Propuesta de Protocolo para la Recolección de Evidencias Digitales Relacionado con la Legislación Peruana

Evelyn Salas Ordinola, Alan Ramírez García y Oscar Núñez Mori

Pontificia UNIVERSIDAD CATÓLICA del Perú

Resumen:

El presente artículo propone la elaboración de un protocolo para la recolección de evidencias digitales adaptado a las leyes y normas vigentes en el Perú.

Palabras claves: Delito Informático, Código Penal Peruano, Evidencias Digitales.

I. INTRODUCCIÓN

Actualmente vemos que el vertiginoso desarrollo de los avances tecnológicos y las comunicaciones, ha traído efectos positivos para el crecimiento económico y social de nuestro país, sin embargo, también ha abierto una puerta para que personas inescrupulosas, hagan uso de los mismos en la comisión de actos delictivos que en la mayoría de los casos dejan tras de sí evidencias digitales en los dispositivos de almacenamiento o en la red. Estas evidencias muchas veces son de vital importancia para la resolución de procesos legales, sin embargo la inadecuada manipulación de las mismas al momento de su recolección o análisis, puede traer como consecuencia la alteración, destrucción parcial o total de la evidencia, lo cual lleva al cuestionamiento o invalidación de las mismas en un proceso legal.

El presente artículo busca dar a conocer la importancia de contar con un conjunto de normas y procedimientos que permitan realizar una adecuada recolección de evidencias digitales para su análisis posterior, a fin de obtener pruebas fehacientes y admisibles ante un tribunal, y así contribuir con una correcta administración de justicia [GI06].

II. MARCO TEÓRICO

Se debe tener en cuenta que, para dar inicio a la investigación de un delito, es necesario realizar un análisis preliminar del entorno en el que este se ejecuto, cabe decir que se debe efectuar un estudio técnico, social y jurídico, que nos permita establecer relación entre el sitio de ocurrencia y un evento específico, así como la relación entre la víctima y el perpetrador, lo que nos ayudará a tipificar el delito y enfocar el sentido, en el cual se deberá orientar la investigación y consecuentemente el análisis de evidencias. [PPER]

Con la finalidad de situarnos en un contexto adecuado, y para lograr un mejor entendimiento de esta propuesta, se considera de importancia tener claros los siguientes aspectos.

A. Delito Informático

Si bien, no hay una convención exacta sobre el alcance de este término, de manera general, se puede definir al delito informático como aquél en el que, para su comisión, se emplea un sistema automático de procesamiento de datos o de transmisión de datos [TI85].

B. Evidencia Digital

La evidencia digital es única, cuando se la compara con otras formas de "evidencia documental". A diferencia de la documentación en papel, la evidencia digital es frágil y la copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. [OL01]

C. Víctima

La víctima de un delito informático es toda persona natural o jurídica, que ha sido perjudicada mediante el uso un sistema automático de procesamiento o transmisión de datos [TI85].

La importancia del estudio de las víctimas de delitos informáticos, radica en analizar la disposición de las misma a cooperar con la investigación, para hallar una relación entres esta y el criminal.

En el caso de las personas natural, el sentir que debido a que el criminal empleo un sistema electrónico para la ejecución del delito, será difícil ubicarlo o inculparlo, por lo que muchas veces prefieren no iniciar un proceso legal contra su victimario.

En el caso de las empresas o corporaciones, el ser víctima de un delito informático, es una clara muestra de que el nivel de seguridad informática de este ente es vulnerable, lo que conlleva a una publicidad negativa para la empresa, por lo que muchas veces deciden no denunciar el hecho. [LU02]

D. Criminal

Para el caso de los delitos informáticos, perpetrados contra empresas o corporaciones, se ha visto que en su mayoría, el acto delictivo ha sido ejecutado por personas que laboraban en la misma y que tenían cierto nivel de conocimientos informáticos [LU02].

Sin embargo la facilidad con la que hoy en día se accede a la tecnología, hace que personas con un nivel de conocimientos mínimos en informática, puedan hacer uso de medios electrónicos para la cometer sus actos delictivos, generalmente contra personas naturales.

E. Aspectos Legales

En la legislación peruana los delitos informáticos han sido tratados como una variante o agravante de delitos tradicionales, como lo son la estafa, delito de daños, falsedad documental, delitos contra la propiedad intelectual, entre otros [BRAM]. Sin embargo el 15 de julio del año 2000, se promulgo la ley 27309, la cual incorporó los delitos informáticos al Código Penal Peruano (Artículos 207-A, 207-B y 207-C).

- Artículo 207 – A, "Delito Informático"
  El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas. Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas [CO00].

- Artículo 207 – B, "Alteración, daño y destrucción de base de datos, sistema, red o programa de computadora"
  El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa. [CO00]

- Artículo 207 – C, "Delito Informático Agravado"
  En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

  1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.
  2. El agente pone en peligro la seguridad nacional [CO00].

III. TRABAJOS RELACIONADOS

La Guía para Recolectar y Archivar Evidencias RFC 3227, publicada en febrero de 2002, fue elaborada por los ingenieros Dominique Brezinski y Tom Killalea con la finalidad de proporcionar orientación para la recolección, protección y almacenamiento de información digital, relacionada con algún hecho punible. Esta guía está estructurada de la siguiente forma [BRKI]:

a. Principios básicos para la recolección de evidencias (Orden de volatilidad de los datos, cosas para evitar, consideraciones de privacidad y aspectos legales).
b. Procedimientos para la recolección de evidencias (Transparencia y pasos para la recolección).
c. Procedimiento para archivar evidencias: (Cadena de custodia, donde archivar y como archivar).

Es importante aclarar que la RFC 3227 da lineamientos generales que deben ser evaluados y adecuados, a las leyes que rigen en cada País.

En el caso del Perú, el Gobierno y el Congreso de la República han promulgado leyes destinadas a garantizar la libertad de información, los derechos de autor y derechos conexos, así como Normas sobre delitos informáticos, firmas y certificados digitales, entre otras. Con la finalidad de difundir las leyes y normas vigentes referentes al uso de las tecnologías, el Instituto Nacional de Estadística e Informática (INEI), elaboro el *"Compendio de Normatividad sobre el uso de Tecnologías de Información en el Perú"*, el cual posee la siguiente estructura [INEI]:

- Norma Constitucional.
- Norma que Garantiza la Libertada de Información.
- Normas de Protección a los derechos de autor.
- Normas Sobre Delitos Informáticos (Código Penal).
- Normas de Firma y Certificaciones Digitales
- Normas que Permiten la Utilización de Medios Electrónicos para la Comunicación de la Manifestación de Voluntad.
- Normas que Regulan el uso de Tecnología de Información en la Gestión de Archivos y Documentos.
- Norma que Fomentan el Uso de los Formatos Electrónicos en las Entidades de la Administración Pública.

IV. PROPUESTA DE PROTOCOLO DE RECOLECCIÓN DE EVIDENCIAS DIGITALES

Como es evidente al seguir un protocolo de recolección de evidencias digitales adecuado, disminuimos la posibilidad de que las mismas se alteren o destruyan, sin embargo para que las evidencias sean consideradas admisibles en un proceso penal, se debe tener en cuenta que el protocolo utilizado, cumpla con las leyes y normas vigentes en el Perú.

El protocolo de recolección de evidencias digitales que se propone, adopta como base la RFC 3227, y la adapta a la legislación vigente en el Perú, a fin de obtener un protocolo, con un adecuado fundamento técnico-legal que me permita la obtención de pruebas irrefutables ante un tribunal.

1. Consideraciones para la Recolección de Evidencias Digitales

A. Principios Básicos [BRKI]:

- Adherirse a las políticas de seguridad del lugar, manipulando adecuadamente el incidente.
- Captura de una imagen del sistema tan exacta como sea posible.
- Mantener notas detalladas. Estas deben incluir fechas y horas. Notas e impresiones debe ser firmadas y fechadas.
- Observe la diferencia entre el reloj del sistema y UTC (Tiempo Universal Coordinado).
- Esté preparado para testificar (tal vez años más tarde), y exponer todas las medidas que tomó y en qué momento. Las notas detalladas son vitales.
- Reducir al mínimo los cambios a los datos durante la recolección. Esto no se limita a los cambios de contenido, sino que se debería evitar también la actualización de archivos o de los tiempos de acceso a los directorios.
- Lacrar las vías de acceso externo, a la información, para evitar cambios o copias no autorizadas.
- Cuando nos enfrentamos a una elección entre la recolectar o analizar la evidencia, se debe priorizar la recolección para el análisis posterior.
- Los procedimientos deben ser puestos en práctica, es decir deben ser probados para asegurar su viabilidad, especialmente en una crisis. Si los posibles procedimientos deben ser automatizados, por razones de velocidad y precisión. Sea metódico.
- Para cada dispositivo, es preciso adoptar un enfoque metódico que siga los lineamientos establecidos en el procedimiento de recolección. La velocidad generalmente será fundamental cuando exista un número regular de dispositivos que requieran ser examinados, por lo que puede ser apropiado distribuir el trabajo en equipos, para reunir las pruebas en paralelo.
- Sin embargo, en una colección único sistema dado debe ser llevada a cabo paso a paso.
- Se debe realizar la recolección de evidencias digitales priorizando el orden de volatilidad.
- Debe realizar una copia a nivel de bits de los medios de comunicación del sistema. Si se va a realizar un análisis forense, debe realizar una copia a nivel de bits de su copia de prueba, ya que el análisis casi con toda seguridad alterara los tiempos de acceso del archivo.

B. Orden de volatilidad

El orden de volatilidad viene determinado por la susceptibilidad de las evidencias al cambio, por tal efecto se deberá priorizar la recolección de las evidencias, iniciando desde las más volátiles hasta las menos volátiles. Ejemplo en orden de volatilidad *[BRKI]*:

- Los registros, la caché.
- tabla de enrutamiento, el caché ARP, tabla de procesos, estadísticas del kernel, memoria.

- Archivos temporales del sistema.
- Disco.
- registro remoto y monitoreo de datos que es relevante para el sistema en cuestión.
- configuración física, topología de la red.
- Medios de almacenamiento.

C. Consideraciones de privacidad

El Código Penal Peruano especifica en su Título IV "Delitos contra la Libertad", algunas consideraciones que se deben tener en cuenta.

- Se debe respetar la privacidad de las personas tanto en la vida personal, como familiar, por lo se debe recolectar información que sea esencial para la investigación, sin atentar contra la privacidad de la persona implicada, a menos que el caso lo amerite, previo mandato del juez, con las garantías previstas por ley [CO01].
- La información obtenida, producto de la investigación, cuya publicación pueda causar daño, no podrá ser publicada sin consentimiento del interesado o previo mandato del juez, con las garantías previstas por ley [CO02].
- Asegúrese de tener el respaldo de la empresa o gobierno para seguir los pasos establecidos en un procedimiento para la recolección de evidencias digitales del incidente [BRKI].

D. Consideraciones Legales [BRKI]

Las evidencias digitales están sujetas a evaluación para ser aceptadas como pruebas en un proceso legal. Algunas de las características que deberían poseer son las siguientes *[BRKI]*:

- *Admisible:* Se debe cumplir con ciertas normas legales antes de que sean expuestas ante un tribunal.
- *Auténtico:* Debe ser posible vincular positivamente pruebas materiales con el incidente.
- *Completa:* Debe contar toda la historia y no sólo una perspectiva particular.
- *Fiable:* No debe haber duda acerca de cómo la evidencia digital fue recolectada y posteriormente analizada.
- creíble: Debería ser fácilmente comprensible y creíble por un tribunal.

E. Aspectos Logísticos

Para efectuar un adecuado estudio de las evidencias digitales se debería contar con los siguientes aspectos logísticos [DB04]:

a) Recursos Humanos: Equipo de profesionales expertos e idóneos para la recolección y análisis de las evidencias digitales.

b) Recursos Materiales: El análisis forense debe ser realizado en una red aislada con un equipo preparado para tal fin Adicionalmente debe contar con:
   - Diario de Campo
   - Fichas de recolección de información.
   - Cámara digital.
   - Guantes.
   - Fundas protectoras.
   - Equipo Informático.
   - Software Apropiado

El Gobierno Peruano, mediante la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), en coordinación con el Instituto Nacional de Defensa de la Competencia y de la Protección de Propiedad Intelectual (INDECOPI), ha elaborado una "Guía Técnica Sobre Evaluación de Software para la Administración Pública", la cual está basada en la norma ISO/IEC 9126. La guía en mención es aplicable para toda evaluación, ya sea de software propietario, software libre o código abierto, así mismo permite evaluar a un solo software o un conjunto de software de naturaleza o funciones similares, lo cual nos permitirá comparar y seleccionar un software que nos garantice una adecuada recolección de evidencias digitales. [ONGE]

Ejemplos de Software [BRKI]:

- Programas para examinar procesos (ps).
- Programas para examinar el estado del sistema (showrev, Ifconfig, netstar, arp).
- Programas para hacer copias poco a poco de la información (dd, Safeback).
- Programas para la generación y firmas de comprobación (Shalsum, checksum habilitado dd, SafeBack, pgp).
- Programas para la generación de imágenes básico y examinarlas (gcore, gdb).
- Scripts para automatizar la recopilación de pruebas (The Coroner´s).

2. Proceso de Recolección Evidencias Digitales

A. Transparencia

Los métodos utilizados para la recolección de evidencias deben ser transparentes y reproducibles. Se debe estar preparado para reproducir con precisión los método que utilizados, y estos métodos deben ser susceptibles de ser probados por expertos independientes [BRKI].

B. Pasos para la Recolección

Se debe realizar una lista de los sistemas que participaron en el incidente y de los que se recogerán las pruebas [BRKI].

- Establecer todo lo que sea probablemente una evidencia, ante la duda es mejor abstenerse de la recolección.
- Obtener el orden de volatilidad de cada sistema.
- Eliminar todos las salidas externas
- Registrar la hora del reloj del sistema
- Preguntarse que otros objetos pueden ser probatorios a medida que avanza la investigación.
- Documentar cada paso.
- Tomar nota de las personas involucradas (y su comportamiento).

3. Proceso de Almacenamiento de Evidencias Digitales

A. Registro y Codificación

Toda evidencia recolectada deberá ser debidamente registrada y codificada, se debe considerar que dicha codificación debe guardar relación con el lugar en el que acontecieron los hechos, así como el caso al que pertenecen las pruebas y la fecha en la que fueron recolectadas [PPER].

B. Registro Fotográfico y Audiovisual [DB04]:

- Fotografiar y/o filmar, el equipo sin desmontar (apagado con el cartel de número de serie).
- Fotografiar y/o filmar, el equipo desmontado (con el cartel visualizando números de serie de hardware).
- Fotografiar y/o filmar, la configuración del equipo por dentro.
- Fotografiar y/o filmar, el disco duro original y las copias (2) juntas (se debe ver la fecha, hora y las etiquetas), pasa corroborar la existencia de las copias y originales entregados al custodio.

C. Cadena de Custodia [DB04]

Es una serie de procedimientos que buscan preservar la evidencia digital. Estos procedimientos son:

- Recolección e identificación de la evidencia.
- Análisis.
- Almacenamiento.
- Preservación.
- Transporte.
- Presentación en el juzgado.
- Retorno al propietario.

Se recomienda para el establecimiento de la cadena de custodia se tenga en cuenta lo siguiente:

- Reducir al máximo la cantidad de agentes implicados en la manipulación y análisis de las evidencias.
- Mantener la identidad de las personas implicadas desde la obtención hasta la presentación de la evidencia.
- Asegurar la inmutabilidad de la evidencia en los traspasos de estas entre agentes.
- Registros de tiempos, firmados por los agentes, en los intercambios entre estos de las evidencias. Cada uno de ellos se hará responsable de las evidencias en cada momento.
- Asegurar la inmutabilidad de las evidencias cuando las evidencias están almacenadas asegurando su protección.

El cumplimiento de las recomendaciones indicadas anteriormente, para la cadena de custodia, permite proteger y dar inmutabilidad a la evidencia, al tener conocimiento de quién obtuvo la evidencia, dónde y cuándo fue obtenida, quién la protegió y quién ha tenido acceso a la evidencia.

V. ANALISIS

La presente propuesta fue planteada en base a la metodología de marco lógico (Apéndice), la cual será evocada en esta sección, para sustentar la funcionalidad del protocolo propuesto.

Se tiene entonces como problema central, la invalidación de evidencias digitales en los procesos legales, el cual se origina por la inadecuada manipulación de las mismas, al momento de su recolección o análisis, que aunados a un marco legal insuficiente, traerá como consecuencia una

inadecuada impartición de justicia, lo que contribuirá a un incremento de la desconfianza en la población hacia sus autoridades.

Como alternativa de solución a este problema se propone la adopción de una serie de procedimientos resumidos en un protocolo de recolección de evidencias digitales, el cual está basado en procedimientos técnicos de uso internacional y adaptado a las leyes y normas peruanas vigentes, a fin de que los peritos informáticos puedan ejecutar dichos procedimientos con el amparo legal correspondiente. Podemos decir entonces que con adecuado marco técnico-legal, se puede evitar la alteración y/o destrucción de evidencias digitales durante su recolección, adicionalmente permitiría un mejor entendimiento e interpretación de las evidencias, colaborando así con una adecuada impartición de justicia.

VI. CONCLUSIONES PARA TRABAJOS FUTUROS

Habiendo realizado el análisis correspondiente se puede concluir lo siguiente:

Debido al protagonismo que están tomando, los delitos informáticos, estos deberían de ser tratados como delitos independientes, con sanciones adecuadas al caso, no como una variación de los delitos tradicionales planteados en la legislación peruana.

Es necesaria la implementación de un protocolo de investigación forense para el caso de los delitos informáticos, a fin de que el mismo sirva de apoyo legal a los procedimientos utilizados por los peritos informáticos durante una investigación.

APÉNDICE

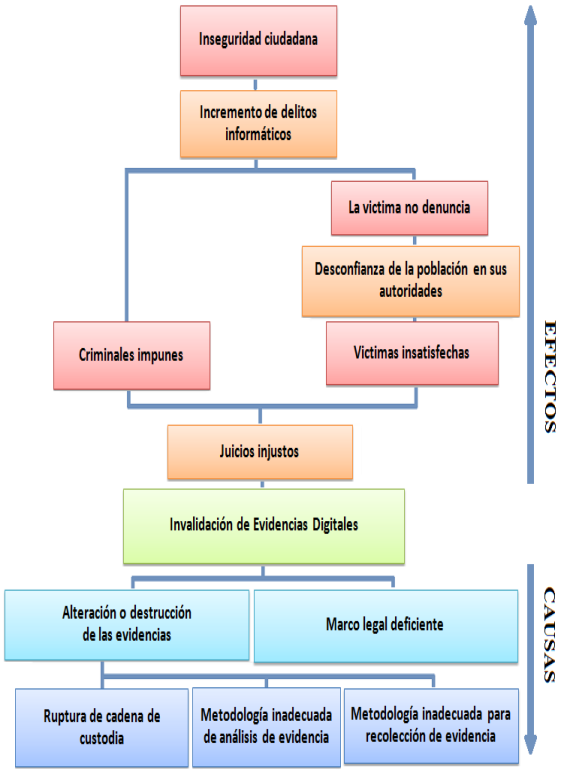
1. Marco Lógico

La presente propuesta ha sido planteada, haciendo uso de la Metodología de Marco Lógico, desarrollada por León Rossenberg y Laurence Posner.

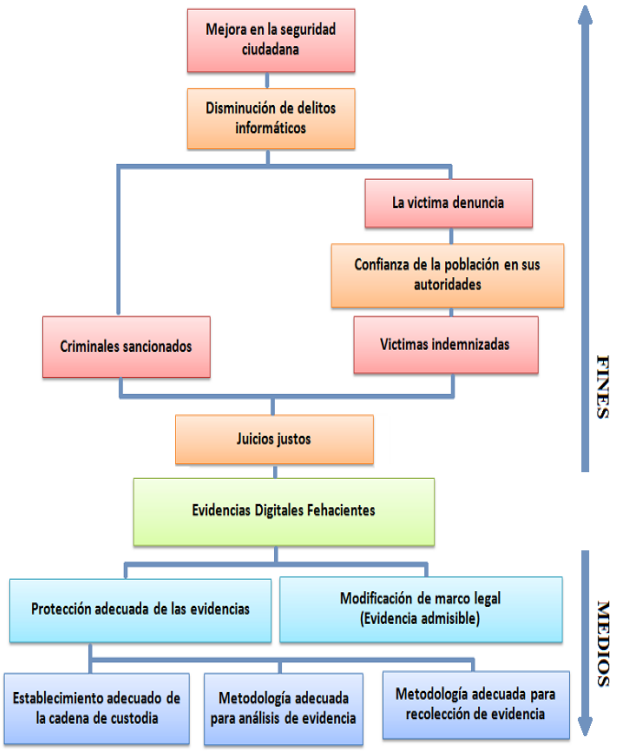
A. Análisis de Participación
(en la siguiente página)

Actor	Problema	Interés Potencial
Víctimas	- No poder hallar al culpable. - No poder denunciar al culpable.	Tener evidencias irrefutables, para que el criminal sea procesado y sancionado.
Inculpados	No poder demostrar su inocencia	Tener evidencias suficientes y fehacientes, para demostrar su inocencia
Población	Incremento de delitos informáticos	Teniendo las evidencias suficientes, los delitos informáticos no quedarían impunes, lo que se puede reflejar en un decremento de la comisión de estos actos
Policía/Poder Judicial /Estado	- Incremento de delitos informáticos. - Pérdida de confianza por parte de la población.	Al seguir un protocolo de recolección de evidencias digitales, se pueden obtener pruebas fehacientes para un proceso legal, lo que contribuirá a un mejor juicio y un aumento en la confianza de la población hacia sus autoridades.
Criminal	Eliminar las evidencias digitales que lo incriminan.	Que las evidencias sean cuestionadas o invalidadas para quedar libre de cargos.

B. Árbol de Problemas



C. Árbol de Objetivos



AGRADECIMIENTOS

REFERENCIAS

[BRKI] BREZINSKI, Dominique, KILLALEA, Tom. *"Guía para recolectar y archivar evidencias – RFC 3227"*, febrero 2002. Consulta: 2 de mayo 2010. (http://www.normesinternet.com/normes.php?rfc=rfc3227&lang=es).

[INEI] Instituto Nacional de Estadística e Informática "*Compendio de Normatividad Sobre el uso de Tecnologías de Información en el Perú"*, Consulta: 23 de julio 2010. (http://www.ongei.gob.pe/publica/metodologias/5125.pdf).

[ONGE] Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), Instituto Nacional de Defensa de la Competencia y de la Protección de Propiedad Intelectual (INDECOPI). *"Guía Técnica Sobre Evaluación de Software para la Administración Pública"*, mayo 2004. Consulta: 20 de julio 2010. (http://www.ongei.gob.pe/Bancos/Banco_Normas/archivos/Guia-Evaluacion-SW.pdf)

[GI06] ZUCCARDI, Giovanni y GUTIÉRREZ, Juan *"Informática Forense"*, Noviembre 2006. Consulta: 5 de mayo del 2010. pag. 9 - 10. (http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf)

[OL01] LÓPEZ, Óscar, AMAYA Haver, LEÓN Ricardo *"Informática Forense: Generalidades, Aspectos Técnicos y Herramientas, 2001"*, Consulta: 2 de abril del 2010.pag. 3. (http://urru.org/papers/RRfraude/InformaticaForense_OL_HA_RL.pdf)

[PPER] "*Protocolo para la investigación Forense en el Perú"*, Julio 2008, Consulta: 20 de abril 2010, pag. 2 – 4 (http://www.scribd.com/doc/2901215/PROTOCOLO-PARA-LA-INVESTIGACION-FORENSE-EN-EL-PERU)

[TI85] TIEDEMANN, "Poder económico y delito, primera edición", Ed. Ariel, Barcelona, 1985, pag. 121-122; Salt, Delitos informáticos de carácter económico, en: Delitos no convencionales, Editores del Puerto, Buenos Aires, 1994, pp. 225-226.

[LU02] REYNA ALFARO, Luis 2002 "Los Delitos Informáticos. Aspectos Criminológicos, Dogmáticos y de Política Criminal", El Jurista, primera edición, pag. 129.

[BRAM] BRAMONT-ARIAS, Luis Alberto.

"Delitos Informáticos", Revista Peruana de Derecho de la Empresa, Derecho Informático y Teleinformática Jurídica N° 51, pag. 2 – 10.

[CO00] Código Penal Peruano, Titulo V, Capítulo X "Delitos Informáticos", Ley Nº 27309, publicada el 15 de Julio 2000.

[CO01] Código Penal Peruano, Titulo IV, Capítulo II "Violación de la Intimidad", Artículo 154.

[CO02] Código Penal Peruano, Titulo IV, Capítulo V "Violación del Secreto Profesional", Artículo 165.

[DB04] FERNÁNDEZ BLEDA, Daniel "Informática Forense Teoría y Práctica", 01 de Noviembre 2004. Consulta.

[CO94] Código Penal Peruano, articulo 186, modificado por la Ley N° 26319, publicada el 27 de Mayo 1994.

[COP2] Código Penal Peruano, art. 19 – art. 427, Decreto Legislativo 681.