Evidencia Digital
Reflexiones Técnicas, Administrativas y Legales

Jeimy J. Cano, M.Sc., Ph.D

GECTI – Facultad de Derecho
Universidad de los Andes
COLOMBIA

jcano@uniandes.edu.co

Créditos y Aclaraciones

- Esta presentación esta basada en los resultados de las investigaciones y comentarios realizados por:
  - Estudiantes curso ISIS337 – Introducción a la Informática Forense (Departamento de Sistemas y Computación – UNIANDES) y
  - Estudiantes curso DERE367 – Internet Principios de Seguridad y Aspectos legales (Facultad de Derecho - UNIANDES)
  - Investigadores del GECTI de la Fac. Derecho – UNIANDES y de la Red ALFA-REDI
- *Las sugerencias efectuadas en esta presentación corresponden a la investigación y análisis de las prácticas y estándares internacionales en el tema de computación forense y evidencia digital.*

JCM-04 All Rights Reserved.

Agenda

- Introducción
- Definiciones
  - Documento Electrónico
  - Evidencia Digital
- Evidencia Digital: ¿Inseguridad Jurídica?
  - Debido registro
  - Admisibilidad
  - Valor probatorio
  - Preservación, Transformación y Recuperación.
- Seguridad Jurídica en medios electrónicos: ¿Posible?
  - Seguridad Informática
  - Computación Forense

JCM-04 All Rights Reserved.

Agenda

- Hacia un escenario conjunto
  - Estrategias Técnicas para Arquitecturas de Computación
  - Consideraciones Organizacionales para Administración de Evidencia Digital
  - Elementos Jurídicos para fortalecer la Evidencia Digital
- Qué sigue?
  - Algunas propuestas para desarrollar
    - Preparación forense de redes
    - Adecuación y aplicación de Estándares Internacionales
    - Adecuación y Preparación de la Administración de Justicia.
- Reflexiones Finales
- Referencias

JCM-04 All Rights Reserved.

Introducción

- La realidad del Comercio Electrónico:
  - Usuarios virtuales e inmateriales
  - Conexiones vía TCP/IP
  - Tránsito y transporte de mensajes en formato electrónico
  - Pagos y transferencias de fondos
  - Registro de transacciones y operaciones

- La realidad del Delito Informático:
  - ¿Sabemos donde están los intrusos?
  - ¿Cómo manipulan las conexiones para evitar el rastreo?
  - ¿Cómo cubren sus rastros?
  - ¿Porqué no se denuncian estos delitos?
  - ¿Estamos preparados para enfrentar y procesar estos delitos?

JCM-04 All Rights Reserved.

Definiciones

- **Documento Electrónico**
  - El documento electrónico en sentido estricto –documento informático- se define como la reprensentación idónea capaz de reproducir una cierta manifestación de la voluntad, materializada a través de las tecnologías de la información sobre soportes magnéticos, *ópticos o similares* (…) que se expresan a través de mensajes digitalizados que requieren de máquinas para ser percibidos y comprendidos por el hombre.
    - Dra. Mariliana Rico – Venezuela (las *cursivas* son el autor)
- **Evidencia Digital**
  - Es un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.(Casey 2000, pág.4).
    - Eoghan Casey, MA.

JCM-04 All Rights Reserved.

Evidencia Digital: ¿Inseguridad Jurídica?

- Debido Registro
  - Registro de transacciones de operaciones, como demostrar que:
    - *No han sido alteradas*
    - *Que con el paso del tiempo puedo tener acceso a ellas.*
    - *Tengo control de acceso a estos registros*
    - *Sólo personal autorizado tiene derecho a verlos*
    - *Puedo verificar cuando un cambio se ha realizado en ellos.*
  - Retos
    - *Políticas sobre Registros Electrónicos*
    - *Estrategias de verificación y control*
    - *Transformación y permanencia en el tiempo*

JCM-04 All Rights Reserved.

Evidencia Digital: ¿Inseguridad Jurídica?

- Admisibilidad
  - Asegurar las características de: Autenticidad, Confiabilidad, Suficiencia y conformidad con la leyes y reglas de la administración de justicia
    - *Cómo se establece la autenticidad en medios electrónicos?*
    - *Son confiables los registros electrónicos que generan los sistemas electrónicos o informáticos?*
    - *Estarán completos los datos que se presenta en los archivos analizados?*
    - *Cómo fueron obtenidas estas evidencias digitales?*
  - Retos
    - *Estrategias de control de integridad*
    - *Correlación de eventos y registros*
    - *Procedimientos y controles para control y manejo de evidencia digital*

JCM-04 All Rights Reserved.

Evidencia Digital: ¿Inseguridad Jurídica?

- Valor Probatorio
  - Si bien no se negará fuerza o capacidad probatoria a los mensajes en medios electrónicos, la pregunta es: ¿ cómo probar ?
    - *Confio plenamente en el dictámen pericial?*
    - *Los procedimientos utilizados por el perito fueron los más adecuados?*
    - *El manejo y control de la evidencia fueron adecuados?*
    - *Son reconocidos tanto los métodos como las herramientas utilizadas por el perito?*
    - *El entrenamiento y habilidades del perito son las indicadas?*
  - Retos
    - *Estándares de Administración de Evidencia Digital*
    - *Formación en Computación Forense*
    - *Investigación y formalización de pruebas sobre las herramientas forenses en informática.*

JCM-04 All Rights Reserved.

Evidencia Digital: ¿Inseguridad Jurídica?

- Preservación, Transformación y Recuperación
  - La evidencia digital debe permanecer en el tiempo, con sus características y propiedades para propósitos históricos y probatorios.
    - *Qué medios son los más adecuados para su almacenamiento?*
    - *Puedo cambiar el formato de la evidencia inicial a otro con idénticas o mejores características? Son válidas?*
    - *Qué ocurre si no puedo recuperar la información previamente almacenada? Puedo incurrir en una falta ante la Administración de Justicia?*
    - *Ante una pérdida de información crítica de la organización, puedo incurrir en sanciones por impericia, imprudencia u omisión?*
  - Retos
    - *Estrategias de Intercambiabilidad de formatos de archivos*
    - *Herramientas de Recuperación de Información y Planes de Recuperación de Negocio.*
    - *Administración de Respaldos de Información.*

JCM-04 All Rights Reserved.

Seguridad Jurídica en medios Electrónicos: ¿Posible?

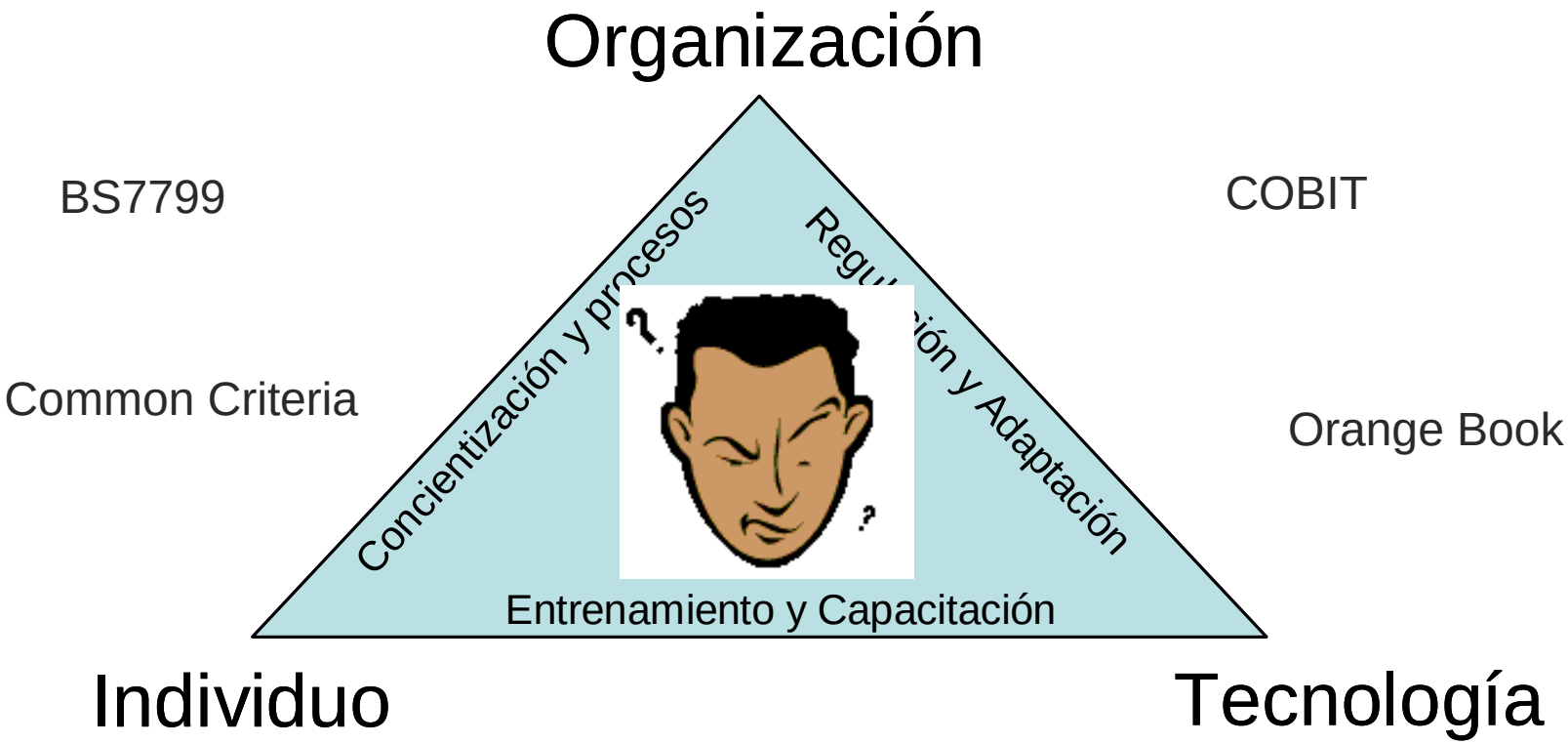
- En el mundo *Offline*, la seguridad jurídica cuenta con procedimientos y ordenamientos jurídicos que salvaguardan la evidencia física.

- En el Mundo *Online*, la seguridad jurídica debe estar asistida por la seguridad informática.
  - La seguridad informática es una disciplina científica que se podría revisar desde tres perspectivas complementarias:
    - Lo tecnológico
    - Lo administrativo
    - Lo humano

JCM-04 All Rights Reserved.

Seguridad Jurídica en medios Electrónicos: ¿Posible?

- Seguridad Informática: Una mirada sistémica

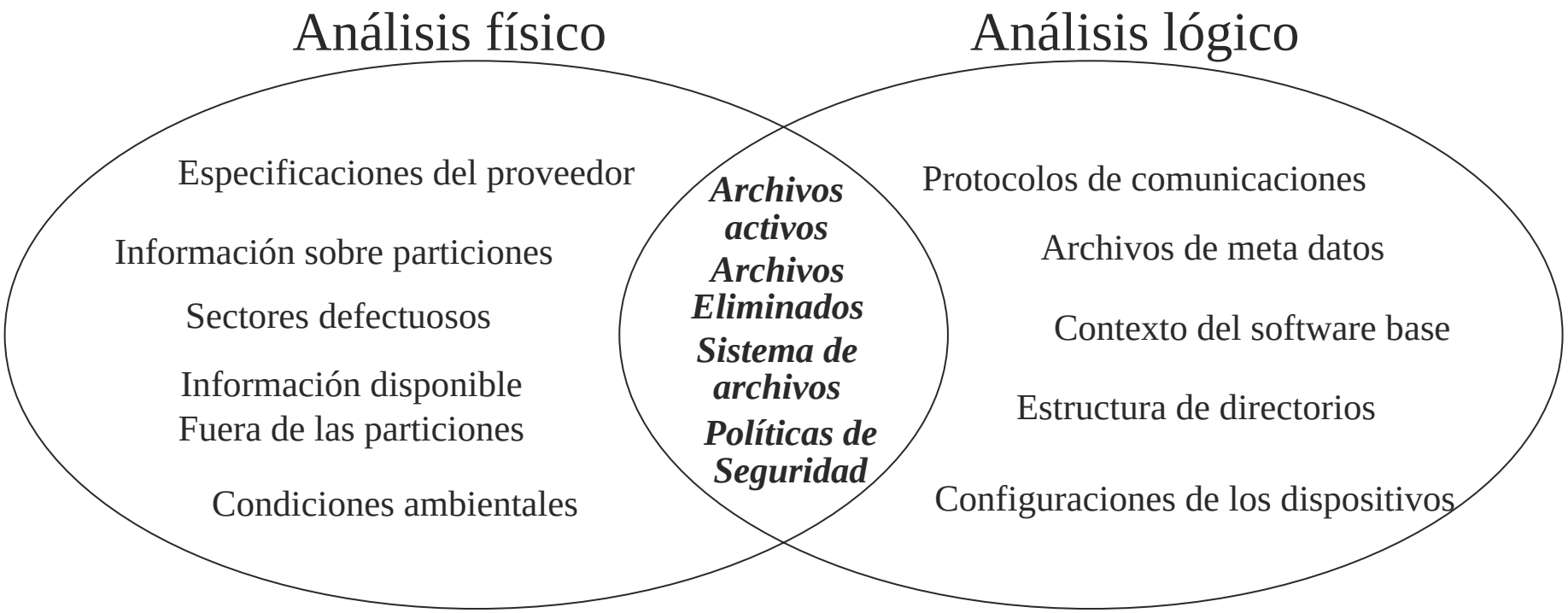


Tomado de: CANO, J. (2004) **Hacia un concepto extendido de la mente segura: pensamiento sistémico en seguridad informática. Documento de Trabajo. Universidad de los Andes. En revisión.**

JCM-04 All Rights Reserved.

Seguridad Jurídica en medios Electrónicos: ¿Posible?

- Computación Forense: Una revisión operacional

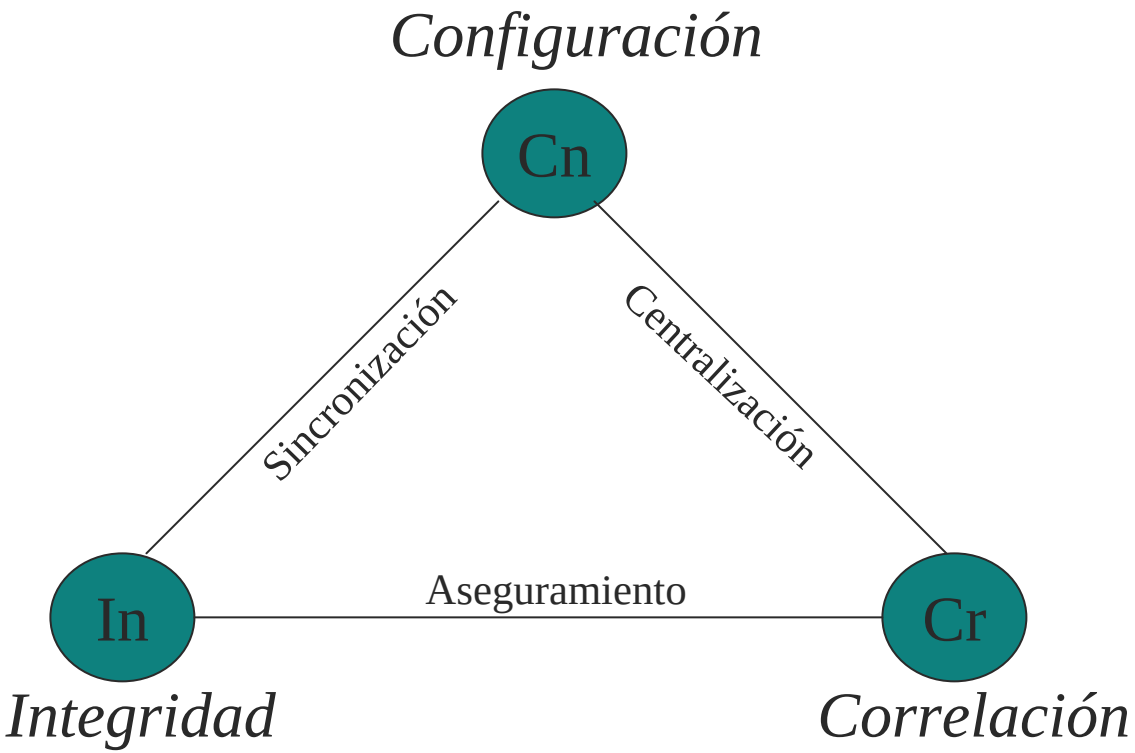


Adaptado de: Mandia y Prosise. 2001. Pág. 118

JCM-04 All Rights Reserved.

Hacia un escenario conjunto

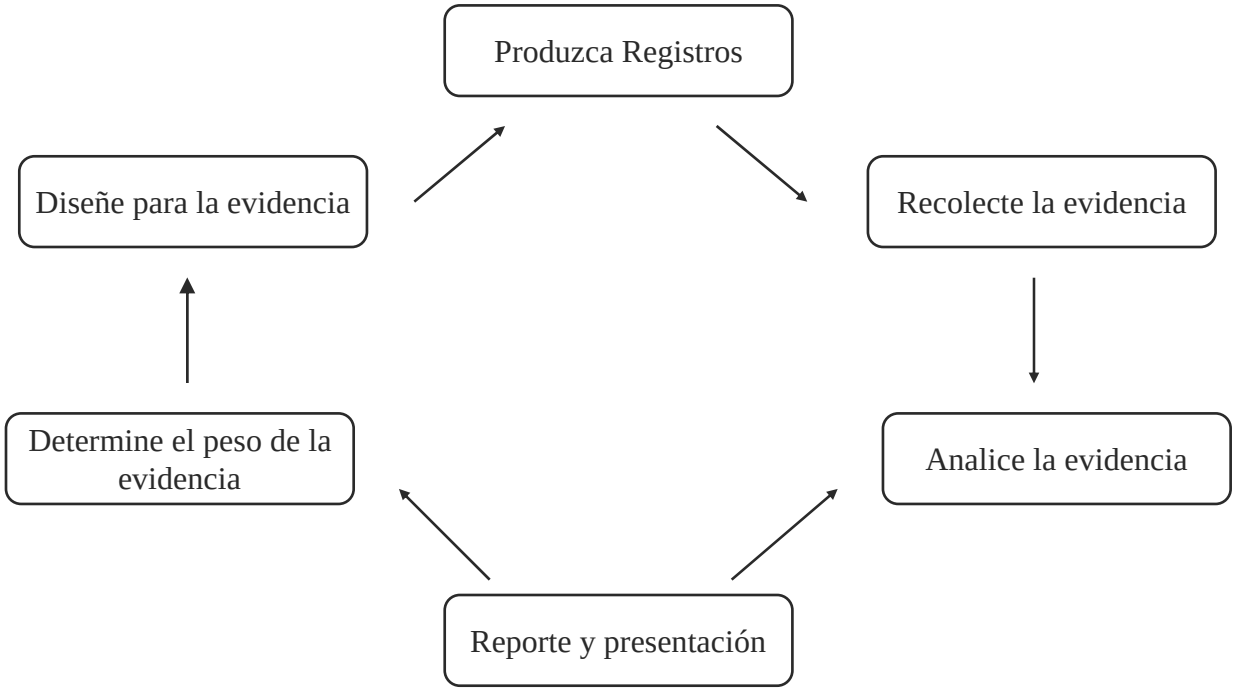
- Estrategias Técnicas para Arquitecturas de Computación



JCM-04 All Rights Reserved.

Hacia un escenario conjunto

- Consideraciones Organizacionales para la Administración de Evidencia Digital

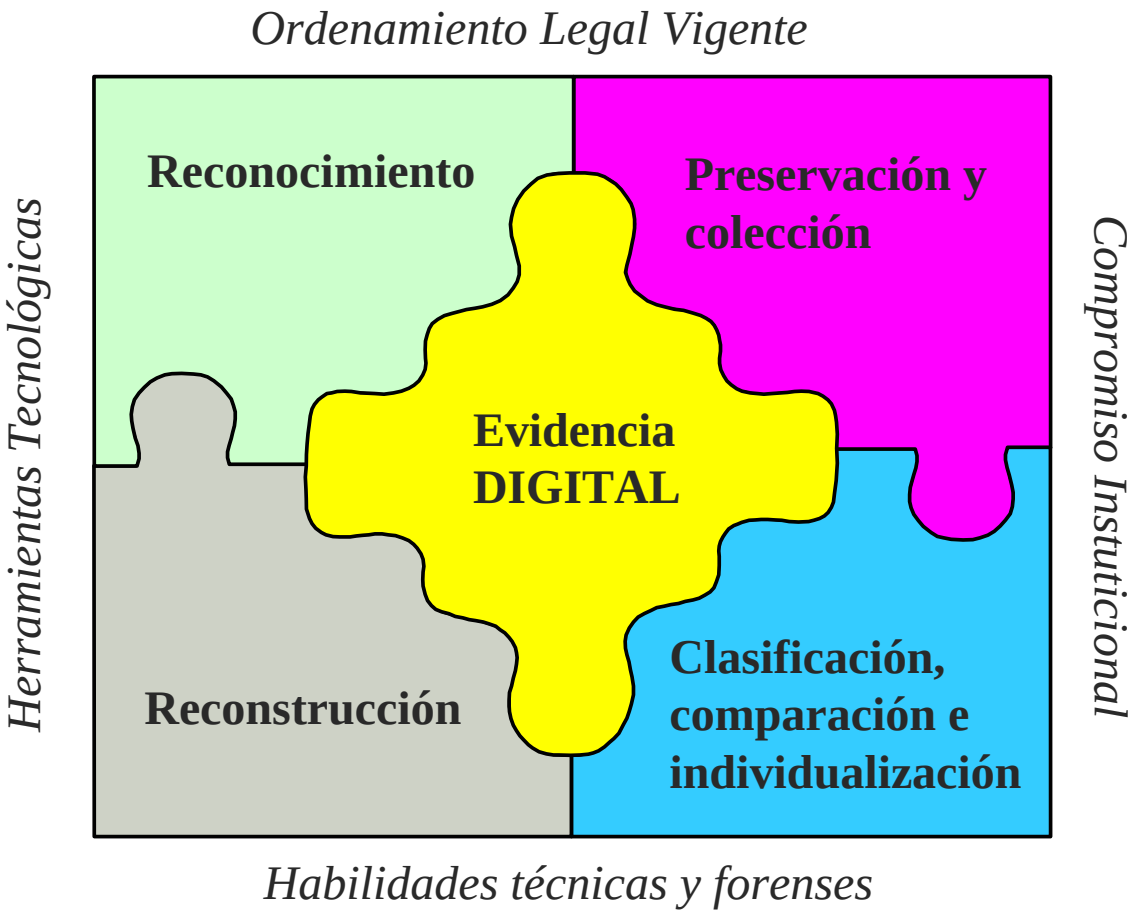


Ciclo de la Evidencia Digital
HB-171-2003 Guidelines for the Management of IT Evidence
Standards Australia

JCM-04 All Rights Reserved.

Hacia un escenario conjunto

- Elemento Jurídicos para fortalecer la Evidencia Digital



JCM-04 All Rights Reserved.

Adaptado de: CASEY 2000. Pág. 47

¿Qué sigue?

- Preparación Forense de Redes

JCM-04 All Rights Reserved.

¿Qué sigue?

- Adecuación y Aplicación de Estándares Internacionales
  - HB 171-2003
    - Determine el peso de la evidencia
      - Clasificación de Información
    - Diseñe para la evidencia
      - Establezca las características de la estrategia de Logging
    - Produzca los registros
      - Confiabilidad de los registros y sistemas que los generan
    - Recolecte la evidencia
      - Estrategias de centralización y control / Cadena de Custodia
    - Analice la evidencia
      - Correlación
      - Exploración y detalle de los medios y registros.
    - Reporte y presente la evidencia
      - Características y alcance de los reportes.

JCM-04 All Rights Reserved.

¿Qué sigue?

- Adecuación y Preparción de la Administración de Justicia
  - Estándares sobre Admisibilidad de Evidencia Digital
  - Desarrollo de buenas prácticas en Computación Forense
  - Entrenamiento y Desarrollo de competencias técnicas para los Jueces y fiscales
  - Adecuación de Procedimientos Civiles y Penales alrededor de la evidencia digital
  - Generación de cultura del registro y seguridad de la información.

JCM-04 All Rights Reserved.

Reflexiones Finales

- ¿Qué es lo que esta pasando?
  - *Existe mucha evidencia de los hechos, pero hay poco tiempo para su análisis.*
  - *Poca conciencia del Legislador sobre las conductas punibles en medios informáticos y telemáticos.*
  - *Conflictos académicos y científicos entre el Derecho y la Tecnología: Un lenguaje no común.*
  - *Limitada formación interdisciplinaria para repensar el derecho a la luz de la tecnología y viceversa.*
  - *Poco interés de las organizaciones alrededor de la evidencia digital y sus implicaciones jurídicas y de negocio.*

JCM-04 All Rights Reserved.

Referencias

- Mandia, K., Prosise, C. y Pepe, M. (2003) Incident Response & Computer Forensics. Second Edition. Mc Graw Hill
- Osterburg, J. y Ward, R. (2000) Criminal Investigation. 3rd Edition. Anderson Publishing Co.
- Marcella, A. y Greenfield, R. (2002) Cyber forensics. Auerbach publications.
- Ackoff, R. (2002) El paradigma de Ackoff. Una administración sistémica. Limusa Wiley.
- Reyes Echandía, A. (2003) Criminología. Cuarta reimpresión de la octava edición. Editorial Temis.
- Parker, D. (1998) Fighting computer crime. A new framework for protecting information. John Wiley & Son.
- Casey, E. (2000) Digital Evidence and Computer Crime. Academic Press.
- Stephenson, P. (1999) Investigation Computer Related Crime. Crc Press.
- Standards Australia International (2003) HB 171-2003 Guidelines for the management of IT Evidence.
- American Bar Association. Section of Litigation (2003) Electronic Discovery Standards-Draft Amendments to ABA Civil Discovery Standards. http://www.abanet.org/litigation
- Cano J. (2004) *Inseguridad Informática. Un concepto dual en Seguridad Informática*. ComputerWorld Colombia. Marzo 1-5/2004. (http://www.virusprot.com/art47.htm)

JCM-04 All Rights Reserved.

Referencias

- Alberts, C. y Dorofee, A. (2002) Managing Information Security Risks: The OCTAVE Approach. Addison Wesley.
- LittleJohn, D. (2002) Scene of Cybercrime. Computer Forensic Handbook. Syngress Publishing Inc.
- ADAMSKI, A. (1999) Crimes related to the computer network. Threats and opportunities: A criminological perspective. http://www.infowar.com/
- Shaw, P. (1998) Managing legal and security risk in computing and communications. Butterworth-Heinemann.
- Peikari, C y Chuvakin, A. (2004) Security Warrior. O'Reilly.
- Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática. (2003) Derecho de Internet & Telecomunicaciones. Universidad de los Andes – Legis.
- Brown, C. (2002) Procedural aspects of obtaining computer evidence with highlights from the DoJ Search & Seizure Manual. Technology Pathways LLC. http://www.techpathway.com (resource center).
- Conway, P. (1999) *The relevance of preservation in digital world*. Yale University Library.
- SOMMER, P. (2000) Digital Footprints: Assessing Computer Evidence. British Computer Society Legal Affairs Committee. http://www.bcs.org.uk/lac/df.htm
- SOMMER, P. (2000b) Downloads, logs and captures: Evidence from Cyberspace. British Computer Society Legal Affairs Committee. http://www.bcs.org.uk/lac/dlc.htm
- SOUS BOIS, R. (2000) Elements for testing of internet investigators. IOCE – International Organization on Computer Evidence. IOCE 2000 Conference. http://www.ioce.org.

JCM-04 All Rights Reserved.

Referencias

- CANO, J. (2001) Credenciales para investigadores forenses en informática. Certificaciones y entrenamiento. Revista Electrónica de Derecho Informático. No.38. Septiembre. http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=114090
- CANO, J. (2001b) Informática Forense, liderando las investigaciones. Portal de Seguridad Virusprot. http://www.virusprot.com/Col8.html
- CASEY, E (2002) Error, uncertainty, and loss in Digital Evidence. International Journal of Digital Evidence. Vol.1. Issue 2. Summer.
- CASEY, E. (2000) Digital Evidence and Computer Crime. Academic Press.
- CASEY, E. (2001) Handbook of Computer Crime Investigation. Academic Press.
- CERT (2002) Overview of attack trends. http://www.cert.org/archive/pdf/attack_trends.pdf
- COUNCIL OF EUROPE. (2001) Convention on Cybercrime. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
- Digital Evidence: Standards and Principles. Scientific Working Group on Digital Evidence (SWGDE). International Organization on Digital Evidence (IOCE). (2000) http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm. Forensic Science Communication Vol2 No.2
- DIGITAL FORENSIC RESEACH WORKSHOP – DFRWS (2001) A road map for Digital Forensic Research. Technical Report. http://www.dfrws.org
- DIPPEL, T. (2000) IT as an Enabler of Computer Fraud. Information Security Technical Report. Vol.5, No.2. pp 60-70

JCM-04 All Rights Reserved.

Evidencia Digital
Reflexiones Técnicas, Administrativas y Legales

Jeimy J. Cano, M.Sc., Ph.D

GECTI – Facultad de Derecho
Universidad de los Andes
COLOMBIA

jcano@uniandes.edu.co