química.
Tinta flexográfica.	Esta tinta se encuentra presente en la impresión de materiales de embalaje como lo son "cajas de cartón, cartón ondulado, bolsas de papel y plástico, envases de alimentación, periódicos, catálogos, etcétera" ²⁴ .
Tinta de anilina.	Es el primer colorante sintético, que se distingue por ser una materia prima para obtener productos empleados en la industria de los colorantes.
Tinta magnética.	Uno de sus elementos es la suspensión de óxido de hierro en excipientes viscosos, que dejan marca, y ejemplo de ello las máquinas de clasificación de billetes de banco.
Tinta metálica.	Si principal componente es el metal en polvo mezclado con goma acuosa arábica.

Colectivo ARCION, 05 de enero de 2012. Se contemplan los diferentes tipos de tintas que existen y que pueden ser impregnadas dentro de un 'soporte' o papel.

La alteración

El ser humano siempre ha tenido la gran habilidad para ingeniárselas y realizar acciones ilegales y salir beneficiado, una de estas habilidades es la alteración de documentos, y por alteración se entiende como el "Cambio en las características, la esencia o la forma de una cosa"²⁵, existen algunos tipos de alteración dentro de los documentos, y ésta es:

- Alteración por medios físicos.

Este procedimiento se lleva a cabo cuando se elimina alguna parte impresa del texto, y para ello se pueden utilizar algunos medios como las gomas que tras su utilización se puede obser-

24 Wikipedia, La enciclopedia libre. 'Tinta Flexográfica'. [En línea]. [consultado: 21 de Febrero de 2012]. Disponible en la web: http://es.wikipedia.org/wiki/Tinta_flexogr%C3%A1fica

25 The free dictionary by farlex. 'Definición de alteración'. [En línea]. [consultado: 23 de Febrero de 2012]. Disponible en la web: <http://es.thefreedictionary.com/alteraci%C3%B3n>

var una "abrasión"²⁶, algunas de ellas están elaboradas de titinilio, plástico, caucho, etcétera, existen varios tipos de gomas como lo son:

- Goma moldeable.
- Goma de caucho lápiz-tinta.
- Goma de plástico duro.
- Goma para tinta.
- Goma de migajón.
- Goma de lápiz.
- Goma entubada.

Existen algunas gomas de colores, y ello depende muchas veces de sus funciones, por ejemplo, la goma de caucho para borrar lápiz-tinta, mientras que otras realizan su borrado delicado para eliminar trazos.

Otro medio físico útil para realizar esta actividad de borrado son las herramientas con filo, ya que con ello se puede realizar un raspado a la impresión, entre ellas se puede utilizar:

- Bisturí.
- Navajas para afeitar.
- Explorador (instrumental en operatoria dental).
- Sonda periodontal (instrumental en operatoria dental).

La utilización de estos medios sirve para extraer la parte superficial de un documento que necesita ser extraído, específicamente para eliminar las impresiones, el único detalle es que a tras luz se puede observar un ligero desgaste y una transparencia de la hoja.

Finalmente otro medio para realizar un borrado es la lija, cuyas propiedades son:

- Grano.
- Papel.
- Tejido de algodón o poliéster.
- Fibra vulcanizada.
- Aglutinante.
- Recubrimiento.

Cabe mencionar que no todas las lijas sirven para realizar un borrado a una hoja, ya que hay algunas donde solo se utilizan granos en mayor proporción y esto hace que sea muy rasposa y pueda romper el soporte, por ello para lograr un borrado delicado se requiere de unas lijas de tipo:

- Lija fina. Está compuesta de 150 a 180 granos.
- Lija muy fina. Contiene de 240 a 400 gramos.

Alteraciones por medios químicos

Otras de las alteraciones que se pueden realizar para eliminar una impresión de un documento es mediante el uso de solventes que sirven para lavar el soporte.

Como ejemplo de ello se tiene el uso de un embudo, también llamado papel fieltro, su finalidad es la de ubicar la sustracción del trazo que se desea eliminar, su uso alcanza aquellas tintas denominadas -lavables-, que son aquellas que se vuelven solubles ante la presencia del agua, éste tipo reacciona de manera benéfica ante

el soluble, mientras que para las tintas férricas parecen resistirse a la reacción, ya que está conformada por una propiedad principal -sal de hierro-, misma que no permite entrar en la sustancia y difuminarla.

Un elemento que se encuentra al alcance de todos es el H₂O mejor conocido como agua, el cual permite disolver las tintas de alinina, pero con ello no quiere decir que se pueda utilizar en todos los aspectos, como es el caso de los bolígrafos, mismas que se resisten a la aplicación de un solvente, ello debido a que están compuestas de elementos pasivos que impiden la reacción química.

Las tintas que penetran las fibras de los documentos dejan un claro indicio para el Criminólogo-criminalista, ya que el grafito así como las copias al carbónico dejan huellas de su existencia.

Otro ejemplo de ello es la llamada -borra tintas- que está hecho de soluciones diluidas de compuestos oxidantes que convierten los componentes pigmentados por un derivado incoloro, reacción oxidativa.

Los elementos que integran el borratintas son:

- "Borrado con sulfitos.
- La perturbación puede realizarse por ejemplo en sulfitos. En esta ocasión los hidroxilos (OH⁻) y los iones bisulfito ó sulfito ácido (HSO₃⁻) se almacenan junto al átomo central de carbono del pigmento. Para esto son aptos por ejemplo el sulfito de sodio (Na₂SO₃), bisulfito sódico (NaHSO₃), y sulfito de potasio (K₂SO₃).
- Borrado con carbonatos.

Otra posibilidad no tan efectiva es la perturbación por medio de carbonatos como el carbonato de sodio (Na₂CO₃) o el bicarbonato de sodio (NaHCO₃). En este caso se almacenan de igual forma los hidroxilos (OH⁻) alrededor del átomo central de carbono.

- Borrado con tiosulfatos e hidrosulfitos.

Por último al lado de algunas sustancias más complejas entran en cuestión los hidrosulfitos o tiosulfatos (por ejemplo Na₂S₂O₃) para el borrador de tinta²⁷.

Las actas de nacimiento apócrifas como vía idónea para conseguir más de una identidad

Queda claro que el primer documento de identidad que se otorga a cualquier recién nacido es el acta de nacimiento, expedida por un Registro Civil de cualquier Estado, y una de sus funciones principales es la de "dar la identidad ante la sociedad y jurídicamente permite establecer un vínculo"²⁸.

Dentro de un Acta de Nacimiento se encuentran ciertas características que dan el vínculo de identidad con la base de datos del Registro del Estado Civil, ello se puede observar dentro de Clave de Registro de Identificación Personal (CRIP), misma que se encuentra de manera numérica, otro gran dato encontrado dentro de la misma base de datos es el nombre del expedidor y firma, nombre del portador o persona identificada y número de

26 Abrasión. Es la acción que consiste en raer o desgastar algo por fricción.

27 Wikipedia, La enciclopedia libre 'Borrador de tinta' [En línea]. [consultado: 23 de Febrero de 2012]. Disponible en la web: http://es.wikipedia.org/wiki/Borrador_de_tinta#Qu.C3.ADmica_del_borrador_de_tinta

28 Extracto obtenido de la entrevista realizada al Abogado Javier Ocelotl López encargado del Registro Civil del Estado libre y soberano de Puebla, mismo que se puede leer detalladamente en anexos dentro de la pregunta número 3.

folio, datos que ayudan a corroborar la existencia y permanencia de una persona ante la sociedad y los órganos jurídicos.

Otro factor importante para que este documento se considere como oficial, es el hecho de estar dotado de fe pública, ya que solo con ello puede tener validez dicho documento, es por ello que se considera como oficial el uso de un Acta de Nacimiento.

Dentro de este fenómeno se puede observar que para realizar una suplantación de identidad se requiere de imprimir datos completamente falsos, ello sucede con frecuencia ya que los falsificadores consiguen medios físicos o químicos para alterar los documentos oficiales, como el caso de las actas de nacimiento, o en algunos casos la delincuencia llega a obtener las formas valoradas de las actas de nacimiento en blanco para poder utilizarlas al beneficio ilícito.

Las alteraciones a las actas de nacimiento así como de cualquier documento oficial para identificar, suelen tener diversos motivos:

- Prácticas fraudulentas.
- Suplantación de identidad.
- "Ocultación de identidad.
- Ingreso o permanencia de inmigrantes en un país si la documentación apropiada.
- Trata de personas.
- Comercio de menores"²⁹.

Si un acta de nacimiento es falsificada y alterada en los datos como nombre o fecha de nacimiento se puede hablar de obtener otra identidad, por tal motivo cualquier documento que se gestione ante autoridad también podrá ser falso, ya que para realizar cualquier trámite se requiere un acta de nacimiento para comprobar la veracidad de los datos, y si son falsos por consiguiente se obtendrá por ejemplo una credencial para votar falsa, un pasaporte falso, una cartilla del servicio militar falsa, un título profesional falso, una credencial del seguro social falsa, o cualquier documento ya sea oficial o particular.

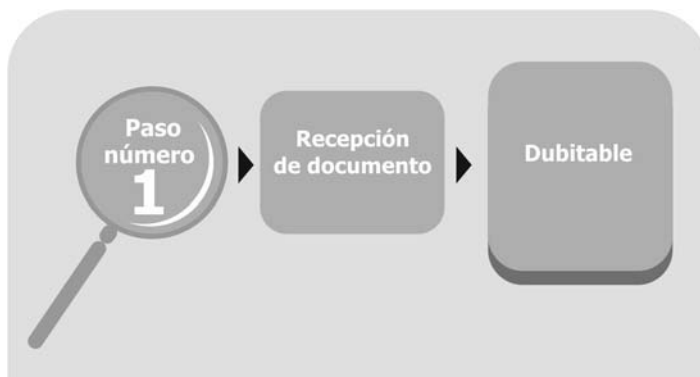
"El requisito indispensable para tramitar algún documento por ejemplo el IFE es el Acta de Nacimiento, esto lleva relación al robo de identidad ya que es muy fácil conseguir un acta de nacimiento y con eso solicitar el IFE y así ir maquillando los documentos para solicitar un crédito o alguien ponerlo en banca rota en sus cuentas bancarias, y a través de medios electrónicos"³⁰.

Con base a ello es necesario que el Registro del Estado Civil de cualquier Estado tenga gran cuidado al

expedir actas de nacimiento y proporcionar las formas valoradas a los diferentes juzgados o presidencias municipales, para evitar una falsificación y alteración de documentos y suplantación de identidad.

Por ello nuevamente aquí se hace referencia de la necesidad de un Criminólogo-criminalista en cada juzgado, presidencia municipal o registro del Estado Civil de cada Estado o municipio, para que se logre identificar plenamente la autenticidad del documento así como la presencia de una suplantación de identidad y se demuestre técnica y científicamente su existencia.

La intervención del Criminólogo-criminalista en el análisis de un documento oficial dudable



Cuando se tiene alguna duda sobre su autenticidad de un documento, se recurre ante las autoridades competentes, y éstas a su vez requieren de un profesional que cuente con amplios conocimientos en la materia de Documentos cuestionados y Grafoscopia, con base a ello aquí se destaca la importancia de la intervención del Criminólogo-criminalista, profesional que cuenta con amplios conocimientos en la rama, por ello a continuación se presenta la labor titánica de dicho profesional ante la suplantación de identidad de tipo físico.

Se tiene a la vista un documento de carácter oficial dudable, mismo que se puede observar dentro de la fotografía número 1.

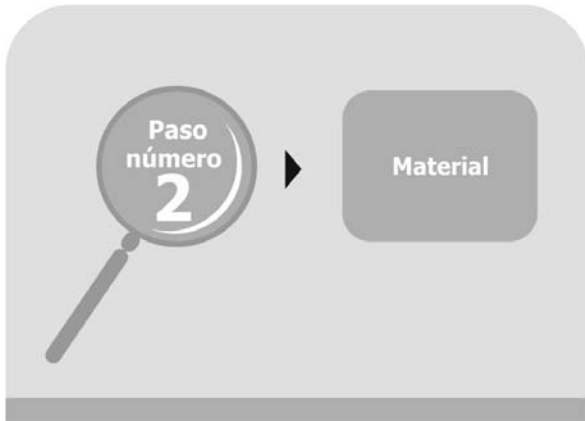
FOTOGRAFÍA NÚMERO 1



Fotografía número 1. Colectivo ARCION, Laboratorio del Colegio Libre de Estudios Universitarios CLEU Plantel Puebla, 21 de febrero de 2012. Acta de Nacimiento dudable. (Véase fotografía a color al final de la revista).

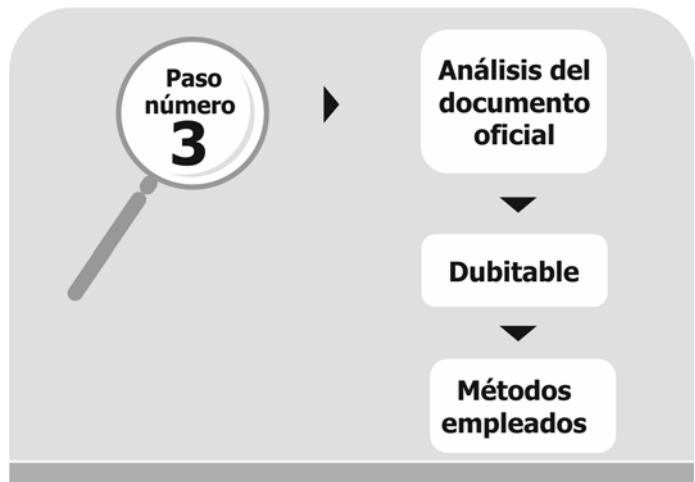
²⁹ Bonilla Carlos, Enrique. Investigación documentológica, Ediciones la Rocca, Buenos Aires 2005, pág. 317.

³⁰ Extracto obtenido de la entrevista realizada al Abogado Javier Ocelotl López encargado del Registro Civil del Estado libre y soberano de Puebla, mismo que se puede leer detalladamente en anexos dentro de nota de complemento.



Una vez presentando el documento del cual se tiene duda de su autenticidad, se procede a realizar un análisis de su estructura y contenido, por ello se requiere el siguiente material:

Bata blanca de algodón
Guantes de látex
Libreta de notas
Bolígrafo de tinta negra
Cuanta hilos de 5x
Luz amarilla
Lámpara de luz UV
Cámara fotográfica digital de 9 megapíxeles
De laboratorio: Microscopio óptico



Para realizar el análisis del documento en cuestión es necesario aplicar una serie de métodos que complementan el estudio del Criminólogo-criminalista, y como base fundamental:

- Método analítico.
- Método deductivo.
- Método inductivo.

Con base en el uso de estos métodos se procede a realizar lo siguiente:

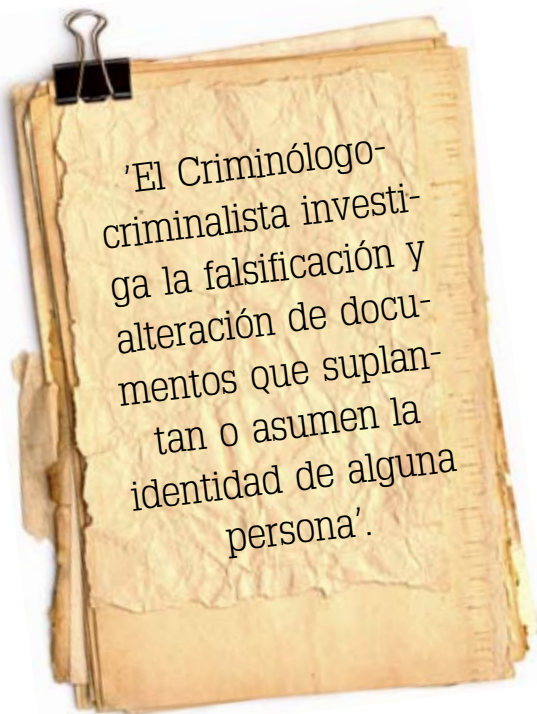
Se tiene a la vista un Acta de Nacimiento actualizada con soporte tamaño oficio que mide 33.0 centímetros de largo por 21.5 centímetros de ancho, expedida el día 04 de enero de 2011, por el Juzgado del Registro Civil de Tochimilco, Puebla, a nombre de María Juana Dávila Caltonco, con fecha de nacimiento 27 de enero de 1958, lugar de nacimiento, Tochimilco, Puebla, sin número de Clave de Registro de Identificación Personal (CRIP) con folio número 8178025, dirección del Registro del Estado Civil número 1206027 y firmado por el C. Juez único Pascual Tufiño Teles, como se pueden observar en las fotografías número 2, 3, 4, 5, 6, 7 y 8.

FOTOGRAFÍA NÚMERO 2



Fotografía número 2. Colectivo ARCION, Laboratorio del Colegio Libre de Estudios Universitarios CLEU plantel Puebla, 21 de febrero de 2012. Sello del Juzgado del Registro del Estado Civil expedido en Tochimilco, Puebla con clave 21-188-01.

Se pueden observar los siguientes sistemas de seguridad:



Sistemas de Seguridad de Acta de Nacimiento a nombre de María Juana Cristina Dávila Caltonco

Sistema de impresión: **red de fondo 1/2 a una sola tinta**
Soporte: **papel**



Fotografía número 3.
Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Sistema de impresión a una sola tinta.

Sistema de impresión: **"Intaglio"³¹ de una sola tinta**
Soporte: **papel seguridad**

³¹ Intaglio se define como un proceso de impresión en la cual una imagen se transfiere en un papel con la tinta que hay en las incisiones hechas en una placa de metal. Etimologías latín. 'Etimología de *intaglio*' <http://etimologias.dechile.net/?intaglio>



Sistema de impresión y soporte: **red de fondo, offset**



Fotografías número 4, 5 y 6.
Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Red de fondo tipo offset.

Sistema de impresión y soporte: **marcas de agua**



Fotografías número 7 y 8.
Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Marcas de agua, donde se puede observar una red y la marca del probable proveedor del papel tipo seguridad.

Sistemas de Seguridad de Acta de Nacimiento a nombre de María Juana Cristina Dávila Caltonco

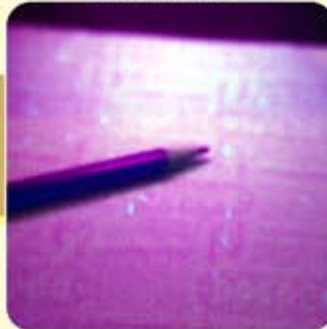
**Papel tipo seguridad
Microfibras visibles a la luz natural.**

FOTOGRAFÍA 9



**Papel tipo seguridad
Microfibras visibles a la luz UV.**

FOTOGRAFÍA 10



FOTOGRAFÍA 11



Fotografía número 10 y 11. Colectivo ARCION, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Fibras visibles ante la luz UV, se puede observar que la fotografía número 17 se obtuvo mediante el uso de microscopio óptico usando sólo el objetivo 10x.

Sistema de seguridad impresa

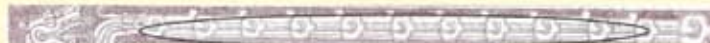
FOTOGRAFÍA 12



Fotografía número 12. Colectivo ARCION, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Se puede observar el escudo de los Estados Unidos Mexicanos como una forma de seguridad impresa.

**Sistemas de seguridad impresa.
Intaglio
Microimpresión Positiva.**

FOTOGRAFÍA 13



Fotografía número 13. Colectivo ARCION, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012.

**Sistemas de seguridad impresa.
Intaglio
Microimpresión Negativa.**

FOTOGRAFÍA 14



Fotografía número 14. Colectivo ARCION, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU) plantel Puebla, 21 de febrero de 2012.

Sistemas de Seguridad de Acta de Nacimiento a nombre de María Juana Cristina Dávila Caltonco

Comparativa de seguridad impresa positiva y negativa.

FOTOGRAFÍA 15



Fotografía número 15. Colectivo ARCION, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Comparativa de seguridad impresa positiva y negativa

Sistemas de seguridad impresas positiva y negativa. Cabezas de línea.

FOTOGRAFÍA 16



FOTOGRAFÍA 17



Fotografía número 16 y 17. Colectivo ARCION, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Sistemas de seguridad impresas positiva y negativa, Cabezas de línea.

Sistema de Seguridad. Guilloche.

FOTOGRAFÍA 18



Fotografía número 18. Colectivo ARCION, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Se puede observar el sistema de seguridad guilloche.

Sistema de seguridad impresa. Red ecualizada

FOTOGRAFÍA 19



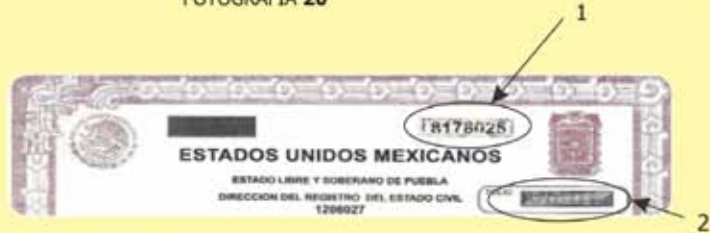
Fotografía número 19. Colectivo ARCION, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Sistema de seguridad impresa, red ecualizada.

Sistemas de Seguridad de Acta de Nacimiento a nombre de María Juana Cristina Dávila Caltonco

Folio con holograma 1

Folio con tinta 2

FOTOGRAFÍA 20



Fotografía número 20
Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012, Se puede observar la impresión y el holograma de folio.

Folio en matriz de mecánica con tinta reactiva a la luz UV.

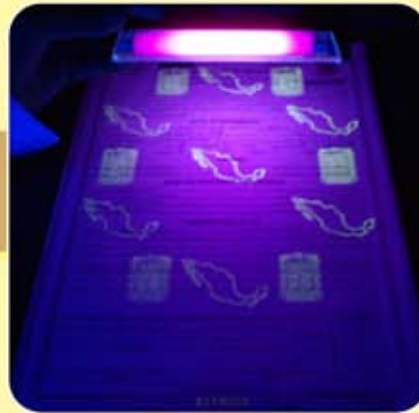
FOTOGRAFÍA 21



Fotografía número 21.
Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Número de folio observable sólo con el uso de la luz UV.

Red impresa con tinta reactiva a la luz UV.

FOTOGRAFÍA 22



FOTOGRAFÍA 23



Fotografía número 22 y 23.
Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Se puede apreciar el Escudo del Estado de Puebla y el contorno de la república Mexicana, mismo que sólo puede ser observado sólo con el uso de la luz UV.

Sistemas de seguridad impresa

FOTOGRAFÍA 24



FOTOGRAFÍA 25



Fotografía número 24 y 25.
Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de Febrero de 2012. Se puede apreciar el Escudo de México.



Alteración física del documento en cuestión

Generalidades del documento. Se observa un ascenso básico –ausente–. Ya que se distinguen 4 alteraciones manuales de tipo físico. La mecanografía general de todo el documento fue realizado por una sola máquina de escribir eléctrica ya que presenta las siguientes características:

- La impresión de la mecanografía es delgada.
- Separación marcada entre los caracteres.

IMAGEN 1



Imagen 1. Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Acta de nacimiento a nombre de María Juana Cristina Dávila Caltonco.

1. Ascenso básico –ausente–. Se advierte que para la impresión de la mecanografía se utilizó otra tinta, el escrito no es auténtico.

FOTOGRAFÍA 26



Fotografía número 26. Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Ascenso básico ausente.

2. Alineación básica –presente–. Ya que se aprecia que todos los caracteres impresos se encuentran alineados de manera adecuada y uniforme.

FOTOGRAFÍA 27



Fotografía número 27. Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Alineación básica presente.

Alteración física del documento en cuestión

Alteración física número 1, observada dentro de la mecanografía –Caltonco-, donde se aprecia lo siguiente:

3. Borradura por medio físico. Se advierte en el carácter –O- un raspado mediante el uso de un elemento filoso, ello se comprueba debido a que a tras luz se aprecia una transparencia "ya que al reducir el espesor del papel los rayos de la luz lo atraviesan, denotando el lugar agredido"³².

FOTOGRAFÍA 28



Fotografía número 28. Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Borrado físico.

4. Tintas

La mecanografía en general está impresa por cinta entintada, pero se puede observar en el carácter –o- un remarque, donde probablemente se utilizó un útil inscriptor con grafito.

FOTOGRAFÍA 29



Fotografía número 29. Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Tintas.

5. Presencia de ápex.

Se advierte en la parte inferior del carácter en cuestión que presenta un ápex, esto se puede corroborar gracias a que con el análisis microscópico se logra apreciar que el remarcado no fue completado en su totalidad, motivo por el cual se puede observar la presencia de dicho elemento.

FOTOGRAFÍA 30

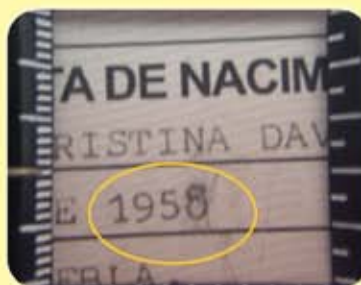


Fotografía número 30. Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Presencia de ápex.

6. Segunda alteración

Se puede observar otra alteración dentro de la mecanografía numérica 1958, apreciándose lo siguiente: Ascenso básico –ausente-. Se advierte que para la impresión de la mecanografía se utilizó otra tinta, el escrito no es auténtico.

FOTOGRAFÍA 31



Fotografía número 31. Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Segunda alteración.

³² Bonilla Carlos, Enrique. Investigación documentológica, Ediciones la Rocca, Buenos Aires 2005, pág. 267.

Alteración física del documento en cuestión

7. Alineación básica –ausente-.
Ya que se aprecia que la mecanografía numérica impresa presenta desalineación superior, y una alineación ascendente de izquierda a derecha.

FOTOGRAFÍA 32



FOTOGRAFÍA 33



Fotografías número 32 y 33.
Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Alineación básica.

8. Borradura por medio físico
Se advierte en el carácter numérico –8- un raspado mediante el uso de un elemento filoso, ello se comprueba debido a que a tras luz se aprecia una transparencia "ya que al reducir el espesor del papel los rayos de la luz lo atraviesan, denotando el lugar agredido".³³

FOTOGRAFÍA 34



Fotografía número 34
Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Borradura por medio físico.

9. Tintas.
La mecanografía en general está impresa por cinta entintada, pero se puede observar en el carácter –8- un remarque, donde probablemente se utilizó un útil inscriptor con grafito.

FOTOGRAFÍA 35



Fotografía número 35.
Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de febrero de 2012. Tintas.

³³ *Ibidem*, pág. 267.

Alteración física del documento en cuestión

10. Tercera alteración.

Se aprecia dentro del rubro –masculino- donde se aprecia de manera continua un círculo donde se advierte la existencia de una borradura por medio físico, siendo éste un raspado mediante el uso de un elemento filoso, ello se comprueba debido a que a tras luz se aprecia una transparencia.

FOTOGRAFÍA 36



Fotografía número 36. Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de Febrero de 2012 Tercera alteración.

11. Cuarta alteración

Se puede observar dentro del rubro –femenino- que dentro del círculo se aprecia una marca diferente a la impresión que deja la máquina de escribir, también se puede apreciar que dicha marca presenta un grosor y que está impresa por lo que al parecer pudiera ser un útil inscriptor de grafito.

FOTOGRAFÍA 37



Fotografía número 37. Colectivo ARCIÓN, Laboratorio del Colegio Libre de Estudios Universitarios (CLEU), plantel Puebla, 21 de Febrero de 2012 Cuarta alteración.

Determinación

1. El documento oficial que corresponde a un acta de nacimiento expedida por el Registro del Estado Civil del municipio de Tochimilco, Puebla a nombre de María Juana Dávila Caltonco, es auténtico, no se encuentra falsificada, ya que se comprobó la existencia de todos los candados de seguridad, y sólo se determinó la existencia de 4 alteraciones físicas.

Observaciones

Se recurrió ante las autoridades competentes de dicho juzgado para comprobar la veracidad de los datos que aquí se obtienen, por lo que se obtuvo:

1. El acta de nacimiento cuyo nombre es María Juana Dávila Caltonco, no corresponde con los registros de dicho juzgado.
2. De acuerdo al número de folio 8178025, se pudo localizar la verdadera identidad de la persona, siendo ésta el nombre verdadero de Juana María Cristina Caltenco, cuya fecha de nacimiento es 27 de enero de 1956.
3. Gracias a esta información así como de la investigación del Criminólogo-criminalista, se pudo concluir que se encontraba ante una suplantación de identidad de tipo físico.

CONCLUSIÓN

Hoy en día, la delincuencia se desarrolla de manera acelerada, donde los delincuentes se sirven de bastantes artimañas para cometer sus fechorías, mientras que en otras utilizan la tecnología para obtener beneficios económicos sin la necesidad de enfrentarse cara a cara a la víctima.

Se debe prestar atención a la conducta antisocial conocida como –suplantación de identidad-, misma que se manifiesta de manera considerable en la actualidad, y promete incrementar sus cifras en un futuro no muy lejano, por ello dentro de esta investigación se consideró como elemental el estudio de la alteración y falsificación física, ya que de manera tangible se observa cómo puede ser suplantada una persona de manera fácil a tal grado de modificar el sentido original de un documento oficial

Los falsificadores llevan a cabo ciertas formas para realizar una alteración a un documento como el uso de gomas, agentes mecánicos con filo, instrumental dental, o agentes químicos como el lavado de documentos, borrratintas, o el uso de solventes.

Es importante poner demasiada atención en el procedimiento realizado por los falsificadores, ya que se pueden concretar actividades ilegales como el ocultamiento de identidad, trata de personas, tráfico de indocumentados, o corrupción de menores, finalidad que debe ser prevista por un profesionista capaz de identificar la presencia de una alteración y falsificación de documentos, tal es el caso del Criminólogo-criminalista, el cual tiene amplio conocimiento en la disciplina conocida como documentos cuestionados.

Dicho profesionista tiene la gran aptitud para demostrar científicamente la existencia de una alteración de tipo físico sobre un soporte, específicamente dentro de los documentos oficiales que identifican a cualquier persona, su análisis versa sobre la intencionalidad de lo elaborado con la conducta que se desea consumir; es decir, poder identificar con base a los indicios tangibles si dicho argumento proviene de la elaboración de sujetos con conocimiento en ello o de personas con nulas erudiciones sobre la falsificación, con ello podría arrojar una hipótesis, y esta es sobre la relación existente entre individuos falsificadores con células delictivas bien organizadas dedicadas a realizar delitos graves mediante la ayuda de dicha actividad ilícita, o establecer si el cambio de datos falseados se concretó para hacerse pasar por una persona y realizar en concreto un delito.

Las Actas de Nacimiento son ejemplo de la falsificación y alteración, ya que en algunos casos se realiza para obtener otra identidad, por ello es necesario realizar ampliamente una investigación sobre su autenticidad, y la veracidad de sus datos, esto se puede realizar en colaboración con las autoridades competentes,

para obtener la recolección de los datos que influyen de manera primordial al profesionista en cuestión.

Es importante y fundamental la intervención del Criminólogo-criminalista dentro de las áreas de:

- Registro del Estado Civil.
- Juzgados.
- Municipios.
- Juntas Auxiliares.

Áreas donde se expiden Actas de Nacimiento, ya que dichos sitios no cuentan con expertos en materia de documentos cuestionados que detecten la falsificación y alteración de documentos, así como de la más y reciente actividad antisocial denominada –suplantación de identidad-.

FUENTES DE INFORMACIÓN

Bibliográficas

- Bonilla Carlos, Enrique. Investigación documentológica, Ediciones la Rocca, Buenos Aires 2005.
- Dzib Aguilar, José Paulino. Glosario Psicológico- Jurídico, México, Editorial de Península, S.A. de C.V., primera edición, 2010.
- G. del Picchia, Ana Maura. et al. Tratado de Documentoscopia, Ediciones la Rocca, Buenos Aires 2006.
- Nando Lefort, Víctor, et al. Diccionario terminológico de Ciencias Forenses, México, Editorial Trillas, 1998.
- Vargas Alvarado, Eduardo. Medicina Legal, México, Editorial Trillas, 2008.

Electrónicas

- Código Penal Federal, Última Reforma DOF 24-10-2011, 'capítulo IV, artículo 244 Falsificación de documentos en general'. [En línea]. [Consultado: 27 de febrero de 2012]. Disponible en la web: <http://www.diputados.gob>
- Instituto José Manuel Estrada Doblas, La Palma, Una pregunta sin respuesta, 'Derecho a la identidad'. [En línea]. [Consultado: 05 de enero de 2012]. Disponible en la web: <http://www.oni.esuelas.edu>
- Real Academia Española. Diccionario de la Lengua Española. 'identidad, identificación, identificar, falsificar, documento, tinta, borrador de tinta'. [En línea]. [Consultado: 05 de enero de 2012]. Disponible en la web: <http://www.rae.es/rae.html>
- Scribd. 'Falsificación de documentos'. [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: <http://es.scribd.com>
- The free Dictionary, by farflex. 'Falsificación, definición de alteración'. [En línea]. [Consultado: 05 de enero de 2012]. Disponible en la web: <http://es.thefreedictionary.com>
- Todo vLex México, concepto falsificación de documentos [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: <http://vlex.com.mx>
- Wikipedia, La enciclopedia libre. 'Documentología y tinta flexográfica'. [En línea]. [Consultado: 05 de enero de 2012]. Disponible en la web: <http://es.wikipedia.org>

ANEXOS

Entrevista de tipo dirigida, realizada el 14 de febrero de 2012.

Lugar: Instalaciones de la Dirección del Registro Civil ubicado en la calle 11 Oriente 2003, colonia Azcarate, Puebla, Puebla.

Directora del Registro Civil de Puebla: Abogada María Elena Torres Machorro.

Entrevistado: Abogado Javier Ocelotl López.

Se agradece las facilidades prestadas por esta dependencia de gobierno, a cargo de la Abogada María Elena Torres Machorro, así como la información brindada por el Abogado Javier Ocelotl López.

1.- ¿Qué es el Registro Civil?

Se encuentra definido dentro del Código Civil de Puebla en el capítulo décimo tercero Actas del registro civil sección primera artículo 828, el cual indica que el Registro del Estado Civil es una institución de carácter público y de interés social, por medio de la cual el Estado de acuerdo con las leyes y reglamentos aplicables inscribe y da publicidad a los actos constitutivos o modificativos del estado civil de las personas.

2. ¿Qué trámites se pueden realizar en el Registro Civil?

Se manejan 32 servicios en cada uno de los juzgados, entre los cuales se encuentran los más importantes:

- Levantamiento de Actas de Nacimiento.
- Reconocimiento.
- Matrimonio.
- Defunciones.
- Presentación Matrimonial.
- Tutela.
- Inscripción de sentencias.
- Constancias de inexistencias de Actas de Matrimonio, de Nacimiento y de Defunción.

Y a través de la caja de finanzas con la que cuenta el Registro Civil se hace el pago de las "dispensas"³⁴ de publicaciones (permiso que se otorga para que una persona pueda contraer matrimonio el mismo día, porque la propia ley marca que deben pasar ocho días sin contar el día que se hace la presentación y el día que se hace el matrimonio).

Otro servicio que se realiza es el de búsqueda de actas.

Con base a lo que marca el Código Civil en su reciente modificación, la cual indica que en el Registro Civil se realicen todas las anotaciones marginales de las resoluciones judiciales, otro procedimiento es el de modificar actas, mismo que debe ser informado al director del Registro Civil, ya que se encuentra fundamentado dentro del artículo 841. Todo ello es de acuerdo a la ley de ingresos, es decir varía de precio.

3. ¿Para qué sirve el Acta de Nacimiento?

Es un documento que da la identidad ante la sociedad y jurídicamente permite establecer un vínculo, el Código Civil establece que a medida de que se realice una actividad del estado civil como el matrimonio o el divorcio, es obligación del juez del

Registro Civil que haga las anotaciones respectivas de ello en el Acta de Nacimiento, esto es como un control que se lleva dentro de dicho documento.

4. ¿Dónde se puede tramitar el Acta de Nacimiento?

Única y exclusivamente cuando es de primera parte tiene que ser en el juzgado del Registro Civil más cercano al domicilio de la persona, se pide como primer requisito un Certificado de Nacimiento el cual está regulado desde el 2008 como obligatorio por parte del sector salud a nivel nacional, es decir ninguna persona se puede registrar sino presenta o acredita dentro del Certificado de Nacimiento en el Registro Civil.

5. ¿Qué finalidad tiene el Certificado de Nacimiento?

Evitar el tráfico de menores, la doble identidad, sobre todo porque hay mucha delincuencia organizada que pretende inscribir y trasladar a menores nacidos en territorio mexicano a otros países.

6. ¿Con qué candados de seguridad cuentan las Actas de Nacimiento?

Con siete candados de seguridad, en el caso de Puebla, mismos que establece el Registro Nacional de Población (RENAPO) a nivel nacional, éstos candados de seguridad varían de acuerdo a cada Estado, porque cada uno realiza sus formas valoradas con diferente proveedor, se mencionan tres:

- Forma valorada con hologramas.
- Impresiones de trasluz que son los escudos del Estado de Puebla y de la República Mexicana.
- Papel especial para el Registro Civil.

7. ¿Qué grado de confianza tienen los candados de seguridad?

La ideología del Registro Nacional de Población es que cada año se implementen medidas de seguridad, pero se admite que la delincuencia organizada siempre da un paso adelante entonces sería inapropiado decir que los sistemas de seguridad con los que cuentan las actas de nacimiento sean de un cien por ciento las formas valoradas, pero si se tiene un aproximado del 75% de seguridad.

Los candados de seguridad cada año pueden ser aumentados o cambiados, para que sean distintos.

8. ¿Existe algún organismo o comisión que dictamine los candados de seguridad?

No, las establece el Registro Nacional de Población a través de un manual de procedimientos para el llenado y para la solicitud de formas valoradas donde establece tener un margen de los candados de seguridad, mismo que debe tener las formas del Registro Civil, y nosotros a través de la Secretaría de Finanzas donde generan una licitación con empresas que se dedican a la realización de formas valoradas y se les da los lineamientos que requerimos con los márgenes de seguridad que se necesitan.

9. ¿Por qué en algunos municipios de Puebla las Actas de Nacimiento se encuentran redactadas con máquina de escribir?

Puebla es el Estado con mayor cantidad de juzgados del Registro Civil con mayor número en el Estado, siendo un total de 744, Puebla es uno de los pocos Estados donde la carga de ser juez del Registro Civil se le otorga por ministerio de ley a los presidentes y filiales municipales, a las presidencias municipales se les otorga recursos a través de sus participaciones Estatales, pero en el caso

34 Permiso que autoriza a una persona el incumplimiento de una obligación o de lo ordenado por las leyes generales. Definición de 'dispensa' <http://es.thefreedictionary.com/dispensa>

de las juntas auxiliares no, entonces no tienen el presupuesto para poder adquirir material de cómputo y se tiene que realizar de manera mecánica.

En Puebla se manejan dos tipos de formatos:

- CIE que son los de sistema computarizado.
- Sistema tradicional y su llenado es de manera mecanográfica.

10. ¿Se proporciona algún tipo de capacitación al personal del Registro Civil?

Se cuenta con un departamento de Atención a juzgados que periódicamente realiza cursos de capacitación principalmente a los jueces del Registro Civil, secretarías y a los encargados para hacerles ver la normatividad y lineamientos por los cuales debe de trabajar el Registro del Estado Civil en Puebla, y los cursos se otorgan al inicio de cada trienio una vez y en los dos siguientes años son dos veces por cada semestre la capacitación, independientemente de ello, se tiene al servicio de los mismos las líneas telefónicas y correo electrónico para que se les pueda resolver alguna duda y mantener así una constante comunicación, una de las recomendaciones que se les emite es que sus formas valoradas sean única y exclusivamente para la utilización de su juzgado es decir no las pueden prestar a otra presidencia o juzgados, ni tampoco se las pueden vender a particulares para evitar la mala utilización de las formas del Registro Civil.

11. ¿Cómo detectan los presidentes municipales y jueces un documento falso?

A través de la capacitación y un curso masivo en forma de convocatoria para jueces conjuntamente con sus secretarías y encargados para recibir la capacitación que es permanente de la actualización del Registro Civil a nivel nacional para poder evitar el mal uso de las formas valoradas.

12. ¿En qué consiste esa capacitación?

En reformas al Código Civil, como es el caso de la aprobación del artículo 67, 931 y 875 bis, donde éste último indica que cuando un mexicano quiera registrar a un niño del extranjero ya no se solicite el Certificado de Nacimiento apostillado, aunque todavía está en discusión ya que con ello se detecta que se pueda dar el tráfico de infantes y robo de identidad porque entre menos requisitos se soliciten margen de error va a ser mayor.

13. Dentro de esta capacitación también se les informa ¿Qué hacer cuando se detecta una alteración y falsificación de las Actas de Nacimiento?

Si, tienen toda la colaboración y en ella participan instituciones como INEGI la cual aporta las estadísticas continuas, el IFE, mismo que se encarga también de dar de baja del padrón electoral a las personas mayores de 18 años que ya fallecieron, porque se detecta a veces que no son dadas de baja del padrón elector-

al y en épocas de elecciones llega a votar 'gente que ya falleció', también participa la PGJ la cual participa para indicarles a los jueces, secretarías y demás personal cuales son los elementos necesarios para presentarse ante un ministerio público para levantar una constancia de hechos por falsificación de documentos.

14. ¿Cómo se da cuenta el personal del Registro Civil que un documento está falsificado?

La primera acción que se realiza es:

1. El Registro del Estado Civil lleva una coordinación muy estrecha en los folios que se le venden a cada juzgado, y cuando nosotros emitimos un informe que contiene la documentación y las actuaciones de los diferentes jueces, presidencias municipales y juntas auxiliares al departamento de servicio a juzgados nos percatamos de que si es mayor de lo que entregaron a lo que compraron, entonces se indica que están infringiendo la normatividad y cabe la siguiente interrogante ¿de dónde pudieron haber salido esas formas valoradas que ocuparon si el Registro Civil no se las vendió?, si esto para nosotros es un control muy estrecho.

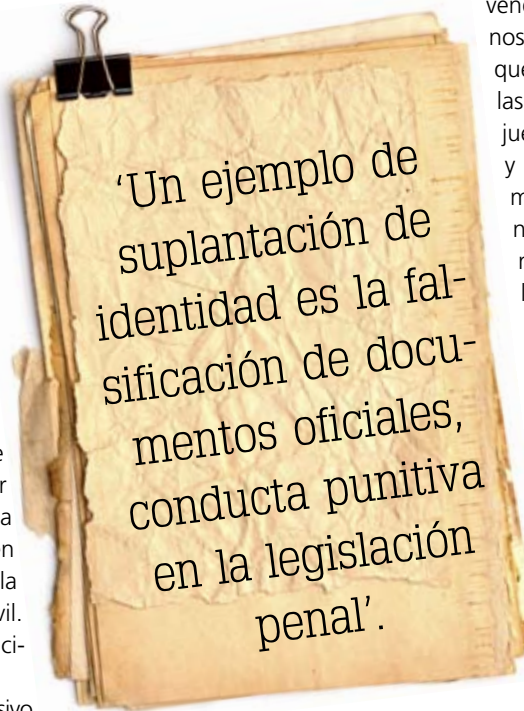
15. ¿Qué tecnologías utilizan en el Registro del Estado Civil?

Lo que se pretende es tener un programa y una base de datos para que el registro civil esté en red, esto es que si alguien solicita o pide un acta del registro civil, la misma base de datos que tenemos nosotros la puedan tener otras instituciones como la SEP, la PGR, la PGJ, el sector salud, registro nacional de población, es decir todas las Instituciones con las que tenemos que ver como Registro Civil.

16. ¿Cuál es el proceso que se tiene con respecto a la base de datos tecnológicos?

Estamos en un avance de sistematización de 744 juzgados llevamos en este momento 186 juzgados sistematizados, estamos hablando que es de un 20% pero la propuesta y la idea de nuestro señor gobernador a través de la secretaría general de gobierno es que antes de que termine el sexenio tengamos por lo menos la mitad de los Registros Civiles sistematizados, el margen de error para equivocarnos en las actas es menor.

17. ¿Dentro de la Dirección General del Registro Civil



tienen algún área donde esté especializada para detectar problemas como la falsificación y alteración o de alguna otra circunstancia que se presente?

Desgraciadamente no, nuestro reglamento no maneja como el de otros Estados de la República en cuanto al Registro Civil un departamento jurídico que sería lo ideal para que pudiera verificar todas estas circunstancias, y cuando hay algún delito se presenta la constancia ante la Procuraduría, lo que si hay que señalar es que ya está en proceso el nuevo proyecto de reglamento para Registro Civil de Puebla, donde comprenda un departamento jurídico, y un departamento de sistemas y de normatividad, para que todos en conjunto estemos hablando un mismo idioma en cuanto a colocar candados de seguridad en nuestras actas del Registro Civil.

18. ¿Se ha detectado algún caso de falsificación y alteración de Actas de Nacimiento?

Si, lamentablemente delegarle la función de ser juez del Registro Civil al presidente, como así nos lo marca nuestra constitución, eso nos conlleva a que cuando ellos llegan a ser jueces del Registro Civil por ministerio de ley mezclen una cuestión que es la política con la del servicio y se presenta mucho que por los compromisos que adquirieron ellos en campaña puedan a gente de su población sin pedirle requisitos ni llevar a cabo el trámite jurídico correcto extenderle actas con documentos apócrifos, Puebla a nivel nacional es el último Estado en presentar este tipo de delitos, pero se reconoce que si hay un porcentaje alto, no hay garantía de que en nuestro Estado, el Registro Civil sea seguro, pero tenemos que implementar ciertas normas para que se pueda alcanzar la meta.

19. ¿Cuáles son las acciones que realiza el Estado o el Registro del Estado Civil ante la falsificación y alteración de documentos?

Si la situación es a través de un Registro Civil, lo que se realiza es pedir un informe al juez de dicho registro, para que nosotros con estos elementos podamos realizar unas líneas de investigación de tipo administrativo y verificar donde se cometió esa acción delictiva.

20. ¿Qué acciones realiza el Registro del Estado Civil ante el robo de identidad?

Nosotros tenemos que estar estrechamente relacionados con la Procuraduría, pero hasta el momento no hemos manejado con ellos en coordinación algún caso de robo de identidad, esto no quiere decir que no suceda.

Sabemos que encontramos a través de la consulta Clave Única de Registro de Población (CURP) o la Clave de Registro de Identificación Personal (CRIP) se encuentra que dos personas pueden utilizar una misma acta con la diferencia de que a veces escriban algún dato incongruente como pudiera ser la fecha de nacimiento o lugar de nacimiento, con lo que nos damos cuenta es que coinciden los nombres de los padres.

-A nota de complemento-

El requisito indispensable para tramitar algún documento por ejemplo el IFE es el acta de nacimiento, esto lleva relación al robo de identidad ya que es muy fácil conseguir un acta de nacimiento y con eso solicitar el IFE y así ir maquillando los documentos para solicitar un crédito o alguien ponerlo en banca rota en sus cuentas bancarias, y a través de medios electrónicos.

Para realizar algún trámite de carácter administrativo se requiere un Acta de Nacimiento actualizada no mayor a cinco años, pero en esta situación aquí lo que debiera ser correcto es que se modifique el Código Civil, porque un acta que se solicitó hace cinco años tiene la misma validez que una del dos mil doce, y la ley indica que toda acta tiene fé pública, y es válida en cualquier lugar y es aquí donde se encuentra una contradicción por ello es que se debe hacer dicha reforma para que se actualicen todos los documentos y que no tengan más de un año de ser expedidos.



Abogado Javier Ocelotl López.

Fotografía número 38. Colectivo ARCIÓN, Instalaciones de la Dirección del Registro Civil ubicado en la calle 11 Oriente 2003, colonia Azcarate, Puebla, Puebla, 14 de febrero de 2012. Abogado Javier Ocelotl López.

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-criminalístico, su actividad científica coadyuva al desarrollo y consolidación del modelo educativo CLEU. "Investigar para la libertad". Representa su filosofía de batalla.



“ 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.

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.

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 profesionalista 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.

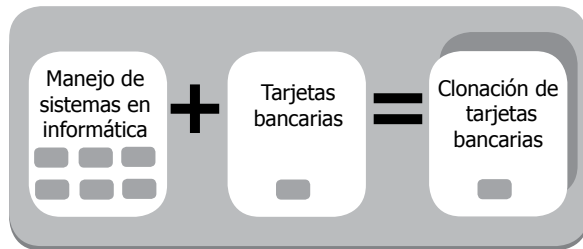
También es importante que las instituciones de gobierno nos puedan brindar recomendaciones que sirvan a la sociedad en el manejo de tarjetas bancarias, con la finalidad de no ser víctimas de alguna conducta, por el mal manejo de cuentas bancarias.

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 grupo 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.

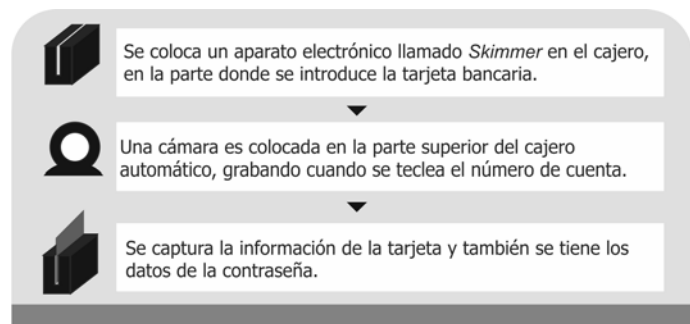
El '*Skimming*'¹, también conocido como clonación de tarjetas de crédito o débito, consiste en la duplicación de tarjetas de crédito o débito sin el consentimiento del dueño de la tarjeta. Los delincuentes que se dedican a esto utilizan diferentes tipos de dispositivos electrónicos que los ayudan a clonar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

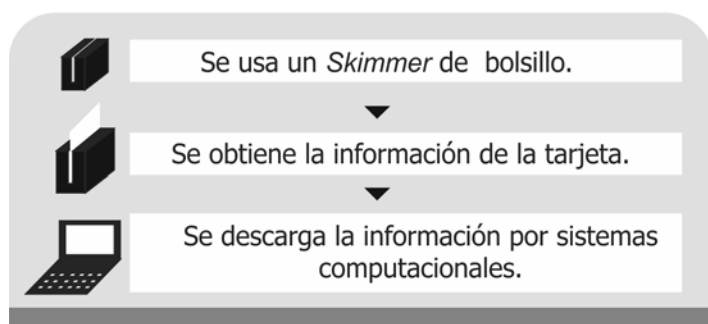
1 Data Security. Skimming: Clonación de tarjetas bancarias. 'skimming'. [En línea]. [Consultado: 06 de enero de 2012]. Disponible en la web: <http://www.wisedatasecurity.com/clonacion-tarjetas-credito.html>
 2 CNN expansión. ¿Cómo clonar tus tarjetas bancarias? 'skimmer'. [En línea]. [Consultado: 06 de enero de 2012]. Disponible en la web: <http://www.cnnexpansion.com/mi-dinero/2011/09/12/como-clonar-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 ARCIÓN, 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 víctima-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 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 manejo 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 ilícito⁸.

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:

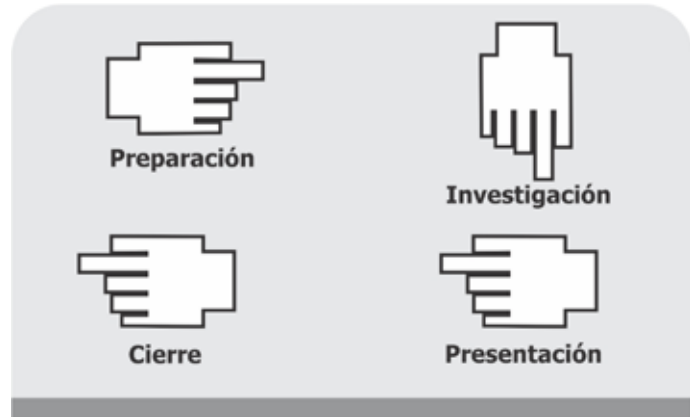
- Guantes de hule.
- Bolsas de plástico de diferentes tamaños.
- Cinta adhesiva.
- Etiquetas.
- Discos o dispositivos electrónicos de datos en estado virgen.
- Bolsas Faraday⁹.

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 forense¹⁰ informático-electrónico.

Las etapas de este proceso que el profesionalista 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):

**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 casos¹¹.

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 proceso¹².”

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

8 Ibidem., 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.

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 Procesoamiento (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), <i>Digital Versatile Disc</i> (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, <i>Iphone</i> , <i>Ipad</i> , 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 pérdida 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 alterar, 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 accedados 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 PDA¹³ 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:

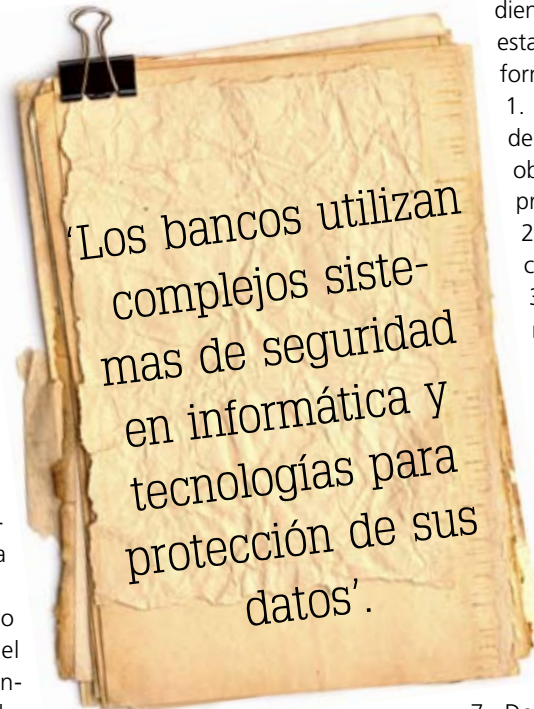
1. “Utilizar más de una herramienta de extracción de información, con el objetivo de dar mayores garantías al proceso.
2. Extraer la información acerca del correo electrónico.
3. Logs¹⁷ del sistema, ingresados al mismo.
4. Identificación de volatilidad de la información más volátil a la menos volátil.
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 Cãmpoli, 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 ARCIÓN, 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 delinquentes 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 varíe 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 víctima 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 gana 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 eviden-

cia 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 presentecadro 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 profesionalista 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**

	Intervención Consiste en que el Criminólogo-criminalista debe de ver que material debe utilizar en el lugar del hecho y prepararse para llegar al hecho.
	Observación Una vez que llega al lugar debe de observar y describir todo lo que encuentre en el lugar del hecho.
	Recolección Recolección 'fijación, levantamiento, embalaje y traslado' de los indicios que intervengan con la clonación de tarjetas bancarias.
	Interpretación Debe de dar un análisis a los indicios encontrados en el lugar, relacionar indicios-lugar, y poder determinar que sujetos fueron los que cometieron la conducta.
	Conclusión El Criminólogo-criminalista debe dar un resultado a través de un dictamen, medio de un análisis que determine la intervención de un individuo en una conducta antisocial.

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 ARCIÓN, 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 realizó 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, Sofoles²⁰, Sofomes²¹, 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 lleva 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 llegó 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 registró 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 Secretaría 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 Conducef 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 Conducef no hace, no interviene, ni cuestiona; toda la 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 Conducef, 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 Conducef 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 Conducef 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 Conducef 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 Conducef.

Medidas de seguridad que da la Conducef 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 Conducef. 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 Conducef 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 víctimas 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, pues 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 Cárpoli, 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 landuntis enduntis eium-tibus, soles re optureprem fugiamet ea sequo

OTRAS ÁREAS LABORALES PARA EL CRIMINÓLOGO-CRIMINALISTA

Ampliando el campo de acción

WAEI HIKAL

Maestría en Trabajo Social con orientación en proyectos sociales y
Licenciatura en Criminología por la Universidad Autónoma de Nuevo León.
Director de la revista Archivos de Criminología, Criminalística y Seguridad
Privada de la Sociedad Mexicana de Criminología capítulo Nuevo León, A.C.,
Página: <http://www.waelhikal.es.tl/>.
Correo electrónico: waelhikal@hotmail.com

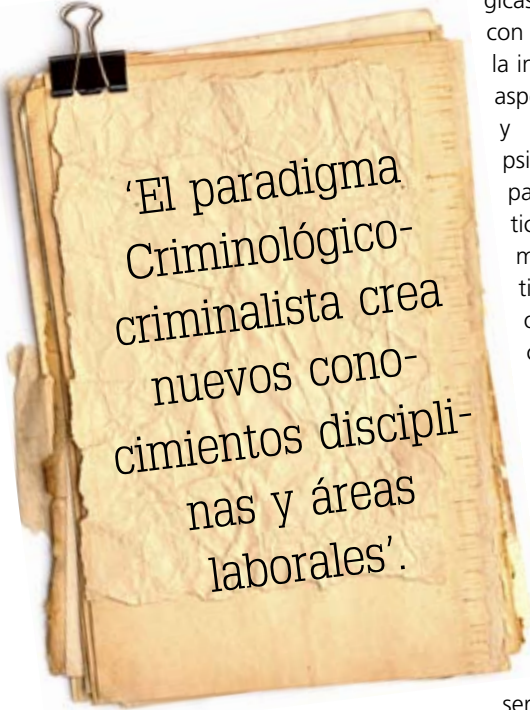
“La Licenciatura en Criminología-criminalística surge ante el crecimiento delictivo en México.”

RESUMEN

La Criminología nace con el objetivo de estudiar las causas antropológicas de la criminalidad, con el tiempo se agregó la interdisciplina con los aspectos sociológicos y psicológicos. Trágicamente a estas intenciones se le han interpuesto una serie de pensamientos y actos contrarios a los científicos: el morbo social que han provocado los medios de comunicación y la necrofilia de muchos receptores ha venido a torcer la perspectiva de la Criminología y Criminalística. De estos hechos puede ser motivo del porqué no se tiene una policía adecuada, leyes con objetivos inalcanzables, políticas ineficientes, programas preventivos inestables, tratamiento penitenciario deficiente y sobre todo falta de credibilidad científica y laborar Criminológica-criminalística. La visión del Criminólogo-criminalista debe trascender y orientarse al aspecto científico de la administración de justicia, prevención del delito y tratamiento del criminal, así como suministrar información al área científica-académica.

INTRODUCCIÓN

La Licenciatura en Criminología y Criminalística nació por una ‘necesidad’, misma que fue por la criminalidad que se ha tenido e incrementado en el país y el mundo entero, y la que ha llevado a que se abran las carreras en diversos Estados y otros países, una carrera surge para darle solución a determinados fenómenos en la sociedad. Actualmente, la criminalidad se ha desbordado, si bien, Rafael Garófalo señalaba que el delito es evolutivo y que los más antiguos (el delito natural) eran el robo y el homicidio, ahora, se tienen modalidades criminales muy avanzadas, lo que fuerza la modernización en las investigaciones criminales, el aumento de policías, entre otras, este motivo ha llevado a que se impartan las enseñanzas de la investigación criminal en las procuradurías de justicia, secretarías de seguridad, escuelas, centros de investigación, materias específicas dentro de los planes de estudio de otras carreras; por ejemplo, Derecho, Psicología, etcétera.



'El paradigma Criminológico-criminalista crea nuevos conocimientos disciplinas y áreas laborales'.

La Criminología nace con el objetivo de estudiar las causas antropológicas de la criminalidad, con el tiempo se agregó la interdisciplina con los aspectos sociológicos y posteriormente los psicológicos; por otra parte, la Criminalística, nace para determinar si un hecho tiene relación penal o no, su reconstrucción, la mecánica con la que sucedió y determinar la participación e interacción de determinados actores en el mismo.

Trágicamente a estas intenciones se le han interpuesto una serie de pensamientos

y actos contrarios a los científicos y a los políticos criminológicos, el morbo social que han provocado los medios de comunicación y la necrofilia de muchos receptores ha venido a torcer la perspectiva de la Criminología y la Criminalística. La sociedad percibe a éstas como ciencia que estudian los muertos o que se estudian los crímenes con placer patológico, así mismo, se ha perdido el objetivo de la Política Criminológica, pues en su mayoría los Legisladores sienten un hueco científico para cubrir dicho aspecto. Mismo desorden que lleve a los aspirantes a estudiar una carrera universitaria a ingresar a la carrera de Criminología con la intención de manipular armas de fuego, intervenir en asuntos médicos forenses, en hechos de sangre, en lugar de orientarse al aspecto científico de la investigación criminal y la prevención del delito.

De todos estos hechos puede ser motivo del porqué no se tiene una policía adecuada, leyes un tanto irreales o con objetivos inalcanzables, políticas ineficientes, programas preventivos inestables, tratamiento penitenciario deficiente y sobre todo falta de credibilidad científica y laborar criminológica. La visión del Criminólogo debe trascender de lo que los medios de comunicación y el desinterés político han accidentado, habrá que lograr crecimiento científico con miras a la Criminología Aplicada con sus áreas Clínica y Política Criminológica.

RESEÑA LABORAL

Se abre el presente con una acertada opinión de Carlos Elbert:

En este acotado espacio debo hablar de cuestiones que deben ser respondidas en cientos, miles de hojas. Sin embargo, recuerdo que durante el siglo ya escribieron millones de textos sobre el tema "Criminología", de modo que se impone saber

qué ha ocurrido con semejante esfuerzo, reconocer cómo estamos y aventurar qué sucederá en el inminente siglo XXI. No me mueve en este esfuerzo más que una profunda preocupación, ciertamente escéptica, sobre el destino inmediato de la humanidad¹.

Con el arribo de una nueva disciplina (Criminología-criminalística) hubo que buscar dónde aplicar dichos conocimientos generados, posterior a su autenticidad científica y aplicativa, la complejidad de los fenómenos sociales da lugar a la creación de nuevos conocimientos y de nuevas áreas laborales, para lo cual se tienen que crear especializaciones en determinadas carreras, o incluso crear nuevas. Dicho es el caso de la Criminología y Criminalística alrededor del mundo, se tiene la idea.

Con los años, se ha creado, desarrollado y reproducido la licenciatura en Criminología y/o Criminalística otros países, las maestrías e incluso los doctorados, países como España, Italia, Bélgica, Estados Unidos de América, Brasil, Canadá, Argentina, Chile, Corea, Japón, India, Alemania, entre tantos, han logrado una evolución extraordinaria en los estudios criminológicos, se han desarrollado maestrías internacionales en Criminología, maestrías internacionales en justicia criminal, en Derecho Humanos internacionales, Doctorados en Filosofía (Ph.D) con orientación en Criminología, Victimología, entre otras, así como licenciaturas en Artes de Criminología, en Justicia Criminal y en Criminalística. Se han desarrollado institutos, departamentos, facultades y demás encargados de la difusión de la Criminología².

Con la tradición que legó César Lombroso y Hans Gross con las aplicaciones de las ciencias correspondientes, se pudo desarrollar el área laboral de estos recién nacientes Criminólogos-criminalistas; así, su campo de desempeño sería: en penitenciarias con los estudios integrales para conocer las causas de la criminalidad, su tratamiento en algunas épocas la medición de las partes del cuerpo para confirmar su física criminal (teoría atávica); de estos hechos, hacer las políticas criminológicas para evitar la criminalidad. Por parte de la Criminalística su intervención encuentra lugar en todo hecho presuntamente criminal.

En México, existen tantas dependencias de gobierno que sería tal vez imposible hablar con certeza de a quien le corresponde la aplicación de la Criminología y Criminalística; de manera general, se puede identificar que son: las secretarías de seguridad las que albergan los reclusorios, y procuradurías de justicia las que llevan a cabo la investigación de los delitos; por ello, en cada Estado y Municipio de la República Mexicana en el que existen dichas dependencias, la labor de los profesionistas en mención se hace presente.

1 Elbert, Carlos Alberto. Bases para un pensamiento criminológico del siglo XXI. La Criminología del siglo XXI en América Latina, Rubinzal-Culzoni, Argentina, 1999, p. 221.

2 Cfr. Sociedad Mexicana de Criminología. Capítulo Nuevo León, A.C. dirección en Internet: <http://somecrimn.es.tl/Links.html>; y UNICRI, Directorio Mundial de Instituciones Criminológicas, Italia, 2009.

No hay duda que la criminalidad es una fuente de trabajo, y por fortuna o por desgracia, existen infinidad de órganos que su actividad primordial es por el crimen, su prevención y tratamiento, así por mencionar algunas y con el riesgo que se desatine al nombre correcto por los 'cambios políticos inmediatos', la ahora Policía Federal Ministerial, antes Agencia Federal de Investigación (AFI), las Agencias Estatales de Investigación (AEI), la Procuraduría General de la República (PGR): www.pgr.gob.mx, las Procuradurías Generales de Justicia (PGJ) de los Estados, el Centro de Investigación y Seguridad Nacional (CISEN): www.cisen.gob.mx, la Secretaría de Seguridad Federal (SSPF): www.ssp.gob.mx, las Secretarías de Seguridad Estatales (SSP) y las municipales (SSPM), Comisiones de Derechos Humanos nacional y estatales: www.cndh.org.mx, esto para el caso de México. En todas las anteriores, hay cabida para el Criminólogo-criminalista, pero esto es lo común que ya se sabe, la intención del presente es precisamente ampliar esa perspectiva laboral, para ello, se pasa a continuación.

Área internacional

Naciones Unidas se divide en: 1) Asamblea General, 2) Secretaría, 3) Consejo de Seguridad, 4) Consejo Económico y Social, 5) Administración y 6) Programas, Fondos y organismos. Cada Oficina tiene un conjunto de actividades que pretenden homologar los criterios de estudio y atención a determinados fenómenos, pero siendo tan compleja la humanidad y su transformación, así como su evolución, además de la necesidad de cubrir más aspectos de la vida, más países se han unido (y otros retirado del Sistema), y se han creado más Oficinas y proyectos con temas específicos, así se tienen alrededor del mundo las siguientes Oficinas (de manera descriptivas más no limitativas): del Trabajo; de la Niñez; de la Educación y Ciencia; de la Droga y el Delito, el Banco Mundial; Institutos de investigaciones (en desarrollo, economía, criminalidad, justicia), Universidad de Naciones Unidas; de Derechos Humanos, de apoyo a proyectos, de Aviación, del Mar; de la Agricultura; asuntos Espaciales, asuntos atómicos, en algunos países en específico, entre otras.

La Organización de las Naciones Unidas es un foro o lugar de reunión que prácticamente incluye a todas las naciones del mundo y proporcionan el mecanismo que ayuda a encontrar soluciones a las controversias o problemas entre países y a adoptar medidas en relación con casi todas las cuestiones que interesan a la humanidad. Estas cuestiones son analizadas de acuerdo a una serie de propósitos y principios establecidos en el capítulo 1 de la "Carta de las Naciones Unidas", teniendo como finalidades³:

1. Preservar a las nuevas generaciones del flagelo de la guerra;
2. Reafirmar la fe en los Derechos fundamentales del hombre;
3. Crear condiciones para mantener la justicia y el respeto a los tratados internacionales;
4. Promover el progreso social y elevar el nivel de vida; y
5. Si bien algunas veces se las describe como un 'parlamento de naciones', las Naciones Unidas no son ni una entidad por encima de los Estados ni un gobierno de gobiernos. No cuentan con un ejército propio y no recaudan impuestos.

Las Naciones Unidas desempeñan un papel criminológico y preventivo enfocado a las siguientes acciones:

1. Reducir las tensiones internacionales; es decir, guerras que pueden ser consideradas como uno de los mayores actos antisociales y criminales de la humanidad después del crimen organizado. Esta deja como consecuencias una enorme cantidad de conductas antisociales y criminales como los son entre otros: violaciones a mujeres, niños, soldados, violación de Derechos Humanos, daños psicológicos y físicos irreversibles. Daños en las vías y medios de comunicación, en hogares, escuelas, dejan en un estado de pobreza extrema que da origen a robos y conductas violentas propias de la sobrevivencia (la ley de que solo los más aptos sobreviven), receso económico y social.
2. Prevenir conflictos entre las Naciones, que ocasiona conflictos como los mexicanos que buscan mayores oportunidades en EUA a falta de desarrollo económico en México. Cabe aclarar que México aun no se encuentra en grave estado comparado con otros países en grandes conflictos en los que se llevan a cabo muertes a todo ser humano y de cualquier edad;
3. Poner fin a las hostilidades que ya se hayan producido;
4. Legislar sobre el medio ambiente, el espacio ultraterrestre y los fondos marinos;
5. Erradicar enfermedades;
6. Incrementar la producción de alimentos, lo que en gran medida previene el robo o el homicidio producido por la lucha de la sobrevivencia;
7. Atender y proteger a los refugiados;
8. Luchar contra el analfabetismo pues sabemos que la falta de educación es un factor criminógeno, que limita a las personas a tener un sano desarrollo social y a ser productivos en la vida, retomando al conductista Skinner, quien señalaba que para alejarse de los malos hábitos se debían tener buenos reforzadores de conducta como son simplemente los libros. Así también lo identificaba Beccaria que la educación era factor causante de la criminalidad, pero sin olvidar la criminalidad dorada o de cuello blanco...;
9. Reaccionar rápidamente en situaciones de desastres naturales, que finalmente muchas veces son provocados por actos criminales;
10. Establecer normas mundiales en materia de Derechos Humanos, atención a víctimas, prevención del delito, de las drogas, de enfermedades, de desarrollo social como reductor de factores criminógenos y la prevención del delito, apoyo a grupos vulnerables, e infinidad de acciones que actualmente realiza Naciones Unidas que tiene

3 Véase Centro de Información para México, Cuba y República Dominicana, Manual de Modelos de Naciones Unidas, Centro de Información para México, Cuba y República Dominicana, México, Cuba y República Dominicana, 2008, p.

siempre como ideología rectora 'la prevención del delito y de las conductas antisociales', pero trasciende de ello al estudiar los factores criminógenos y se extiende a actividades de interés espacial, de enfermedades y más, y

11. Proteger y promover los derechos de todas las personas, seres vivos y situaciones de interés humano.

Red de las Naciones Unidas de institutos, centros y universidades para la prevención del delito

El Programa de la Red de las Naciones Unidas de Prevención del Delito y Justicia Criminal consiste en la Oficina de las Naciones Unidas contra la Droga y el Delito y un número de Institutos regionales e interregionales alrededor del mundo, así como Centros especializados. La Red se ha desarrollado para asistir a la comunidad internacional en el fortalecimiento y cooperación el área crucial del crimen y la justicia criminal. Sus componentes proveen de una variedad de servicios, incluyen intercambio de información, investigación, entrenamiento y educación pública⁴. En las siguientes líneas se enlistan algunos de éstos, aclarando que solo se describe de manera breve su función y ubicación, así como su sitio y contacto, esto por cuestiones de espacio, si el lector desea ampliar su conocimiento se recomienda ampliamente visite las webs que se muestran.

La **Universidad Naif Arab para las Ciencias de la Seguridad (NAUSS)** es una institución intergubernamental, que opera bajo el financiamiento del Consejo Interior de Ministerios árabes. Fue establecido para cubrir las necesidades de las agencias de seguridad y refuerzo desde una perspectiva académica en investigaciones de seguridad, además de ofrecer cursos de posgrado y cursos de preparación corta. Su página: www.nauss.edu.sa.

El **Instituto Interregional de las Naciones Unidas para la Investigación sobre el Crimen y la Justicia (UNICRI)**, fue creado en 1968 con la finalidad de asistir a nivel intermunicipal, gubernamental y no gubernamental, en la formulación e implementación de las Políticas Criminológicas y la justicia criminal. Dentro de los objetivos principales del Instituto se encuentran el desarrollo de seguridad avanzada, servicios legales y construcción y mantenimiento de la paz. Sus actividades se concentran en estudios sobre la corrupción, seguridad gubernamental y crimen organizado (en particular al tráfico de humanos y de drogas).

El Centro de Documentación/Información del Instituto alberga investigaciones, cursos. La Librería incluye trabajos de prevención del delito, justicia criminal, terrorismo y abuso de drogas. Guarda alrededor de 20,000 monografías, revistas, anuarios. Además de esto se encuentra el Directorio Mundial de Instituciones Criminológicas: www.unicri.it/wwwk/documentation/worlddir.php y el Calendario Mundial de Eventos Criminológicos: www.crimeday.net/month.php?user=UNICRI#unicri. Su página web es: www.unicri.it.

El **Instituto de las Naciones Unidas para Asia y Extremo Oriente para la Prevención del Crimen y el Tratamiento de los**

Delincuentes (UNAFEI), fue establecido en 1962 con el objetivo de promover el desarrollo en materia de justicia criminal y cooperación mutua entre Asia y la Región Pacífica. Las actividades del Instituto se enfocan a la realización de cursos y seminarios para los administradores de justicia, investigadores y clínicos penitenciarios. Así mismo, promueve eventos y actividades multinacionales. Su página: www.unafei.or.jp.

El **Instituto Latinoamericano de las Naciones Unidas para la Prevención del Delito y el Tratamiento de los Delincuentes (ILANUD)** fue establecido en la ciudad de San José, Costa Rica en 1975. El Acuerdo de Creación del Instituto establece en su artículo primero inciso 2 que el objetivo principal del Instituto es colaborar con los gobiernos en el desarrollo económico y social equilibrado de los países de América Latina y el Caribe, mediante la formulación e incorporación en los planes nacionales de desarrollo, de políticas e instrumentos de acción adecuados en el área de la prevención del delito y la justicia penal. Para alcanzar su objetivo principal, el Instituto lleva a cabo una serie de actividades. Su página en Costa Rica: www.ilanud.or.cr, y en Brasil: www.ilanud.org.br.

El **Instituto Europeo para el Control y la Prevención del Delito afiliado a Naciones Unidas (HEUNI)**, fue establecido en 1987 por Acuerdo entre Naciones Unidas y el Gobierno de Finlandia. El objetivo del Instituto es promover el intercambio de información relativa a la prevención del delito entre los Estados de la Unión Europea. Los temas que cubre son crimen organizado, violencia contra la mujer, tráfico de órganos, correccionales y sistema jurídico europeo. Por otra parte, analiza los cuestionarios que se utilizan en Europa y Norteamérica para diagnosticar las tendencias en el contexto criminal y la justicia. Su página: www.heuni.fi.

El **Instituto Africano de las Naciones Unidas para la Prevención del Crimen y el Tratamiento a los Delincuentes (UNAFRI)**, es una organismo gubernamental cuyos objetivos son los de promover la cooperación activa de los Gobiernos, las Instituciones académicas, las OGN's y de los expertos en las áreas de prevención del delito y la justicia criminal. En su mandato por los Estados Africanos, se determina que su labor es la de movilizar gente y administrar lo necesario para el desarrollo social, y reforzar las prevención del crimen. Además realiza investigaciones en políticas públicas, entrenamientos, documentación e información, así como emitir recomendaciones a los gobiernos. Su página: www.unafri.or.ug.

El **Instituto Australiano de Criminología (AIC)**, es el Centro Nacional Australiano para el análisis y la difusión de la información criminológica. Responde a las necesidades del Gobierno Australiano y de la comunidad con respecto a las políticas en justicia criminal y prevención del crimen, y provee información a nivel nacional. Su página: www.aic.gov.au.

4 V. "Red de Institutos de las Naciones Unidas para la Prevención del Delito y la Justicia Criminal", Oficina de las Naciones Unidas contra la Droga y el Delito, dirección en Internet: www.unodc.org/unodc/en/commissions/CCPCJ/institutes.html, Italia, 2009.

El Centro Internacional para la Reforma de la Ley y Política Criminal (ICCLR&CJP), fue fundado y formalmente adherido a Naciones Unidas en 1991. La misión del Centro es promover la Ley, los Derechos Humanos, la Democracia y el buen Gobierno, contribuyendo de manera local, nacional e internacional en iniciativas para reformar la ley y la administración de justicia. Se enfoca en la cooperación técnica, la investigación, el entrenamiento, y las Políticas de Justicia y prevención. Su página: www.icclr.law.ubc.ca.

El Instituto Internacional de Altos Estudios en Ciencia Criminal (ISISC), fue fundado en 1972, se especializa en diseñar e implementar los Derechos Humanos, la Ley, justicia e implementar programas alrededor del mundo, con especial atención en los países árabes y musulmanes. Conduce de manera escolar investigaciones y ha producido una gran cantidad de publicaciones sobre Derecho Humanos, Derecho Internacional, y conflictos de justicia. Ha mantenido firmemente los estándares y normas internacionales de Naciones Unidas respecto la justicia. Su página: www.isisc.org.

El Instituto Nacional de Justicia (NIJ), es la Agencia de investigación, desarrollo y evaluación del Departamento de Justicia de los Estados Unidos de América. La misión del Instituto es la investigación científica, desarrollo y evaluación de la administración de justicia y la seguridad pública. El Instituto promueve nuevas herramientas en justicia criminal. Se enfoca en asuntos de terrorismo, crimen organizado, corrupción, tráfico de personas, Derecho Internacional ciberdelitos y temas emergentes. Su página: www.ojp.usdoj.gov/nij.

El Instituto Raoul Wallenberg para los Derechos Humanos (RWI), es una institución académica fundada en 1984 en la Facultad de Derecho en la Universidad Lund de Suecia, que promueve el respeto a los Derechos Humanos y el Derecho Humanitario a través de la investigación, la educación académica. Participa en diversas redes nórdicas, europeas y con otras instituciones internacionales, además de ser miembro de la Red de Institutos de Naciones Unidas. Su página: www.rwi.lu.se.

El Consejo Internacional Científico y Profesional (ISPAC), fue fundado en 1991, coloca especial énfasis en fortalecer las contribuciones de instituciones científicas y profesionales, así como de ONG's, para el desarrollo de material para la prevención del delito y la justicia criminal. Al igual que los demás institutos provee de asistencia técnica, entrenamiento,

educación, investigación y monitoreo del crimen. Además de celebrar una Convención Anual sobre determinados temas. Su página: www.ispac-italy.org.

El Centro Internacional para la Prevención del Delito (ICPC), fue fundado en 1994, y funciona como un foro internacional para los Gobiernos, autoridades locales, agencias públicas, instituciones especializadas y ONG's, para intercambiar experiencias, crear conocimientos, políticas y programas en prevención del crimen y comunidades seguras. Asiste a las Ciudades y los Países para reducir la delincuencia, la violencia y la inseguridad. Su página: www.crime-prevention-intl.org.

El Instituto para los Estudios de la Seguridad (ISS), es un tanque de pensamiento cuyo trabajo es exclusivo para África, tiene Oficinas en Addis Ababa, Cape Town, Nairobi y su central en Pretoria. Su misión es conceptualizar, informar y mantener un debate sobre la seguridad humana en África para dar soporte y promover Políticas y decisiones a cualquier nivel. Su forma de trabajo es el desarrollo sustentable, los Derechos Humanos, la Ley, la Democracia y la Seguridad. Su página: www.issafrica.org.

El Instituto Coreano de Criminología (KIC), es la única Agencia Nacional de Investigación Criminal y Justicia Criminal en la República de Corea. Considerando los cambios rápidos en la criminalidad, el Instituto conduce de manera comprensiva e interdisciplinaria la investigación en cuanto a reforma de la ley, el fortalecimiento de ésta, el crimen organizado internacional, el tráfico de humanos, las drogas y la corrupción, la tecnología relacionada con delitos, cibercrimenes. Con más de 30 investigadores en Derecho, Sociología, Psicología y Criminología, el Instituto publica más de 50 investigaciones cada año, además el Instituto publica el Resumen Criminal Coreano, la revista de mayor difusión en Corea. Su página: www.KIC.re.kr.



El Centro Internacional para el Resarcimiento (ICAR) del Instituto Basel de Gobernanza, fue creado en el 2006, en el 2007, se unió a Naciones Unidas y es uno de sus últimos miembros. El Instituto es un tanque de pensamiento dedicado a la investigación, política de desarrollo, consultoría y capacitación en áreas corporativas, así como en Gobierno. Se enfoca principalmente para el resarcimiento en los casos de crímenes, así como otros temas como el crimen organizado. Su página: www.baselgovernance.org.

La **Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD)**, anteriormente denominada **Oficina de Fiscalización de Drogas y Prevención del Delito**, fue creada en 1997 con el fin de reforzar la capacidad de las Naciones Unidas para abordar las cuestiones de la fiscalización de drogas, la prevención del delito y el terrorismo internacional, que están relacionadas entre sí. La Oficina está integrada por un programa que se ocupa de los temas relacionados con las drogas y otro con el delito.

Ofrece asesoramiento técnico a los Estados Miembros sobre temas relacionados con la fiscalización de drogas; prepara estadísticas sobre el consumo y la incautación de drogas y las tendencias en esa esfera y ayuda a redactar textos legislativos y a capacitar a funcionarios judiciales. El programa también se ocupa de informar a la opinión pública mundial sobre los peligros del consumo de drogas y de reforzar las iniciativas internacionales contra la producción, y el tráfico de drogas y los delitos conexos. La Oficina de las Naciones Unidas contra la Droga y el Delito tiene en una red de 22 oficinas repartidas por todo el mundo y dos oficinas de enlace ubicadas en Nueva York y Bruselas. Su página: www.unodc.org.

Además de la Organización de los Estados Americanos (OEA): www.oas.org/es.

El área internacional ha sido casi en su totalidad olvidada y no contemplada por el Criminólogo-criminalista, en los congresos casi siempre suele haber algún ponente, o en los libros, clases u otros, resalta el aspecto internacional, que suele percibirse como algo alejado e inalcanzable, no lo es del todo, tampoco lo será fácil, Naciones Unidas en sus diversas páginas electrónicas ofrecen convocatorias con los requisitos para ingresar, si el alumno o egresado de Criminología-criminalística se prepara con tiempo y en lo adecuado, sin duda podrá tener una silla en las agencias especializadas de las Naciones Unidas.

Área legislativa

El Criminólogo-criminalista debe tener participación en la política electoral -es común escuchar el relato de estos profesionistas argumentando que lo 'político' no es lo de ellos, entonces cómo se pretende lograr ese liderazgo de dirección en las diversas áreas que corresponden. El involucrarse a la política no implica necesariamente ser funcionario público de más alto nivel jerárquico, no se debe confundir el ser presidente municipal o gobernador,

con lograr ser secretario de seguridad, subsecretario, director, coordinador, jefe, entre tantos más puestos, si bien, un currículo amplio a veces no reluce entre los políticos, sí hay que cambiar ese aspecto en lo que nos corresponda-

Por otro lado se tienen otras áreas de acción como las Senadurías, Diputaciones locales, federales y asambleístas del Distrito Federal por ejemplo, también, los síndicos y regidores, asesores de las cámaras alta y baja, de seguridad, entre otros. En el relato común entre el pueblo se llega a la reflexión de que las cosas "deberían de cambiar", pero para que ese cambio surja se debe participar en él y no permanecer como espectador externo.

El área legislativa ofrece mucho campo laboral para el Criminólogo-criminalista, no se llegará rápidamente al ser recién egresado, pero si con la constancia desde que se es estudiante y haciendo el adecuado uso de la diplomacia, retórica, 'ética' y liderazgo.

Seguridad privada

Actualmente un área en la que se identifica a los profesionistas es la seguridad privada, área que en sus inicios y en el presente ocupan ingenieros, juristas o psicólogos, incluso médicos, ello, por el motivo de que ciertas zonas en los espacios laborales requieren de ciertas especialidades científicas; por ejemplo, los riesgos químicos, de salud, psicológicos, ambientales, entre otros. En el momento los licenciados y/o maestros en Criminología-criminalística tienen conocimientos de Psicología, Derecho Penal, Psiquiatría, Sociología, Policiología, entre otras disciplinas que le han permitido introducirse en dicho mercado. Las lagunas que le pueden restar labor son la falta de conocimientos en análisis de riesgos químicos, incendio, explosivos, protección a ejecutivos, emergencia médica, entre otras.

Por otra parte con los conocimientos que la carrera proporciona, se pueden identificar diversos problemas, el Derecho Penal Especial, permite conocer de los delitos tipificados en el código penal de aplicación correspondiente para determinar qué conducta es o no delictuosa y la penalidad correspondiente, el Derecho Procesal Penal, permite conocer qué procedimientos deben ocurrir para la denuncia o querrela, aportar evidencias y llegar al arresto o la medicación. La Criminalística permite hacer una identificación y reconstrucción de un hecho delictuoso (o no), resguardar las evidencias, la escena y la protección de indicios. La Psicología permitirá conocer de los trastornos de personalidad que hagan que una persona tenga cierto tipo de conducta, sus motivos, su historia de vida, sus posibles causas para cometer alguna conducta criminal o antisocial, no se limita solo a estas ciencias, para cada una que conforma su plan de estudios podrá adquirir conocimientos que le permitan hacer una prevención de la criminalidad dentro de un ámbito privado, comúnmente llamada prevención de pérdidas o prevención de riesgos.

El problema de la seguridad privada en algunas ocasiones es que mantienen en secreto los hechos que dentro de la corporación ocurren, les falta la cultura de la denuncia y la colaboración con el ministerio público, la solución en la mayoría de las veces es despedir al empleado en el caso de -robo hormiga- o algún otro delito menor y queda exento de denuncia, en otros casos se realiza la denuncia pero con poca colaboración a menos que sea un delito grave. Esto incrementa la cifra oculta de la criminalidad.

Área científica

Otra área es: el desarrollo científico y tecnológico, a manera de investigar e innovar las formas de tratamiento penitenciario, la clínica criminológica, Política Criminológica, técnicas periciales, entre otras, en forma de plasmar nuevos conocimientos en artículos, libros, capítulos en libros, conferencias, eventos de divulgación, mejorando y fortaleciendo la educación escolar, posgrados de calidad nacional e internacional, entre otros. Se debe estar en posibilidad de incorporar especialistas en el área criminológica al Sistema Nacional de Investigadores del Consejo Nacional de Ciencia y Tecnología (CONACYT), cuyo prestigio, alcances y retribución es atractivo, la especialización a través de estudios de posgrado nacional o internacional, las investigaciones científicas y demás se debe en México al CONACYT: www.conacyt.gob.mx.

Importante, sobre este tema es conocer las revistas científicas más conocidas y comercializadas en México que se encargan de la divulgación criminológica y criminalística, a saber: Archivos de Criminología, Criminalística y Seguridad Privada de la Sociedad Mexicana de Criminología capítulo Nuevo León: www.somecrimnl.es.tl, Iter Criminis. Revista de ciencias penales del Instituto Nacional de Ciencias Penales www.inacipe.gob.mx, Criminogénesis. Revista Especializada en Criminología y Derecho Penal de Alejandro Carlos Espinosa: www.criminogenesis.com y la más antigua Criminalia de la Academia Mexicana de Ciencias Penales. Entre otras están Revista Sistema Penal del Instituto de Formación Profesional: www.ifp.pgjdf.gob.mx y Visión Criminológica-criminalística del Colegio Libre de Estudios Universitarios: www.cleu.com.mx.

Los Criminólogos-criminalistas (de licenciatura, maestría y escasos 4 doctorados⁵ -que hasta la fecha no se ha identificado algún criminólogo que lleve esta secuencia; es decir, hay juristas-criminólogos, psicólogos-criminólogos, médicos-criminólogos, pero no

criminólogos-criminólogos, el peor de los casos es que los criminólogos de licenciatura estudian una maestría y no se dedican a la sistematización científica de ideas-) deben especializarse en el desarrollo científico y tecnológico, a manera de investigar e innovar los conocimientos. La investigación científica es una actividad orientada a la obtención de nuevos conocimientos y a través de ésta dar solución a problemas o interrogantes de carácter científico.

Una investigación se identifica por ser un proceso con las siguientes características:

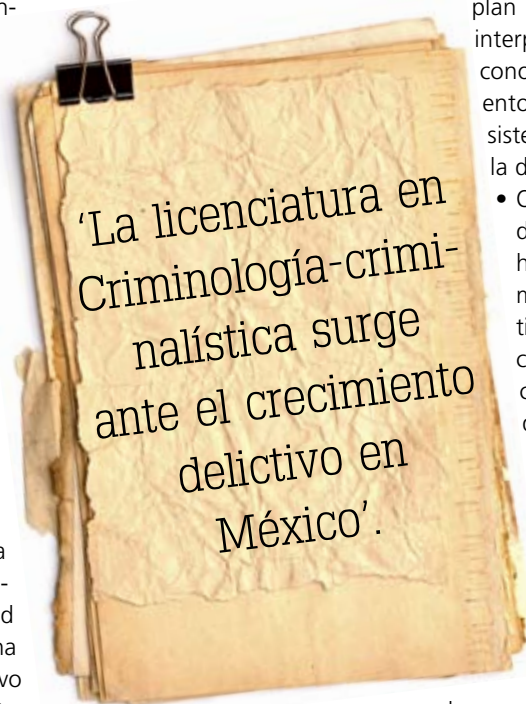
- Sistemática: a partir de la formulación de una hipótesis u objetivo de trabajo, se recogen datos según un plan preestablecido que, una vez analizados e interpretados, modificarán o añadirán nuevos conocimientos a los ya existentes, iniciándose entonces un nuevo ciclo de investigación. La sistemática empleada en una investigación es la del método científico;
- Organizada: todos los miembros de un equipo de investigación deben conocer lo que deben hacer durante todo el estudio, aplicando las mismas definiciones y criterios a todos los participantes y actuando de forma idéntica ante cualquier duda. Para conseguirlo, es imprescindible escribir un protocolo de investigación donde se especifiquen todos los detalles relacionados con el estudio, y
- Objetiva: las conclusiones obtenidas del estudio no se basan en impresiones subjetivas, sino en hechos que se han observado y medido, y que en su interpretación se evita cualquier prejuicio que los responsables del estudio pudieran hacer⁶.

La divulgación científica puede entenderse como el conjunto de actividades que interpretan y hacen accesible el conocimiento científico al público general; es decir, a todas aquellas labores que llevan el conocimiento científico a las personas interesadas en entender o informarse de ese tipo de conocimiento. La divulgación pone su interés no sólo en los descubrimientos científicos del momento, sino también en teorías más o menos bien establecidas o aceptadas socialmente o incluso en campos enteros del conocimiento científico.

También la divulgación científica mal practicada puede ser engañosa: algunas obras de divulgación son escritas por gente que no es experta en el tema que dan a conocer, otras por personas parcializadas. Por desgracia, suele resultar difícil para una persona sin excesiva formación el identificar los artículos o documentales fraudulentos.

De acuerdo con el CONACYT, la divulgación tiene como objetivos:

- Divulgar en la sociedad la ciencia y tecnología.
- Fomentar la tecnología local y adaptarla a la tecnología extranjera.
- Innovar en la generación, desarrollo, asimilación y aplicación del conocimiento de ciencia y tecnología.



⁵ “Doctorado en Ciencias Penales y Política Criminal” del Instituto Nacional de Ciencias Penales; “Doctorado en Ciencias Forenses” del Instituto Zacatecano de Estudios Universitario; “Doctorado en Criminología y Ciencias Forenses” del Centro de Estudios Avanzados de Veracruz, y “Doctorado en Criminología” de la Universidad Autónoma de Nuevo León.

⁶ C/r: Wikipedia. La enciclopedia libre, ‘Investigación’, dirección en internet: <http://es.wikipedia.org/wiki/Investigaci%C3%B3n>, fecha de consulta: 21/09/2011.



- Vincular la ciencia y tecnología en la sociedad y el sector productivo para atender problemas.
- Crear y desarrollar mecanismos e incentivos que propicien la contribución del sector privado en el desarrollo científico y tecnológico.
- Incorporar estudiantes en actividades científicas, tecnológicas y de vinculación para fortalecer su formación.
- Fortalecer la capacidad institucional para la investigación científica, humanística y tecnológica.
- Fomentar y promover la cultura científica, humanística y tecnológica de la sociedad mexicana⁷.

El Criminólogo-criminalista tiene amplias posibilidades de desarrollarse en esta área tan poco explorada, dedicarse a lo académico también es experiencia laboral y a la vez se puede lograr una retribución salarial muy atractiva a través de las diversas áreas de posgrado e investigación y con apoyo de otros órganos como Gobierno Federal y dependencias internacionales que destinan recursos a la investigación científica.

CONCLUSIÓN

En la actualidad en que la criminalidad está tan avanzada, el Criminólogo-criminalista no debe ser un profesionalista más de labor común o repetitiva, si bien cada profesión atiende fenómenos de importancia, así como la Medicina es inseparable de la humanidad, la Criminología-criminalística debe llevar a cabo su función restauradora de la sociedad o como se le llama en otros países: *peacebuilding* o *peacekeeping*, el terror colectivo se vive en todos y cada Estado de la República Mexicana. Son muchas otras áreas más en las que este profesionalista se puede desarrollar más allá de las sobreesaturadas de servicios periciales principalmente y los centros penitenciarios, las áreas internacional, científica, legislativa y privada urgen de este profesionalista. Ahora más que antes se está en obligación de cumplir con la responsabilidad social que exige cada profesión.

FUENTES DE INFORMACIÓN

Bibliográficas

- Carlos Alberto Elbert (coord.), La Criminología del siglo XXI en América Latina, Rubinzal-Culzoni, Argentina, 1999.
- Centro de Información para México, Cuba y República Dominicana, Manual de Modelos de Naciones Unidas, Centro de Información para México, Cuba y República Dominicana, México, Cuba y República Dominicana, 2008.
- Consejo Nacional de Ciencia y Tecnología, "Centros de investigación", dirección en internet: www.conacyt.gob.mx/Centros/Paginas/Default.aspx, fecha de consulta: 21/09/2011.
- Oficina de las Naciones Unidas contra la Droga y el Delito, dirección en Internet: www.unodc.org/unodc/en/commissions/CCPCJ/institutes.html, Italia, 2009.
- Sociedad Mexicana de Criminología capítulo Nuevo León, dirección en Internet: <http://somecrimnl.es.tl/Links.html>, fecha de consulta: 21/09/2011.
- UNICRI, Directorio Mundial de Instituciones Criminológicas, Italia, 2009.
- Wikipedia. La enciclopedia libre, dirección en internet: <http://es.wikipedia.org/wiki/Investigaci%C3%B3n>, fecha de consulta: 21/09/2011.

⁷ Consejo Nacional de Ciencia y Tecnología, "Centros de investigación", dirección en internet: <http://www.conacyt.gob.mx/Centros/Paginas/Default.aspx>, fecha de consulta: 21/09/2011.

SECCIÓN

Tópicos

Delito.com

Algunas notas de la delincuencia *online*

COLECTIVO ARCIÓN

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

“Al unísono en que se desarrolla una nueva tecnología es casi probable que se esté desarrollando una paralela con fines delictivos.”

RESUMEN

Es evidente el constante desarrollo experimentado en las filas de la delincuencia, pues en éstas se han generado modalidades delictivas otrora inconcebibles. Sin lugar a dudas, internet, la informática y la programación han sido explotadas por los delincuentes en su provecho dándole el espacio necesario al establecimiento de la delincuencia *online* (*ciberdelincuencia*), orillando tanto a los cuerpos y aparatos de administración y procuración de justicia, especialistas en la materia, así como de los individuos en común a hacerle frente a esta latente amenaza en línea. Pero antes de dar marcha a cualquier acción de respuesta es necesario estar al tanto de las herramientas, medios y técnicas que los agresores han sabido hacer uso, pues es de esta manera como se tendrán los conocimientos pertinentes en cuanto a la amenaza a la que se enfrenta. Por esto el presente trabajo pone de manifiesto a los lectores algunos rasgos significativos de esta forma de delinquir.

INTRODUCCIÓN

Internet¹ ha proporcionado en nuestros días nuevas formas de interactuar entre las personas dando lugar a espacios virtuales de encuentro y en estos la frecuente e intensa compartición y transferencia de datos e información. Una imagen, un comentario, un *link*² compartido o quizás un archivo de cualquier naturaleza, son en definitiva datos e información.

Tal información y datos pueden ser o no de carácter restringido, pues depende de la importancia y valor que pueda poseer para quién la emite, porque de alguna manera esa realidad virtual tiene implicaciones en la realidad como tal, es decir, que todo ese cúmulo de archivos que trafican en un ir y venir por las 'autopistas' del ciberespacio tienen efectos directos y proporcionales en la vida y realidad de los individuos, junto a las implicaciones que en ésta se generen.

1 Es un sistema global interconectado de redes de computadoras para servir a miles de millones de usuarios en todo el mundo. Se trata de una red de redes que consiste en millones de éstas de tipo privado, público, académico, empresarial y de gobierno de alcance local a global que están unidos por una amplia gama de tecnologías de redes electrónicas, inalámbricas y ópticas.

2 Un hipervínculo (también llamado enlace, vínculo, o hiperenlace) es un elemento de un documento electrónico que hace referencia a otro recurso.

Por lo anterior, de modo alguno encontraríamos que existe un vínculo de cierta medida de nuestra realidad reflejada en el ciberespacio, todo esto debido a la cada vez más creciente comunidad de usuarios de internet –que en provecho de los beneficios de este medio– han optado por su incorporación en el uso de la red informática como una forma de asociarse a ese ‘mundo’, a sus ‘habitantes’, a sus ‘espacios’ y como ya se infirió a sus ventajas como medio de comunicación.

Delincuencia online

Tomando en cuenta lo expuesto en los párrafos anteriores es conveniente señalar que buena parte de las actividades sociales y demás que se llevan a cabo en nuestra realidad pueden ser realizadas vía internet: desde enviar un saludo a un amigo y que éste responda dentro de un *chat room*³ hasta realizar conexiones a través de Red Privada Virtual⁴ (VPN por sus siglas en inglés) para la práctica de una cirugía a distancia, pasando por las innumerables transferencias bancarias electrónicas, así facilitando estas operaciones sin sacar físicamente el dinero. Pero a pesar de todas estas ventajas que nos ofrece este medio sería aceptable cuestionarse qué tan seguro es transitar por estas ‘autopistas’ y si no lo son, qué riesgos se pueden encontrar en el ‘camino’. Sólo el hipotético escenario en que una mala conexión exista en una telecirugía supondría un riesgo de alto alcance.

Internet ha proporcionado indiscutiblemente beneficios a la sociedad, sin embargo, a su vez ha traído consigo peligros en los que se puede caer en nuestra ‘navegación’ por la red, muchos de ellos no son tan sólo errores técnicos o humanos, sino también los hay intencionales. Es bien sabido que en esta comunidad –la virtual como suele llamársele– de usuarios de internet existen quienes sacan partida de esta interacción no presencial para poner en práctica –por diversas razones principalmente las de lucro– sus conocimientos en informática y programación al servicio de la delincuencia para atentar en contra de la seguridad y confidencialidad de los demás miembros de esa comunidad. Desde luego que estaríamos hablando de personas, organizaciones e instituciones de las más diversas índoles hasta naciones como víctimas y por su parte a este usuario mal intencionado como victimario, pues irrumpe en los recursos informáticos ajenos.

Todos estos miembros de la red pueden ser víctimas de estos ‘delincuentes informáticos’, pero al igual como sucede en la vida tal cual: los más vulnerables en estas embestidas son las personas o individuos comunes.

3 Cualquier forma de conferencias sincrónicas y en ocasiones asincrónicas. El uso principal de una sala de chat es el de compartir información a través de texto con un grupo de otros usuarios.

En términos generales es la capacidad de conversar con varias personas en la misma conversación. La diferencia de las salas de chat de los programas de mensajería instantánea, es que los últimos son típicamente diseñados para uno-a-uno.

4 “Red Privada Virtual”. Wikipedia la enciclopedia libre. [consultado: 23 de enero de 2012].

Algunos de los espacios virtuales de los que se ha servido esta modalidad de la delincuencia son las redes sociales, pues su acelerada y cada vez creciente afiliación de nuevos miembros⁵ hacen de éstas un amplio repertorio de posibles víctimas de sus fechorías, además que en estos espacios es posible encontrar una gran cantidad de datos e información de utilidad para el delincuente, ya que en ella se pueden describir los gustos, preferencias, condiciones socioeconómicas, ‘movimientos’ y otras particularidades de un miembro en específico que pueda resultar atractivo.

Es necesario establecer qué es lo que hace de las redes sociales sitios encantadores y propicios para que el delincuente actúe. Aunque una cuenta en estos dominios pueda contener información no fiable –llamémosle chatarra–, cabe la posibilidad que en medio de toda esa falaz ‘ficha técnica’ del afiliado exista datos a manera de indicios que nos acerque un poco a éste –como analogía tomemos el ejemplo cuando se hurga en medio de la basura para conocer un poco más al objetivo– en cambio, existe otro tipo de afiliado más ‘transparente’ que en diferente magnitud se muestra tal como es.

TABLA 1
EVOLUCIÓN DE NÚMERO DE USUARIOS ACTIVOS DE FACEBOOK

Año	Usuarios activos en millones
2004	Nace Facebook 1
2005	5.5
2006	12
2007	50
2008	100
2009	350
2010	500
2011	750

Fuente: <http://facebook.com/press>

TABLA 2
REDES SOCIALES MÁS POPULARES EN MÉXICO

Porcentaje de usuarios mexicanos	Red Social
39%	Facebook
28%	You Tube
20%	Twitter
6%	Hi5

5 Facebook. “Biografía”, [en línea]. 2012, [consultado: 23 de enero de 2012]. Disponible en la Web: <http://www.facebook.com/press/info.php?timeline> De acuerdo a la cifra presentada por el portal de Facebook es cercana a las 750 millones de cuentas de usuarios activos en julio de 2011.

3%	Badoo
2%	Sonico
1%	MySpace
1%	Linkendln

Fuente: Diario Milenio. Corona, Jessica. 'Facebook es la red social más usada por los mexicanos; Twitter, la tercera'. 17 mayo 2011, [consultado: 23 de enero de 2012]. Disponible en la web: <http://www.milenio.com/cdb/doc/noticias2011/58c0b884bd6410700b50e014116375b1>

TABLA 3
SUSCRIPCIONES DE INTERNET (TOTALES) POR CADA
100 HABITANTES. SERIE ANUAL

Año	Suscripciones por Cada 100 Habitantes
2000	1.1
2001	1.9
2002	2.1
2003	2.4
2004	3.0
2005	3.7
2006	4.6
2007	5.5
2008	7.7
2009p/	9.4
2010p/	10.8

Fuente: Comisión Federal de Telecomunicaciones (COFETEL), Secretaría de Comunicaciones y Transportes. 'Suscripciones de Internet (totales) por cada 100 habitantes. Serie Anual', [en línea]. 2010, [consultado: 23 de enero de 2012]. Disponible en la web: <http://siemt.cft.gob.mx/SIEM/#!/prettyPhoto/84/>

TABLA 4
COMPARATIVO INTERNACIONAL DE SUSCRIPCIONES DE INTERNET
DE BANDA ANCHA POR CADA 100 HABITANTES. SERIE ANUAL

País	2008	2009 p/	2010 p/
Alemania	27.49	30.31	31.59
Argentina	8.02	8.67	9.56
Australia	23.94	23.25	23.19
Austria	20.73	22.06	23.85
Brasil	5.37	6.09	7.23
Canadá	29.53	30.51	29.81
Chile	8.5	9.76	10.45
China	6.24	7.79	9.42

Colombia	3.27	4.43	5.66
Corea del sur	33.35	35.03	36.63
Dinamarca	36.48	37.18	37.38
España	20.06	21.27	22.96
Estados Unidos	24.82	26.23	26.34
Finlandia	30.43	29.31	29.07
Francia	28.71	31.76	33.92
Irlanda	20.29	21.8	22.82
Islandia	33.38	33.93	34.65
Italia	18.84	20.42	22.13
Japón	23.8	25.01	26.91
Malasia	4.79	5.98	7.32
México	7.07	9.05	10.54
Noruega	33.19	33.87	34.6
Nueva Zelanda	21.39	22.69	24.93
Perú	2.55	2.81	3.14
Reino unido	28.19	30.4	31.38
Rusia	6.48	9.02	10.98
Singapur	22.45	23.67	24.72
Suecia	31.43	31.63	31.59
Uruguay	6.8	8.96	11.37
Venezuela	4.74	4.72	5.37

Fuente: Comisión Federal de Telecomunicaciones (COFETEL), Secretaría de Comunicaciones y Transportes. 'Comparativo Internacional de suscripciones de Internet de Banda Ancha por cada 100 habitantes.

Serie Anual', [en línea]. 2010, [consultado: 23 de enero de 2012]. Disponible en la web: <http://siemt.cft.gob.mx/SIEM/#!/prettyPhoto/91/>

Como menciona este trabajo al iniciar: una imagen, un comentario, un *link* compartido o archivo cualquiera puede decir o contener mucho o poco, pero el caso es que si se pone atención a esos 'movimientos informáticos hablan más' que de la razones por los que fueron concebidos por el cibernauta que las emitió y usó.

Con anterioridad son descritos algunos de los motivos que llevan a estos 'ciberdelincuentes' a elegir estos espacios, pero no sólo están a la espera de que puedan conocer a su víctima por los recursos que ésta le proporciona indirecta e indiscriminadamente, sino que ellos de manera activa son impulsores a que existan las condiciones para el robo de información y datos de utilidad para él mismo, pues dependiendo de su ingenio y conocimientos técnicos puede tomar dos vías posibles. Por una parte tendría lugar una manipulación en una interacción social víctima-victimario, aunque dependería en gran medida

de que tal dinámica pudiese llevarse a cabo y mantenerse. Existen diversos escenarios posibles que llevarían a la misma y diferentes consecuencias, pero es de resaltar el factor de manipulación en que por medio de un juego de emociones anómalas inducidas sobre el receptor –donde el delincuente es el emisor– es posible que durante un determinado tiempo en el *chat room* o en cualquier otro sitio de encuentro pueda este emisor ganar simpatía y consiguientemente la confianza sin que su interlocutor conozca sus verdaderas intenciones. Resumamos esta idea de la siguiente manera, por una parte tendríamos a un actor con una capacidad superior en la dinámica social sobre otro que es sometido y manejado en su contra.

Es pertinente rescatar para este asunto esa noticia que apareció en algunos diarios en la que dos jóvenes del municipio de Nogales fueron detenidos por citar a una persona por medio de Facebook con la intención de asaltarla y luego asesinarla⁶. La fuente nos dice que los dos jóvenes contactaron a un hombre de 41 años del que conocían sus actividades. De acuerdo al informe dado por el Procurador de Justicia del Estado los dos fueron detenidos por ser presuntos autores de aquel asesinato perpetrado tras darle un disparo en el tórax a la víctima después de haberle quitado sus pertenencias, posteriormente fue sepultada en el patio del domicilio donde se llevó el encuentro. Además se presentó la noticia de la existencia de un tercer inculpado del que se desconoce su identidad. La nota anterior es muestra clara de aquellos encuentros indeseados que pueden darse en torno a las redes sociales como medio o herramienta para los delincuentes.

Por otra parte resulta ingenioso y de requerimientos más especializados en el campo informático al usar conocimientos en cuanto a informática⁷ y progra-

mación⁸ a favor de la delincuencia. Ya que de esta forma se pueden desarrollar una variedad de virus informáticos y otros software mal intencionados con las más diversas finalidades, una de ellas infiltrarse en una computadora sin el consentimiento de su propietario con el objetivo de sólo dañar el buen funcionamiento del equipo atacado o resultar molesto, realizar una broma hasta recopilar información de un ordenador y transmitirla al origen como sucede con los denominados *spyware*⁹. Este último resulta una amenaza en contra de la seguridad en cuanto a la confidencialidad informática de los usuarios de la red.

A continuación se presenta una breve descripción de los *softwares* malintencionados o *malware* más comunes. Cabe mencionar que en un principio éstos fueron elaborados como un experimento, una broma o algo molesto hasta llegar al punto de ser diseñados para sacar beneficios con los mismos.

Para empezar con el listado de estos ‘intrusos’ vale presentar qué es un *software*¹⁰ de la forma más sencilla posible, para esto lo definiremos como un conjunto de programas de cómputo de componentes lógicos necesarios que hacen posible la realización de tareas específicas basadas en instrucciones a un ordenador.

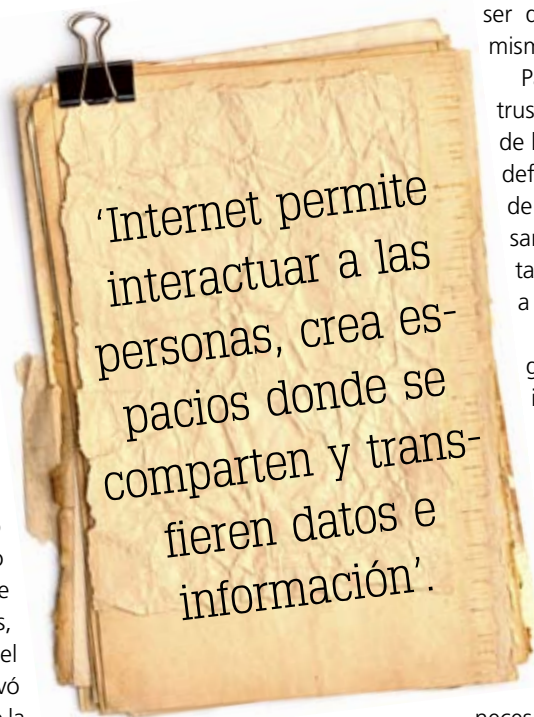
*Malware*¹¹ (*malicious software* en inglés) es un tipo de *software* diseñado para infiltrarse en el sistema de una computadora o bien para dañarla sin el consentimiento de su propietario. Es considerado como tal de acuerdo a las intenciones de su creador y de éstas los efectos que tengan sobre equipos informáticos ajenos. El término *malware* es usado para incluir a los virus, gusanos, troyanos y algunos *rootkits*, *spyware*, *adware* intrusivo, *crimeware* y otros más. Es

necesario diferenciar un *malware* de un *bug* o *software* defectuoso el cual resulta igualmente peligroso pero de carácter no intencional.

Malware infeccioso

Virus informáticos son aquellos programas que al ejecutarse se propagan y afectan a otros *software* del equipo alterando su buen funcionamiento. A la vez hay una variedad que contienen un *payload*¹² que realiza una acción maliciosa como borrar archivos.

Gusano informático tiene la característica de duplicarse a sí mismo, éste no altera a los archivos de los programas instalados, sino que atacan



6 El Universal. Beyliss, Marcelo /corresponsal. “Lo contactan por Facebook para robarlo y asesinarlo”, [en línea]. Hermosillo/sábado 14 de enero de 2012, [consultado: 23 de enero de 2012]. Disponible en la Web: <http://www.eluniversal.com.mx/notas/822601.html>

7 Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores. Este término se le define como la información que se genera de manera automática y de manera digital a través de un sistema de cómputo. Conceptualmente, se puede entender como aquella disciplina encargada del estudio de métodos, procesos, técnicas, desarrollos y su utilización de computadoras con el fin de almacenar, procesar y transmitir información y datos en formato digital.

8 La programación es el proceso de diseñar, escribir, depurar y mantener el código fuente de programas computacionales. El proceso de escribir el código requiere frecuentemente conocimientos en varias áreas distintas, además del dominio del lenguaje a utilizar, algoritmos especializados y lógica formal. El propósito de la programación es crear programas que exhiban un comportamiento deseado por el programador.

9 “Spyware”. Wikipedia la enciclopedia libre. [consultado: 23 de enero de 2012].

10 “Software”. Ibidem.

11 “Malware”. Ibid.

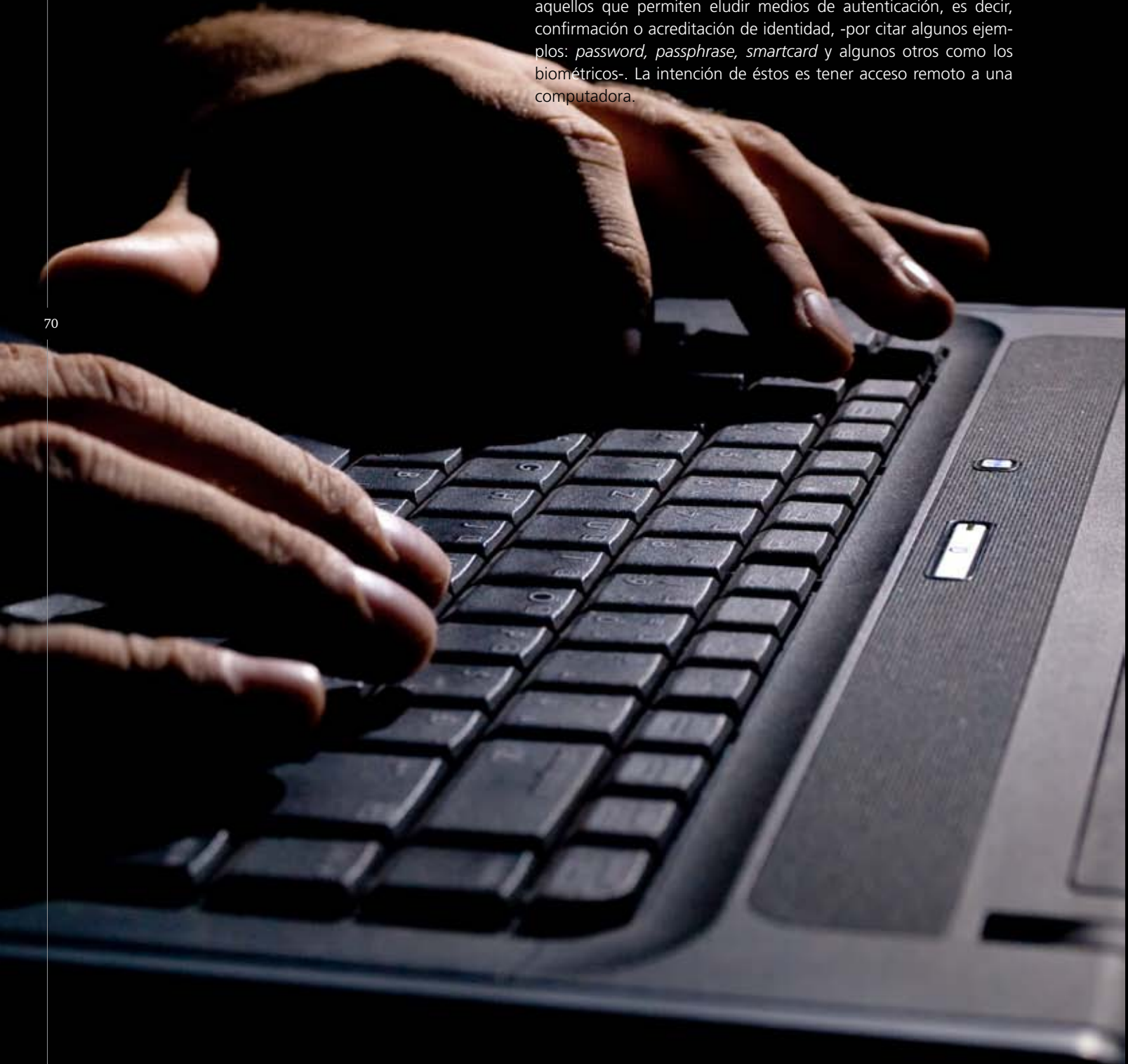
12 Payload en seguridad informática se refiere a la parte de un virus que realiza una acción maliciosa.

a la memoria al punto de alentar el equipo computacional, a su vez causan problemas en la red consumiendo ancho de banda. También son usados como medio de propagación de algún otro *software*.

Malware oculto

La condición subrepticia de un *malware* de esta clase es su principal arma, pues es de esa manera en la que actúa para alcanzar sus objetivos sin que el usuario del equipo atacado pueda eliminarlo antes de que empiece a realizar las operaciones programadas en el mismo.

Backdoors también conocidos como puertas traseras son aquellos que permiten eludir medios de autenticación, es decir, confirmación o acreditación de identidad, -por citar algunos ejemplos: *password*, *passphrase*, *smartcard* y algunos otros como los biométricos-. La intención de éstos es tener acceso remoto a una computadora.



Drive-by Downloads estos son instalados al acceder a algún sitio que instala spyware o códigos que dan información del equipo sin autorización del usuario. Se puede decir que existen páginas o sitios web¹³ maliciosos.

Rootkits permiten el acceso continuo a un equipo manteniéndose activamente ocultos para extraer información, además de ocultarse a sí mismo permiten ocultar a otros malware que mantienen tal conexión.

Trojanos son programas que se presentan disfrazados para resultar atractivos e inofensivos al usuario -como los instaladores de programas y archivos adjuntos- invitándolo a ejecutarlo en un segundo plano, así permite la administración remota creando muchas veces *backdoors* que pueden causar efectos negativos como el robo de datos bancarios o información personal. Algunas de las funciones que realizan los trojanos están la instalación de otros programas maliciosos, captura de pulsaciones de teclado, impresiones de pantalla y borrado de archivos.

Hasta este punto se han descrito de manera básica las operaciones que realizan estos programas maliciosos, sin embargo es oportuno hacer algunas observaciones en cuanto a su uso, pues como lo mencionábamos anteriormente surgen como un experimento o una burla informática, pero al unísono del paso del tiempo han sido incorporadas en actividades criminales y de espionaje. Estos son los nombres que aparecen en escena: *spyware* o programa espía, *adware* y el *hijacking*.

Los *spyware* son aquellos programas que utilizan una conexión de internet para recopilar información de una computadora y transmitirla a otra sin que el propietario de la primera esté por enterado, monitorean la navegación en la red, cambian la configuración de los equipos provocándoles que se ralenticen tanto en memoria como en conexión a la red.

Adware son los programas que de manera automática se ejecutan y muestran publicidad web -anuncios, ventanas emergentes y otros similares-. Algunos de estos realizan un seguimiento de información personal retransmitiéndola a terceros sin consentimiento del usuario dando así el carácter de *spyware*.

Hijacking o secuestro son todas aquellas técnicas ilegales que pretenden robar algo, es un término muy amplio, aunque por lo regular se aplica cuando se ha efectuado un secuestro de conexiones de red, sesiones de terminal, módems y cualquier otro tipo de servicios informáticos.

Delitos informáticos y otros ataques

Hasta ahora se han presentado las herramientas -por así llamarlas- y las modalidades más frecuentes para irrumpir en la privacidad y estabilidad informática que en su conjunto formulan actividades delictivas que en términos informáticos denominan a un delito específico en agravio de algunos de los miembros de la comunidad virtual por parte de los malhechores como a continuación se muestra:

Crimeware es un *software* que ha sido específicamente diseñado para cometer delitos financieros en conexiones a la red con el objeto de robar la identidad de un usuario para tener acceso a los servicios financieros que una compañía ofrece. El término es aplicado cuando la finalidad de este programa es producir pérdidas económicas al afectado.

*Phishing*¹⁴ es la denominación que reciben las estafas cibernéticas que intentan obtener nombres de usuario, contraseñas, detalles de tarjetas de crédito, números de seguridad social que tienen como recurso hacerse pasar por entidades de confianza en la transmisión de información electrónica atacando principalmente a usuarios descuidados que hacen uso de las redes sociales -actualmente el blanco principal-, subastas electrónicas, pago en línea y más donde la apariencia en definitiva engaña. Los métodos usados por el *phisher* (nombre que se le da al farsante) para obtener tales datos radica en el engaño o disfraces como una URL¹⁵ (localizador de recursos uniforme) mal escrita haciéndose pasar por los de una organización seria que envía un correo electrónico o con el uso de la arroba en direcciones electrónicas que la contengan para preguntar usuario y contraseña y luego redireccionarlos a otro sitio cuando se accede a internet.

Existen otras formas como el uso de los *Javascrrips*¹⁶ en los que se alteran la barra de direcciones cerrando la barra genuina y abriendo una fraudulenta, también está otro método llamado *Cross-site scripting* que consiste en que el atacante utiliza el mismo código de programa del portal de alguna compañía bancaria, de esta forma el usuario inicia su sesión en dicho portal y tiene que verificar sus cuentas con un enlace aparentemente genuino en el que se copian datos valiosos para su posterior uso. Además se conoce otra técnica de engaño -aunque no tan común- en la cual se usan nombres de dominios de tal parecido que no se pueden distinguir fácilmente, ya que suelen cambiar caracteres por otros muy similares, se les conoce como ataques homógrafos, pues en estos casos se cambian letras de una palabra escrita en determinado alfabeto por otras tan parecidas pertenecientes a otro, por citar algún ejemplo están los intercambios del alfabeto latino por caracteres del alfabeto griego o cirílico.

14 "Phishing". Wikipedia la enciclopedia libre. [consultado: 23 de enero de 2012].

15 Localizador de recursos uniforme, más comúnmente denominado URL (sigla en inglés de uniform resource locator), es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación, como por ejemplo documentos textuales, imágenes, videos, presentaciones, presentaciones digitales, etc.

El URL es la cadena de caracteres con la cual se asigna una dirección única a cada uno de los recursos de información disponibles en la Internet.

16 JavaScript es un prototipo basado en un lenguaje de programación (*scripting*) de alto nivel que en su uso en las páginas web tiene entre otras funciones la apertura de una nueva ventana su posición y tamaño, validar los valores de un formulario web que permite al usuario introducir los datos que se envía a un servidor para su procesamiento, cambio de imágenes, transmitir información sobre hábitos de lectura y navegación web para seguimiento de anuncios, personalización y más.

13 En informática, la World Wide Web (WWW) o Red informática mundial es un sistema de distribución de información basado en hipertexto (nombre que recibe el texto que en la pantalla de un dispositivo electrónico permite conducir a otros textos relacionados pulsando con el ratón en ciertas zonas sensibles y destacadas) o hipermedios enlazados y accesibles a través de Internet. Con un navegador de Internet, uno puede ver páginas web que pueden contener texto, imágenes, videos y multimedia para navegar entre ellos a través de hipervínculos o enlaces.

Lavado de dinero por actividades delictivas derivadas del uso de *phishing* son oportunidades de trabajo en línea en la que una empresa ficticia oferta vacantes atractivas –por las comisiones recibidas- de trabajo sin salir de casa en las que el contratado tiene la tarea de realizar el depósito de cantidades de dinero en bancos y de hacer varias transferencias electrónicas manteniendo el dinero en movimiento para dificultar su rastreo haciéndolas pasar por ingresos ganados derivados de actividades legítimas para circular en sistema financiero sin ningún problema.

Pharming es aquel ataque que pretende redirigir el tráfico de un sitio web a otro sitio falso, desde luego manejado por una máquina distinta. Este término guarda cierta relación con el de *phishing*.

*Spoofing*¹⁷ es el término usado para referirse a las técnicas de suplantación de identidad con propósitos maliciosos y de investigación. Existen cinco tipos de estas técnicas dentro de este mismo:

IP *spoofing* suele ser el más conocido y tiene por objeto sustituir una dirección IP¹⁸ por otra a través de programas concebidos para esto que logran ocultar un remitente o simplemente hacerse pasar por otro equipo.

ARP *spoofing* esta modalidad de *spoofing* está basada en la falsificación de la tabla ARP o *Address Resolution Protocol* (Protocolo de resolución de direcciones) que es la encargada de encontrar la dirección hardware¹⁹ que corresponde a una dirección IP determinada, con esto se pretende falsear la relación IP-MAC²⁰ con lo que consigue enviar paquetes a un *host*²¹ distinto al legítimo, en este caso al *host* del atacante.

DNS *spoofing* es el falseamiento por suplantación de identidad por el nombre de dominio, es decir, que se falsea la relación Nombre de dominio-IP o más bien un DNS²² con una dirección IP falsa o viceversa.

Web *Spoofing* es una página web espuria con función de *proxy*²³ de otra genuina en que la conexión de la víctima es enrutada para que en ella se pueda obtener información y datos.

Mail spoofing se refiere a la suplantación de un correo electrónico ajeno o manipulado en la dirección del remitente y otras partes de la cabecera del correo para que parezca como si el correo electrónico se originó en una fuente diferente, es usado

como conducto para el envío de correos electrónicos de tipo *hoax*²⁴ o bulo con los que es posible obtener una lista de direcciones de correos electrónicos para la difusión de una noticia falaz o algún *malware* a gran escala.

Tráfico online de contenidos protegidos o piratería

Mientras uno navega en la red puede toparse con algún sitio en los que se puede adquirir y compartir distintos tipos de archivos como música, películas, libros, obras artísticas y otros productos informáticos copiados o falsificados de contenido protegido que no reportan su correspondiente tasa a los propietarios de los derechos de autor o de invención. De esta manera, se estarían violando a los ya indicados –sin que se pueda estar completamente consiente de esta situación- dando lugar a lo que suele denominarse como tráfico *online*²⁵ de contenidos protegidos o mejor conocida como piratería. Tal situación es similar a la que se vive en el comercio informal en las calles de productos con contenidos de iguales o parecidas condiciones.

Existen distintos y muy diversos factores que promueven esta actividad y su derivado crecimiento y daño a estos propietarios, por citar algunos, tendríamos situaciones como ver la película en cartelera y de recién estreno en la pantalla grande sin tener que salir de casa o tener en nuestro reproductor de mp3 las canciones más escuchadas en la radio sin la necesidad de comprar un álbum o quizás realizar una descarga con su respectivo costo.

La ley SOPA *Stop Online Piracy Act* (Acta de cese a la piratería en línea) o Ley H.R. 3261 es un proyecto de ley presentado en la Cámara de Representantes de los Estados Unidos el 26 de octubre de 2011. Es considerada por sus opositores como un enorme recorte a las libertades de navegación en la red, en cambio los autores o propietarios de los derechos de contenidos protegidos y todos aquellos que se ven implicados apoyan esta medida, ya que la piratería atenta en contra de sus intereses en cuanto derechos de autor o de propiedad intelectual.

Esta ley convierte al *streaming*²⁶ sin autorización en un delito que viola a los derechos morales y patrimoniales que la ley concede a los autores (copyright) por el sólo hecho de la creación de una obra, esté publicada o inédita.

17 "Spoofing". Wikipedia la enciclopedia libre. [consultado: 23 de enero de 2012].

18 Dirección IP es una tarjeta numérica de identificación de una tarjeta de red de una computadora que usa el protocolo IP (Protocolo de Internet por sus siglas en inglés) que tienen las funciones de enrutamiento de los datos en bloques conocidos como paquetes o datagramas en una conexión de un *host* (computadora conectada a una red) origen a otro *host* destino. Esta dirección puede cambiar en una reconexión por lo que se le llama dirección IP dinámica, existen otras, las direcciones IP fijas que no cambian con el tiempo para aquellos sitios de Internet que requieren estar conectados permanentemente.

19 Dirección asignada a la computadora que se conecta a una red. Los cuadros enviados de una computadora a otra deben contener la dirección de hardware del receptor. Las direcciones de hardware también se conocen como direcciones físicas.

20 Se conoce también como dirección física, y es única para cada dispositivo.

21 Computadora conectada a una red.

22 Domain Name System o DNS (en español: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

23 Un *proxy*, en una red informática, es un programa o dispositivo que realiza una acción en representación de otro que sirve para interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc.

24 Son noticias falsas que intentan hacerse pasar por verdaderas de divulgación masiva por los medios de comunicación, en la actualidad, son mayoritariamente difundidos vía Internet. Se han encontrado principalmente en foros y cadenas de mensajes –como las ya frecuentes cadenas de la buena suerte-. No buscan fines de lucro en cambio pueden resultar destructivos. Con éstos es posible obtener direcciones de correo electrónico (para enviar virus masivos, mensajes con suplantación de identidad o más de los mismos) engañando al destinatario para aceptarlo, ya que son mensajes que tratan de los más diversos temas de interés y de opinión pública.

25 En general, se dice que algo está en línea, on-line u online si está conectado a una red o sistema mayor.

26 Es la distribución de multimedia a través de una red de computadoras de manera que el usuario consume el producto al mismo tiempo que se descarga. Se aplica habitualmente a la difusión de audio o video.

Se han tomado medidas para detener a las principales webs de intercambio de archivos como la ejecutada por el FBI y dada a conocer recientemente por los medios: la inhabilitación de *Megaupload* que fue un sitio web de servicios de alojamiento de archivos la cual se encontró culpable de violar los derechos de autor, a su fundador y demás involucrados como los responsables –que de acuerdo con el Departamento de Justicia de los EEUU- de “piratería masiva en todo el mundo de diferentes tipos de obras protegidas por derechos de propiedad intelectual”²⁷.

En relación a la industria musical, para la mayoría de músicos su verdadera fuente actual de ingresos está en la actuación en vivo y no en la venta de discos, de la misma forma la industria cinematográfica ha sufrido los estragos de la piratería y ha optado por manifestarlo²⁸. En cambio existen grupos de cibernautas que promueven de alguna manera el libre tráfico de archivos manifestada en la libre expresión e independencia de Internet como la postura que adopta *Anonymous*²⁹.

CONCLUSIÓN

En fin son tantas las técnicas, herramientas y modalidades de la delincuencia informática y de tales especificaciones técnicas que es un tanto difícil describirlas todas en este trabajo, ello requeriría de una labor extensa y en constante actualización, pues al unísono en que se desarrolla una nueva tecnología es casi probable que se esté desarrollando una paralela con fines delictivos. Por lo anterior se concluye con lo siguiente: la delincuencia en su desarrollo histórico ha incorporado sin dudar las novedades tecnológicas que cada época le ofrece para lograr su cometido en este caso la web. Por su lado los aparatos de administración y procuración de justicia de nuestro país, así como de la legislación existente para la sanción y penalización de estas actividades no van a la par, pues la modesta voluntad en hacer contemplar su inserción en este ámbito³⁰ y en algunos otros casos la omisión total del tema como sucede en los códigos penales de las diferentes Entidades Federativas, promueven a que dicha modalidad delictiva se desarrolle sin trabas en la impunidad en línea.

En tanto al Criminólogo-criminalista en su que hacer profesional debe de tomar en cuenta el estudio de los problemas delictivos en la red para estar a la par de las tendencias en el uso de Internet, informática y programación que la delincuencia incorpora día con día. De esa manera, este profesional conseguirá ampliar su campo de acción a la vez mantenerse a la vanguardia, de lo que sólo se exige su constante actualización puesto que el mundo tecnológico evoluciona

a pasos agigantados. Cabe aclarar que no se pretende que sea un especialista en la materia, sino que este profesional posea los conocimientos y herramientas básicas para comprender la problemática.

FUENTES BIBLIOGRÁFICAS

Electrónicas

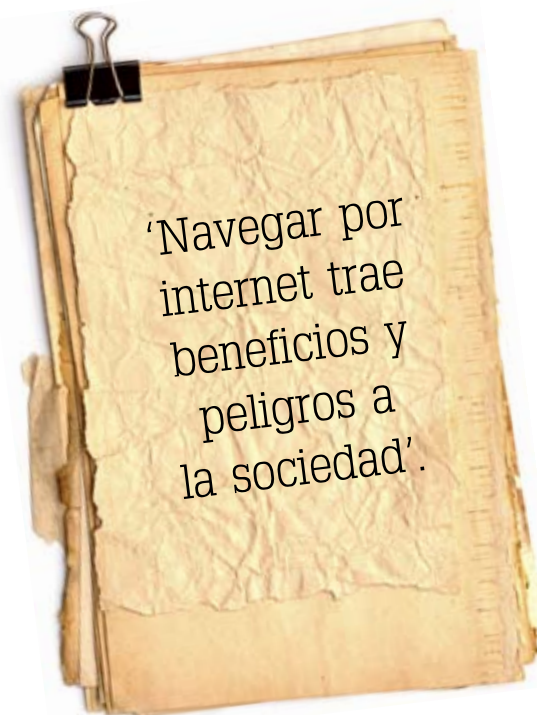
- Código Penal Federal. Ley Federal del Derecho de Autor. Cámara de diputados. [En línea]. [Consultado: 24 de enero de 2012]. Disponible en la web: <http://www.diputados.gob.mx>
- Comisión Federal de Telecomunicaciones (COFETEL), Secretaría de Comunicaciones y Transportes. [En línea]. [Consultado: 23 de enero de 2012]. Disponible en la web: <http://siemt.cft.gob.mx>
- El Mundo. Rodríguez, Sergio. [En línea]. [Consultado: 24 de enero de 2012]. Disponible en la web: <http://www.elmundo.es>
- El Universal. Beyliss, Marcelo /corresponsal. [En línea]. [Consultado: 23 de enero de 2012]. Disponible en la web: <http://www.eluniversal.com.mx>
- Facebook. [En línea]. [Consultado: 23 de enero de 2012]. Disponible en la web: <http://www.facebook.com>
- Diario Milenio. Corona, Jessica. [consultado: 23 de enero de 2012]. Disponible en la web: <http://www.milenio.com>
- Wikipedia la enciclopedia libre. [En línea]. [Consultado: 23 de enero de 2012]. Disponible en la web: <http://es.wikipedia.org>

27 El Mundo. Rodríguez, Sergio. “El FBI cierra Megaupload, una de las mayores webs de intercambio de archivos”. [en línea]. 20 de enero de 2012, [consultado: 24 de enero de 2012]. Disponible en la web: <http://www.elmundo.es/elmundo/2012/01/19/navegante/1327002605.html>

28 El Universal. García, Patricia. “Se baten en la SOPA”. [en línea]. Viernes 20 de enero de 2012, [consultado: 24 de enero de 2012]. Disponible en la web: <http://www.eluniversal.com.mx/espectaculos/110743.html>

29 Anonymous. Wikipedia la enciclopedia libre.

30 El artículo 167 fr.VI del Código Penal Federal sanciona con prisión y multa al que intencionalmente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de vídeo o de datos. También es necesario para este fin consultar los artículos 211 bis 2 y 211 bis 3. En cuanto a piratería véase la Ley Federal del Derecho de Autor. Título IV, capítulo IV. Aunque se contempla en la legislación estas actividades existen muchos vacíos, omisiones y sobre todo seguimiento, especificidad y actualización.



El problema de la explicación de la criminalidad

y sus causas, desde teorías socio-cognitivas y epistemológicas.

EDGARDO NOÉ RUBIO MONTALVO

Lic. Filosofía por parte de la Universidad de Guadalajara.
 Maestría en Sociología cultural por la Universidad Viadrina,
 Frankfurt, Oder, Alemania.



“Se plantean dos teorías, una sobre la conciencia y otra sobre el comportamiento cultural, distintas de las clásicas y las hoy en día usadas.”

INTRODUCCIÓN

Descartes descubre la experiencia consciente, aquello que nos hace ser lo que somos, lo que algunos llaman alma, y que al parecer es inherente al cuerpo. Éste conocimiento dio otra perspectiva al entendimiento de nuestra naturaleza.

La parte física de ésta, ofreció bríos del funcionamiento humano, y gracias al materialismo cartesiano, nos dio una nueva perspectiva acerca de cómo entendernos a nosotros mismos, sólo que, este nuevo matiz se complicó, al momento de querer encontrar, que tipo de relación se encuentra entre la parte física de la conciencia y la parte mental de la misma, así, surge el problema por primera vez en la historia, de la relación mente-cerebro.

La conciencia es la experiencia subjetiva, la mente y el mundo. Todos somos seres conscientes. Hay algo que consiste en qué se siente al ser nosotros, al ser yo, al ser tú, 'desde adentro'. Hay algo que es qué se siente al ver, al pensar, al tener emociones, al oír. Ese 'algo' que se siente al tener esa experiencia es la conciencia. Y la pregunta es: ¿cómo puede encajar la experiencia subjetiva en el mundo objetivo caracterizado por la ciencia moderna?

El problema de la relación física y mental de la conciencia es bastante discutida en diferentes campos de la filosofía de la mente, ciencias cognitivas y neurociencia, las cuales tienen peso y relevancia en sí, de ésta manera al reflexionar sobre dicho tema, surgen diferentes tipos de explicaciones tanto especulativas como con bases más científicas como la que se realiza a través de la neurociencia y con las consecuencias epistemológicas que ello implica.

“Si tienes un familiar que está en coma, querrás saber: ¿está consciente? Esto es lo más importante. De no ser conscientes tal vez no importe si están muertos. Si lo son están vivos, hay alguien ahí, eso quizá sea vital para preservar sus vidas. Su conciencia es lo fundamental”¹.

Las investigaciones dentro del área Psicológica hablan de posibles relaciones intrínsecas entre la cognición y el comportamiento, las cuales dicen que si se carece de supuestas herramientas lógicas y de interpretación por parte del individuo, generará comportamientos distorsionados y hasta antisociales en personas tales como criminales. Aquí Psicólogos, como Vicente Garrido, Per Standgeland y Santiago Redondo, parten del supuesto, que por falta de desarrollo de dichos elementos, se puede llegar a una inhibición de ciertos mecanismos cognitivos y de comportamiento, donde se manifiestan las ya mencionadas características.

Así mismo fenómenos médicos donde se presentan síntomas en pacientes, que no pueden explicarse con infecciones virales o bacteriales, sino desde ciertas constelaciones mentales que afectan físicamente al cuerpo, de éste modo se entrevé la vigencia del problema de la conciencia.

Daniel Denneth en su teoría de la conciencia, la cual se ha hecho desde el reduccionismo, nos ha brindado datos interesantes y útiles para la continuación de este tipo de investigaciones, ahora bien, así podemos entrever un trabajo que se debe realizar conjuntamente entre neurociencias y filosofía y más allá de esto, desde la interdisciplinariedad, por lo menos hasta llegar a una teoría más contundente acerca de la conciencia y así mismo a una explicación concreta de la violencia y el comportamiento desviado.

En los casos descritos por Robert Aunger, sobre una transmisión de una enfermedad, la transmisión de las ideas de una persona a otra, y la transmisión por medios no biológicos, se plantea el contexto siguiente.

Aquí de lo que se habla es de transmisión de información de un punto A hacia un punto B. En el primer caso, de la transmisión de una enfermedad, vemos detalles interesantes de cómo dicha enfermedad de KURU, se conservo de algún modo, en algún tipo de vector en el cuerpo sin vida de una mujer, y al ser su cerebro comido por su nieta, ésta con el tiempo comienza a presentar síntomas, degenerando su cerebro, hasta finalmente morir. ¿Cómo podemos explicar que un virus, pueda retenerse dentro de un cuerpo muerto, lo suficiente para poder sobrevivir y posarse en otro al haber sido comido?

En otro tipo de fenómeno de transmisión, tenemos el de Mahltus a Darwin, quien al leer su libro, pasa la idea del uno al otro. Que por algún tipo de particula-

ridad, pregno la mente de Darwin y origino finalmente la idea del origen de las especies.

Y por último en el caso de la transmisión de un virus informático a una ordenador, donde destruye el orden de los archivos almacenados, vemos que la transmisión fue efectiva y muy tangible, así que su explicación debe ser basada y fundada, si lo entendemos desde la analogía del contagio, que dicha información, biológica (en el caso del virus o incluso de un prion), de una idea (en el caso de la lectura de la obra de Mahltus por Darwin), o en el caso más particular de un virus informático que viaja por medio de un vector en el ciberespacio y finalmente se hace física su información al hacer caos en un ordenador específico), tenemos que entender que la transmisión se da, y así, por lo tanto, buscar un replicador, ya que uno de éstos, podría ser el eslabón responsable de dicho fenómeno.

Un virus que contiene información biológica, parece depender de los productos genéticos para poder replicarse. Un prion es más peligroso, ya que éste depende totalmente de los productos genéticos para su replicación, estos portadores de información biológica son la explicación para dicha transmisión, sólo que aún falta determinar qué tipo de replicadores necesitan para la transmisión. Igualmente en la transmisión de ideas, vemos que la explicación de ésta, se da si suponemos al meme entendido como un virus o un prion, pero faltaría explicar que replicador necesita, para su transmisión.

El problema subyacente es demostrar la existencia de tal cosa.... sólo que para los propósitos que me propongo, la noción de su existencia será sólo entender como su replicación se da, igual que como los virus o priones se replican.

De éste modo, se quiere decir que si se entiende la replicación del meme, se estará hablando de un tipo específico de existencia, es decir, la metafísica del meme. Y ésta misma al ser algo concreto, es el contexto donde se debe buscar la relación entre la información cultural, su vector y su transmisión, el vector que aquí debemos entender es la ‘imitación’.

PRINCIPIO DE COHERENCIA ESTRUCTURAL

Para comenzar a desarrollar una teoría de la conciencia, lo interesante es considerar como base los planteamientos que Chalmers nos ha presentado, porque en ellos es notable la coherencia entre la experiencia consciente y la estructura cognitiva, es decir entre la Fenomenología y la Psicología de la mente: estas no son independientes una de la otra, ya que están relacionadas de un modo sistemático. Lo que supone que:

“Las leyes físicas fundamentales explicarán las características de los procesos físicos; las leyes Psicofísicas explicarán las experiencias conscientes asociadas y todo el resto será una consecuencia”².

Los principios no absolutos que se deben plantear ahora se deducen desde la inquietud de si deseamos saber qué tipo de experiencia está teniendo en este momento una persona, ¡hay que preguntarle! y así ir haciendo restricciones en estas generalidades que aún son en un nivel alto o macroscópico. ¿Cómo se llevan a cabo estas restricciones?

Bien. De acuerdo con Chalmers, sólo a partir de los juicios de lo mental: ...tres clases de juicios fenoménicos:

1 Peregrín Fernando, entrevista a David Chalmers, junio 2010 publicado por José Diez y Eva Sierra: <http://www.terceracultura.net/tc/?p=2063>

2 Chalmers, David J. The Conscious Mind. In Search of a Fundamental Theory. Oxford University Press, 1996, p. 275.

1. juicio de primer orden, ¡eso es rojo!
2. juicio de segundo orden: estoy teniendo una sensación de rojo en este momento.
3. juicio de tercer orden: las sensaciones son misteriosas³.

Los juicios de segundo orden son por lo general correctos y esto podría llamarse principio de fiabilidad, ya que cuando se juzga que se está experimentando una sensación auditiva, se está experimentando una sensación auditiva, o cuando se cree que se experimenta un dolor usualmente se está experimentando un dolor. Chalmers lo expresa así:

Nuestros juicios de segundo orden pueden a veces ser erróneos, lo que provee excepciones al principio de fiabilidad. Esto podría ocurrir debido a fallos en la atención (si estoy distraído, puedo creer que acabo de experimentar un dolor cuando en realidad sólo experimente un ruido fuerte), dificultades en la captación de las categorías pertinentes (como cuando rotulo equivocadamente una experiencia de carmesí como de castaño), enfermedad mental o patología neurofisiológica (como en los casos de negación de ceguera, en la que los sujetos hacen afirmaciones falsas acerca de sus experiencias) y por otras diversas razones⁴.

Un principio recíproco al de fiabilidad es -el principio de detectabilidad-, que dice que cuando ocurre una experiencia por lo general se tiene la capacidad de formar juicios de segundo orden sobre ella; es decir que aunque para algunas experiencias no prestamos atención, sí se tiene la capacidad de advertirlas.

Ahora bien, existe coherencia entre la conciencia y la cognición; esta noción que es importante no involucra los juicios de segundo orden, sino más bien a los juicios de primer orden: es decir a la coherencia entre la conciencia y los juicios de primer orden.

Pero en el modelo de Chalmers estamos hablando de coherencia entre la conciencia y percatación: la percatación es la otra característica de lo mental, el correlato Psicológico de la conciencia, en otras palabras, es como un estado de alguna información que está directamente accesible y disponible para el control deliberado de la conducta y para su manifestación conductual; así, el contenido de la percatación corresponde a el contenido de los juicios fenoménicos de primer orden, que no son acerca de la conciencia, sino paralela a ella.

Entonces, donde hay conciencia hay percatación. Por ejemplo la estimulación óptica se procesa y transforma, y mis sistemas perceptuales registran que existe un objeto de tal y cual forma y color sobre el escritorio; esta información está disponible para el control de la conducta, lo mismo ocurre para los detalles específicos de lo que se experimenta: cada detalle está cognitivamente representado en la percatación. En un nivel cognitivo más cercano, obsérvese que alguien puede hacer comentarios sobre esos detalles y dirigir mi conducta de modos que dependen de ellos.

Lo que podemos ver aquí, es que los juicios de primer orden representan lo importante del carácter fenoménico de lo mental, porque los juicios de primer orden son concomitantes a la conciencia. En cambio, los juicios de segundo orden no son tan frecuentes y a veces son erróneos; en ellos sólo se percibe su propio contenido, pero una no experiencia consciente.

Lo que significa que los juicios de segundo orden son poco frecuentes, mientras que los juicios de primer orden ocurren permanentemente. El vínculo más directo es, por lo tanto, el vínculo entre la conciencia y los juicios de primer orden.

Por ejemplo, referente a los juicios de segundo orden, cuando alguien se percató de que Busch es presidente, en el sentido de que tiene acceso a esa información, puede comunicarla verbalmente y puede utilizarla en la dirección deliberada de su conducta. Sin embargo si no existe un pensamiento recurrente al efecto, no parece que pueda existir una experiencia consciente correspondiente, o si la hay es una muy débil.

De aquí se formula el principio de coherencia estructural, que es una versión revisada de lo que ya tenemos. La hipótesis dice: allí donde hay conciencia hay percatación y donde hay el tipo correcto de percatación hay conciencia.

Pero la experiencia consciente de un individuo, nos dice Chalmers, no es en general una masa informe homogénea, sino que posee una estructura interna detallada. Por ejemplo, en el campo visual hay patrones de franjas y todo lo que se refiere a patrones geométricos; así en tres dimensiones tengo experiencias en formas como cubos, experiencias de qué cosa está detrás de cuál otra y otras manifestaciones de la geometría de la profundidad. El campo visual consiste en una vasta masa de detalles que encajan en una estructura general.

Todos estos detalles están representados dentro de lo que se concibe como la estructura de la percatación. Por ejemplo, el tamaño y la forma de los diversos fragmentos están representados en mi sistema visual, quizás en un mapa topográfico relativamente directo.

La geometría del campo visual puede comprenderse mediante un análisis de la información que el sistema visual pone a disposición de los procesos de control posteriores, así en la conducta o en su verbalización; de este modo, si la información está disponible para su verbalización se deduce que está presente en algún lugar. De este modo se puede ver que la estructura de la conciencia se refleja en la estructura de la percatación.

Otras características son, por ejemplo, la estructura de los colores y la intensidad de la experiencia, que son evidentes porque marcan una diferencia en el procesamiento posterior, de manera que debe estar representada de alguna forma en la estructura de la percatación, pero no se mencionarán en este trabajo ya que considero explicado el principio de coherencia estructural que Chalmers propone.

Entonces, así se tiene una versión más refinada del principio: la estructura de la conciencia se refleja en la estructura de la percatación y la estructura de la percatación se refleja en la estructura de la conciencia. Esta es una relación central y sistemática entre la Fenomenología y la Psicología y a su vez entre la Fenomenología y los procesos físicos subyacentes.

3 Ibid. p. 231.

4 Ibid., p. 280.

Aunque muy frecuentemente la conciencia es dejada de lado en campos de investigación que trabajan con leyes físicas o que la explican reductivamente, existen, como este libro, trabajos de cierta importancia en los que se pueden extraer conclusiones acerca de la experiencia consciente a partir de resultados empíricos. Pero ¿cómo es esto posible debido a las dificultades en la observación directa de la experiencia? Si todo lo que puede observarse son procesos físicos, entonces ¿qué justifica cualquier conclusión?

La respuesta de Chalmers es que, cada vez que se extraen conclusiones acerca de la experiencia a partir de resultados empíricos, un principio puente realiza el trabajo.

Un principio puente definirá un criterio para la presencia de la conciencia en un sistema, un criterio que se aplica en un nivel físico. Un principio de este tipo actuará como una palanca epistémica que permite pasar del conocimiento de los procesos físicos al conocimiento acerca de la experiencia. La palanca epistémica no es en ella misma experimentalmente verificable, al menos desde el punto de vista de tercera persona; en cambio actúa como un tipo de supuesto general previo, estos no siempre se hacen explícitos, pero son el único modo como este tipo de trabajos logra alguna base en la experiencia consciente.⁵

Lo que quiere decir el autor es que estos principios deben ser considerados explícitamente. Así por ejemplo, cualquiera que recurra a un principio puente hace filosofía, ya que estos no son ellos mismos conclusiones experimentales; es decir que se basan en datos de primera persona y en principios generales de plausibilidad.

Por ejemplo cuando un sistema se peca de alguna información, en el sentido que la información está directamente disponible para el control global, entonces la información es consciente. El principio puente más común aquí es el uso de la informatividad como criterio para la experiencia. Al menos en un sistema que utiliza un lenguaje se considera que, por lo general, la información es consciente si es comunicable; así la informatividad es una versión de la percatación y vemos que concuerda claramente con el principio de coherencia.

En este caso, toda la evidencia que se posee proviene del vínculo con la informatividad y la percatación; la experiencia no se puede medir, por lo tanto se debe basar en criterios indirectos y estos criterios de informatividad y percatación parecen ser lo único mejor que hay, y se sabe que son subdeterminados, y por eso pueden ser falsos.

La hipótesis de que el principio de coherencia estructural puede ser una ley de la naturaleza, es decir una ley subyacente, se puede entender así: hasta ahora lo que se sabe es que la conciencia surge de alguna manera de lo físico, pero no en virtud de qué propiedades, es decir que no se sabe qué propiedades son parte, del lado físico, de la conexión, pero con el principio de coherencia hay una respuesta

parcial, que es que la conciencia surge en virtud de la organización funcional asociada a la conciencia, es decir que no sólo la conciencia surge de la percatación, también su estructura esta determinada por la estructura de aquella.

¿Por qué podría aceptarse estos principios de coherencia como leyes? Porque:

...en última instancia para mí en mi propio caso. Las correlaciones evidentes entre la percatación y la conciencia en mi propio caso son tan detalladas y notables que debe haber algo más que una mera regularidad aleatoria, debe haber una ley subyacente, pero ¿qué ley?, esta ley debe implicar que, en mi propio caso, la percatación siempre es junto con la conciencia y viceversa y además que las estructuras de éstas están en correspondencia⁶.

La concepción memética de Susan Blackmore

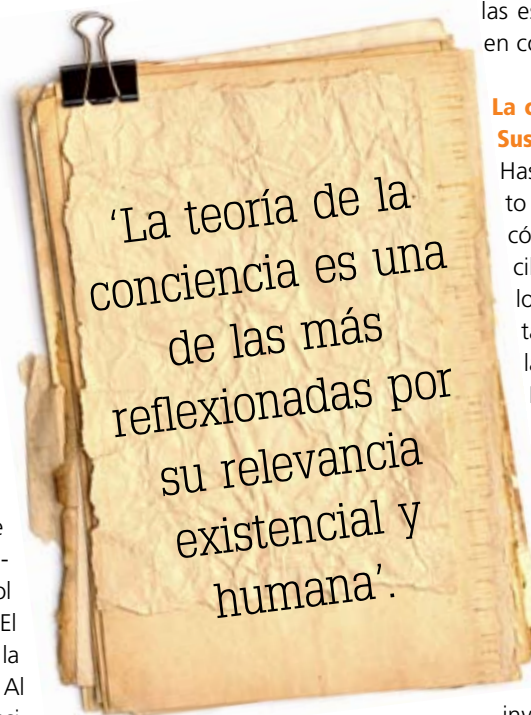
Hasta ahora hemos expuesto el punto de vista de cómo Robert Aunger concibe el funcionamiento de los *memes*. Complementaremos la exposición con la manera en que Susan Blackmore comprende los *memes*. Porque de ambas concepciones serán conformadas las definiciones y términos (aunque aun no hay una terminología establecida en la memética) con los cuáles se trabajará en esta investigación.

Un *meme*⁷ es para la doctora Blackmore todo lo que se transmite de una persona a otra. De este modo un *meme* incluye por ejemplo, el vocabulario que utilizamos, las historias que conocemos, las habilidades que hemos adquirido de otros y los juegos que preferimos, las leyes que acatamos. Cada uno de estos *memes* ha evolucionado por imitación según el trecho histórico que haya recorrido, pero al fin y al cabo, transmitidos a través de nuestra conducta con el afán de reproducirse.

⁶ Ibid., p. 310.

⁷ El meme simplemente se envuelve en un vector, algún tipo de icono portador de información, como un mensaje hablado, un comportamiento motor observado, un fragmento de texto, una imagen o una laja de piedra. Cuando un patrón en potencia se pone en contacto con dicho vector, es decir, cuando se lee el texto u oye el mensaje, el meme salta de ese vehículo (descodificado) haciéndose activo de nuevo, e infecta a la persona, que se convierte en un nuevo patrón.

⁵ Ibid., p. 302.



En concordancia con Aunger vemos que en la definición de Blackmore la imitación es la forma en que los seres humanos hacen adaptaciones para su conducta frente a los otros.

Sin embargo, en la concepción de Blackmore vemos una característica que Aunger pasó por alto: el hecho de que no todo lo que se imita es un *meme*, ya que en su análisis sobre la imitación Blackmore descubre que es posible diferenciar qué es y qué tipos de imitación hay que considerar como *memes*, acto seguido de ver cómo se dan por el contagio y el aprendizaje social.

Imitación, contagio y aprendizaje social

Para la autora es importante saber distinguir entre imitación, contagio y aprendizaje social para evitar confusiones de terminología en el estudio de los memes. Así, contagio es por ejemplo las modas o el ser aficionado del fútbol; en general transmisión de conductas. Esto contrasta no con la imitación como lo entiende Aunger, sino con otra forma que se denomina imitación instintiva, contagio conductista, facilitación social, acción conjunta o

simplemente contagio.

Bostezar, toser o reír son actividades muy contagiosas. Ésto se asocia a una característica de estímulo específico que detecta el bostezo o la risa en otra persona y que transmite una conducta de respuesta innata e idéntica. Cuando comenzamos a reír porque los demás también lo hacen no se debe a que hayamos aprendido a hacerlo, porque ya sabíamos de antemano cómo hacerlo; la risa que se manifiesta no está copiada de la que oímos, porque la risa como el bostezar son conductas innatas, por lo tanto no vale dentro de la memética.

La imitación es un acto no muy frecuente, sin embargo sí es algo especial. En experimentos de imitación con bebés y niños la imitación es abundante; también en el ámbito deportivo, de conformidad social y en otras cuestiones. Por ejemplo, el contenido violento en televisión puede inducir un comportamiento violento; el suicidio, los accidentes e incluso los asesinatos pueden aumentar por conductas de imitación violentas.

Blackmore comienza a especular sobre su ejemplo planteando lo siguiente: vamos a imaginar una acción sencilla, supongamos que se llevan las manos a la boca como si se fuera a tocar la trompeta, se levantan y se emiten sonidos característicos. De este modo todo el mundo será capaz de copiar esto y nadie tendrá demasiada dificultad en juzgar la actuación.

Sin embargo, Blackmore está segura de que hay mucha dificultad en esto, porque en primer lugar la persona que copia, o mejor dicho algún mecanismo inconsciente de su cerebro tendría que decidir qué aspectos o acciones desea copiar: ¿importa la postura?, ¿la posición de los pies?, ¿es más importante concentrarse en las manos para que ejecuten las funciones de una trompeta o quizás para que se parezcan a las manos que hacen los ademanes ya mencionados? Por otra parte ¿debería tararearse en la misma nota?, ¿la misma melodía?, así cada quien resolvería sus propios enigmas.

Una vez hecho esto y tomado todas las decisiones pertinentes, se procederá con un conjunto de transformaciones muy complejas. Supóngase que algún imitador lo imitó de perfil, ninguna de las acciones corresponderá con el aspecto de las mismas vistas de frente o desde la perspectiva elegida para imitarse. El cerebro del imitador deberá esforzarse para recrear su transformación de la acción que le permita instruir a sus músculos a fin de que lleven a cabo una actuación que a juzgar del público sea similar, de este modo vemos que no es tan simple.

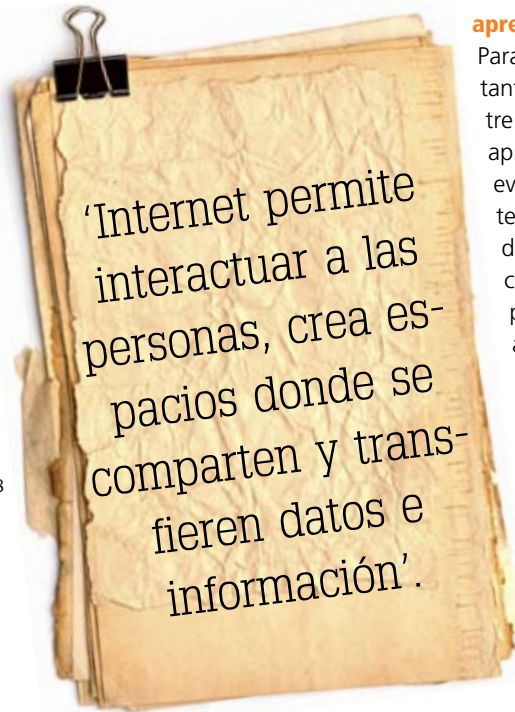
Para Blackmore, la imitación por definición precisa de:

- Decisiones sobre qué imitar, o sobre qué es igual o similar.
- Transformaciones complejas desde un punto de vista u otro.
- Producción de funciones corporales idóneas.

De esta forma se muestra que la imitación no es tan simple y que siempre se subestima su propia complejidad porque la imitación nos parece normal y sencilla. Cuando nos copiamos, algo se transmite, por intangible que sea y ese algo es un *meme*.

En general, el contagio y el aprendizaje social se traspone con lo que ya habíamos analizado con Aunger. Ya visto el funcionamiento de la transmisión de información, los criterios de la replicación y del darwinismo universal, y habiendo visto que el *meme* no se puede replicar solo, sino que necesita estructuras genéticas ya hechas, en éste caso el cerebro, donde se encuentran materia energética y un ambiente protegido de interferencia, pues uno de sus modos de pasar de un cerebro a otro es el contagio a través de señales captables por los sentidos, hemos aprendido un poco más sobre la naturaleza del *meme*. Por ser ésta su forma de transmisión, por ser similar al contagio de un virus, se denomina también al meme por lo tanto como un superparásito (así Aunger los clasifica), igual que los virus informáticos.

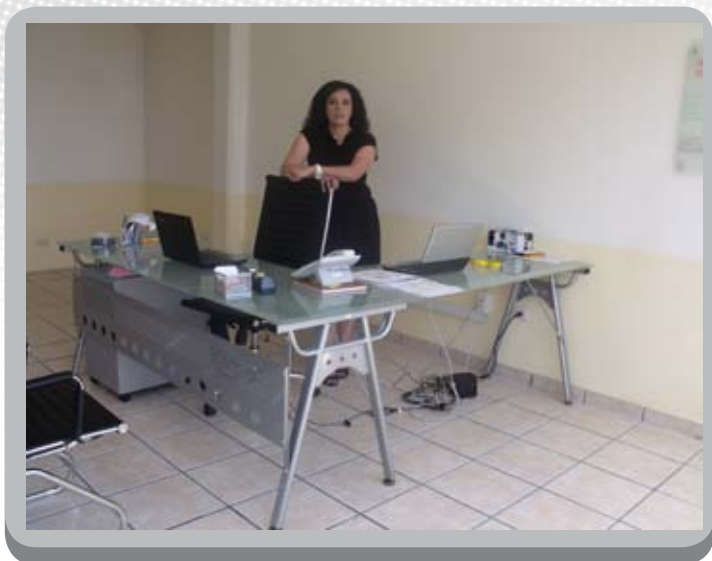
Argumentos del reduccionismo neurológico de Deneth, nos hablan de la explicación en base a resultados obtenidos de aparatos de medición modernos, se cree que los mapas topográficos cerebrales, deducidos en base a los encefalogramas y otros estudios, nos ayudarán a localizar, en donde se encuentra la parte del cerebro que se activa según la actividad mental. De éste modo, nos lleva más cerca a buscar patrones sistemáticos





SECCIÓN

Personajes CLEU



Beatriz Yarce Alfaro

PERSONAJE CLEU

Comunicóloga

Nació en Puebla, Puebla.

Estudios realizados: Licenciada en Ciencias de la Comunicación en la Universidad de las Américas Puebla. Cuenta con estudios en la Universidad de Quebec en Tres Ríos y con la maestría en Comunicación Estratégica por la Benemérita Universidad Autónoma de Puebla, además de la especialización en Dirección de Proyectos.

Actividades laborales: desde 2002 ha estado vinculada intensamente en el ámbito de la comunicación, tecnologías y coordinación de equipos de alto desempeño. Asidua a la academia, su preparación constante la ha llevado a explorar también ámbitos del *marketing* digital, la creatividad y el desarrollo empresarial. Creó, cimentó e impulsó la plataforma informativa *periodicodigital.com.mx* de Grupo Tribuna Comunicación; un concepto integral en la web que se convertiría en un referente noticioso en la entidad y en el extranjero. De manera paralela ha sido articulista de la Revista Poder con secciones como 'Éxito empresarial' y 'Servicios Ciudadanos'. Asimismo, en la administración pública coordinó las actividades mediáticas y servicios informativos digitales del Congreso del Estado de Puebla durante la LVII Legislatura. Al tiempo condujo los programas 'Acuerdos Radio' y 'Acuerdos Televisión' del Poder Legislativo producidos por el Sistema de Comunicación e Información del Estado de Puebla (SICOM) hoy Puebla TV. Además ha fungido como consultora estratégica para el Ayuntamiento de Huejotzingo en la administración 2011-2014.

Actividades Directivas en el CLEU: Directora Universidad Virtual CLEU.

SECCIÓN

Recomendaciones

UNIVERSIDAD VIRTUAL CLEU

Mtra. Beatriz Yarce Alfaro
Directora Universidad Virtual CLEU

Surge a partir de la preocupación del Doctor José Luis Pérez Ángeles y de la Licenciada Elia Moreno Martínez por diversificar la oferta educativa y satisfacer las demandas sociales más allá de las fronteras; un aula sin paredes y sin límites.

La necesidad de fortalecer la educación superior en el ámbito de la Criminología-criminalística motivó al CLEU a visibilizar una Institución de educación superior con un nuevo enfoque que promueva la globalización del proceso de enseñanza y el conocimiento. Su principal propósito se plantea en educar a personas más capaces, responsables, críticas y cooperativas, que propongan soluciones factibles a los problemas que aquejan a la sociedad.

Universidad Virtual CLEU se contempla como una comunidad compuesta por académicos que buscan extender el servicio educativo a públicos nacionales e internacionales, enriquecer y ampliar el conocimiento de los alumnos, así como proporcionarles flexibilidad en tiempo y espacio, crear y difundir una nueva concepción de la enseñanza, fomentando el desarrollo de grupos multidisciplinarios y cooperativos.



Fotografía número 1
Colectivo ARCIÓN. Instalaciones de la Universidad Virtual
Sala de Videoconferencias

Universidad Virtual CLEU será un puente que permita acercar a los más reconocidos profesores del Sistema CLEU, con estudiantes de todas las demarcaciones, a través de las más novedosas tecnologías y redes de comunicación.

Universidad Virtual CLEU propone una Institución sin recinto tal y como lo conocemos, un sistema de educación basado en competencias e interacción en la red, donde el estudiante asume la necesidad de aprender y establecer su propio ritmo de aprendizaje, sin tener que asistir a las clases físicamente.

Universidad Virtual CLEU es una realidad, es una oportunidad, es una forma de aprendizaje, es una experiencia única capaz de integrar nuevos procesos de transmisión del conocimiento a través de un entorno diferente, y así formar nuevos Criminólogos-criminalistas ejemplares, con dominio de la tecnología de punta y con aptitud para integrarse a cualquier medio.

Universidad Virtual CLEU no busca ni pretende en ningún caso competir con otras Instituciones, por que siempre hemos sido y seguiremos siendo los primeros, y con hechos lo estamos demostrando.



84



Fotografía número 2. Colectivo ARCION. Instalaciones de la Universidad Virtual CLEU. Sala de atención personalizada de profesores a alumnos.

3



Fotografía número 3 y 4. Colectivo ARCION. Instalaciones de la Universidad Virtual CLEU. Biblioteca



PLANTEL CLEU MÉRIDA

PRÓXIMAS PUBLICACIONES

REVISTA VISIÓN CRIMINOLÓGICA-CRIMINALÍSTICA

- Revista  El Criminólogo-criminalista en el lugar del hecho
- Revista  El Criminólogo-criminalista en la búsqueda del material sensible significativo

2da. de Vicente Suárez no. 2520,
colonia Bella Vista, C.P. 72500
Puebla, Puebla, México.
Teléfono:(01 222) 2 11 00 48
cleu_desicyc@hotmail.com
desicyc@yahoo.com.mx

