Fecha de recepción: 30 de enero de 2012 / Fecha de aprobación: 27 de febrero de 2012

Revista de Derecho Comunicaciones y Nuevas Tecnologías

Documento Gecti nro. 14

Descubrimiento electrónico: evidencia digital en el contexto empresarial

Jeimy J. Cano Martínez

Universidad de los Andes
Facultad de Derecho
Revista de Derecho, comunicaciones y Nuevas Tecnologías
N.º 7, Junio de 2012. ISSN 1909-7786

Documento Gecti nro. 14
Descubrimiento electrónico: evidencia digital en el contexto empresarial

Jeimy J. Cano Martínez[1]

GECTI

El GECTI (*Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática*) fue creado el 5 de octubre de 2001 en la Facultad de Derecho de la Universidad de los Andes. Busca fomentar el trabajo multidisciplinario y establecer un puente entre la Universidad y la sociedad para procurar reflexiones y acciones en materia de la internet, la Sociedad de la Información y temas convergentes.

DE LOS DOCUMENTOS GECTI

La colección de documentos GECTI fue creada en 2004. Estos representan reflexiones académicas en torno a aspectos de interés nacional o internacional en materia de la internet, el comercio electrónico, la sociedad de la información, las TIC´s y temas convergentes.

No necesariamente se trata de artículos académicos, científicos o críticos. En algunos casos son una especie de *"White paper"* y en otras una clase de *RFC* (Request for Comments) en el sentido de ser notas documentadas sobre algún tema relacionado con TIC.

Los documentos GECTI puede consultarlos en:

http://gecti.uniandes.edu.co/documentos.php

1 Miembro investigador del Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes (Colombia); profesor distinguido de la misma Facultad; ingeniero y magíster en Ingeniería de Sistemas y Computación de la mencionada Universidad. Ph.D in Business Administration de Newport University, California, USA. Executive Certificate in Management and Leadership de MIT Sloan School of Management, MA-USA. Profesional certificado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners y Cobit Foundation Certificate por ISACA. Miembro del subcomité de publicaciones de ISACA. Contacto: jjcano@yahoo.com

OBJETIVO DEL PRESENTE DOCUMENTO

La evidencia digital como información en formato digital es un reto permanente tanto para las organizaciones como para la administración de justicia. Si bien este término se ha venido revisando y analizando en el contexto de la justicia criminal para enfrentar las conductas punibles en medios informáticos, poca difusión se le ha brindado respecto de las estrategias corporativas para protegerse frente a reclamaciones o litigios en temas propios de su actividad comercial. En dicho contexto, en este documento se presenta una síntesis de los principales elementos del denominado descubrimiento electrónico, como estrategia legal informática empresarial, analizando su ciclo de vida, su modelo de costos y los retos emergentes en el contexto de las organizaciones del siglo XXI.

Introducción

Procesar conductas punibles en un mundo digital establece un reto técnico, administrativo y legal para la gobernabilidad de cualquier nación o empresa. Por consiguiente, conocer con claridad la estructura técnica de los elementos materiales probatorios en medios tecnológicos, sus medidas de aseguramiento y estrategia de presentación se convierte en una prioridad para todos los operadores de la administración de justicia y los profesionales del derecho de un país o corporación. En este contexto toma especial importancia establecer y desarrollar protocolos que permitan identificar, recoger y custodiar los rastros electrónicos propios de cada escena del crimen digital o situación corporativa particular, de tal forma que al presentarse en audiencia no se encuentren reparos o anotaciones que puedan llegar a desvirtuar la misma, privilegiando el espacio de la duda razonable que actúa a favor de los posibles involucrados.

En tal sentido, es clave establecer una base conceptual técnica de buenas prácticas y estrategias que, desde el punto de vista técnico y con miras al soporte jurídico posterior, puedan brindar a las entidades del Estado y a la sociedad en general, una confianza razonable en los procedimientos aplicados para asegurar elementos materiales probatorios digitales a los que puedan tener acceso tanto los particulares como los servidores públicos en el ejercicio de sus funciones.

En consecuencia, los temas relacionados con la computación forense y el descubrimiento electrónico se advierten como dos elementos fundamentales tanto en la administración de justicia como en el ámbito corporativo respectivamente, para comprender con un mismo nivel de certidumbre cómo ocurrió un incidente informático, sus móviles y posibles participantes, así como establecer y ubicar la información electrónicamente almacenada, relevante para preparar a una organización frente a demandas o litigios donde este tipo de datos digitales son claves para plantear los argumentos requeridos en orden a reclamar o reconocer los derechos de las personas naturales o jurídicas. (CANO 2010, cap. 7)

Así las cosas, a continuación revisaremos los asuntos relativos al descubrimiento electrónico indicando sus puntos claves y cuidados

requeridos, su ciclo de vida, el modelo de costos y retos emergentes, con el fin de refinar las acciones y reflexiones necesarias y suficientes cuando de aplicar estos temas se trate.

Comprendiendo el descubrimiento electrónico

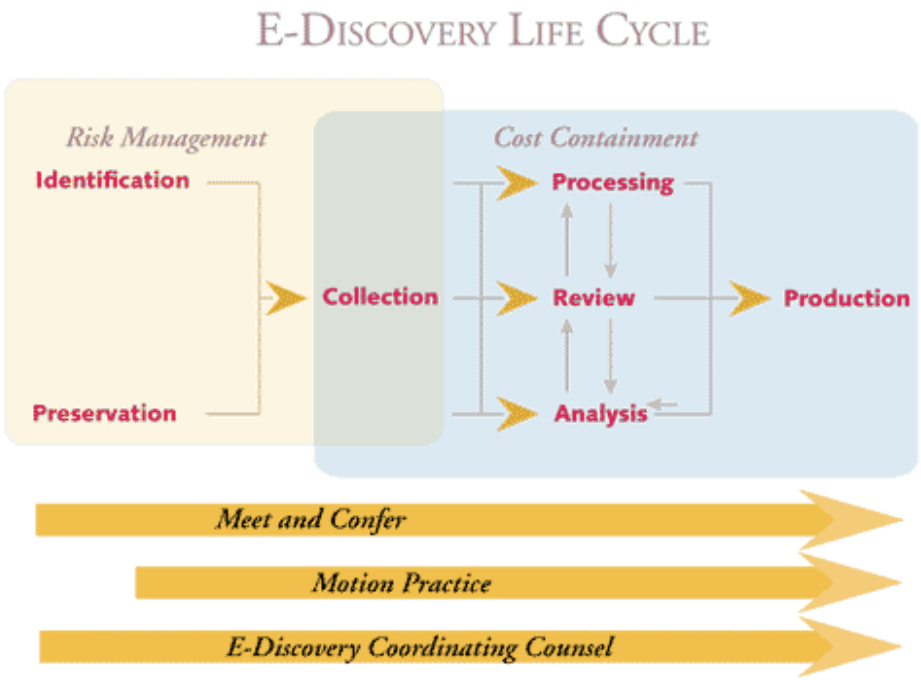
En primer lugar, hablamos de una disciplina cercana a la computación forense que denominamos "descubrimiento electrónico", en inglés "*electronic discovery*" o *e-discovery*. Una breve definición de qué es *e-discovery* sería: procedimiento legal donde se le ordena a una de las partes involucradas la producción de pruebas electrónicas. Generalmente el resultado de este procedimiento implica el análisis de un amplio número de dispositivos electrónicos o medios de almacenamiento, para recabar la evidencia electrónica requerida. (ISF 2008, pág. 2)

En este contexto, se revela el deber que tienen las organizaciones de preservar información relevante, para anticiparse a un posible litigio jurídico. Por tanto, las empresas deben establecer políticas de retención de información electrónica para eventos como: injurias (preservación de datos de empleados o clientes ante injurias, especialmente aquellas donde la empresa pueda aparecer como negligente), despidos (registros de pagos, préstamos, liquidaciones salariales, prestaciones) e incidentes donde estén involucrados ejecutivos de la empresa (políticas de conservación electrónica de las actuaciones de los ejecutivos, particularmente cuando ya no están en la empresa). (CIO EXECUTIVE BOARD 2011b, pág. 10)

Para ello, se deben identificar y revisar los tipos más comunes de información electrónicamente almacenada disponibles en la organización, para que considerando las reflexiones anteriores se establezca el ciclo de vida y un modelo base de costos de una estrategia de *e-discovery* así como los potenciales beneficios de esta frente a eventos que impliquen un litigio jurídico empresarial que pueda impactar el buen nombre de la empresa.

Ciclo de vida del descubrimiento electrónico en la empresa

En línea con lo anterior, el abogado especializado en temas de información electrónicamente almanacenada (IEA), Michael R. Arkfeld, en su libro *Electronic discovery and evidence*. *2011-2012 Edition*, publicado por LawPartner publishing, LLC., establece un ciclo de vida para desarrollar el concepto de descubrimiento electrónico en una empresa, siguiendo cinco pasos fundamentales basados en el modelo de e-discovery de FULBRIGHT y JAWORSKI, para balancear la administración del riesgo corporativo y la estimación y contención de los costos propios del tratamiento de la información electrónica en una organización. Los pasos son: (ARKFELD 2011, cap. 3)



Tomado de: FULBRIGHT y JAWORSKI (?) eDIG: E-Discovery and Litigation Readiness. Disponible en: http://www.fulbright.com/index.cfm?fuseaction=description.subdescription&site_id=1197&id=1195 (Consultado 15-10-2011).

Paso 1: Identificar, preservar y recolectar

Identificar: se adelanta de manera paralela con la acción de "preservar". Se entiende como el tipo, fuente y localización de toda la IEA que debe ser preservada. Es importante anotar que, con base en la naturaleza del caso que se lleve, se define el tipo y las fuentes de IEA requeridas, considerando todo el tiempo los costos de localizar y convertir la IEA en formatos legibles y usables que permitan una presentación adecuada frente a los terceros y autoridades involucradas.

Preservar: la obligación de preservar puede provenir de diferentes fuentes: leyes, estatutos, regulaciones u órdenes de cortes. Dependiendo del tipo de regulaciones o exigencias legales, el deber de preservar las pruebas o evidencia se establece cuando el litigio es: razonablemente anticipado, razonablemente predecible, inminente o pendiente. En este sentido, para minimizar el riesgo de la destrucción de la evidencia y evitar sanciones, la evidencia digital debe ser preservada tan pronto como la parte notifique sobre las potenciales reclamaciones que se pueden presentar. (ARKFELD 2011b, sección 7.9)

Recolectar: es el proceso de reunir potenciales datos relevantes para ser procesados y revisados. Considerando la gran cantidad de IEA almacenada en múltiples ubicaciones, con variedad de formatos, se debe asegurar que el procedimiento que se establezca para ello sea comprensible y legalmente defendible. Es importante anotar que el incremento de datos

informáticos almacenados fuera del control directo de la empresa, generalmente en dispositivos personales o en la nube, representa un reto adicional en este proceso de recolección. (CIO EXECUTIVE BOARD 2011b, pág. 11)

Paso 2: Filtrar y convertir a información electrónicamente almacenada (IEA)

Filtrar significa reducir y asegurar la precisión de la IEA. Esto es, aplicar una serie de criterios que permitan afinar lo requerido según el caso, efectuar revisiones más focalizadas y mantener controlados los costos de producción de la evidencia. Las consideraciones claves que se sugieren para adelantar este paso son:

Negociación del cumplimiento. La premisa en este punto es reunirse y acordar con el abogado de la contraparte los alcances de la preservación de la IEA, con el fin de limitar los costos de producción y mantenimiento de la misma. En este punto se sugiere que durante la negociación esté presente el personal del área de tecnología de información, o si la negociación se torna tensa o difícil, asistirse de una tercera parte neutral.

Considerar las protecciones legales. Existen declaraciones y disposiciones legales que dan forma y moderan las peticiones de IEA, evitando la extralimitación en su solicitud, incluso considerando el hecho de que no esté razonablemente accesible. Los tribunales revisan con detalle las peticiones de protección efectuadas por la parte, para establecer si ésta es una carga, si no es excesivamente amplia, si es pertinente, si está razonablemente accesible, y así decidir si se autoriza o no dicha solicitud.

Filtrado de la IEA. Este paso reduce el tamaño de la población de IEA disponible. El proceso de filtrado responde a una "valoración temprana del caso" o su revisión "analítica". Se estima que aproximadamente entre el 75 y 95 por ciento de los datos inicialmente recolectados en respuesta a una solicitud de descubrimiento electrónico serán eliminados, pues no responden a lo requerido y podrán ser filtrados para su no revisión posterior.

Siguiendo lo establecido en Judges' Guide to Cost-Effective E-discovery (http://www.ediscoveryinstitute.org/JudgesGuide/ consultado el 11-01-2012), detallamos algunos de los métodos técnicos conocidos para efectuar el filtrado de IEA:

- Limitar la búsqueda de términos (palabra clave, expresiones booleanas y sistemas de búsqueda conocidos) a nombres específicos, fechas y código predictivo.

- Restringir la búsqueda hacia archivos específicos (Word, Excel, PDF, etc.) o filtrado por extensión (.pdf, .docx, .pst, etc.)

- Reducir la duplicación de archivos.

- Remover los archivos conocidos del sistema, de las aplicaciones y software base, utilizando para ello la lista general de estos archivos provista por el NIST –National Institute of Standard and Technology– (para comparar sus respectivas firmas de HASH).

- Revisar cadenas de texto en correos electrónicos.
- Analizar los nombres de dominio.
- Establecer una muestra de la IEA disponible con el objeto de determinar la relevancia para el caso y el costo de su procesamiento.

Conversión de la IEA. La conversión es el proceso de extracción de los datos de usuario, texto o metadata de los archivos que representan la IEA. Durante la extracción se convierten en un formato para ser importados a otras aplicaciones; eventualmente los datos se convierten en imágenes o se imprimen en papel para revelarlos y presentarlos en una corte. Es importante anotar que la IEA no se convierta a archivos PDF o TIFF, sin antes cursar la revisión inicial de la relevancia de la misma.

Paso 3: Revisar y analizar

Luego de filtrar la información no relevante, los profesionales del derecho deben revisar los datos seleccionados para determinar los subconjuntos necesarios, que no sean de acceso privilegiado, y que respondan a lo solicitado. El costo real del descubrimiento electrónico no está en la solicitud o la adquisición de datos, sino en el costo del profesional que asiste la revisión de la información para almacenar o localizar información confidencial o reservada antes de su revelación.

Generalmente este paso se apoya en herramientas informáticas como los sistemas automatizados para soporte de litigios (*Automated litigation support systems* –ALS), los cuales cuentan con capacidades de búsqueda y acceso a documentos, reorganización de hechos, registro de análisis previos, puntos de vista, entre otros, que permiten colaborar con el equipo de apoyo al proceso jurídico.

Paso 4: Revelar y "Formularios o formas"

Para adelantar este paso es importante establecer la forma como se va a recibir o a divulgar la IEA. En este contexto, se detallan a continuación algunos criterios relevantes:

- ¿La IEA es apta para hacer búsquedas? Los archivos en formato nativo, bases de datos, texto plano, etc., son susceptibles de búsquedas pero es probable que deban ser convertidos a un formato conveniente para efectuar las mismas.
- ¿La metadata de la IEA está incluida en el formato? Existen algunos formatos de archivo que no contienen metadata.
- ¿Es posible identificar o resaltar la información privilegiada o confidencial? En los archivos con formato nativo no es posible identificar esta información sin cambiar el archivo. Es viable, con algún código o funcionalidad, indicar que la información confidencial se ha retirado electrónicamente.
- ¿Es posible sellar los documentos a ser divulgados? Se recomienda utilizar firma digital o certificados digitales para asegurar la autenticidad de los documentos requeridos para ser presentados.

Es importante anotar que si la contraparte en su requerimiento no especifica la forma o formularios para producir la IEA, la otra parte debe producirla o entregarla en la forma o en los formularios en los cuales ordinariamente es administrada o razonablemente utilizada. Por tanto, la otra parte no debe producir o entregar la misma IEA en más de una forma.

Paso 5: Presentar

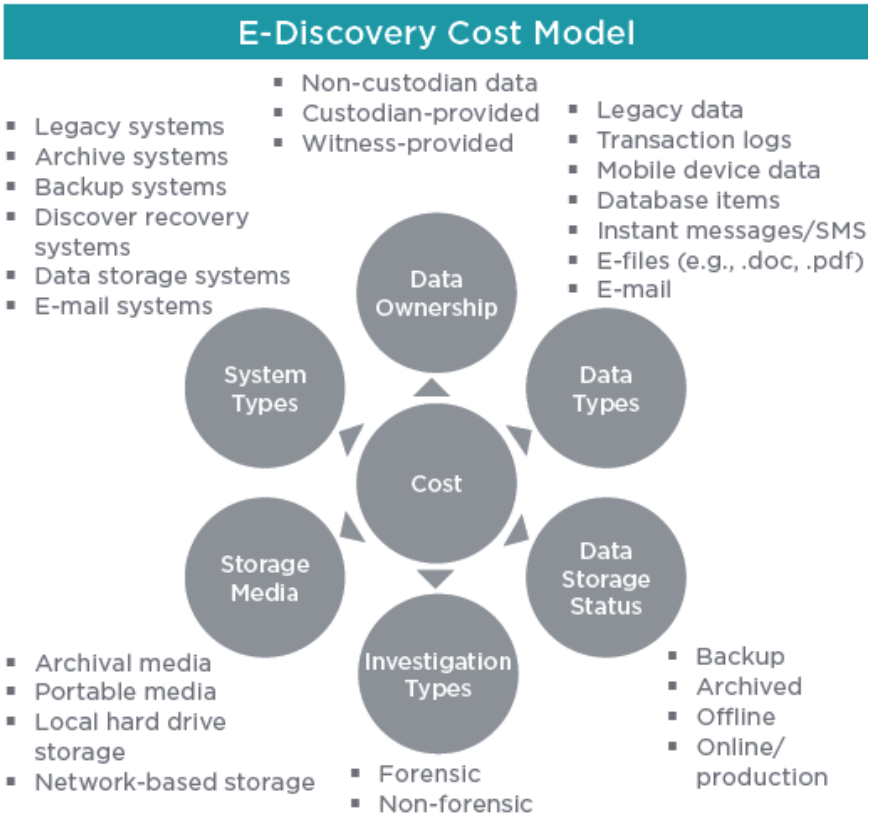
Este es el paso final, que incluye la planeación de la presentación de la evidencia siguiendo el procedimiento legal establecido. Para ello, debe considerar los equipos de apoyo disponibles en recinto de las audiencias, asegurando que se cuenta con el software y hardware requerido para ilustrar con detalle lo requerido durante el despliegue de la presentación.

En razón con lo anterior, resulta conveniente desarrollar al interior de las organizaciones una política o lineamiento corporativo relacionado con la información electrónicamente almacenada de tal forma que se identifique sus periodos de retención, los procedimientos asociados y la persona encargada de la IEA, que permitan recuperar su información para reconstruir los eventos relacionados con reclamaciones o solicitudes que impliquen algún tipo de proceso en el contexto jurídico o empresarial.

Modelo de costos de una estrategia de descubrimiento electrónico

Como quiera que cualquier organización es susceptible de llevar un litigio donde la información electrónicamente almacenada sea parte fundamental de los elementos probatorios del mismo, se hace necesario establecer una estrategia de descubrimiento electrónico que le permita anticiparse a solicitudes que le puedan hacer en este contexto.

Por tanto, dicha estrategia requiere una revisión detallada de sus costos, de tal forma que la empresa dimensione con claridad aquellos elementos claves que debe considerar cuando implemente las acciones que la materialicen. A continuación detallamos algunos aspectos concretos del modelo de costos para descubrimiento electrónico preparado por el CIO Executive Board.



Tomado de: CORPORATE EXECUTIVE BOARD. (2011). E-discovery tools. IREC Executive cheat sheet series. Disponible en: http://www.irec.executiveboard.com (require suscripción).

- Propiedad de los datos

En las organizaciones es importante establecer quién es el dueño de los datos o el responsable del tratamiento de los mismos, cómo se custodian y cómo ellos nos pueden apoyar frente a requerimientos de terceros. En este contexto, la propiedad de los datos establece la responsabilidad y control de los mismos como elementos fundamentales frente al desarrollo de un proceso jurídico y los impactos respecto a su uso. En consecuencia, se debe identificar el tipo de estrategias de seguridad y control que se tienen previstas para los datos e información que se requiere resguardar.

- Tipos de datos

Esta variable nos habla del alcance de la estrategia de descubrimiento electrónico. Dentro de los tipos de datos tenemos: datos de sistemas "legacy", archivos de auditoría de transacciones, datos de dispositivos móviles, tablas de bases de datos, mensajes instantáneos, archivos electrónicos en todos sus formatos, correo electrónico. Cada uno de ellos define una forma de conservación y almacenamiento que debe ser revisada y asegurada para efectos de solicitudes posteriores.

- Estado del almacenamiento de datos

  Un elemento más de aseguramiento son las estrategias de almacenamiento de datos e información. Cualquiera que sea la estrategia que se adopte, se debe asegurar la disponibilidad de la misma, esto es: detallar los tiempos de conservación, definir e implementar las características de confiabilidad de los medios, y asegurar un correcto acceso a la información a través de un formato que perdure en el tiempo.

- Tipos de investigación

  La organización debe tener identificados los tipos de requerimientos que puede recibir para establecer con claridad y eficacia la información que debe guardar y asegurar con miras a responder a los mismos. Generalmente las investigaciones pueden ser de dos tipos: de carácter forense, donde se requiere encontrar y analizar con detalle las características técnicas de la evidencia y sus procedimientos de aseguramiento, y de carácter no-forense (solicitudes de IEA, presente en procesos civiles) en las cuales la información se adjunta según los protocolos establecidos y se verifica frente a la estrategia de descubrimiento electrónico.

- Medios de almacenamiento

  Como bien se anotó en el punto Estado del almacenamiento de datos, la confiabilidad de los medios es un factor crítico a la hora de desarrollar una estrategia de descubrimiento electrónico. Establecer el medio tecnológico y su administración posterior es una variable fundamental para asegurar el acceso a la información en el futuro. Así las cosas, seleccionar el medio de archivo: discos duros, dispositivos móviles, almacenamiento en red (*Network Access Storage*), almacenamiento en la nube, entre otras, son alternativas a evaluar y revisar no sólo desde la perspectiva de costos, sino frente a la seguridad y control de la información y los datos.

- Tipos de sistemas

  Finalmente y no menos importante es establecer los tipos de aplicaciones y sus perfiles frente a la generación de información para la empresa. En este orden de ideas, así como en el área de documentación y archivo se tienen identificados los tipos documentales de los procesos y las áreas, es menester del área de negocio, con el apoyo del área documental y tecnología de información, establecer los perfiles de las aplicaciones por los documentos formales que genera para la toma de decisiones en la organización. Con este insumo, se cuenta con un instrumento que permite dimensionar el esfuerzo de respaldo de información y aseguramiento de la misma.

Este breve listado de consideraciones nos permite ver con mayor precisión las implicaciones de una estrategia de descubrimiento electrónico y los impactos en los costos frente a la conservación, archivo y recuperación de la información cuando se adelanten requerimientos propios de un proceso jurídico o litigio. En consecuencia, sabiendo que este tipo de iniciativas pueden

requerir importantes inversiones tecnológicas, procedimentales y de personal, se requiere un análisis en contexto respecto al ciclo de vida del descubrimiento electrónico, para que se balanceen los riesgos y alcances de contar o no con esta clase de estrategias en materia de información electrónicamente almacenada relevante para la empresa.

Retos emergentes para el descubrimiento electrónico

Si bien estamos frente a una amenaza emergente del siglo XXI como lo es la sobrecarga de información, cuando cada día tenemos mayor cantidad de ella circulando por diferentes medios, desde distintas fuentes, distribuida por numerosos sitios y con diversos dueños, es claro que no toda ella será necesaria para sustentar o apoyar un proceso jurídico en el que una organización esté vinculada como parte interesada.

En este sentido, avanzar en una estrategia corporativa de descubrimiento electrónico define un reto en sí misma dado que se hace necesario vincular al menos tres vistas que permitan sintonizar los esfuerzos para beneficio de la organización: el negocio, la tecnología de información, y los referentes de conservación y archivo. Cada uno de ellos establece connotaciones particulares que articuladas en el proceso de sustentación de pruebas informáticas, fortalecen y aseguran la posición de la organización frente al ciclo de vida del descubrimiento electrónico.

En razón a lo anterior, se presentan tres retos claves (CORPORATE EXECUTIVE BOARD 2011) para considerar a nivel organizacional, con el fin de visualizar los aspectos sensibles que deben mantenerse en la agenda de los responsables organizacionales de asegurar una posición apropiada de la empresa frente a litigios con información electrónicamente almacenada.

1. Mapa de datos e información de la organización

   Este es un elemento crítico para la estrategia de descubrimiento electrónico. Contar con un inventario o mapa de información de una empresa[2] exige de ésta un alto nivel de madurez en conservación y archivo, así como la declaración de la información como un activo de la corporación. Mientras esto no sea la constante, las organizaciones mantendrán un espíritu reactivo frente a requerimientos legales con registros electrónicos.

2. Información almacenada o residente dentro de dispositivos móviles o en equipos propios de terceros que prestan servicios

   Con la alta penetración de dispositivos electrónicos móviles como teléfonos inteligentes y tabletas, las organizaciones cambian su forma de movilizarse en relación con la IEA. Ahora la información no permanece en los equipos de cómputo personal, sino que viajan en los medios móviles, generalmente sin un control definido, y bajo la responsabilidad

2 Es importante anotar que en el mundo empresarial existen muchas categorías jurídicas de información como, entre otras, las siguientes:

Libros y papeles del comerciante

Secretos empresariales

Datos personales

del usuario del dispositivo tecnológico. Sin una adecuada orientación y guía de la empresa en este tema, muchas serán las brechas sobre fuga y/o pérdida de información que se reportarán.

3. Información generada y distribuida a través de redes sociales

   La expresión natural de los seres humanos, ahora a través de la web 2.0, es la creación y exposición de sus ideas en la red. Por tanto, es lógico que los empleados de una organización mantengan estrecha coherencia entre las vivencias y los comentarios y apreciaciones que publican a través de sus blogs y redes sociales. En razón a lo anterior, controlar o asegurar este tipo de información, o mantener su trazabilidad, se convierte en un reto de confianza, ética y procedimientos empresariales, que los trabajadores deben asumir con toda la formalidad del caso, para limitar posibles acciones o declaraciones que puedan atentar contra el buen nombre o imagen de la corporación.

REFLEXIONES FINALES

Cuando hablamos de evidencia digital en el contexto empresarial generalmente la asociamos con aquella prueba requerida para sustentar o probar algún evento, acción o situación organizacional que permita tener la certeza de que algo ha ocurrido. Por ello el artefacto tecnológico que la produce cuenta con las estrategias de seguridad y control requeridas para conocer de primera mano el usuario, sus perfiles, los procedimientos asociados y los mecanismos de monitoreo que acompañan el uso del mismo.

Sin embargo, esta realidad solamente se hace evidente cuando ocurre un hecho desafortunado, particularmente asociado con un incidente de seguridad de la información que manifiesta alguna vulnerabilidad, falla o error en algún momento o accionar de los sistemas de información disponibles en la organización. Esto explica porqué las investigaciones informáticas se convierten en las primeras solicitantes de información para esclarecer los hechos acontecidos, y es entonces cuando la computación forense toma la mayor relevancia como esa disciplina especializada que revisa y analiza sistemas informáticos y dispositivos electrónicos que generan, procesan y almacenan evidencia electrónica con base en la cual determinar la ocurrencia de un hecho y dar las explicaciones científico-técnicas de lo que ha ocurrido.

De otra parte y tan importante como encontrar a los atacantes, sus rastros y acciones realizadas, es la función del descubrimiento electrónico como estrategia legal informática de la organización. Ella permite proteger los intereses de ésta frente a litigios o reclamaciones; los soportes documentales solicitados, ya en formato electrónico, son aportados siguiendo las formalidades de ley requeridas; queda pues mantener la vista del proceso en los hechos y no en las evidencias electrónicas que se aportan al mismo.

En consecuencia, no solamente se requiere una vista criminalística sobre la evidencia digital en las organizaciones sino una visión legal informática que, recabando en los riesgos propios de

las empresas en sus diferentes relaciones de negocio, corporativas y con terceros, pueda establecer los elementos documentales electrónicos que soportan las mismas y prepararse para enfrentar un eventual proceso jurídico en el que la información electrónicamente almacenada es factor determinante para lograr un fallo a favor o en contra.

Finalmente, el descubrimiento electrónico como disciplina emergente que busca una comprensión más sistémica de la evidencia digital, más allá de los procesos propios de la justicia criminal, requiere mayor investigación y relevancia para que pasando de una vista focalizada en los aspectos civiles del derecho, se incorpore al ordenamiento jurídico general de las naciones como factor clave de éxito en la formulación de modelos de administración de evidencia digital tanto en el sector público como privado.

Referencias

ARKFELD, M. (2011). *Electronic discovery and evidence. 2011-2012 Edition*. Law Partner Publishing, LLC.

ARKFELD, M. (2011b). *Guide for legal hold*. Law Partner Publishing, LLC.

CANO, J. (Autor y coordinador). (2010). *La evidencia digital y el peritaje informático en Colombia*. Bogotá: Editorial Temis-Uniandes.

CORPORATE EXECUTIVE BOARD. (2011). E-discovery tools. *IREC Executive cheat sheet series*. Disponible en: http://www.irec.executiveboard.com (requiere suscripción).

CORPORATE EXECUTIVE BOARD. (2011b). The IT Manager's guide to E-Discovery. Information Risk Executive Board Council. Disponible en: http://www.irec.executiveboard.com (requiere suscripción).

FULBRIGHT y JAWORSKI (?) *eDIG: E-Discovery and Litigation Readiness*. Disponible en:

http://www.fulbright.com/index.cfm?fuseaction=description.subdescription&site_id=1197&id=1195 (Consultado 15-10-2011)

INFORMATION SECURITY FORUM – ISF. (2008). ISF *Briefing: Electronic Evidence*. Documento interno. Disponible en: https://www.securityforum.org/whatwedo/publicresearch/ (requiere suscripción).