Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática - GECTI
Facultad de Derecho
Universidad de los Andes

BUENAS PRÁCTICAS EN LA ADMINISTRACIÓN DE LA EVIDENCIA DIGITAL

INTRODUCCIÓN

Este documento es un compendio de prácticas internacionales en el tema de evidencia digital disponibles a la fecha, que busca ofrecer un conjunto de elementos teóricos y prácticos para apoyar procesos donde este tipo de evidencia es fundamental para avanzar en la solución de un caso.

NOTA ACLARATORIA

Las aplicaciones o detalles que se relacionan en este documento son recomendaciones o sugerencias académicas, las cuales no pretenden ser un conjunto formal de prácticas que obliguen para demostrar la pertinencia o admisibilidad de una evidencia digital.

PRÁCTICAS EN ADMINISTRACIÓN DE EVIDENCIA DIGITAL

Las prácticas relacionadas a continuación se agruparán alrededor de lo establecido en el HB171:2003 *Handbook Guidelines for the management of IT evidence*, desarrollado en Australia.

De acuerdo con lo previsto en el documento referenciado en el párrafo anterior, se detallará el ciclo de administración de evidencia digital y sus respectivos elementos, los cuales se complementarán con prácticas (cinco prácticas básicas) y procedimientos que permitan a los responsables establecer directrices claras sobre la administración de este tipo de evidencia.

El ciclo de vida para la administración de evidencia digital consta de seis pasos a saber:

1. Diseño de la evidencia
2. Producción de la evidencia
3. Recolección de la evidencia
4. Análisis de la evidencia
5. Reporte y presentación
6. Determinación de la relevancia de la evidencia

2006 - All rights reserved. *Jeimy J. Cano, Ph.D, CFE* - Documento GECTI

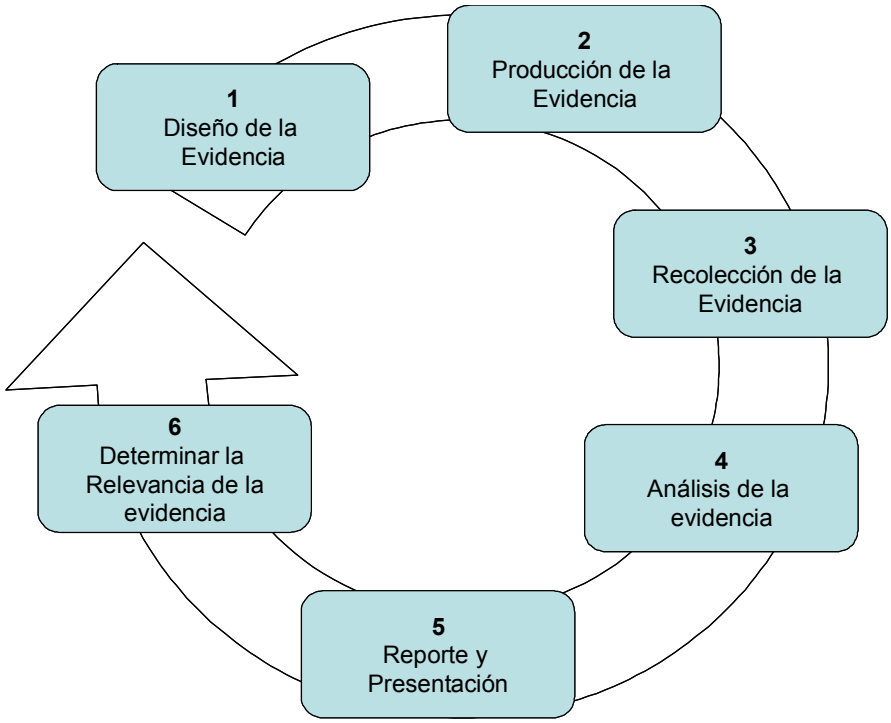

Figura No.1 Ciclo de vida de la administración de la evidencia digital. [Tomado de: HB171:2003 Handbook Guidelines for the management of IT Evidence.]

1. Diseño de la evidencia

Concepto

Con el fin de fortalecer la admisibilidad y relevancia de la evidencia producida por las tecnologías de información, se detallan a continuación cinco objetivos que se deben considerar para el diseño de la evidencia digital: [STANDARDS AUSTRALIA INTERNATIONAL 2003, pág.13]

a. Asegúrese de que se ha determinado la relevancia de los registros electrónicos, que éstos se han identificado, están disponibles y son utilizables.
b. Los registros electrónicos tienen un autor claramente identificado.
c. Los registros electrónicos cuentan con una fecha y hora de creación o alteración.
d. Los registros electrónicos cuentan con elementos que permiten validar su autenticidad.
e. Se debe verificar la confiabilidad de la producción o generación de los registros electrónicos por parte del sistema de información.

Prácticas

Algunas de las prácticas asociadas para procurar lo establecido por esta primera fase son:

1. Clasificar la información de la organización, de tal forma que se pueda establecer cuál es la evidencia más relevante y formal que se tiene. Para ello, las oficinas de archivo o documentación en conjunto con el área de tecnología deben adelantar un estudio de las características de la información que soporta decisiones

administrativas y sus medidas tecnologías de protección, almacenamiento y recuperación posterior.
2. Determinar los tiempos de retención de documentos electrónicos, la transformación de éstos (cambios de formato) y la disposición final de los mismos.
3. 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.
4. 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.
5. 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.

2. Producción de la Evidencia

Concepto

Esta fase, de acuerdo con el estándar, requiere el cumplimiento de los siguientes objetivos: [idem, pág.20]

a. que el sistema o tecnología de información produzca los registros electrónicos
b. identificar el autor de los registros electrónicos almacenados
c. identificar la fecha y hora de creación
d. verificar que la aplicación está operando correctamente en el momento de la generación de los registros, bien sea en su creación o modificación.
e. Verificar la completitud de los registros generados

Prácticas

1. Desarrollar y documentar un plan de pruebas formal para validar la correcta generación de los registros de la aplicación.
2. 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.
3. 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.
4. Contar con pruebas y auditorías frecuentes alrededor de la confiabilidad de los registros y su completitud, frente al diseño previo de los registros electrónicos.
5. Diseñar y mantener un control de integridad de los registros electrónicos, que permita identificar cambios que se hayan presentado en ellos.

3. Recolección de la Evidencia

Concepto

El objetivo de esta fase en el ciclo de vida de administración de la evidencia digital es localizar toda la evidencia digital y asegurar que todos los registros electrónicos originales (aquellos disponibles y asegurados en las máquinas o dispositivos) no han sido alterados. Para ello el estándar establece algunos elementos a considerar como:

a. Establecer buenas prácticas y estándares para recolección de evidencia digital
b. Preparar las evidencias para ser utilizadas en la actualidad y en tiempo futuro
c. Mantener y verificar la cadena de custodia
d. Respetar y validar las regulaciones y normativas alrededor de la recolección de la evidencia digital
e. Desarrollar criterios para establecer la relevancia o no de la evidencia recolectada.

Prácticas

1. Establecer un criterio de recolección de evidencia digital según su volatibilidad: de la más volátil a la menos volátil. [BREZINSKI, D. y KILLALEA, T. 2002]
    a. Registros de memoria, memoria cache
    b. Tablas de enrutamiento, cache de arp, estadísticas del funcionamiento del sistema operacional.
    c. Archivos temporales
    d. Almacenamiento en diskettes, memorias USB, CD, DVD.
    e. Registro remoto de las actividades de la aplicación y monitoreo del tráfico de los datos
    f. Configuración física de dispositivos y topología de red
    g. Manuales y registros disponibles de los dispositivos y software bajo estudio.
2. 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.
3. 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.
4. Registrar en medio fotográfico o video la escena del posible ilícito, detallando los elementos informáticos allí involucrados.
5. 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.

4. Análisis de la Evidencia

Concepto

Una vez se ha recolectado la evidencia, tomado las imágenes de los datos requeridos y su debida cadena de custodia, es tiempo para iniciar el ensamble, análisis y articulación de los registros electrónicos para establecer los hechos de los eventos ocurridos en el contexto de la situación bajo análisis o establecer si hacen falta evidencias para completar o aclarar los hechos.

Prácticas

1. Efectuar copias autenticadas de los registros electrónicos originales sobre medios forenses estériles para adelantar el análisis de los datos disponibles. [INFORMATION SECURITY AND FORENSICS 2004, pág.23]
2. Capacitar y formar en aspectos técnicos y legales a los profesionales que adelantarán las labores de análisis de datos. Para ver un posible plan de formación en estos temas ver. "*Estado del arte del peritaje informático en Latinoamérica*". http://www.alfa-redi.org/ar-dnt-documento.shtml?x=728
3. Validar y verificar la confiabilidad y limitaciones de las herramientas de hardware y software utilizadas para adelantar los análisis de los datos.
4. Establecer el rango de tiempo de análisis y correlacionar los eventos en el contexto de los registros electrónicos recolectados y validados previamente. [US DEPARTMENT OF JUSTICE 2004, pag. 16]
5. Mantener la perspectiva de los análisis efectuados sin descartar lo obvio, desentrañar lo escondido y validando las limitaciones de las tecnologías o aplicaciones que generaron los registros electrónicos.

5. Reporte y Presentación

Concepto

El profesional a cargo de la investigación es responsable de la precisión y completitud del reporte, sus hallazgos y resultados luego del análisis de la evidencia digital o registros electrónicos. En este sentido toda la documentación debe ser completa, precisa, comprensiva y auditable.

En este sentido las prácticas internacionales aconsejan:

a. Documentar los procedimientos efectuados por el profesional a cargo.
b. Mantener una bitácora de uso y aplicación de los procedimientos técnicos utilizados.
c. Cumplir con exhaustivo cuidado con los procedimientos previstos para el mantenimiento de la cadena de custodia

Prácticas

1. Mantener una copia de la cadena de custodia y de la notificación oficial para adelantar el análisis de los registros electrónicos.
2. Incluir las irregularidades encontradas o cualquier acción que pudiese ser irregular durante el análisis de la evidencia.
3. Preparar una presentación del caso de manera pedagógica, que permita a las partes observar claramente el contexto del caso y las evidencias identificadas.
4. Detallar las conclusiones de los análisis realizados sustentados en los hechos identificados. Evitar los juicios de valor o afirmaciones no verificables.
5. Contar con un formato de presentación de informe de análisis de evidencia digital que detalle entre otros aspectos los siguientes:[US DEPARTMENT OF JUSTICE 2004, pág. 20]
    a. Identificación de la agencia o empresa que adelantó el análisis.
    b. Identificador del caso
    c. Investigador o profesional que ha adelantado el caso

d. Identificación de las entidades que han provisto las evidencias
e. Fechas de recepción y reporte
f. Lista detallada de elementos recibidos para análisis donde se detallen aspectos como serial, marca y modelo
g. Breve descripción de los pasos metodológicos seguidos
h. Resultados de los análisis donde se detallen con claridad los hallazgos
i. Conclusiones

6. Determinar la relevancia de la evidencia

Concepto

El estándar en esta fase establece valorar las evidencias de tal manera que se identifiquen las mejores evidencias que permitan presentar de manera clara y eficaz los elementos que se desean aportar en el proceso y en el juicio que se lleve. El objetivo es que el ente que valore las pruebas aportadas observe en sus análisis y aportes los objetos de prueba más relevantes para el esclarecimiento de los hechos en discusión.

En este sentido el estándar sugiere dos criterios para tener en cuenta a saber: [STANDARDS AUSTRALIA INTERNATIONAL 2003, pág.26]

a. Valor probatorio: que establece aquel registro electrónico que tenga signo distintivo de autoría, autenticidad y que sea fruto de la correcta operación y confiabilidad del sistema.
b. Reglas de la evidencia: que establece que se han seguido los procedimientos y reglas establecidas para la adecuada recolección y manejo de la evidencia.

Prácticas

1. Demostrar con hechos y documentación que los procedimientos aplicados para recolectar y analizar los registros electrónicos son razonables y robustos.
2. 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.
3. Auditar periódicamente los procedimientos de recolección y análisis de registros electrónicos, de tal manera que se procure cada vez mayor formalidad y detalles en los análisis efectuados.
4. Fortalecer las políticas, procesos y procedimientos de seguridad de la información asociados con el manejo de evidencia digital.
5. Procurar certificaciones profesionales y corporativas en temas relacionados con computación forense, no como signos distintivos de la experiencia de la organización en el área, sino como una manera de validar la constante revisión y actualización del tema y sus mejores prácticas.

RECOMENDACIONES ADICIONALES

- Recuerde que como profesional a cargo de una investigación usted debe proveer un concepto de los hechos identificados en sus análisis. Usted es un científico y como tal debe ser concreto y claro en sus afirmaciones.

- Los reportes que como profesional encargado de una investigación adelante deben ser concreto, libres de jerga propia de su disciplina, pedagógicos y sobre manera, consistentes con los hechos y resultados obtenidos.
- Si al preparar un reporte de un análisis de datos, considera que puede estar incompleto o no cuenta con las calificaciones y condiciones requeridas para efectuarlo, debe documentarlo en el informe o manifestar esta condición a la parte que ha solicitado sus servicios.
- Los profesionales que apoyan las labores en el ciclo de administración de la evidencia digital no deben contar con altos niveles de ética, sino con los más altos estándares y niveles de ética, pues en ellos recaen los conceptos sobre los cuales el juez toma sus decisiones.
- Documéntese muy bien sobre la normatividad y regulaciones vigentes alrededor del tema de evidencias digitales en su nación de tal forma que los procedimientos se ajusten a tales disposiciones y las buenas prácticas internacionales.

REFERENCIAS

INTERNATIONAL ORGANIZATION OF COMPUTER EVIDENCE –IOCE. (2002) Guidelines for the best practices in the forensic examination of digital technology. http://www.ioce.org/2002/ioce_bp_exam_digit_tech.html. Consultado: 22-04-2006.

BREZINSKI, D. y KILLALEA, T. (2002) RFC 3227: Guidelines for Evidence Collection and Archiving. Network Working Group. February. http://www.rfc editor.org/rfc/rfc3227.txt

CANO, J. (2003) Admisibilidad de la evidencia digital: Algunos elementos de revisión y análisis. Revista Electrónica de Derecho Informático. No. 61. Agosto. http://www.alfa-redi.org/rdi-articulo.shtml?x=1304. Consultado: 22-04-2006

ASOCIATION OF CHIEF POLICE OFFICERS (1999) Good practice guide for computer based evidence. http://www.digital-detective.co.uk/documents/acpo.pdf. Consultado: 22-04-2006

US DEPARTMENT OF JUSTICE. (2004) Forensic examination of digital evidence. A guide for law enforcement. Special Report.

STANDARDS AUSTRALIA INTERNATIONAL. (2003) HB171:2003 Handbook Guidelines for the management of IT evidence.

INFORMATION SECURITY AND FORENSICS. (2004) Computer forensics. Part2. Best practices. http://www.isfs.org.hk/publications/ComputerForensics/ComputerForensics_part2.pdf. Consultado: 22-04-2006