

## Forensía TI mediante la asociación de datos

**La expansión mundial de las organizaciones, así como la adquisición y fusión de empresas de forma inorgánica, ha implicado la necesidad de compartir información y de disponer de ésta globalmente. Pero, ¿qué nuevos riesgos ha conllevado? ¿Qué impacto tiene en el vector del fraude? Y, si cada vez más, es necesario ser colaborativo, ¿cómo se puede estar seguro de que se ofrece lo necesario para el negocio? La respuesta a estas preguntas se trata a continuación.**



Daniel Solís Agea / José Antonio Lancharro Bervel

### ¿QUÉ ES LA INFORMATION FORENSICS?

La *information forensics* o forensía mediante asociación de datos, es el conjunto de técnicas de recolección de datos presentes en diferentes entornos que, posteriormente, son normalizadas en un formato inteligible y procesable para ser almacenado y tratado con objeto de análisis forenses. Todo ello mediante la relación de la información (datos normalizados y vinculados entre sí).

El proceso no intrusivo (figura 1), que se lleva a cabo para el análisis, sigue técnicas de inteligencia competitiva y *data mining*. Dichas técnicas permiten la búsqueda, extracción y explotación de la información disponible en Internet sobre unos vectores de búsqueda específicos (todo ello basado en mecanismos de I.A.). Por otro lado, para la búsqueda de información, se utiliza un sistema basado en *plug-ins*. Cada uno de estos *plug-ins* permite explorar determinadas fuentes de información: *whois*, DNS, redes sociales, redes P2P, foros de noticias, etc. De este modo, se puede extender el rango de búsqueda, añadiendo nuevas fuentes de datos, de especial interés para el desarrollo de búsquedas por la red de redes.

Posteriormente, la información es normalizada bajo un esquema de datos, definido según las necesidades, que permite representar las diferentes entidades de interés [1]; por ejemplo: una compañía, una red, un segmento, una IP, un servicio, una persona, una noticia, un proceso o, en general, cualquier elemento susceptible de ser considerado como activo. Finalmente, la información es estructurada en forma de grafo, lo que permite dibujar las relaciones existentes entre las diferentes entidades y facilitar la comprensión e interpretación para los seres humanos. Por ejemplo: una persona (entidad) administra (relación) una red (entidad) de una compañía (entidad).

Tras este proceso, se puede repetir la búsqueda en N iteraciones, según la profundidad deseada, y como valor de entrada se usarán las entidades,

que han sido previamente detectadas, adquiridas y normalizadas, consiguiendo así una nueva búsqueda que, esta vez, tendrá en cuenta múltiples factores.

A partir de aquí, la información está lista para ser explotada y correlacionada en proyectos de prevención y detección del fraude, *tests* de intru-

intervención humana para dar los pesos reales a la relación entre entidades; esto es, priorizando según la importancia de los vínculos que tiene un negocio y en sí una organización. Por ejemplo, siguiendo esta premisa, se puede encontrar que el vínculo entre dos empresas, que en un pasado tenía un peso fuerte, puede tener una prioridad inferior o incluso deba ser eliminado, ya que una de las citadas empresas ha sido vendida. Con lo cual el vínculo o relación ha dejado de existir, pero la información disponible en Internet sobre la relación mercantil anterior no puede ser interpretada por la inteligencia de las herramientas. Cabe destacar que, implícitamente a este hecho, está la caducidad y la validez temporal de la información (ciclo de vida de la información).

Otro caso ilustrativo (figura 2) se da entre búsquedas no ligadas a patrones y comportamientos. Por ejemplo, el directivo A, que dirige la compañía X, tiene como proveedor de servicios a la empresa Z, en donde trabaja la persona C. En una primera instancia, no se aprecian vínculos

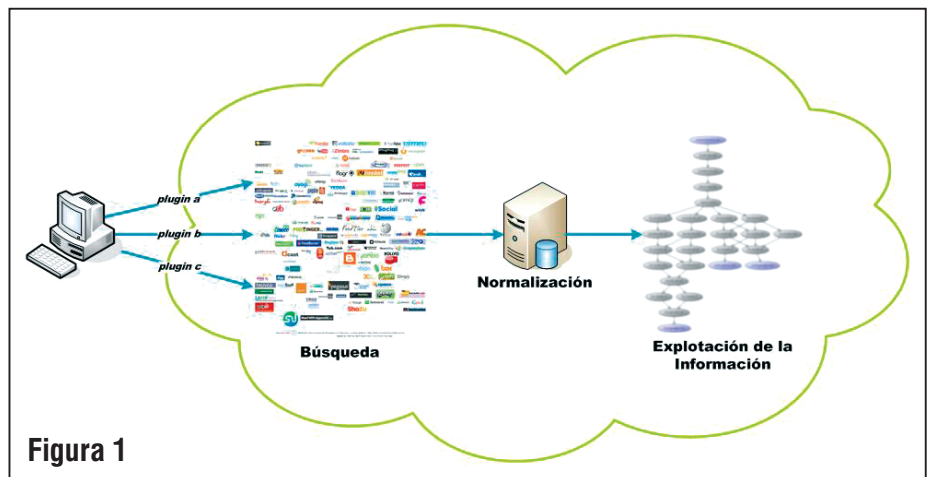


Figura 1

**Aunque existen productos comerciales que realizan las búsquedas automatizadas y aplican técnicas de inteligencia artificial, es necesaria la intervención humana para dar los pesos reales a la relación entre entidades; esto es, priorizando según la importancia de los vínculos que tiene un negocio y en sí una organización.**

sión e ingeniería social, control de información pública, detección de fugas de datos confidenciales, (re)construcción de relaciones entre entidades y personas, uso fraudulento de marcas, atentados a la dignidad de las personas, difamaciones, etc.

### ¿CUÁL ES EL PESO QUE SE OTORGA A LAS RELACIONES ENTRE ENTIDADES?

Aunque existen productos comerciales que realizan las búsquedas automatizadas y aplican técnicas de inteligencia artificial, es necesaria la

en los cuales estas dos personas tienen relación mercantil, laboral o personal alguna. Pero aplicando las técnicas de *information forensics*, se puede observar que comparando los usuarios A y C con el uso de las diferentes redes sociales existentes, se obtiene una predisposición a la existencia de un vínculo personal de algún tipo. Esto es de vital importancia si otra tercera empresa Y va a comprar a la empresa X, ya que el vínculo que resulta del análisis puede ser muy relevante en el proceso de compra (véase el caso práctico *Análisis forense en due diligences*).

En este contexto, la frase “dime con quién andas y te diré quién eres” toma un nuevo sentido, no ciñéndose a relaciones entre personas, sino también a activos de cualquier índole. Mediante la ponderación de las relaciones entre activos, todo activo puede ser evaluado desde la óptica de la dependencia de cualquier otro activo. La relación hace que los atributos presentes en un activo sean propagados (con diferentes pesos) a otros con los que existe relación.

De este modo, se obtienen predisposiciones a que un sujeto pueda llegar a conocer a otro, potenciales pruebas de que un empleado pueda llegar a filtrar información confidencial a otro que trabaja para la competencia, o incluso el índice de probabilidad de que una determinada página web pueda ser objetivo de un determinado grupo de *hacktivistas*.

## ¿QUIÉN UTILIZA EN LA ACTUALIDAD ESTA TECNOLOGÍA?

Esta tecnología se emplea con diferentes finalidades, no exclusivamente forenses. En la actualidad existen diversas áreas de las organizaciones privadas y gubernamentales que utilizan estos servicios (figura 3), pero cabe destacar que los departamentos de riesgos, auditoría y seguridad de la información están empleando estas técnicas para vigilar los activos de sus empresas y apoyar el desempeño de su negocio.

Por otro lado, en cuanto a los proveedores de servicios de seguridad de la información se refiere, estas técnicas son necesarias para la correcta realización de las revisiones de seguridad y para poder vislumbrar la correcta evaluación de impactos, sobre los activos que están siendo revisados [2].

Del mismo modo, la información presente debe ser controlada y monitorizada, ya que ésta puede vislumbrar riesgos importantes, tales como fuga de información o debilidades en los activos tecnológicos, así como daño reputacional, ya sea por difamación de terceros o por empleados descontentos.

Por estos motivos, los SOC internacionales están ofreciendo este servicio para controlar los cambios en las organizaciones y las consecuencias que pudiesen tener sobre los diferentes perfiles de riesgos. De la misma manera, este tipo de técnicas, que usan la inteligencia competitiva, se utilizan para controlar la correcta actualización y protección de activos relegados al *outsourcing* o a terceros, como la gestión de servidores de nombres [3] o el desarrollo de aplicaciones.

## CASOS PRÁCTICOS FORENSES

Las técnicas anteriormente descritas están siendo utilizadas en la detección y prevención

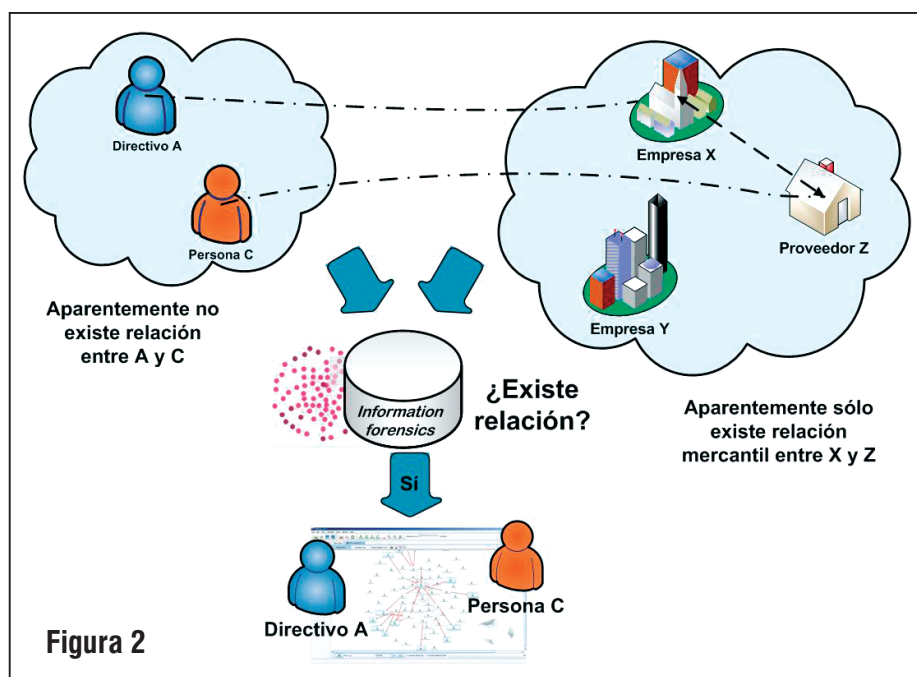


Figura 2

**En la actualidad existen diversas áreas de organizaciones privadas y gubernamentales que utilizan estos servicios de forensics, pero cabe destacar que los departamentos de riesgos, auditoría y seguridad de la información están empleando estas técnicas para vigilar los activos de sus empresas y apoyar el desempeño de su negocio.**

del fraude en relaciones mercantiles, tales como las compraventas de activos o para evidenciar la existencia de pruebas en investigaciones [3], ya sean privadas o de organismos de seguridad del estado. Véanse a continuación algunos casos prácticos.

### Análisis forense en due diligences

La *information forensics* se está utilizando como respuesta a la necesidad de una correcta ejecución de la adquisición de compañías. Cada día, las limitaciones humanas y temporales de los *data rooms* y la revisión que realizan terceras compañías, contratadas a tal efecto, son más palpables. Por ello, se están utilizando estas técnicas forenses con el objeto de buscar relaciones entre terceras empresas proveedoras y personas, factores que no se tienen en cuenta en su totalidad en dichas situaciones, por lo que existen potenciales riesgos financieros; por ejemplo, el fuerte incremento en la tarificación de servicios que pueden estar vinculados a la titularidad *no formalizada* de alguno de los accionistas o personas claves (*C Level* en general). Otro ejemplo sería la existencia de un servicio de telefonía, ofrecido más barato al CEO de una empresa, de modo que cuando éste vende dicha empresa, esta ventaja competitiva desaparece

resultando en un desorbitado aumento de las tarifas de telefonía, lo cual encarece de inmediato el gasto real de la empresa adquirida.

Esta técnica va más allá en cuanto a la asociación entre acciones fraudulentas en compraventas, como puede ser la monitorización y filtrado de potenciales difamaciones por parte de un comprador sobre una empresa, emitiendo noticias falsas que pudiesen dañar la imagen de la compañía que se pretende adquirir y conseguir así un mejor precio.

### Evidencia en Internet

Actualmente, los Cuerpos y Fuerzas de Seguridad del Estado suelen buscar información en investigaciones que afectan a la seguridad nacional, así como sobre casos de abusos de los recursos de Internet que atentan contra las personas o activos de una empresa. Esta labor se ve complementada para averiguar orígenes, en cuanto a:

- Daños, difamación e injurias contra las personas: es necesario mantener la validez de aquellas publicaciones que afecten a personas.
- Robos (ya sean de índole física o tecnológica) o fugas de información: en este caso en particular es de vital importancia establecer mecanismos de firma digital para saber quién

ha liberado la información con carácter confidencial y no público. Un sencillo ejemplo de detección de daño sería la monitorización de las trazas públicas que relacionen a personas capaces de acceder a los activos a proteger, de modo que en el momento en que se detecta una traza en la que se relaciona un sujeto con alguno de los activos a custodiar (por ejemplo, opiniones públicas en las que un administrador de sistemas realiza comentarios sobre los sistemas que administra), se emitirá una alerta proporcional al valor del activo que se desea custodiar, requiriendo investigación inmediata y evaluación de riesgos.

En cuanto a la adquisición de evidencias forenses, toda información recogida es contrastada y tratada con la debida diligencia profesional:

- Contrastando las fuentes: cerciorándose de que los indicios, o ya evidencias, apuntan a un *site web* y/o a una persona u organización como autora. Esta parte es esencialmente importante en cuanto aparecen delitos vinculados al fraude.

- Adquiriendo la información: y añadiendo las correspondientes marcas temporales, así como la firma digital para salvaguardar la existencia, en un momento dado, de la información de la red.

- Facilitando fuentes alternativas de información: sobre el origen de fraudes de diferentes tipologías.

## CONCLUSIONES Y CONTRAMEDIDAS

La información presente en Internet es muy vasta, y escapa al control de las organizaciones, dados los requerimientos para compartir ésta. Por ello, resulta crítico ponderar entre la necesidad de publicar información y los requerimientos de negocio. Por estos motivos, las técnicas de inteligencia competitiva son un aliado muy importante en cuanto al apoyo de la detección del fraude (vinculado a relaciones personales e interempresariales) y las *due diligences*, las revisiones de seguridad y la monitorización de los activos expuestos en la red de redes. Aún así, es necesaria la intervención humana para el procesamiento de ciertos vínculos y alinear el uso de estas técnicas con el negocio.

Área de la Organización	Algunas aplicaciones de las técnicas de <i>information forensics</i>
Seguridad de la Información	<ul style="list-style-type: none"> <li>• Crecimiento de redes de usuarios y comportamientos de consumo de la red que pudiesen determinar el nivel de madurez de la empresa en materia de seguridad.</li> <li>• Evolución del nivel de concienciación de la Organización (usuarios, directivos, etc.)</li> <li>• Prevención ante ataques de Ingeniería social.</li> <li>• Revelación de información crítica a través de <i>posts</i> en foros, buscadores, <i>metadata</i> en los archivos publicados, etc.</li> <li>• Impacto en el perfil del riesgo en donde residen activos de la compañía o vinculados a estos.</li> <li>• Predisposición a la fuga de información.</li> <li>• Detección de violación de la Política de Seguridad.</li> </ul>
Riesgo operacional	<ul style="list-style-type: none"> <li>• Control de la imagen de la Organización y gestión de su imagen pública.</li> <li>• Detección de crecimientos inorgánicos que pudiesen llegar a desestabilizar diferentes áreas de negocio.</li> <li>• Riesgos dentro de acciones de compra o <i>Due diligences</i>.</li> <li>• Evaluación reputacional (comparativas contra otras empresas del sector): Cómo niveles de noticias o información pueden afectar en el tiempo a una empresa.</li> <li>• Búsqueda de las causas que originan una anomalía en la evolución prevista de una empresa y consecuente identificación de puntos de mejora en el apoyo al negocio.</li> </ul>
Recursos Humanos	<ul style="list-style-type: none"> <li>• Uso de los empleados de los recursos tecnológicos.</li> <li>• Gestión de la exposición pública de la alta dirección, con el objeto de minimizar impactos negativos.</li> </ul>
Estrategia	<ul style="list-style-type: none"> <li>• Crecimiento de redes de usuarios y comportamientos de consumo de la red, que pudiesen determinar cambios en la estrategia de negocio.</li> <li>• Estudios de mercado para determinar el nivel de competencia del sector y nuevos focos de negocio no explotados hasta el momento.</li> <li>• Evolución de la competencia con respecto a una empresa determinada, permitiendo extrapolar su situación futura.</li> <li>• Compra de nuevas empresas y crecimientos inorgánicos.</li> <li>• Detección de causas no conocidas hasta el momento, que pudiesen impactar contra la evolución de la empresa.</li> </ul>
Legal	<ul style="list-style-type: none"> <li>• Fugas de información que pudiesen impactar contra la regulación legal vigente.</li> <li>• Violaciones del uso fraudulento de marcas o plagio.</li> </ul>
Marketing	<ul style="list-style-type: none"> <li>• Inteligencia competitiva (estudios de mercado y de la competencia).</li> <li>• Evaluación de la difusión y efectividad de campañas de Marketing (<i>sharing</i>): Campañas informativas (positiva), desinformativa (negativa: difamación, etc.), y gestión de su evolución temporal.</li> </ul>

Figura 3

**La información presente en Internet es muy vasta y escapa al control de las organizaciones; por ello, resulta crítico ponderar entre la necesidad de publicar información y los requerimientos de negocio. Por estos motivos, las técnicas de inteligencia competitiva son un aliado muy importante en cuanto al apoyo de la detección del fraude (vinculado a relaciones personales e interempresariales) y las due diligences, las revisiones de seguridad y la monitorización de los activos expuestos en la red de redes.**

En cuanto a las contramedidas, es aconsejable realizar todas aquellas acciones que marcan las políticas de seguridad y que el negocio considere necesarias, para proteger sus ventajas competitivas y asumir riesgos que no supongan grandes esfuerzos. Actualmente las compañías están teniendo en cuentas los aspectos legales ligados a la información disponible en sus páginas web. Éstas, están modificando las directrices para restringir o prohibir el uso de la información pública, además de no permitir a terceros:

- La presentación de una página del *website* en un marco de otra página web ajena, mediante *framing* y/o hipervínculos (*in line linking* y *hotlinking*).

- Técnicas de *web-spiding* y peticiones contra los activos tecnológicos de las organizaciones.

Por otra parte, existen iniciativas para establecer caducidad a la información que se publica,

tales como Vanish [4], pero distan mucho de otros factores que es necesario tener en cuenta, como la usabilidad (muy presente en los negocios B2C, tiendas en línea y banca *online* principalmente), el rechazo cultural y el propio hecho que hace que la información perezca, que es dependiente de cada modelo de negocio e incluso de cada proceso de éste, así como de los interlocutores que manejen el conocimiento. ■

### DANIEL SOLÍS AGEA

Vocal de Estudios y Proyectos de AEDEL

Director de Operaciones

**BLUELIV**

daniel.solis@blueliv.com

### JOSÉ ANTONIO LANCHARRO BERNEL

Director Técnico

**BLUELIV**

joseantonio.lancharro@blueliv.com

## REFERENCIAS

[1] [http://ctas.paterva.com/view/Userguide#Selecting\\_entities](http://ctas.paterva.com/view/Userguide#Selecting_entities)

[2] <http://www.blackhat.com/presentations/bh-europe-08/Temmingh-Bohme/Presentation/bh-eu-08-temmingh-bohme.pdf>

[3] SIC 85, Seguridad Inteligente, Daniel Solía Agea. Pág. 70-76

[4] <http://vanish.cs.washington.edu/>