Riesgos emergentes para los informáticos forenses.

Retos y oportunidades

Jeimy J. Cano, Ph.D, CFE
Profesor Distinguido
GECTI - Facultad de Derecho
Universidad de los Andes

¡ NOTA DE ADVERTENCIA !

- La presentación que se desarrolla a continuación es producto del análisis de fuentes y mejores prácticas en computación forense y anti-forense, y su aplicación en diferentes contextos tecnológicos.

- Las reflexiones y propuestas que se presentan en este documento son una excusa académica para continuar aprendiendo de este novedoso y exigente mundo de la computación forense y anti-forense.

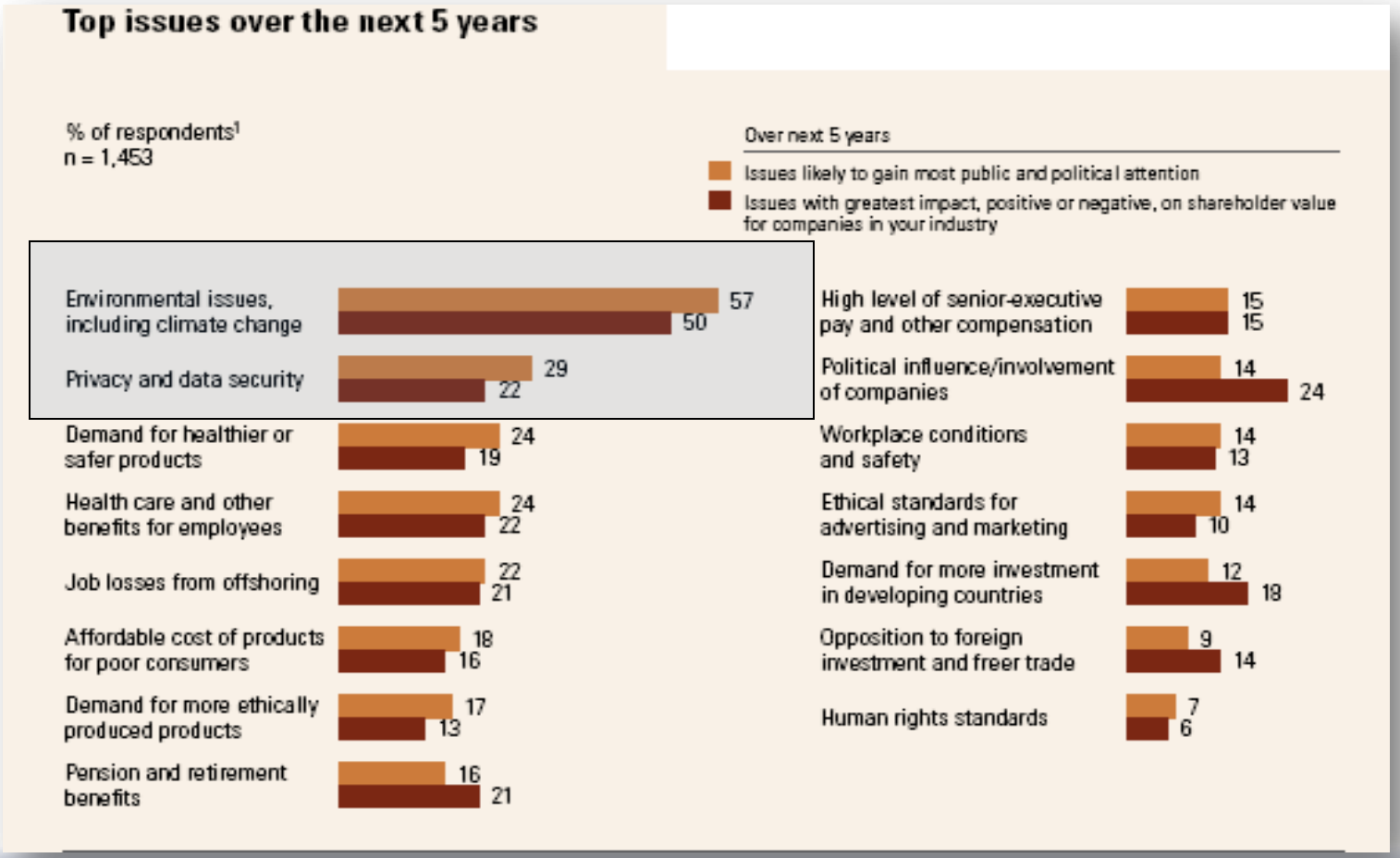
JCM10-All rights reserved

Agenda

1. Introducción (Preocupaciones de los CEO y CIO)
2. Estado de la investigación en computación forense
3. Retos emergentes en seguridad de la información
4. Desafíos de la computación forense
5. Reflexiones finales
6. Referencias

JCM10-All rights reserved

Preocupaciones de los CEO



Tomado de: Mckinsey Quarterly Sept.2008 – How global executives view sociopolitical issues. Pag 5

JCM10-All rights reserved

Preocupaciones de los CIO

Figure 2: Top 10 Management Concerns—Ranking of Importance Based on All Respondents (Number of Respondents Shown in Parentheses)

	(105)	(182)	(301)	(108)	(104)	(68)	(54)	(417)
	2005	**2004**	**2003**	**1994**	**1990**	**1986**	**1983**	**1980**
IT and business alignment	1	1	1	9	7	5	7	-
Attracting, developing, and retaining IT professionals	2	2	4	8	4	12	8	7
Security and privacy	2	3	3	-	19	18	14	12
IT strategic planning	4	4	2	10	3	1	1	1
Business process engineering	5	11	11	2	-	-	-	-
Introducing rapid business solutions	6	14	-	-	-	-	-	-
Measuring the value of IT investments	7	11	5	-	-	-	-	-
True return on IT investment What is true return and why was it newly listed this year?	7	-	-	-	-	-	-	-
Complexity reduction	9	6	8	-	-	-	-	-
IT governance	10	10	10	-	-	-	-	-
Project management capability	10	-	-	-	-	-	-	-

Tomado de: LUFTMAN, J., KEMPAIAH, R. y NASH,E. 2006. pag.83

JCM10-All rights reserved

Estado de la investigación en cómputo forense

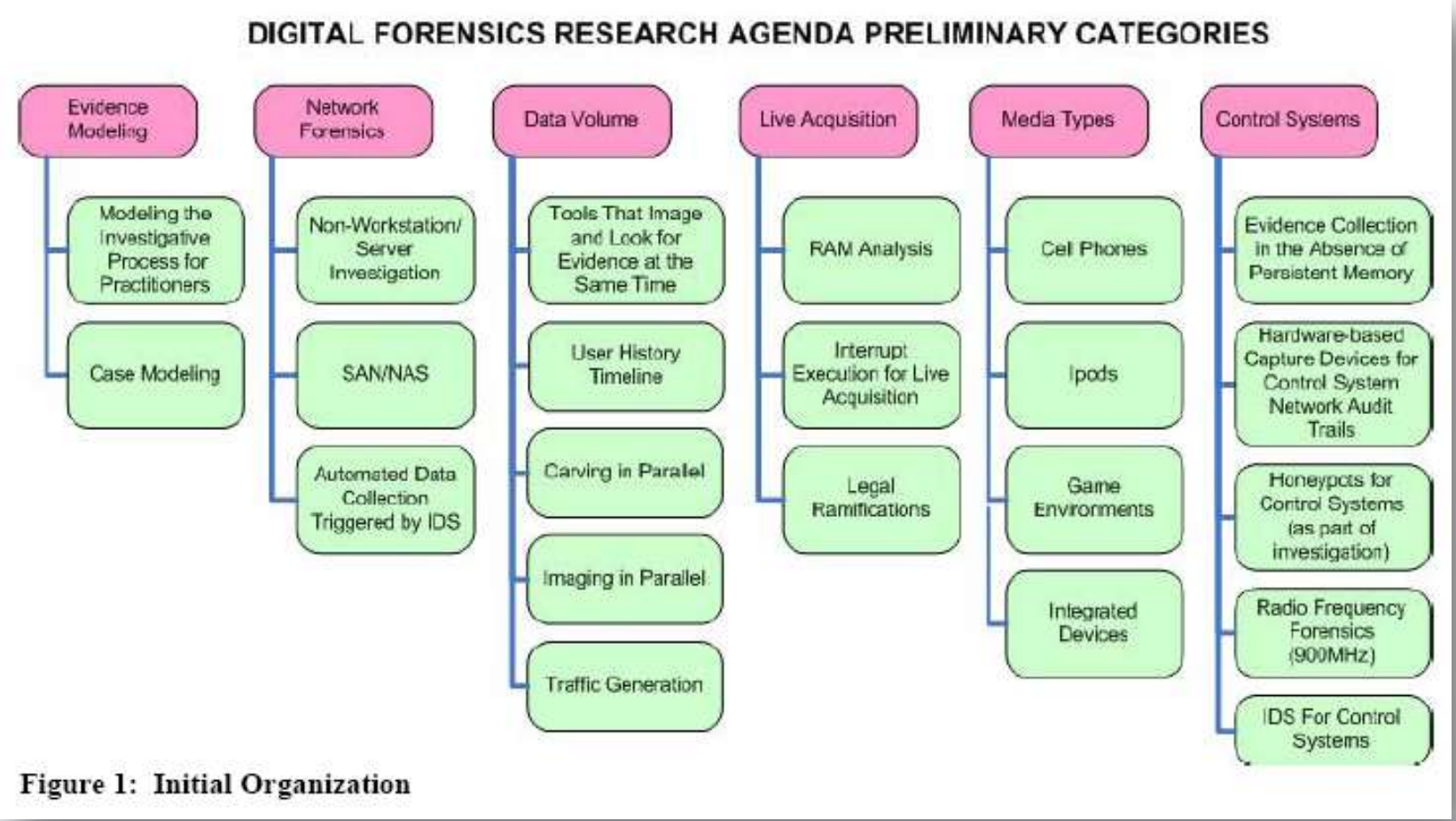


Figure 1: Initial Organization

Tomado de: Nance, Hay y Bishop 2009.

JCM10-All rights reserved

JCM10-All rights reserved

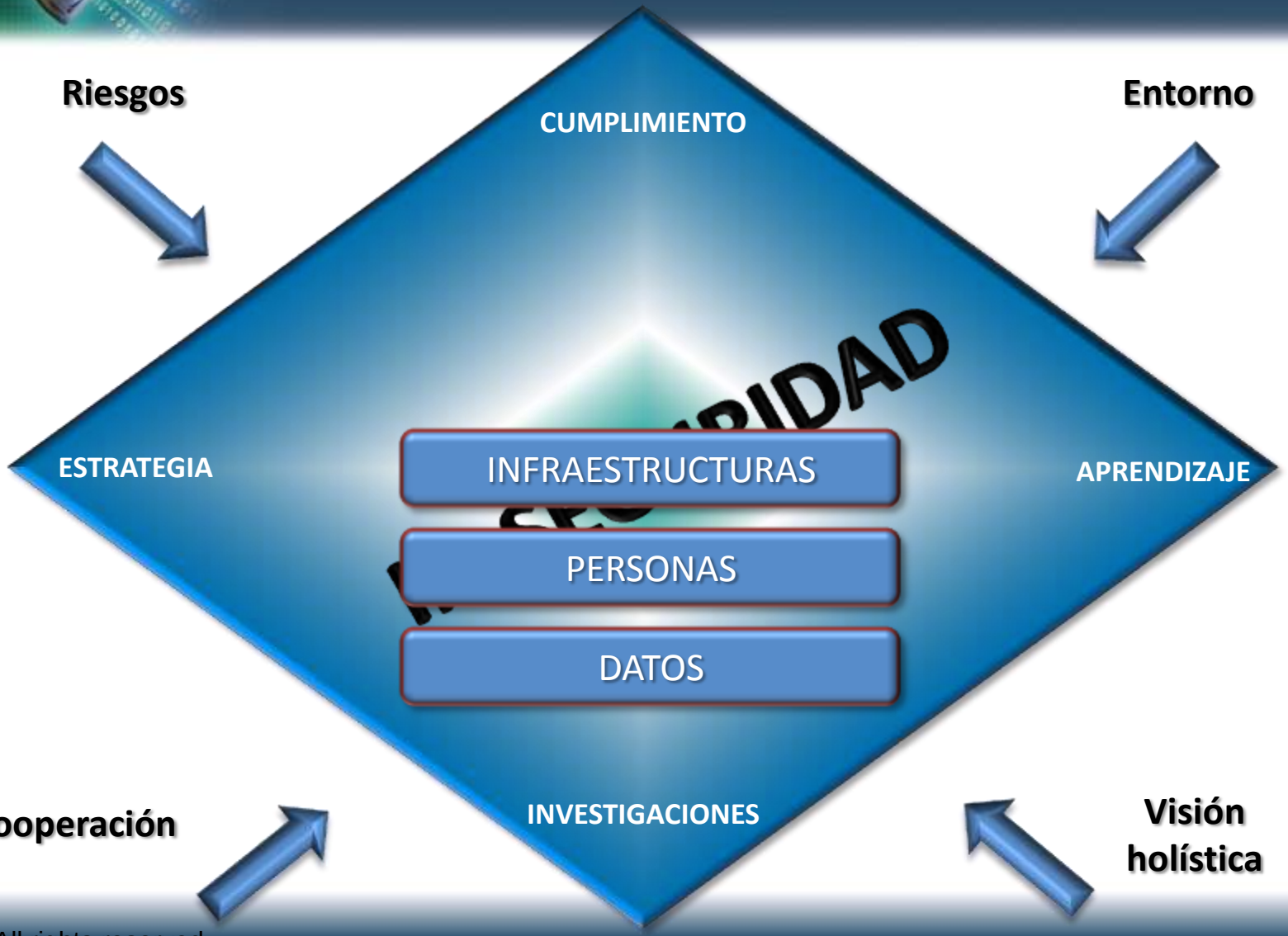
Retos emergentes en seguridad de la información

JCM10-All rights reserved

Retos emergentes en seguridad de la información

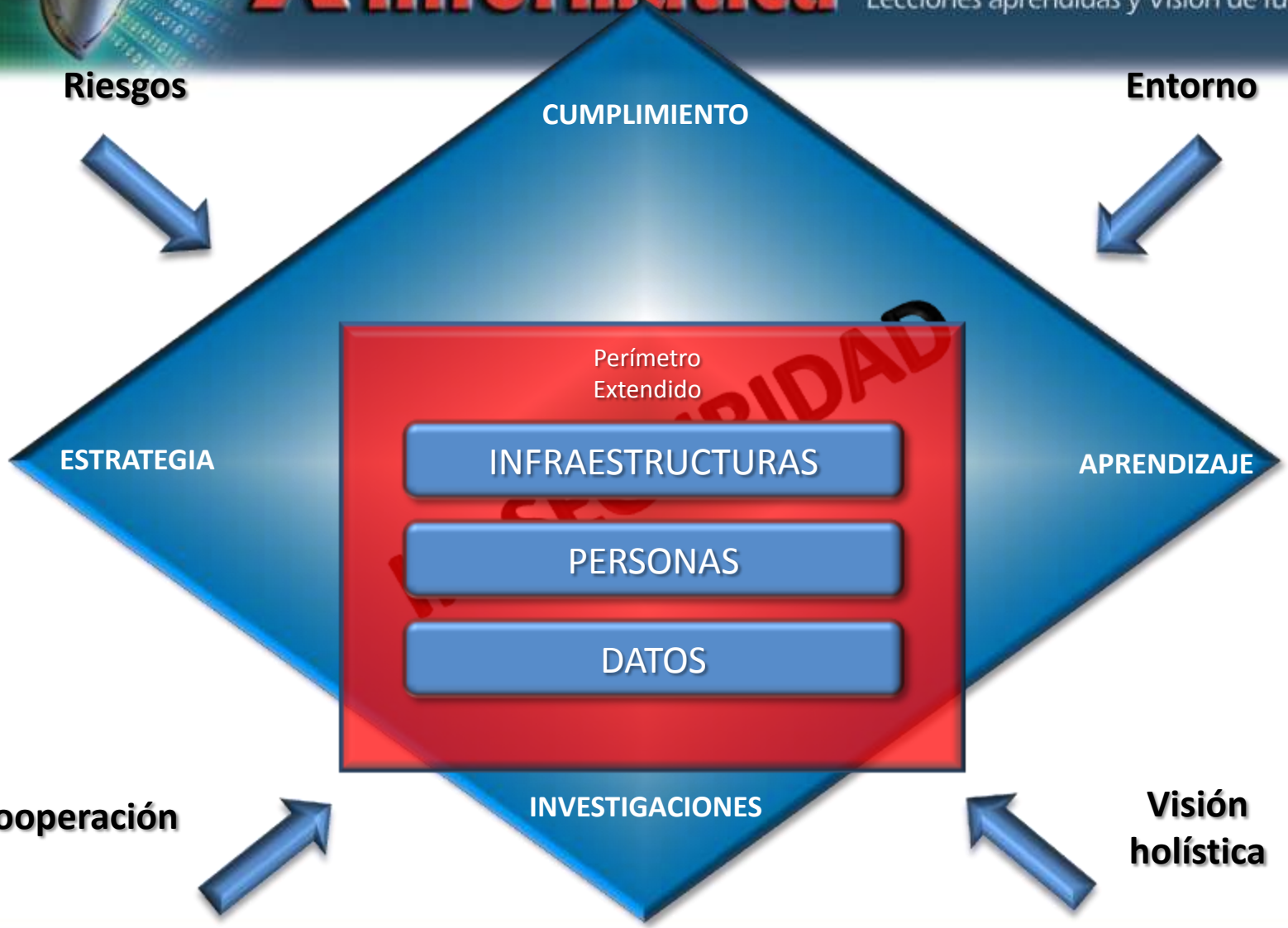
JCM10-All rights reserved

Retos emergentes en seguridad de la información



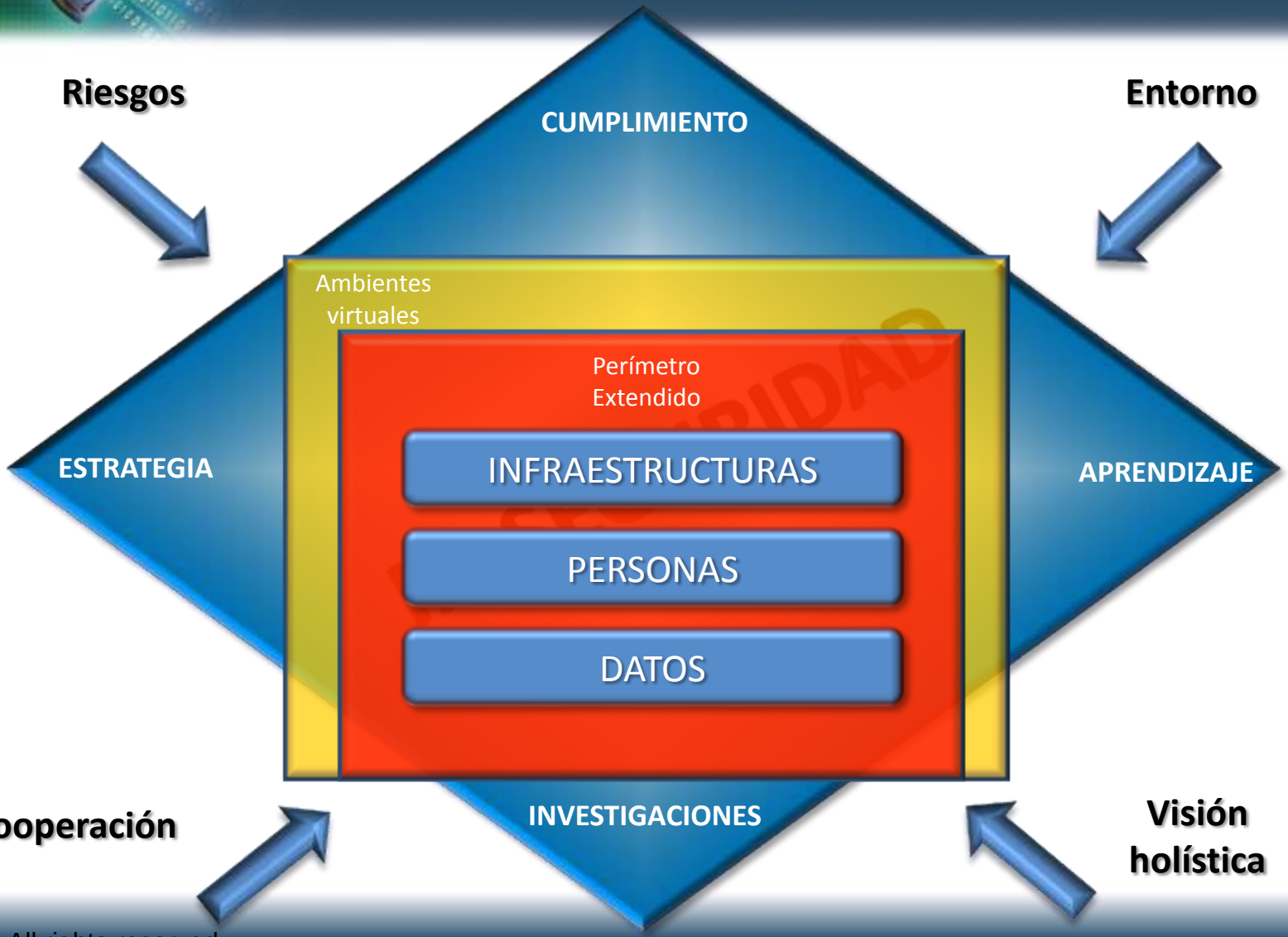
JCM10-All rights reserved

Retos emergentes en seguridad de la información



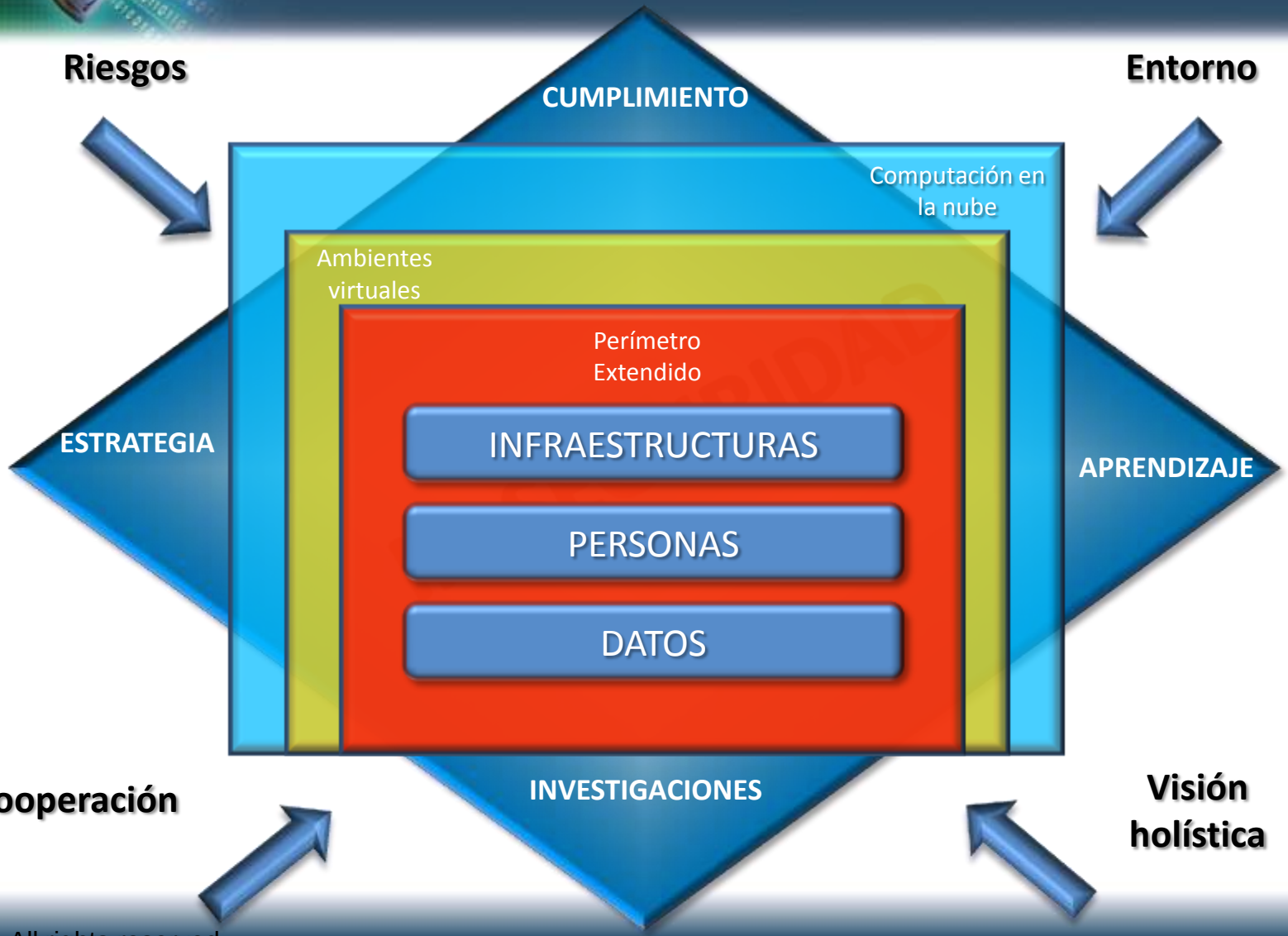
JCM10-All rights reserved

Retos emergentes en seguridad de la información



JCM10-All rights reserved

Retos emergentes en seguridad de la información

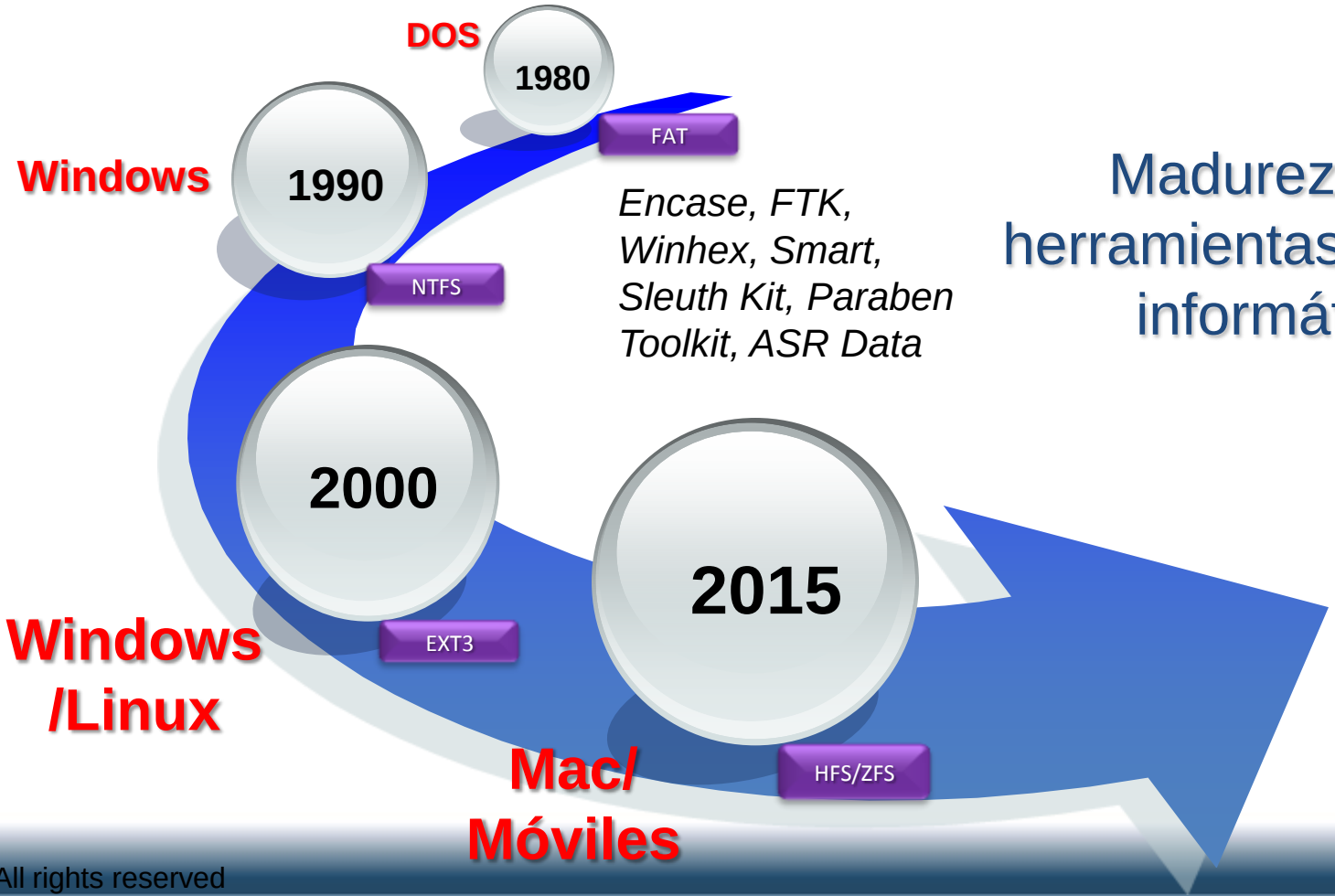


JCM10-All rights reserved

Desafíos de la computación forense

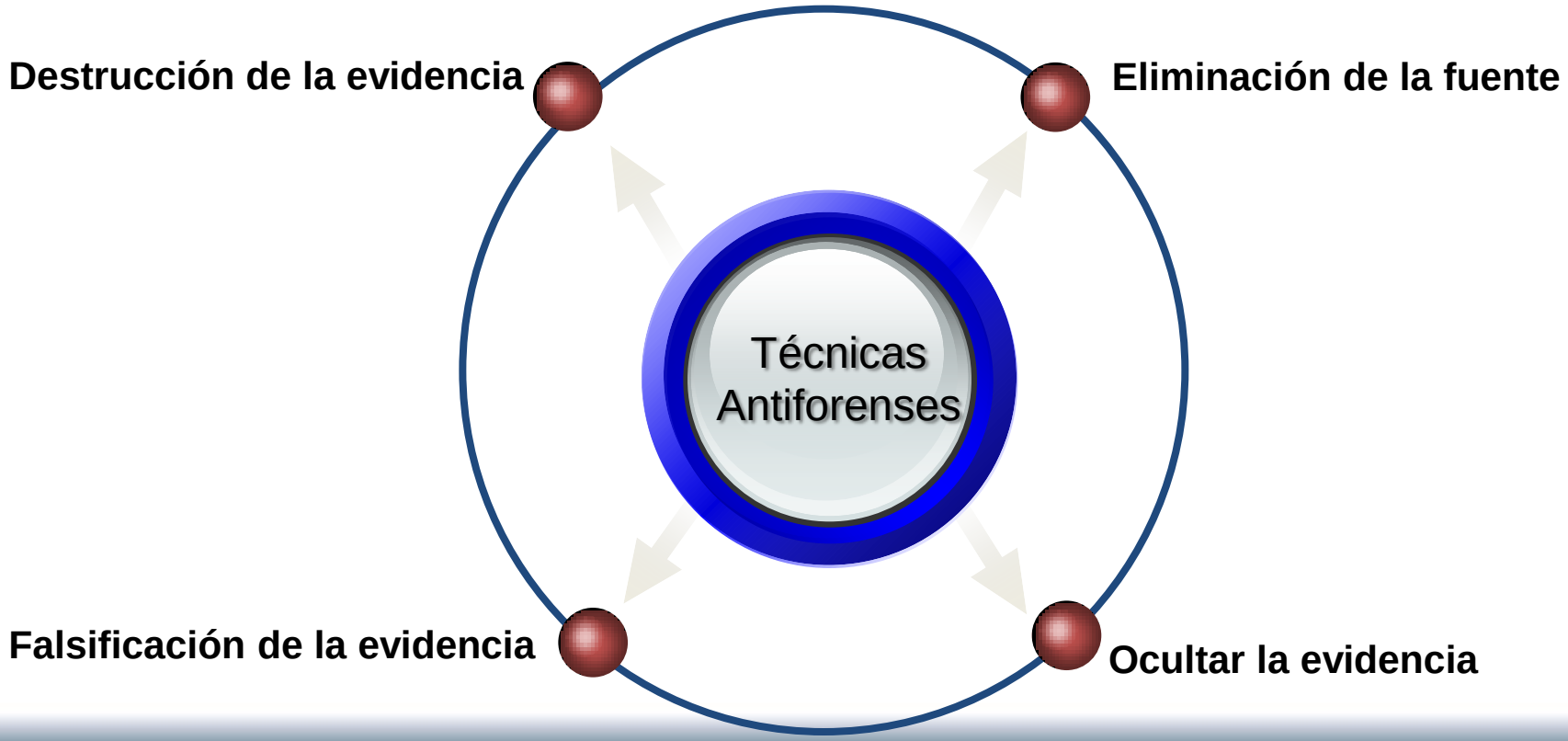
JCM10-All rights reserved

Desafíos de la computación forense



JCM10-All rights reserved

Desafíos de la computación forense



JCM10-All rights reserved

Desafíos de la computación forense

- Técnicas antiforenses -

- Una definición base:
  - *"Cualquier intento exitoso efectuado por un individuo o proceso que impacte de manera negativa la identificación, la disponibilidad, la confiabilidad y la relevancia de la evidencia digital en un proceso forense*".

JCM10-All rights reserved

Desafíos de la computación forense

- ¿Qué buscan las técnicas antiforenses?

- *Limitar la detección de un evento que haya ocurrido.*
- *Distorsionar la información residente en el sitio.*
- *Incrementar el tiempo requerido para la investigación del caso.*
- *Generar dudas en el informe forense o en el testimonio que se presente.*
- *Engañar y limitar la operación de las herramientas forenses informáticas.*
- *Diseñar y ejecutar un ataque contra el investigador forense que realiza la pericia.*
- *Eliminar los rastros que pudiesen haber quedado luego de los hechos investigados.*

Tomado de: CANO 2009, Cap.4

JCM10-All rights reserved

MoDeRaTA - Consideraciones

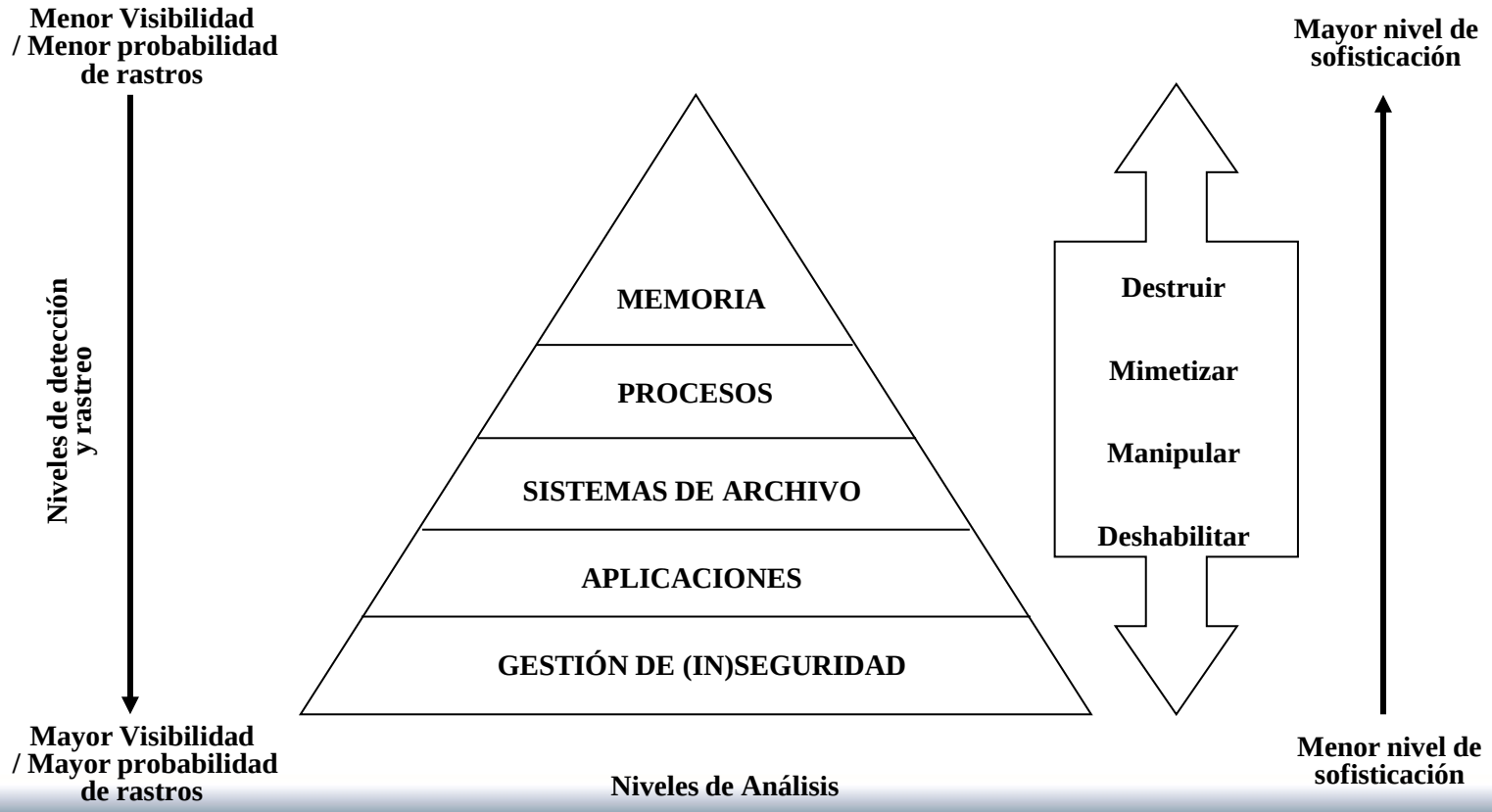
- Niveles
  - Definen los elementos susceptibles donde se pueden materializar las técnicas antiforenses

- Detección y Rastreo
  - Establece los rangos y grados en los cuales es posible detectar y rastrear la materialización de técnicas antiforenses
  - Incluye el nivel de esfuerzo (sofisticación) requerido por el atacante para materializar la técnica antiforense

- Técnica utilizada
  - Destruir / Mimetizar / Manipular / Deshabilitar, las cuales se pueden materializar en todos los nivel definidos en el modelo

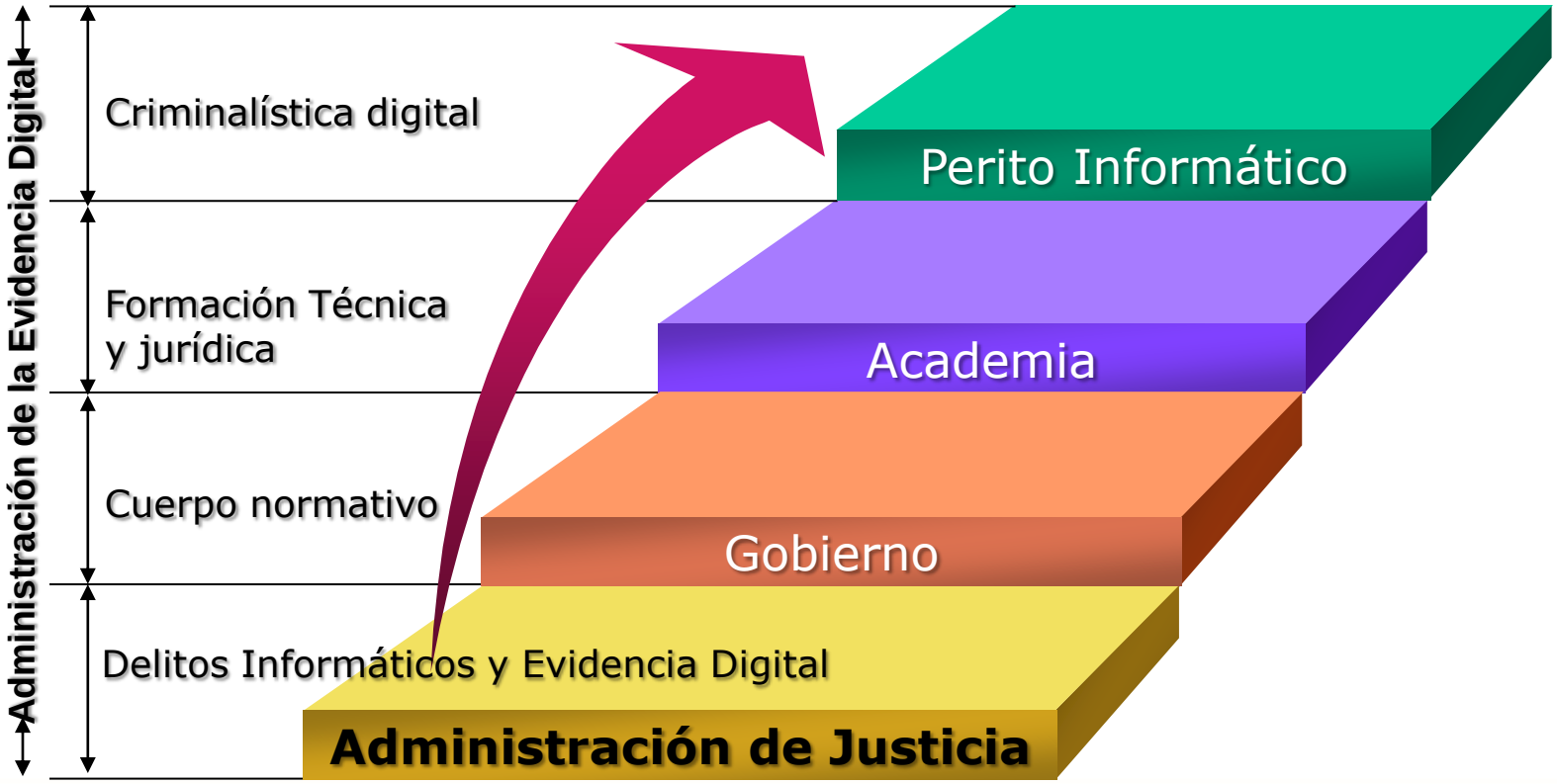
JCM10-All rights reserved

Modelo Conceptual de detección y rastreo de técnicas antiforenses – MoDeRaTA



JCM10-All rights reserved

Desafíos de la computación forense



JCM10-All rights reserved

El proceso forense y la administración de justicia

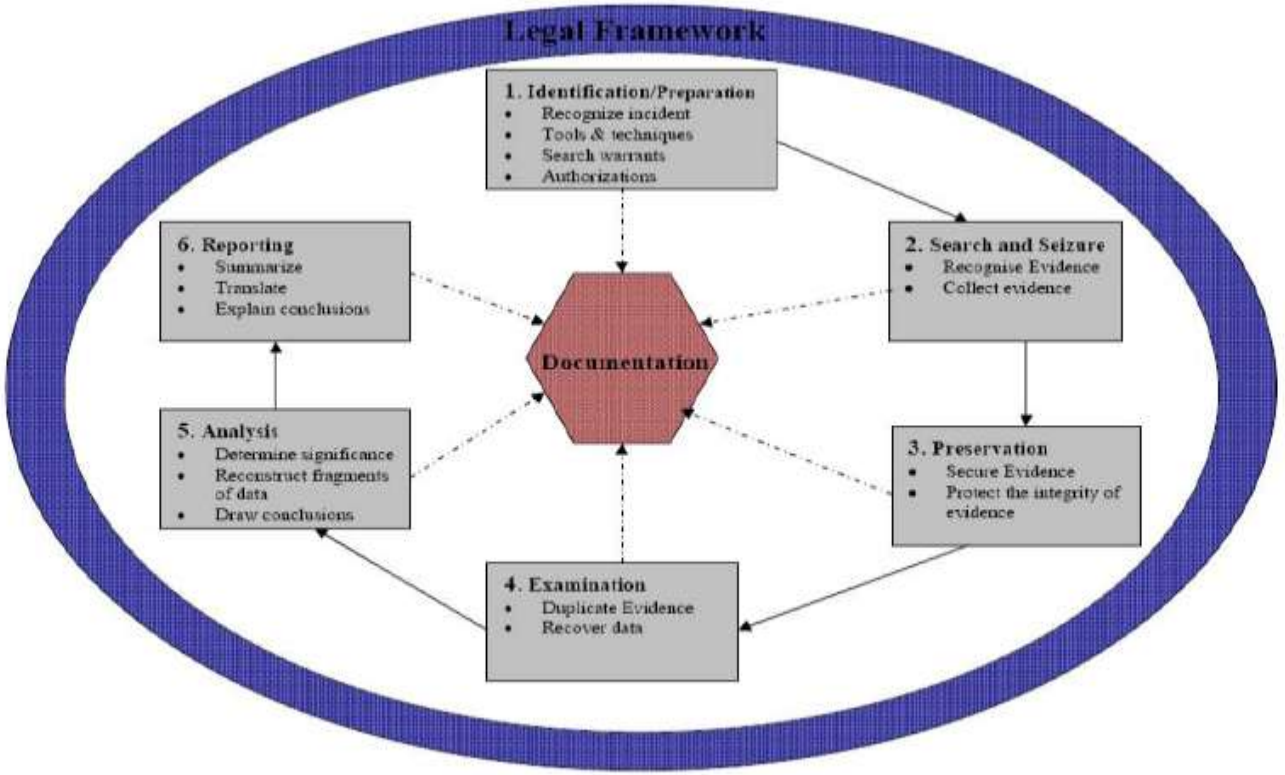
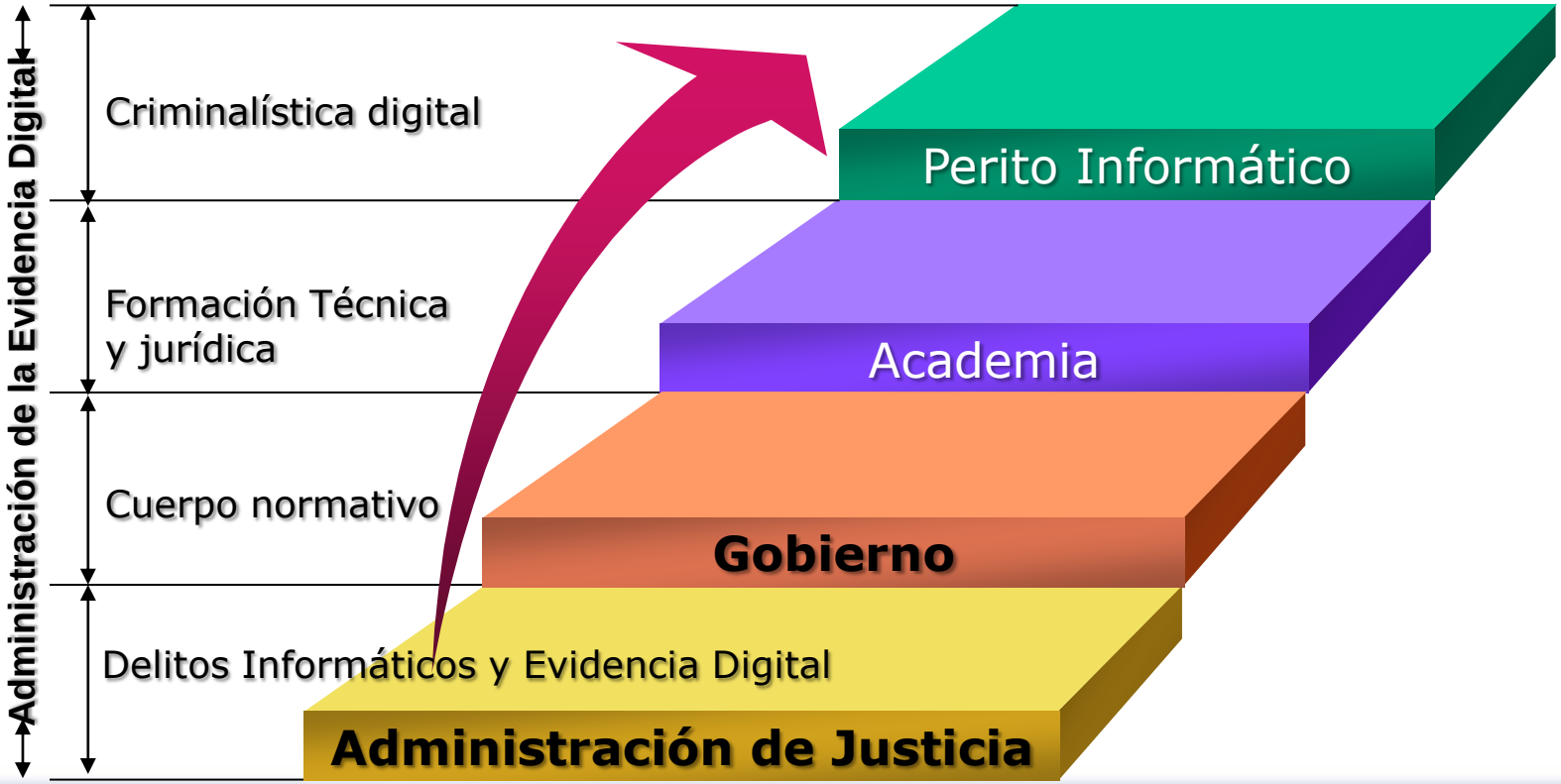


Figure 1: A process Model for seizure and handling of forensic evidence

Tomado de: Digital Forensics and the legal System. James Tetteh Ami-Narh y Patricia A H Williams. Edith Cowan University. Australia. *Proceedings of The 6th Australian Digital Forensics Conference*. 2008

JCM10-All rights reserved

Desafíos de la computación forense



JCM10-All rights reserved

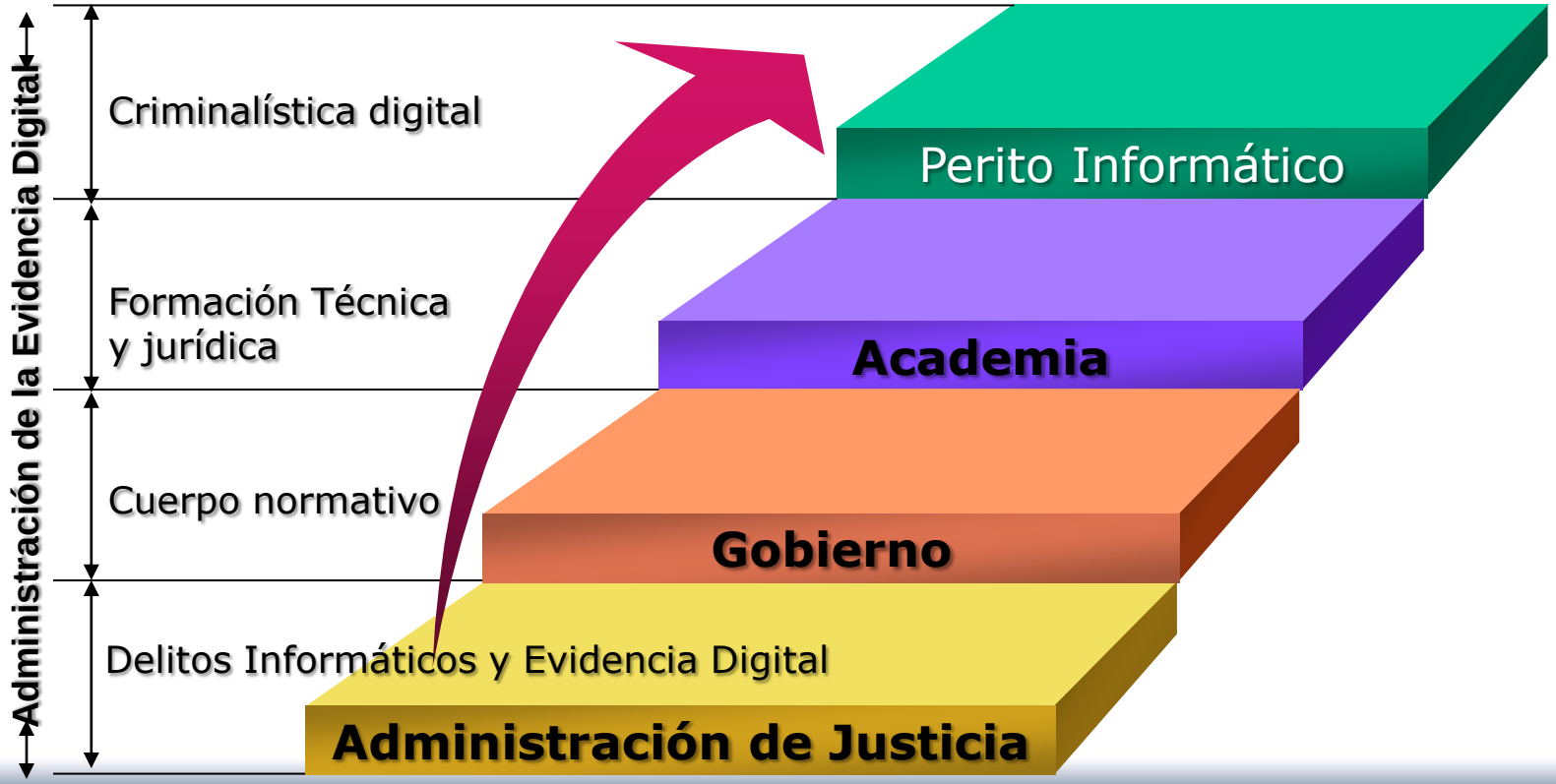
Necesidades identificadas por los gobiernos

- **Estados Unidos – National Institute of Justice - 2001**
  - ***Principales preocupaciones alrededor de la delincuencia informática***
    - Concientización del público
    - Estadísticas y datos sobre delitos informáticos
    - Entrenamiento uniforme y cursos de certificación para investigadores
    - Asistencia en sitio para las unidades de lucha contra el delito informático
    - Actualización del marco normativo
    - Cooperación con los proveedores de alta tecnología
    - Investigaciones y publicaciones especializadas en crímenes de alta tecnología
    - Concientización y soporte de la gerencia
    - Herramientas forenses y de investigación criminal informática
    - Estructuración de Unidades de lucha contra el delito informático

Tomado de: Electronic crime needs assessment for state and local law enforcement. National Institute of Justice. Disponible en: http://www.ojp.usdoj.gov/nij/pubs-sum/186276.htm . 2001

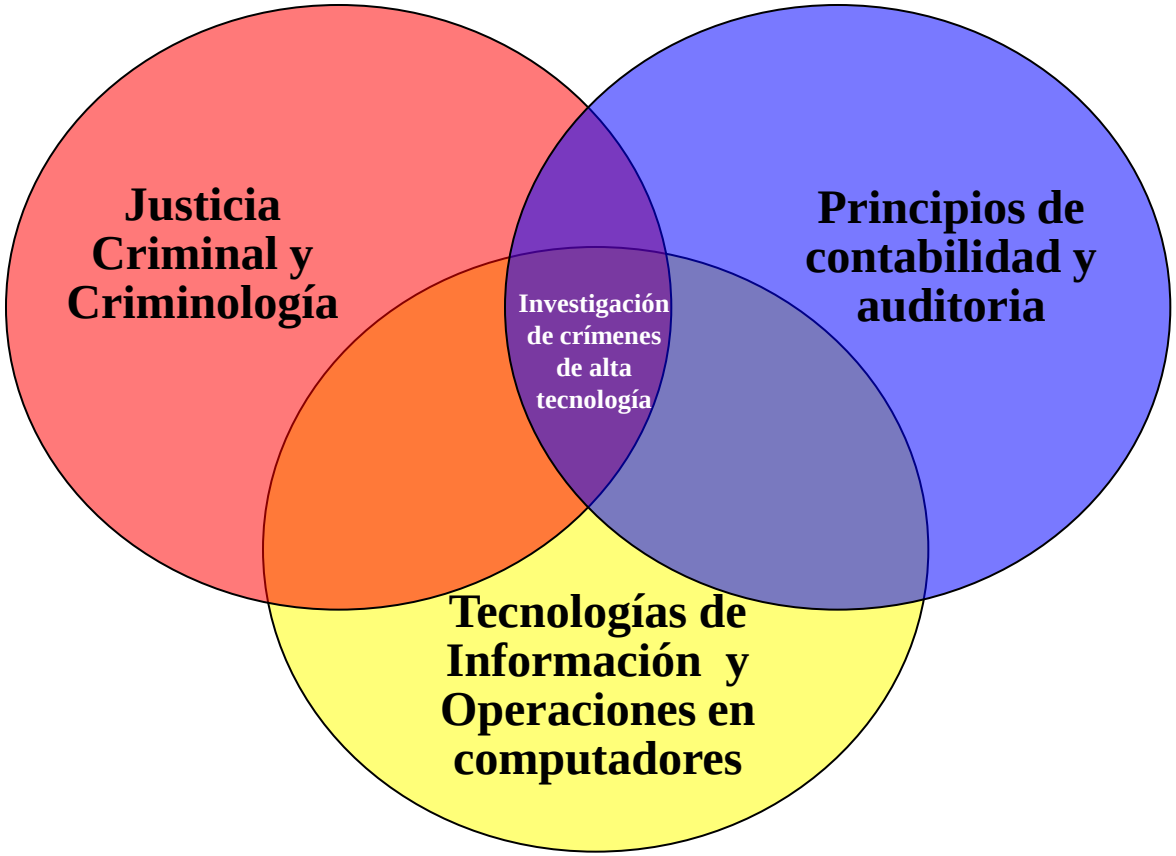
JCM10-All rights reserved

Desafíos de la computación forense



JCM10-All rights reserved

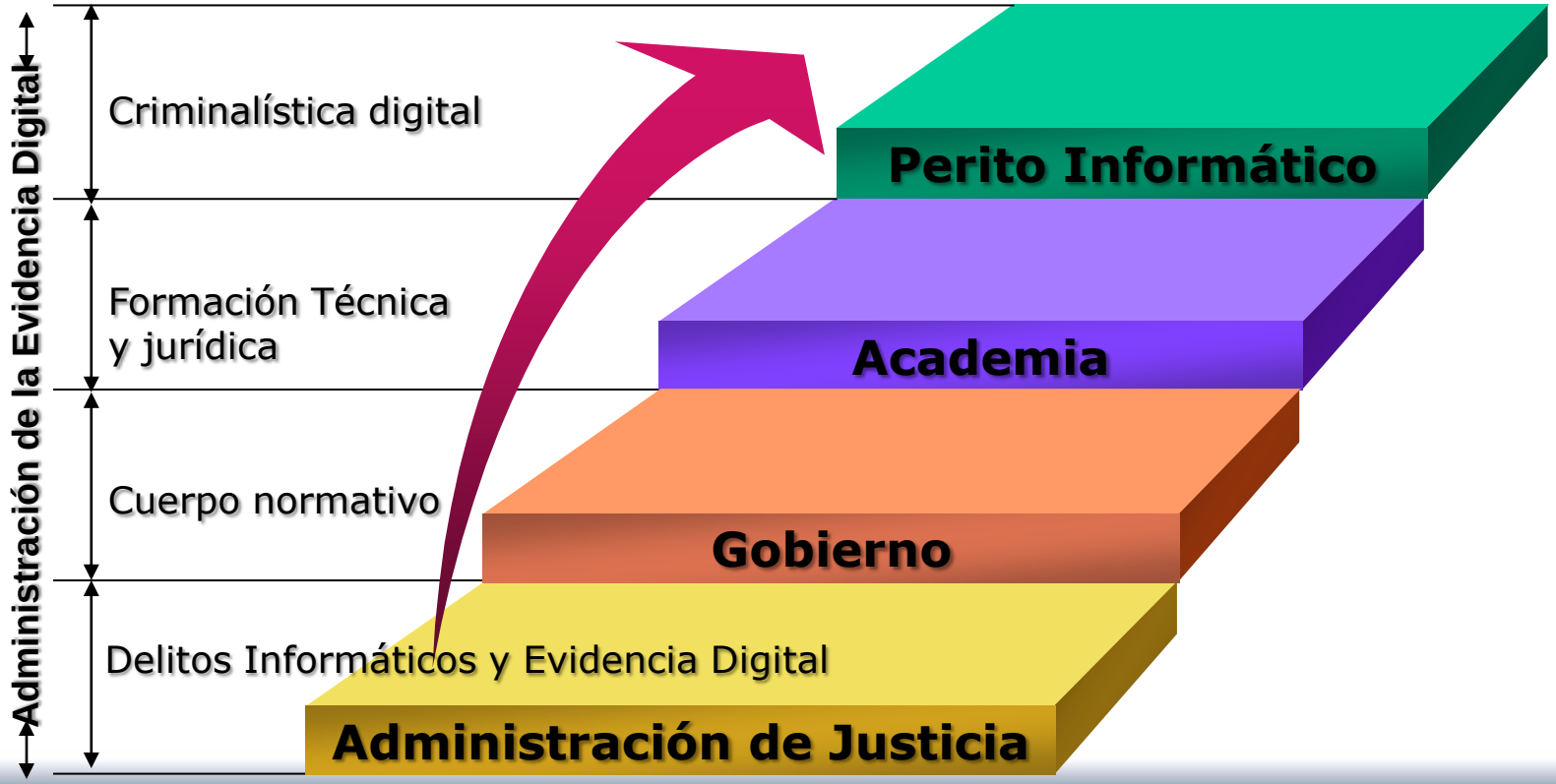
El informático forense – Formación



En Cano 2009, Cap.3, tomado de: MYERS JAY, Larry. *High Technology Crime Investigation: A Curricular Needs Assesment Of The Largest Criminal Justice And Criminology Programs In The United States*, Tesis Doctoral Diciembre de 2000

JCM10-All rights reserved

Desafíos de la computación forense



JCM10-All rights reserved

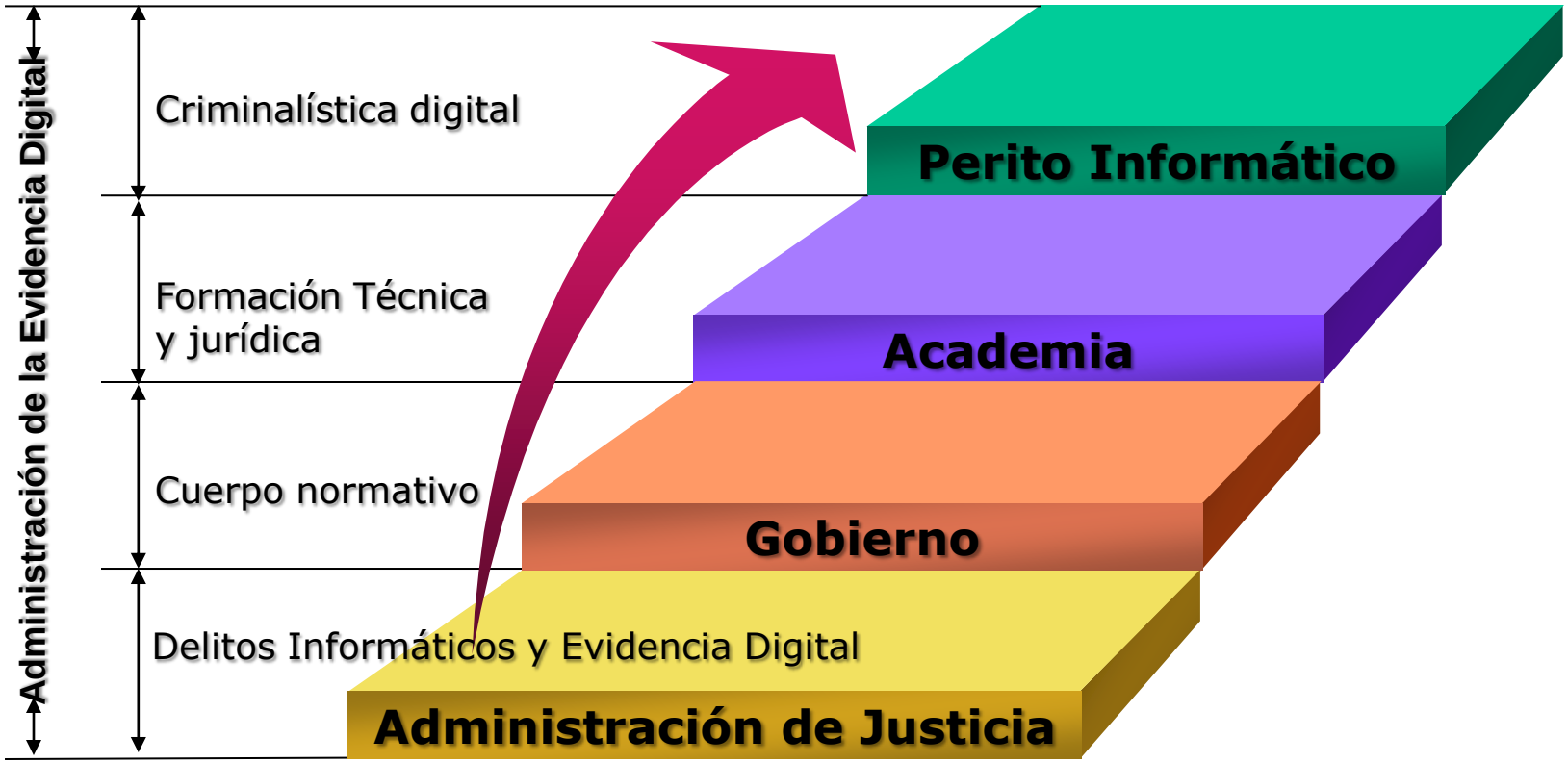
Contraste de tres perfiles

Característica	Auditor TI	Examinador Fraude	Informático Forense
Temporalidad	Recurrente	No recurrente	Por demanda
Alcance	General	Específico	Específico
Objetivo	Opinión	Acusación	Análisis técnico
Relación	No controversia	Controversia	No controversia
Metodología	Técnicas de auditoria	Técnicas Ex. Fraude	Técnicas de Inf. Forense
Presunción	Excepticismo Profesional	Pruebas	Pruebas
Buenas Prácticas	ISACA/IIA	AICPA/ACFE	HTCIA/IACIS

Adaptado de: WELLS, J. (2005) Principles of fraud examination. John Wiley & Sons. Pag.4

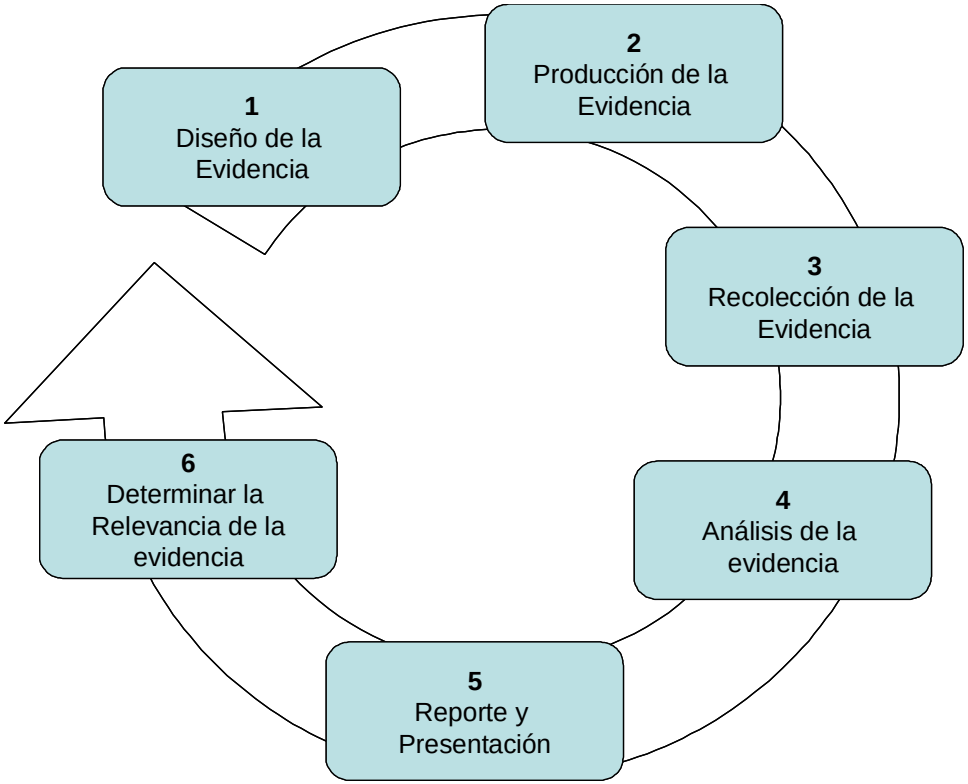
JCM10-All rights reserved

Desafíos de la computación forense



JCM10-All rights reserved

Ciclo de Vida
Administración de la Evidencia Digital



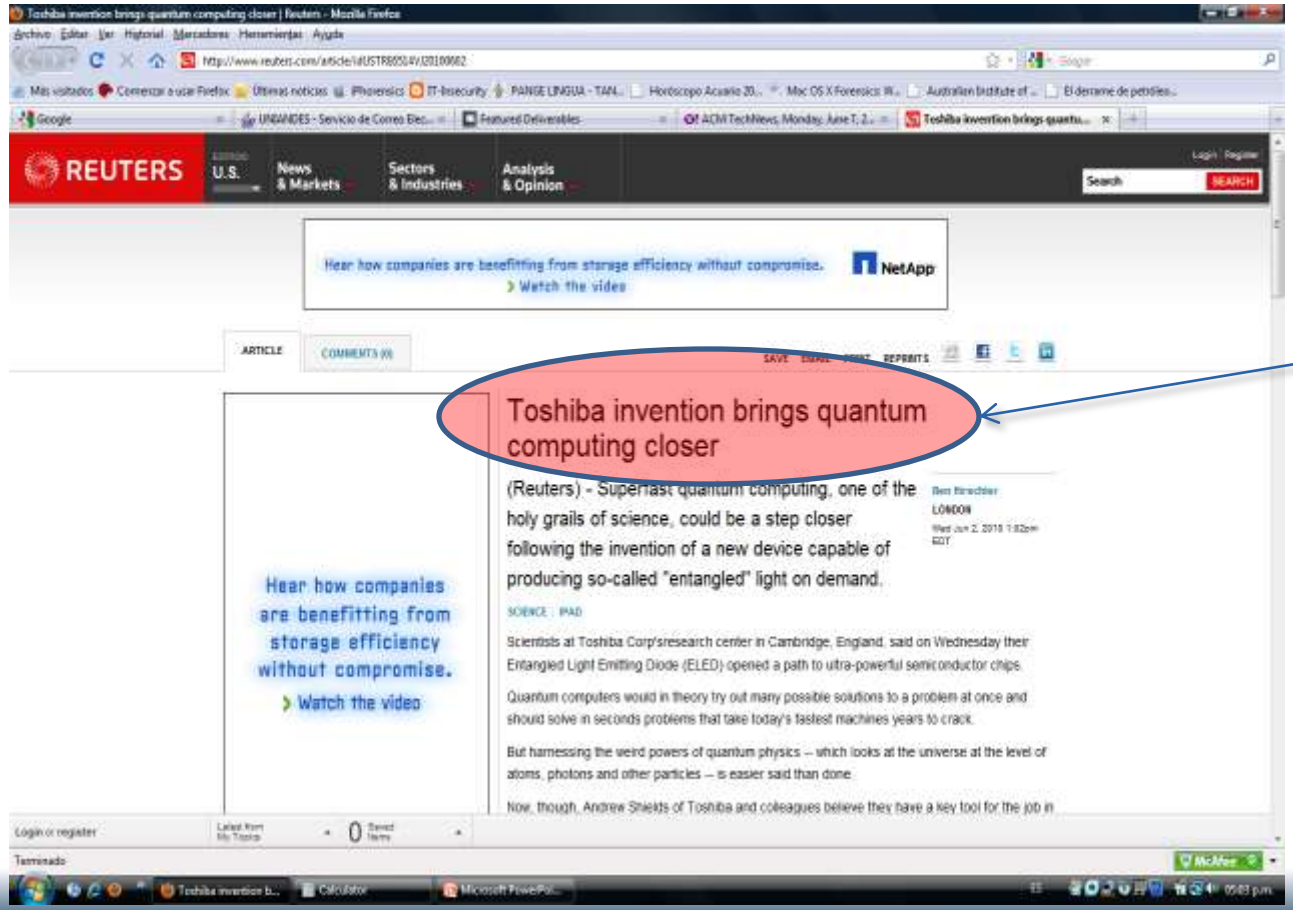
Ciclo de vida de la administración de la evidencia digital.
(Tomado de: HB171:2003 Handbook Guidelines for the management of IT Evidence)

JCM10-All rights reserved

¿Algunas ideas sobre el futuro cercano?

JCM10-All rights reserved

¿Algunas ideas sobre el futuro?



Computación Cuántica

JCM10-All rights reserved

¿Algunas ideas sobre el futuro?

Second life

¿Ciencia – Ficción?

¿Ficción hecha Realidad?

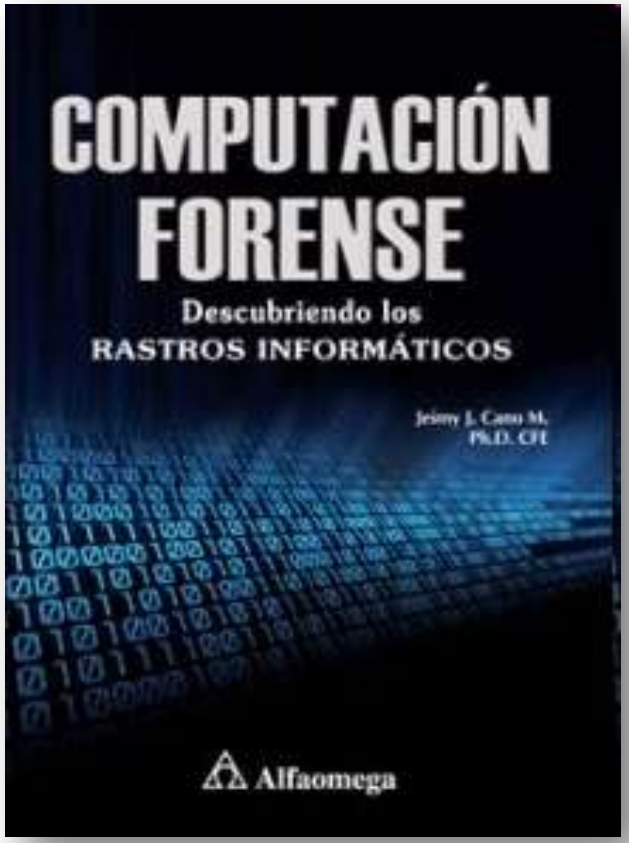
JCM10-All rights reserved

Reflexiones finales

- *"No podemos resolver un problema en el mismo nivel de pensamiento que fue creado"* – A. Einstein
- "No existen crímenes perfectos, sino investigaciones imperfectas" – V. Cobarrubias – Chile
- *"Siempre habrá alguien que supere las medidas de seguridad de un sistema", pero no sabemos cuándo.* – Adaptado de R. Ackoff.
- "A *menor visibilidad* de la materialización de los ataques, *mayores los riesgos* contra la relevancia y confiabilidad de las investigaciones forenses en informática." – J.Cano – Colombia
- *"Es mejor pensar en posibilidades, que en probabilidades"* – R. Ackoff.

JCM10-All rights reserved

Para continuar aprendiendo…



Datos de la publicación:

Autor: Jeimy J. Cano, Ph.D, CFE

Año: 2009

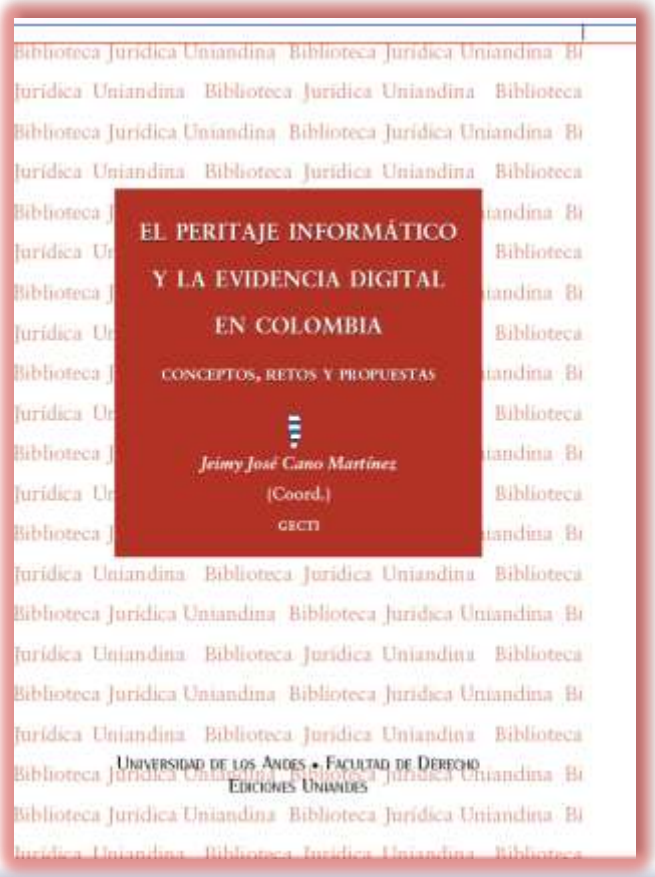
Editorial: AlfaOmega

ISBN: 978-958-682-767-6

Disponible en:
http://www.alfaomega.com.co

JCM10-All rights reserved

Para continuar aprendiendo…



Datos de la publicación:

Autor: Jeimy J. Cano, Ph.D, CFE (Coordinador y autor)

Año: 2010

Editorial: Ediciones Uniandes

ISBN: 978-958-695-491-4

Disponible en:
http://libreria.uniandes.edu.co

JCM10-All rights reserved

Para finalizar….

- *"Es más fácil aprender del camino exitoso de otros, que de los errores propios."*
  - *David Lacey, autor de "Managing the Human Factor in Information Security". How to win over staff and influence business managers.* John Wiley & Sons. 2009

JCM10-All rights reserved

Referencias

- CANO, J. (2009) *Computación Forense. Descubriendo los rastros informáticos*. Editorial AlfaOmega.
- CANO, J. y PIMENTEL, J. (2008) Consideraciones sobre el estado del arte del peritaje informático y los estándares de manipulación de pruebas electrónicas en el mundo. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*. Fac. de Derecho. Universidad de los Andes.
- CANO, J. (2007) Estrategias anti-forenses en informática: Repensando la computación forense.*Revista Electrónica de Derecho Informático*. ISSN: 1681-5726. No.110 Septiembre. Disponible en: http://www.alfa-redi.org/rdi-articulo.shtml?x=9608
- CANO, J. (2007) Inseguridad informática y Computación antiforense: Dos conceptos emergentes en seguridad informática. *Information Systems Control Journal* – ISACA. Vol.4. http://www.isaca.org (Versión revisada)
- CANO, J. (2007) Estrategias anti-forenses en informática: Conceptos y reflexiones. *Revista del INEGI.* ISSN: 1870-3224 Septiembre-Diciembre. Vol.3, No.3. México
- CANO, J. (2006) Introducción a la informática forense. Una Disciplina Técnico-Legal. *Revista SISTEMAS*. Asociación Colombiana de Ingenieros de Sistemas – ACIS. No.96. Abril-Junio.
- CANO, J (2005)Estado del Arte del peritaje informático. Documento de investigación. ALFA-REDI. Disponible en:http://www.alfa-redi.org/noticia.shtml?x=810
- CANO, J. (2007) Informáticos forenses: los criminalistas informáticos en la sociedad de la información. *Revista Derecho y Tecnología*. U. Católica del Táchira. Venezuela. No. 9.

JCM10-All rights reserved

Referencias

- MCKINSEY QUARTERLY Sept. 2008 – How global executives view sociopolitical issues.
- LUFTMAN, J., KEMPAIAH, R. y NASH,E. (2006) Key issues for IT Executives. *MIS Quarterly Executive*. Vol.5. No.2. June
- NANCE, K., HAY, B. y BISHOP, M. (2009) Digital Forensics: Defining a research agenda. *Proceedings of 42nd Hawaii International Conference on System Sciences*. January 5-8. Hawaii.

JCM10-All rights reserved

JCM10-All rights reserved

Riesgos emergentes para los informáticos forenses.

Retos y oportunidades

Jeimy J. Cano, Ph.D, CFE
Profesor Distinguido
GECTI - Facultad de Derecho
Universidad de los Andes

Blog Personal:
IT-Insecurity
http://insecurityit.blogspot.com/