Administración de la Evidencia Digital

De la teoría a la práctica

Jeimy J. Cano, Ph.D, CFE
GECTI – Facultad de Derecho
Universidad de los Andes
http://www.gecti.org

Agenda

- Introducción
- Evidencia digital: Análisis en contexto
  - Admisibilidad
  - Valor probatorio
- Auditabilidad Vs Trazabilidad
- Inseguridad en los sistemas de logging
  - Confidencialidad
  - Integridad
  - Disponibilidad

Agenda

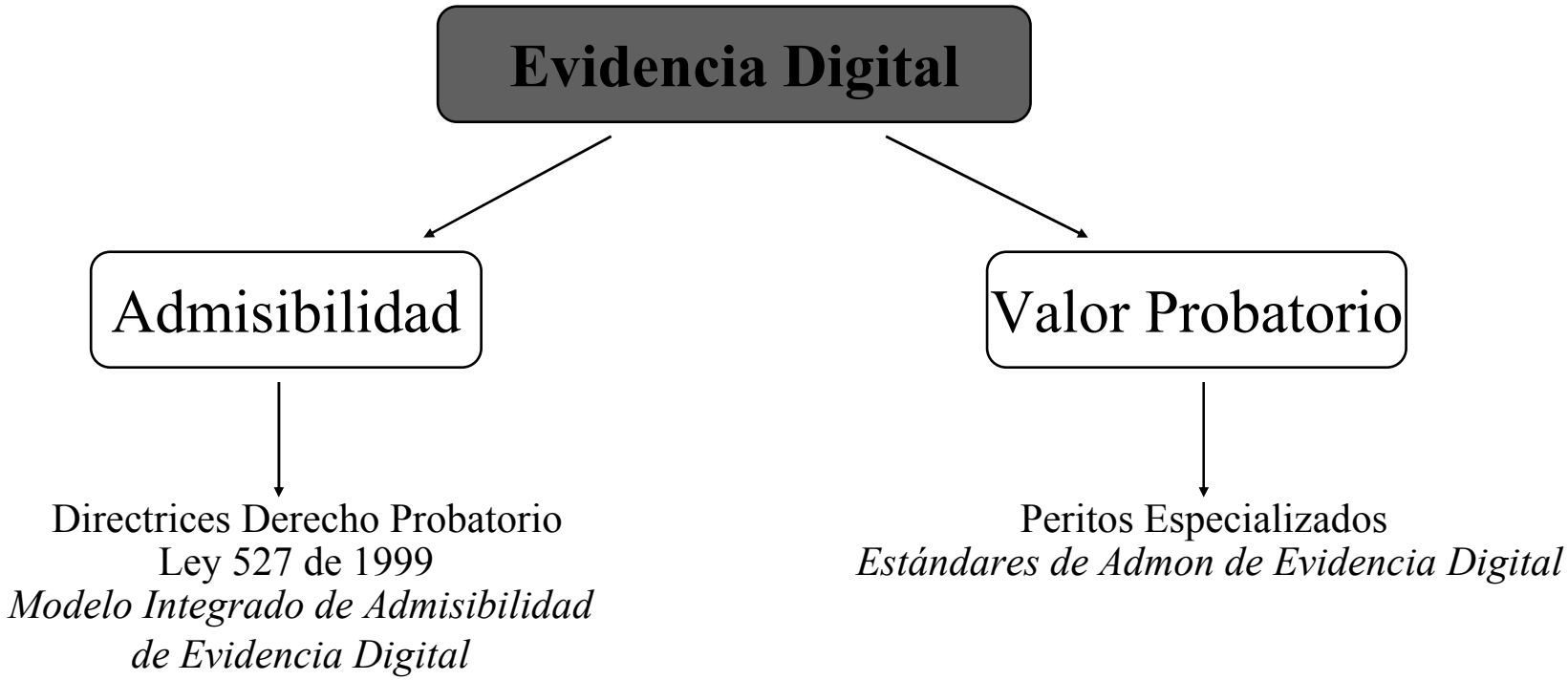
- Network Security Monitoring- NSM
  - Recolección
  - Análisis
  - Escalamiento
  - Indicadores
  - Advertencias
- Una mirada práctica
- Reflexiones finales
- Referencias

Introducción

- La criminalidad informática organizada viene creciendo de manera exponencial.
- Los intrusos cada vez más conocen en profundidad los detalles de las tecnologías y sus limitaciones
- Se hace cada vez más fácil desaparecer la evidencia y confundir a los investigadores forenses en informática
- Las autoridades de justicia poco a poco se involucran en temas de delito informático
- Las organizaciones diariamente desarrollan operaciones de negocio donde la evidencia de los mismos es digital.

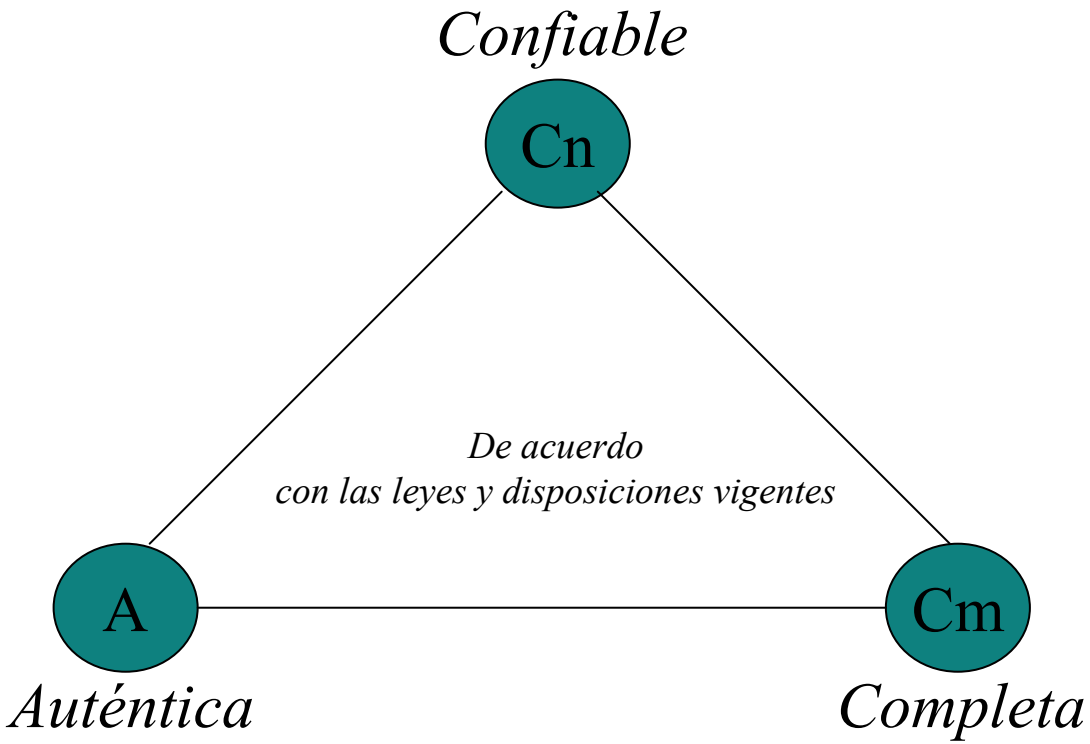
Evidencia digital

Análisis en contexto

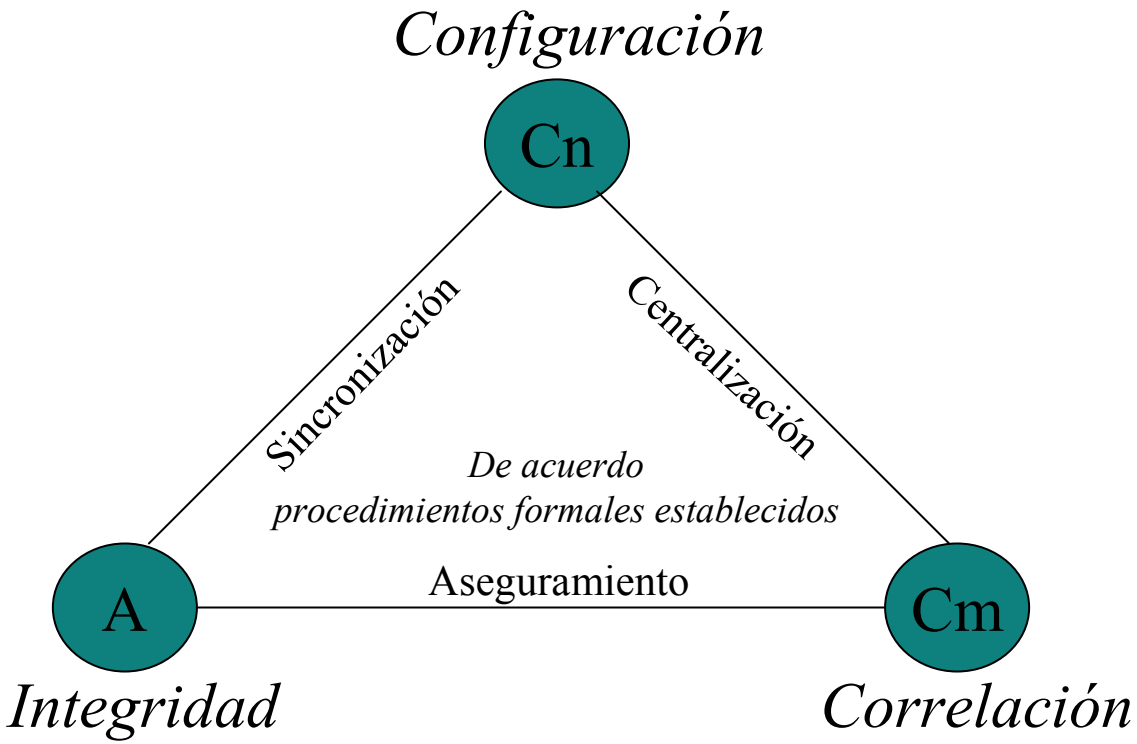


Admisibilidad de la evidencia digital

Conceptos legales

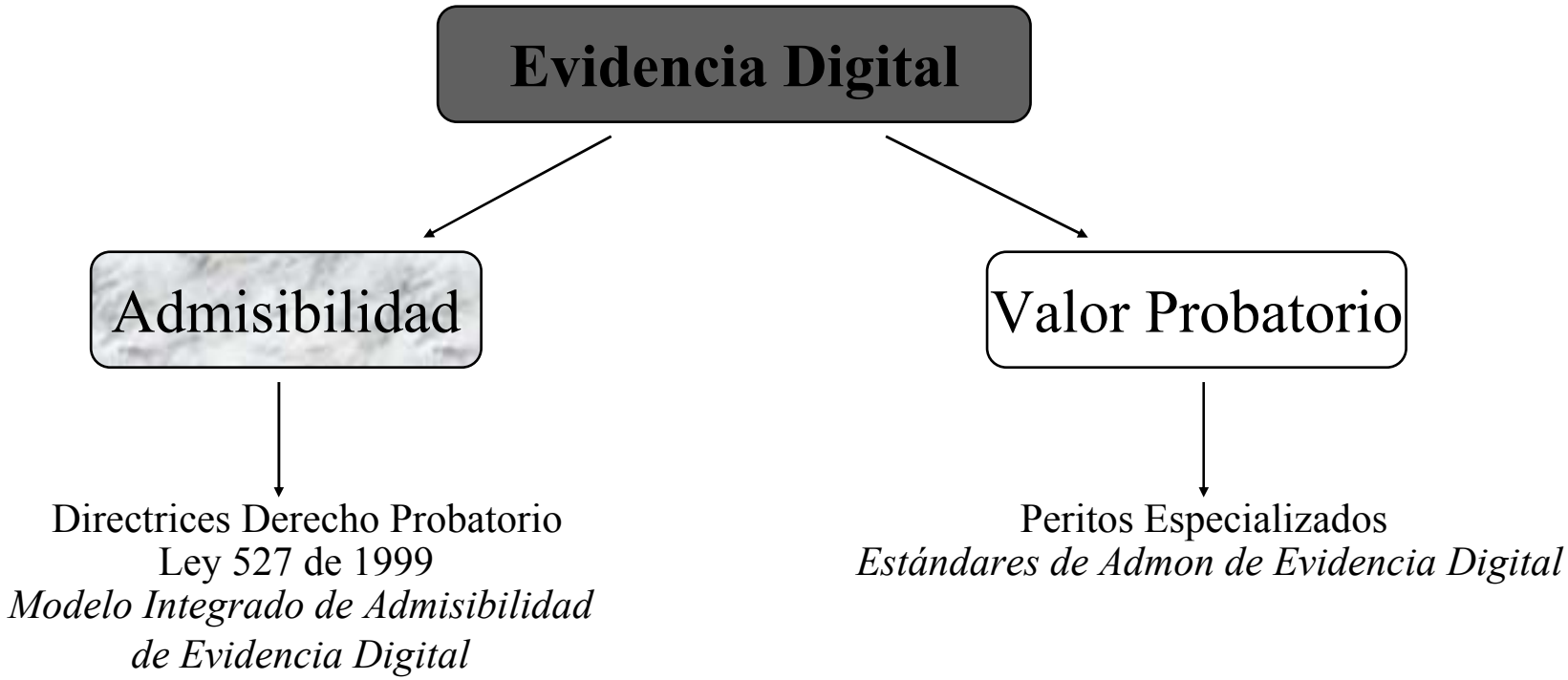


Admisibilidad de la evidencia digital
Implementación técnica



Evidencia digital

Análisis en contexto



Peritos especializados

- Pericia:
  - *"Sabiduría, práctica, experiencia y habilidad en una ciencia u arte". Diccionario de la Lengua Española*

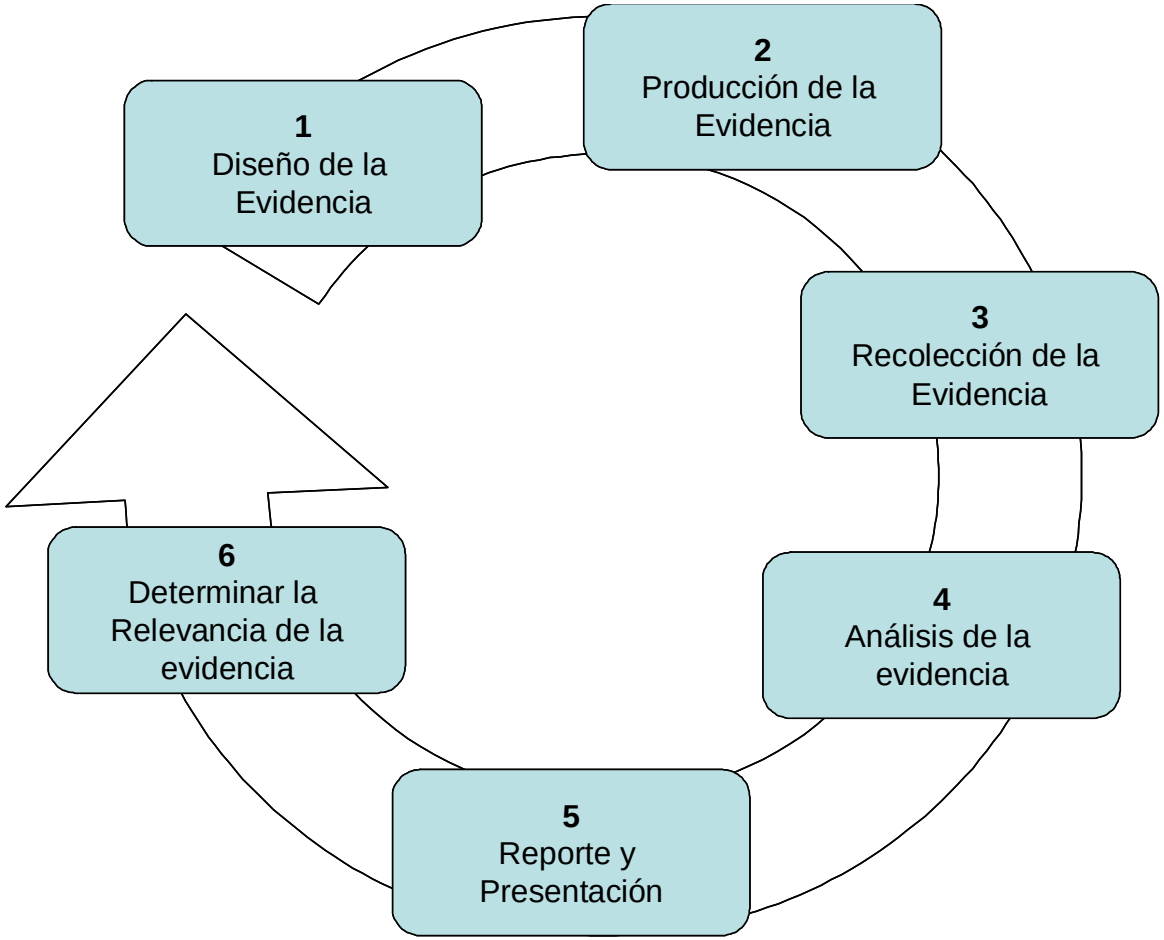
- Perito:
  - *"Persona que, poseyendo especiales conocimientos teóricos o prácticos, informa bajo juramento, al juzgador sobre puntos litigiosos en cuanto se relaciona con su especial saber o experiencia". Diccionario de la Lengua Española.*

- Dictámen:
  - Es un informe escrito sobre una determinada materia que debidamente motivado y razonado es emitido por un profesional versado en la materia. (Tomado de: Emilio del Peso Navarro. (2001) Peritajes Informáticos. Segunda edición. Ed. Diaz de Santos. Pág. 39)

Peritos especializados

- Al realizar una pericia forense en informática existen al menos siete (7) pasos que se deben efectuar para hacerla de manera competente y válida:
  - Se deben utilizar medios forenses estériles
  - Mantener la integridad del medio original
  - Identificar las posibles evidencias en la escena del delito
  - Etiquetar, controlar y transmitir adecuadamente las copias de los datos, impresiones y resultado de la investigación.
  - Análisis de los datos identificados
  - Presentación y sustención de resultados
  - Validación y verificación de los procedimientos aplicados

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.]

Ciclo de Vida
Administración de la Evidencia Digital

1. Diseño de la evidencia

- Clasificar la información de la organización, de tal forma que se pueda establecer cuál es la evidencia más relevante y formal que se tiene.
- Determinar los tiempos de retención de documentos electrónicos, la transformación de éstos (cambios de formato) y la disposición final de los mismos.
- Diseñar los registros de auditoría de las aplicaciones, como parte fundamental de la fase de diseño de la aplicación. Este diseño debe considerar la completitud y el nivel de detalle (granularidad) de los registros.
- Utilización de medidas tecnológicas de seguridad informática para validar la autenticidad e integridad de los registros electrónicos. Tecnologías como certificados digitales, token criptográficos, entre otras podrían ser candidatas en esta práctica.
- La infraestructura tecnológica debe asegurar la sincronización de las máquinas o dispositivos que generen la información, de tal manera que se pueda identificar con claridad la fecha y hora de los registros electrónicos

Ciclo de Vida
Administración de la Evidencia Digital

- **2. Producción de la evidencia**
  - Desarrollar y documentar un plan de pruebas formal para validar la correcta generación de los registros de la aplicación.
  - Diseñar mecanismos de seguridad basados en certificados digitales para las aplicaciones de tal forma que se pueda validar que es la aplicación la que genera los registros electrónicos.
  - En la medida de lo posible establecer un servidor de tiempo contra los cuales se pueda verificar la fecha y hora de creación de los archivos.
  - Contar con pruebas y auditorías frecuentes alrededor de la confiabilidad de los registros y su completitud, frente al diseño previo de los registros electrónicos.
  - Diseñar y mantener un control de integridad de los registros electrónicos, que permita identificar cambios que se hayan presentado en ellos.

Ciclo de Vida
Administración de la Evidencia Digital

- **3. Recolección de evidencia**
  - Establecer un criterio de recolección de evidencia digital según su volatibilidad: de la más volátil a la menos volátil.
  - Documentar todas las actividades que el profesional a cargo de la recolección ha efectuado durante el proceso de tal manera que se pueda auditar el proceso en sí mismo y se cuente con la evidencia de este proceso.
  - Asegurar el área dónde ocurrió el siniestro, con el fin de custodiar el área o escena del delito y así fortalecer la cadena de custodia y recolección de la evidencia.
  - Registrar en medio fotográfico o video la escena del posible ilícito, detallando los elementos informáticos allí involucrados.
  - Levantar un mapa o diagrama de conexiones de los elementos informáticos involucrados, los cuales deberán ser parte del reporte del levantamiento de información en la escena del posible ilícito.

Ciclo de Vida
Administración de la Evidencia Digital

- **4. Análisis de la evidencia**
  - Efectuar copias autenticadas de los registros electrónicos originales sobre medios forenses estériles para adelantar el análisis de los datos disponibles.
  - Capacitar y formar en aspectos técnicos y legales a los profesionales que adelantarán las labores de análisis de datos.
  - Validar y verificar la confiabilidad y limitaciones de las herramientas de hardware y software utilizadas para adelantar los análisis de los datos.
  - Establecer el rango de tiempo de análisis y correlacionar los eventos en el contexto de los registros electrónicos recolectados y validados previamente.
  - Mantener la perspectiva de los análisis efectuados sin descartar lo obvio, desentrañar lo escondido y validar las limitaciones de las tecnologías o aplicaciones que generaron los registros electrónicos.

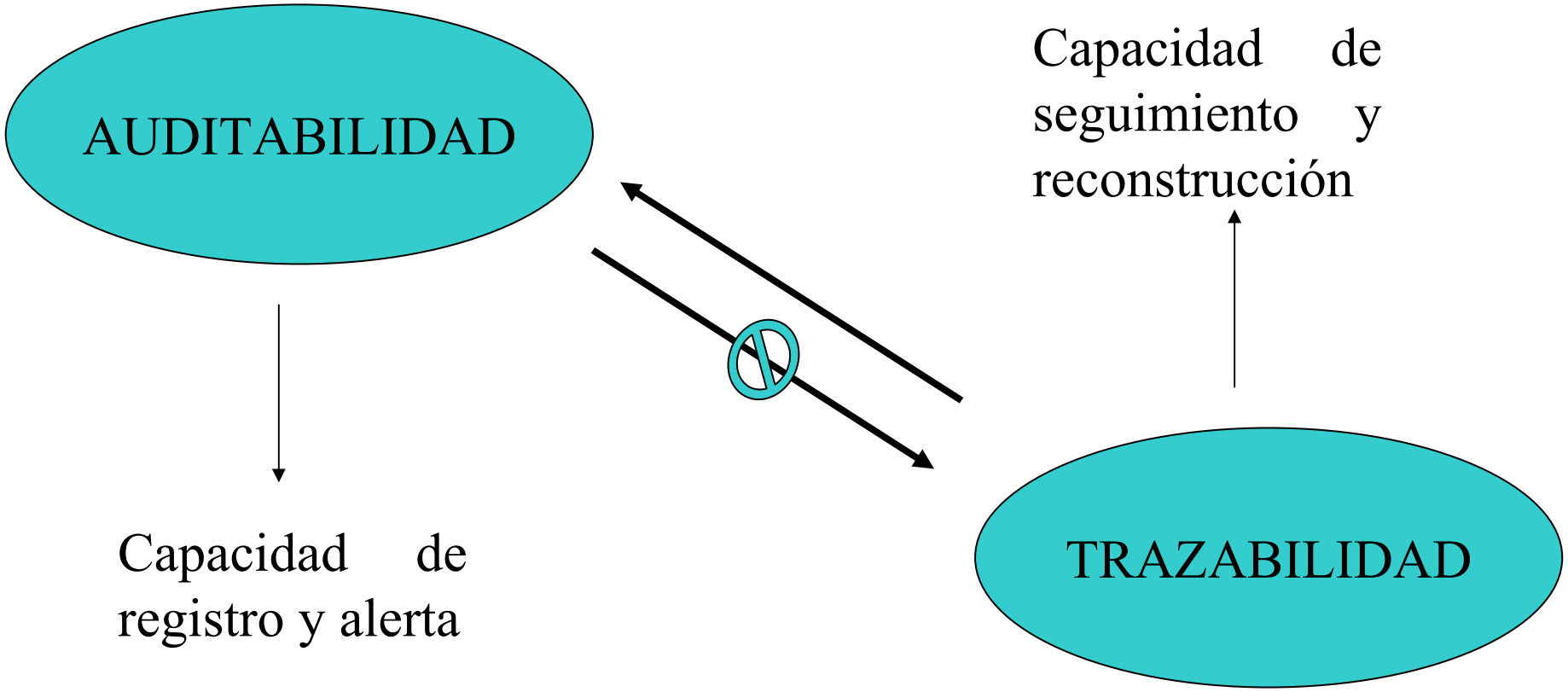
Ciclo de Vida
Administración de la Evidencia Digital

- **5. Reporte y presentación**
  - Mantener una copia de la cadena de custodia y de la notificación oficial para adelantar el análisis de los registros electrónicos.
  - Incluir las irregularidades encontradas o cualquier acción que pudiese ser irregular durante el análisis de la evidencia.
  - Preparar una presentación del caso de manera pedagógica, que permita a las partes observar claramente el contexto del caso y las evidencias identificadas.
  - Detallar las conclusiones de los análisis realizados sustentados en los hechos identificados. Evitar los juicios de valor o afirmaciones no verificables.
  - Contar con un formato de presentación de informe de análisis de evidencia

Ciclo de Vida
Administración de la Evidencia Digital

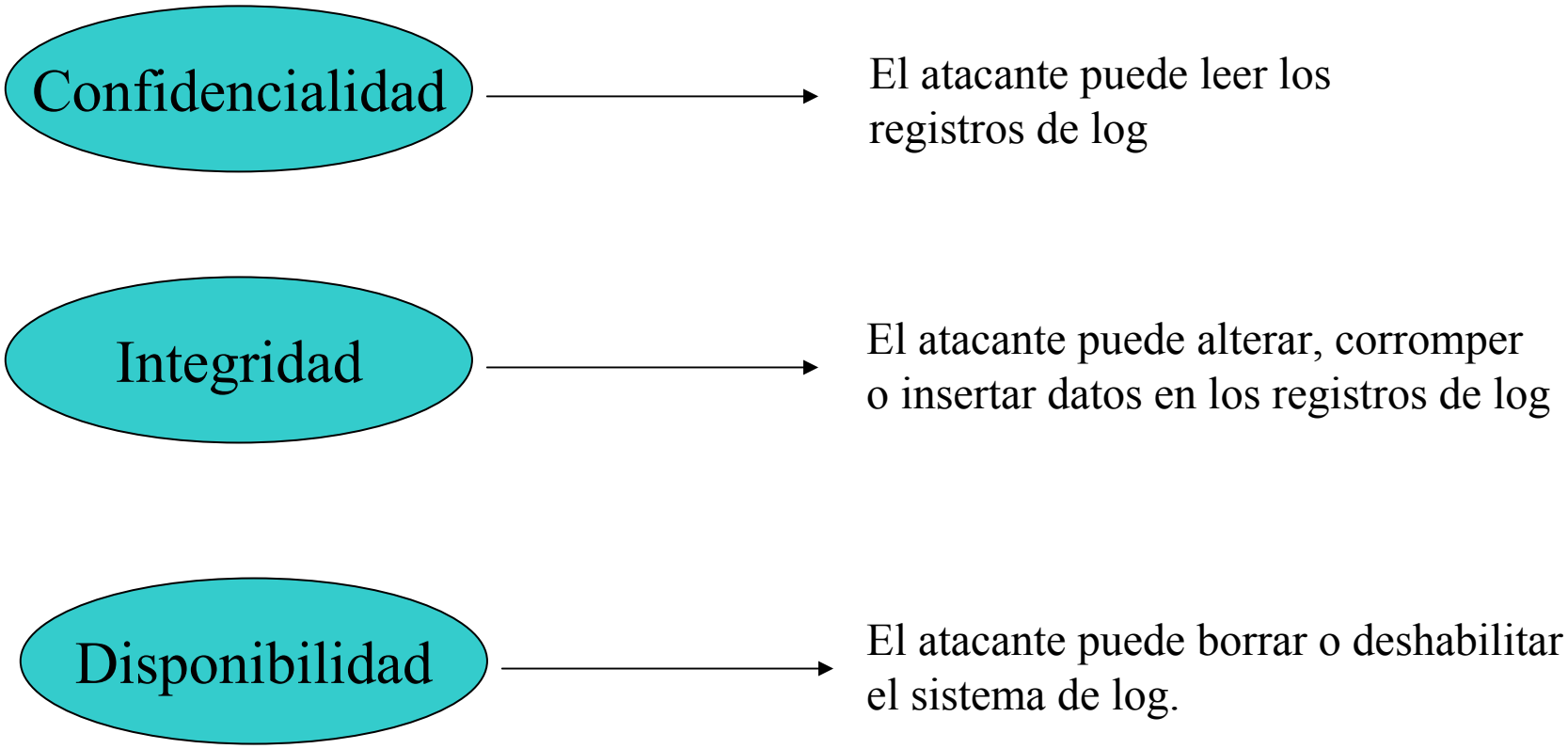
- **6. Determinar la relevancia de la evidencia**
  - Demostrar con hechos y documentación que los procedimientos aplicados para recolectar y analizar los registros electrónicos son razonables y robustos.
  - Verificar y validar con pruebas que los resultados obtenidos luego de efectuar el análisis de los datos, son repetibles y verificables por un tercero especializado.
  - Auditar periódicamente los procedimientos de recolección y análisis de registros electrónicos.
  - Fortalecer las políticas, procesos y procedimientos de seguridad de la información asociados con el manejo de evidencia digital.
  - Procurar certificaciones profesionales y corporativas en temas relacionados con computación forense y seguridad informática, como una manera de validar la constante revisión y actualización del tema y sus mejores prácticas.

Auditibilidad Vs Trazabilidad



Tomado de: Cano, J. (2005) Information System Control Journal. December.

Inseguridad en los sistemas de logging



Tomado de: Chuvakin y Singer 2005.

Network Security Monitoring -NSM

- Algunas consideraciones
  - Buena práctica de seguridad y control diseñada por Richard Betjlich.
  - Definición
    - NSM es la recolección, análisis y escalamiento de indicadores y advertencias para detectar y responder a intrusiones.

Network Security Monitoring -NSM

- Definición
  - NSM es la recolección, análisis y escalamiento de indicadores y advertencias para detectar y responder a intrusiones.

- Explicación
  - Recolección
    - Efectuada por productos de software o cajas (appliances)
  - Análisis
    - Realizado por las personas en el contexto de la arquitectura
  - Escalamiento
    - Entregar información para soportar requerida para la toma de decisiones
  - Indicadores
    - Acciones observables o discernibles que confirman o no las capacidades del intruso. Generalmente generadas por IDS
  - Advertencias
    - Son los resultados del análisis de los indicadores. Están basados en juicios humanos.

Network Security Monitoring -NSM

- En ***contexto de seguridad*** es integrar las tecnologías, fortalecer los procedimientos y afinar la capacidad de análisis de los profesionales de seguridad.

- En el ***contexto forense*** es concebir un proceso que procure una red autodefensiva y trazable. Es decir, una infraestructura con elementos que permitan la administración de la inseguridad de la información y la evidencia digital.

Una mirada práctica

Recolección heterogénea de registros y análisis de vectores de amenazas

Utilidades:
- Tendencias en uso de puertos
- Caracterización del tráfico de red
- Visualización holística
- Apoyo a labores forenses

Configuración y control de agentes de monitoreo

Tipo de Datos:
- Alertas
- Datos de sesión
- Contenido
- Estadístico

Soluciones específicas instaladas

Diseño de logging:
- Sincronización
- Control de integridad
- Centralización
- Autodefensivo

Adaptado de: Event Correlation. Security's holy grail. Matthew Caldwell, CSO, GuardedNet. Black Hat . 2002

Reflexiones finales

- Los mecanismos de seguridad son elementos de la arquitectura computacional que exigen su propia autoprotección.
- Los registros que se generan del uso de las TI deben seguir los principios de la AED.
- Consideraciones sobre defensa en profundidad, punto de choque y aislamiento deben ser considerados en redes autodefensivas.
- La NSM es una práctica que procura la administración de la inseguridad informática y promueve la AED.
- La trazabilidad de las operaciones es un requisito fundamental de las aplicaciones y arquitecturas modernas.

Referencias

- Bejtlich, R., Jones, K. y Rose, C. (2006) Real digital forensics. Computer security and incident response. Addison Wesley.
- Bejtlich, R. (2006) Extrusion detection. Security monitoring for internal intrusions. Addison Wesley.
- Chuvakin, A. y Singer, A. (2005) Attacks against logging systems. Computer Security Journal. Vol.21 No.4.
- Bejtlich, R. (2005) Using attacks responses to improve intrusion detection. http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1138756,00.html
- Bejtlich, R. (2005) The Tao of Network Security Monitoring. Beyond intrusion detection. Addison Wesley.
- Inside Network Perimeter Security. SAMS Publishing. Second edition.
- Chuvakin, A. (2004) Five mistakes of log analysis. ComputerWorld. http://www.computerworld.com/printthis/2004/0,4814,96587,00.html
- Chuvakin, A. (2002) Advanced log processing. http://www.securityfocus.com/infocus/1613

Referencias

- HOGLUND, G. y BUTLER, J. (2006) Subverting the windows kernel. Rootkits. Addison Wesley
- RUSSINOVICH, M y SOLOMON, D. (2005) Windows Internals. Fourth Edition. Microsoft Press.
- KASPERSKY, K. (2005) Shellcoder's programming unconvered. A List Publishing.
- FARMER, D y VENEMA, W. (2005) Forensic discovery. Addison Wesley.
- EILAM, E. (2005) Reversing. Secrets of reverse engineering. John Wiley & Son.
- CARRIER, B. (2005) File system forensic analysis. Addison Wesley.
- Gutmann, P. (1996) *Secure Deletion of Data from Magnetic and Solid-State Memory* http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
- Lopez, O., Amaya, H y Leon, Ricardo. (2002) *Generalidades, aspectos técnicos y herramientas*. Artículo presentado en el CIBSI- Congreso Iberoamericano de Seguridad Informática. Morelia. México. http://www.criptored.upm.es - Sección Docencia.
- CERT (2002) Overview of attacks trends. http://www.cert.org/archive/pdf/attack_trends.pdf

Referencias

- CANO, J. (2003) Adminisibilidad de la evidencia digital. De lo conceptos legales a las implementaciones técnicas. En GECTI. Derecho de Internet & Telecomunicaciones. Universidad de los Andes – Legis.
- CANO, J. (2005) Borrando archivos. Conceptos básicos sobre la dinámica del funcionamiento de los sistemas de archivo. http://www.virusprot.com/filesystems05.pdf
- CANO, J., CERTAIN, A. y MOSQUERA, A: (2005) Evidencia digital: Contexto, situación e implicaciones nacionales. *Revista de Derecho Comunicaciones y Nuevas Tecnologías*. Facultad de Derecho. Universidad de los Andes. Disponible en http://www.gecti.org
- CANO, J. (2005) Estado del arte del peritaje informático en latinoamérica. Comunidad Alfa-Redi. Investigación. Disponible en http://www.alfa-redi.org/ar-dnt-documento.shtml?x=728
- CANO, J. (2005) Trazabilidad de las operaciones electrónicas. Un reto para la gerencia de TI. ISACA *Information System Control Journal*. Vol 6. December.
- CANO, J. (2006) Buenas prácticas en la administración de la evidencia digital. Documento GECTI No.6. Disponible en http://www.gecti.org.
- CANO, J. y RUEDA, A. (2006) La administración de la evidencia digital en el contexto de la administración de justicia en Colombia. Conceptos y Propuesta. *Revista de Derecho Comunicaciones y Nuevas Tecnologías.* Facultad de Derecho. Universidad de los Andes (En publicación)

Administración de la Evidencia Digital

De la teoría a la práctica

Jeimy J. Cano, Ph.D, CFE
GECTI – Facultad de Derecho
Universidad de los Andes
http://www.gecti.org