CAPÍTULO

CONSIDERACIONES TECNOLÓGICAS EN LOS MERCADOS ELECTRÓNICOS

M. Mercedes Martínez González
mercedes@infor.uva.es
Departamento de Informática, Universidad de Valladolid, Edificio TIT s/n, 47011 Valladolid (España)

I. INTRODUCCIÓN

Este capítulo revisa los aspectos técnicos que afectan a las plataformas utilizadas en los mercados electrónicos. Se trata de una revisión de nivel introductorio, realizada para el proyecto de investigación *VA195A12-2, Problemas jurídicos de los mercados electrónicos: sus efectos en el acortamiento de las cadenas de distribuci*ón. La revisión se ha centrado en aspectos que atañen a estas plataformas de un modo particular. No obstante, conviene recordar que cualquier sistema informático que utiliza una red de ordenadores es susceptible de todas las consideraciones sobre búsqueda y recuperación de información en sistemas de información, y sobre seguridad aplicables a cualquier transmisión de datos. Sin embargo, incluir también estos aspectos haría este documento excesivamente extenso y denso.

La naturaleza del proyecto en que se enmarca este capítulo determina sus destinatarios, y su finalidad. Se trata, pues, de un capítulo destinado a usuarios sin formación especializada en tecnologías, y cuyo fin es facilitar la comprensión de aquellos elementos tecnológicos que influyen en sus decisiones en relación con estos sistemas, de modo que éstas se vean facilitadas.

Los aspectos abordados en este capítulo se han clasificado en tres categorías, que son a su vez las que determinan sus apartados. En primer lugar abordamos los aspectos relacionados con la búsqueda de información. Esto es así porque una de las funciones de un mercado electrónico es dar publicidad a sus usuarios y permitirles a ellos mismos darse a conocer a otros usuarios. Es decir, aportar información sobre uno mismo y buscar información sobre otros. En segundo lugar nos ocuparemos de los aspectos

relacionados con la seguridad. La privacidad, la seguridad en la transmisión de la información, o en los pagos o transacciones que se realizan por mediación de estas plataformas es, lógicamente, uno de los aspectos que más preocupan a sus usuarios. Por último, trataremos algunas consideraciones adicionales, que no encajan en ninguna de las dos categorías anteriores.

Sobre mercados electrónicos en general, y en particular sobre aspectos tecnológicos que les afectan, se puede encontrar en nuestro país una interesante web del ICEX[1], dedicada específicamente a este tema, con interesantes manuales y material de ayuda, algunos de los cuales incluimos en las referencias de este capítulo, y que constituyen una valiosa fuente de información complementaria.

Los *mercados electrónicos* se definen como "foros en los que se realizan intercambios entre numeros agentes (*Many-to-Many*)" (López San Miguel, 2004). En ellos los compradores y vendedores interaccionan. Asimismo, se distinguen los *mercados privados*, aquellos "en los que se relacionan un agente y muchos otros (*One-to-Many*)" (López San Miguel, 2004). Para los efectos de este capítulo, se consideran todos ellos conjuntamente, de modo que los conceptos abordados son aplicables a cualquiera de estas categorías.

II. ACCESO A LA INFORMACIÓN

Las plataformas B2B (Business To Business), entre las que se encuentran los mercados electrónicos, incluyen entre sus funciones comerciales las siguientes: Motores de búsqueda y directorios de proveedores, servicios de licitación, anuncios clasificados, subastas y subastas inversas (Wichmann). Esto supone que un usuario de estos sistemas debe poder publicar información sobre si mismo, para aparecer en los directorios pertinentes y poder ser encontrado por otros usuarios, y también que debe poder buscar información, de modo que encuentre aquellos proveedores, clientes… que le puedan interesar. Estamos pues, en el problema de la búsqueda de información, que se engloba dentro del conocido como problema de la Recuperación de Información (Baeza-Yates y Ribeiro-Neto, 2011). Aunque en la recuperación de información se engloban cuantas consideraciones técnicas afectan a esta función, tanto en sistemas de información, la web, u otros, las cuestiones más básicas que se abordan en esta disciplina afectan, lógicamente, a los buscadores utilizados en una plataforma de mercado electrónico. Así pues, se introducen en este capítulo nociones básicas sobre esta cuestión.

En particular, en una plataforma que se dedica a poner en relación a clientes y proveedores, existen algunos puntos que influyen en la calidad del servicio que ofrece a sus usuarios. Entre ellos se encuentran la calidad del sistema de indexación que acompaña a la plataforma, el soporte que la plataforma proporciona para introducir la información del usuario (normalmente será la información de la empresa), qué tipo de

[1] http://www.icex.es/icex/cda/controller/pageICEX/0,6558,5518394_5593136_5589197_0_0_-1,00.html (último acceso: 28 de febrero de 2014)

vocabularios se utilizan para describir, o catalogar, la información sobre la empresa, los mecanismos que aporta la plataforma para hacer búsquedas precisas, el soporte disponible para contextualizar las búsquedas y los instrumentos que permiten garantizar la fiabilidad de la información. En la tabla 1 se resumen algunos de los factores que condicionan estas funciones y que se tratarán en lo que resta de sección.

1. Sistema de indexación y buscador

El sistema de indexación es la base de las búsquedas. Una buena indexación permite unas búsquedas con mejores resultados. Las búsquedas se apoyan en índices que se construyen analizando los ítems de información disponibles. En el caso de un sistema donde los usuarios introducen su propia información, serán los registros donde ésta se guarde los que se analizan para construir los índices en los que se apoyan las búsquedas.

Los buscadores son bien conocidos en el contexto de la web (Google es, de hecho, el más conocido y utilizado actualmente). Pero estas herramientas existen también disponibles para su instalación en portales y/o plataformas. De modo que una plataforma incorpora un buscador que permite a sus usuarios hacer búsquedas restringidas a la información disponible dentro del sistema. En algunos casos, de modo complementario (pero no sustitutivo) también aportan la posibilidad de realizar búsquedas en la web.

Sobre la búsqueda, y los modos de buscar, se puede encontrar gran número de referencias, que abordan desde las cuestiones más elementales a aspectos técnicos de desarrollo de complejidad elevada. En particular sobre el diseño y desarrollo de herramientas de búsqueda se puede abordar su arquitectura, los modelos utilizados, cómo evaluar las herramientas de búsqueda, o la conocida como búsqueda social en (Croft, Metzler y Strohman, 2010). Sobre variaciones sintácticas en las búsquedas de un usuario y su tratamiento, clasificación, o búsqueda en la web se encuentra amplia información en (Manning, Raghavan y Schütze, 2008). Sobre estos mismos aspectos, y algunos otros como su particularización al caso de las búsquedas en entornos empresariales, se puede consultar (Baeza-Yates y Ribeiro-Neto, 2011). Finalmente, de modo breve, introducimos los principios básicos de un índice en (Martínez-González, 2014).

Los indexadores construyen un índice, similar al que se encuentra en un libro, que permite localizar rápidamente la localización de un determinado término o términos introducidos en una búsqueda por el usuario. El índice almacena, para cada término, la posición donde se encuentra, que en el caso de una plataforma o sistema web, será el registro o documento donde aparece. De este modo, en una plataforma de esta naturaleza el resultado sería un conjunto de empresas o productos cuyos descriptores contienen el término o términos introducidos en la búsqueda.

Pero además los buscadores asignan un peso a los términos, que refleja su importancia relativa en los registros disponibles, y que se utiliza en los cálculos de los ranking por los que se ordenan los resultados (Croft et al., 2010, cap. 2).

Otro de los aspectos que influyen en el funcionamiento de un indexador es el *lenguaje de consulta* utilizado, que en definitiva forma parte de la interacción con el usuario. El lenguaje de consulta más sencillo que se puede utilizar, pero que es el más utilizado en la web y, por consiguiente, en los buscadores que emulan ese comportamiento en plataformas privadas, proporciona un pequeño conjunto de *operadores*. Se analizarán los tipos de búsquedas que se pueden hacer (por tanto, que un sistema de búsqueda puede soportar o no), en el apartado donde se discuten los mecanismos para hacer búsquedas precisas.

Por otro lado, también existe la posibilidad de mejorar la consulta inicial mediante lo que se conoce como *transformación de las consultas*. Entre estas transformaciones se incluyen la comprobación o corrección ortográfica (*spell checking*), que consiste en revisar la consulta introducida por el usuario y *sugerirle una consulta alternativa*, ortográficamente correcta en este caso --un ejemplo muy conocido de esto, que se muestra en la figura 1, se da en Google, cuando ante una consulta incluye una alternativa precedida por la frase "Quizás quisiste decir:"--. También pueden servir para sugerir consultas mejores las técnicas conocidas como *expansión de consultas* (*query expansion)*, donde se sugieren o añaden términos adicionales a la consulta del usuario. Estas sugerencias se basan en un análisis de la ocurrencia de los términos en un documento.

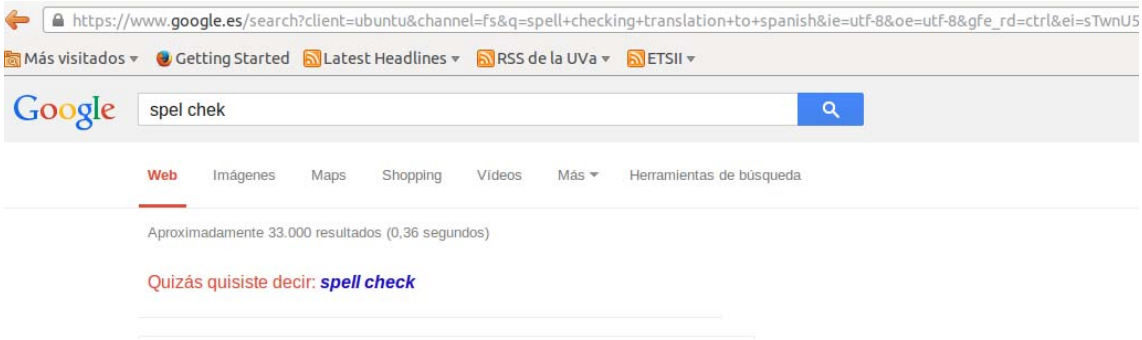

Figura 1. *Spell checking* en Google

Cabe también hacer una mención al conjunto de resultados y el modo en que son presentados al usuario. En función de la orientación de la plataforma, se presentarán al usuario resúmenes de los resultados, datos especialmente relevantes (nombre de la empresa, localización, …), o incluso fotografías del producto ofertado. En todo caso, dado que el usuario debe hacerse una idea inicial de la bondad de cada uno de los ítems encontrados respecto de sus intereses, debe ser información que le permita obtener de manera rápida una impresión adecuada y suficiente de la oferta que está viendo. Es decir, debe ser breve, pero suficiente. El modo en que los resultados son presentados es también un elemento importante, ya que influirá en la capacidad para atraer la atención del usuario sobre ellos.

Además del modo en que se muestra cada registro al usuario, en la presentación de los resultados es de suma importancia el modo en que éstos se ordenan, es decir, el

modo en que se hace el *ranking* de los resultados. La puntuación que se asigna a cada uno de ellos depende del modelo utilizado para la recuperación de información por el buscador. Sobre los aspectos técnicos de los modelos y las formas de puntuar los resultados en cada uno de ellos se pueden encontrar amplios capítulos en cualquiera de los libros sobre recuperación de información referenciados al principio de esta sección.

2. Soporte para introducir información

La particularidad de una plataforma respecto a un sistema abierto como la Web es que en ellas son los usuarios registrados quienes introducen la información que estará disponible en el sistema. Esto permite un mejor ajuste de las herramientas disponibles para este fin, que deben facilitar la tarea a sus usuarios, no sólo en términos de facilidad de uso, sino también en lo que se refiere a la calidad de la información que introducen. Debe tenerse en cuenta que la calidad de la información introducida es trascendental, ya que de ella depende que otros usuarios la encuentren, y que sean los usuarios que "deben encontrarla" (por ejemplo, clientes realmente interesados en los productos ofertados, con los que finalmente se concrete una transacción, o proveedores capaces de proporcionar en las mejores condiciones el producto que se está buscando).

La introducción de información por parte de los usuarios de una plataforma puede ser básicamente de dos tipos: manual, adaptándose a los formularios que la herramienta le presenta (esto es, rellenando los campos correspondientes), o automática, con herramientas capaces de extraer la información que se almacenará en el sistema a partir la información de los sistemas de la propia empresa.

En el primer caso se trata de una situación clásica, como la que se da en cualquier sistema web en el que se puede realizar un registro, donde los aspectos más importantes a considerar son la calidad de la interfaz de usuario y, en consecuencia, la comodidad con la que un usuario se mueve por el formulario e introduce la información, y la calidad de los campos utilizados en el formulario, es decir, si son los adecuados para describir la empresa y sus productos y si el usuario los entiende correctamente, de modo qué información debe introducir en cada caso. Sobre este último aspecto cabe referirse al uso de vocabularios conocidos y estándar, que se aborda en siguiente subapartado.

En el segundo caso se plantea un problema característico en el tratamiento de información empresarial, que es la extracción y transformación de la información ya disponible en unos sistemas, para obtener a partir de ella aquella que debe ser almacenada en un tercero, en este caso, en la plataforma en la que el usuario se ha dado de alta. Los problemas que conlleva esta tarea son complejos, y han llevado de modo general a la aparición de un tipo de herramientas conocidas como ETL (*Extract/Transform/Load*), cuya finalidad, como su propio nombre indica es actuar en tres fases: primero, extraer la información de las bases de datos o portales de la empresa; segundo, realizar una serie de transformaciones que permitan pasar de los formatos y esquemas originales a los utilizados en la plataforma, por ejemplo, de una base de datos relacional a ficheros XML ajustados a unos determinados esquemas; finalmente, cargar (introducir) esa información, que ya está adaptada a los modelos de datos de la plataforma, en sus bases de datos o almacenes de información. Sobre las estrategias y soluciones tecnológicas disponibles para ello puede consultarse el capítulo 10 de (Doan, Halevy e Ives, 2012). Para un usuario hay dos cuestiones que debe

considerar: en primer lugar, que estas herramientas le sean proporcionadas por la propia plataforma, de modo que no constituya un esfuerzo adicional en su empresa su desarrollo o adaptación; en segundo lugar, que su integración con los propios sistemas de información o bases de datos sea sencilla.

3. Vocabularios estándar

El uso de vocabularios bien conocidos y cuyo significado es fácilmente comprendido por una amplia comunidad facilita, sin lugar a dudas, varios aspectos. En primer lugar, cuando los términos (por ejemplo, los usados para los campos de un formulario) son conocidos por los usuarios que deben darles valor, estos últimos se sienten más cómodos con esta tarea, puesto que no les surgen dudas sobre su significado (dudas que se traducen en que no se sabe qué debe introducirse en dicho campo). En segundo lugar, porque esto mismo es aplicable a los usuarios que buscan información; cuando se entiende qué campos se están utilizando para describir las empresas y productos disponibles en un sistema, es más fácil hacer búsquedas más precisas, esto es, mejores. Esto también es cierto para el almacenamiento de los datos: si se utilizan vocabularios estándar será más fácil facilitar su integración posterior con otros datos.

Se pueden utilizar vocabularios estándar tanto para los campos que se van a presentar a un usuario como para los valores que los usuarios introducen para describir sus productos. En este último caso los vocabularios suelen estar organizados como clasificaciones, de modo que se introduce como valor del campo uno de los disponibles en la clasificación. Lo que se consigue con ello es precisamente que resulta mucho más fácil "clasificar" los productos bajo clases o categorías, de modo que ante una búsqueda por una de ellas aparezcan en los resultados aquellos productos que han sido descritos con el término utilizado.

Un ejemplo de este tipo de vocabulario es CPV (Vocabulario Común de Contratación), el vocabulario utilizado en la versión en línea del "Suplemento al Diario Oficial de la Unión Europea" dedicado a la contratación pública europea, TED (*Tenders Electronic Daily*)[2]. La figura 2 muestra un fragmento. El uso de este vocabulario común por parte de los empleados que introducen las ofertas de contratación permite a quienes buscan en ellas encontrar aquellas que fueron catalogadas bajo una determinada categoría. Incluso puede afirmarse que cuanto más preciso sea el término introducido, mejores opciones de encontrar buenos resultados tendrá un usuario.

Por ejemplo, si un concurso ha sido clasificado bajo la categoría *03211000 – Cereales* esta clasificación será más útil que si lo ha sido bajo la categoría *03200000 - Cereales, patatas, hortalizas, frutas y frutos de cáscara*. La más específica facilitará que quienes no estén interesados en cereales, pero sí en frutas, no lo encuentren, mientras que en el segundo caso aparecerá tanto a unos como a otros. Sin embargo, en el primer caso, quienes busquen únicamente concursos relacionados con los cereales (bajo la categoría 03211000) podrán encontrarlo, y también quienes busquen concursos relacionados con la categoría más general, en la que se subsume ésta (la 0320000). No

[2]ted.europa.eu (última visita: 10 de marzo de 2014)

ocurre así en el segundo caso, donde sólo lo encontrarán quienes busquen por la categoría más general.

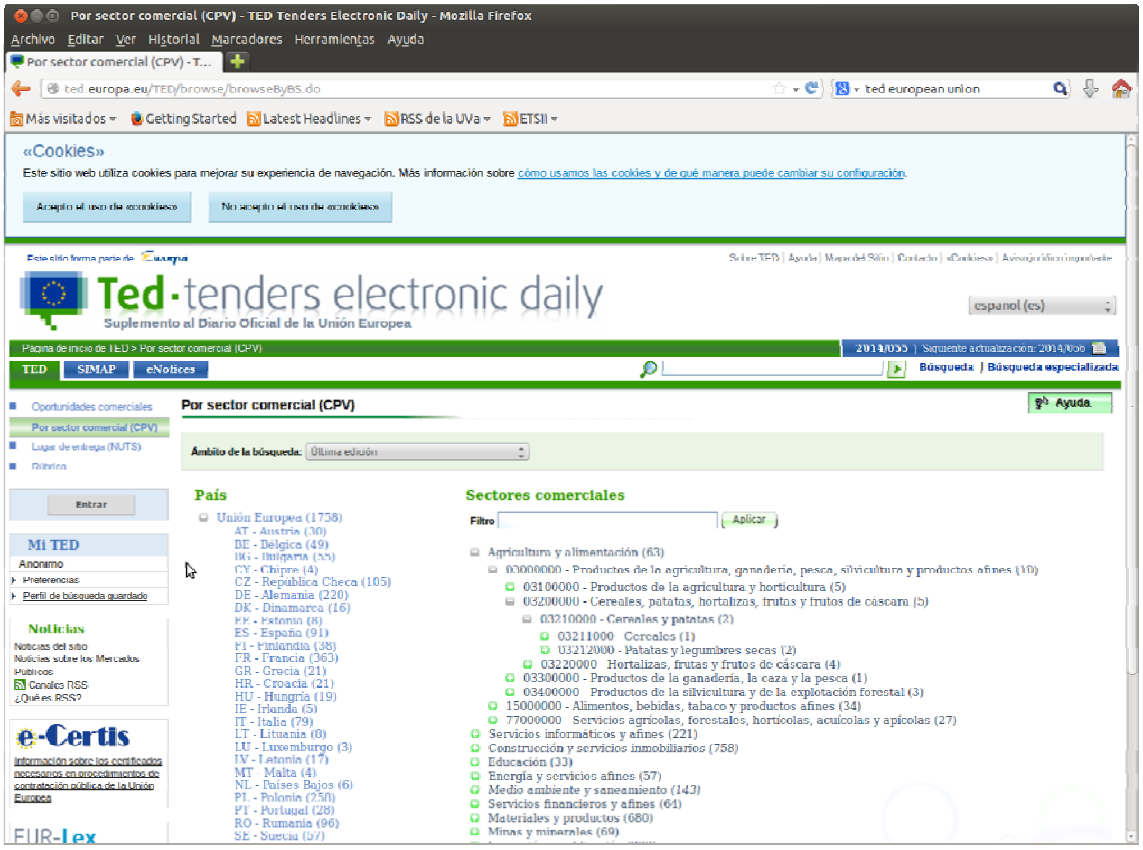

Figura 2. El vocabulario CPV en el portal TED de la Unión Europea.

Existen muchas propuestas de vocabularios estándar relacionados con el comercio electrónico, que pueden ser utilizadas en el contexto de los mercados electrónicos. Entre las propuestas de vocabularios que se usan en este tipo de transacciones mencionamos una, que figura entre las que más difusión y estabilidad ha conseguido, XBRL (eXtensible Business Reporting Language), un estándar que se usa para intercambiar información financiera y empresarial. En España existe una asociación que se encarga de su difusión[3]. El uso de vocabularios como éste, que han conseguido un alto nivel de estabilidad y difusión, facilitará que otras empresas y agentes también lo utilicen, lo cual ya hemos indicado resulta beneficioso. Es por eso que una de las cuestiones que se puede valorar a la hora de utilizar una plataforma es si los vocabularios que ofrece son los comúnmente aceptados en la comunidad de usuarios con la que estamos interesados en relacionarlos.

[3] http://www.xbrl.es/es/ (última visita: 10 de marzo de 2014)

FUNCIÓN	FACTORES
Búsqueda	Indexador; pesos de los términos; lenguaje de consulta; transformación de consultas: sugerencias de consultas alternativas, expansión de consultas; presentación de los resultados: resumen, ranking; uso del contexto
Inserción de información	(si es manual) calidad de los formularios y de los campos; (si es automática) disponibilidad y facilidad de uso de las herramientas ETL; vocabularios

Tabla 1. Factores que condicionan algunas funciones de acceso a la información.

4. Mecanismos para hacer búsquedas precisas

Además del uso de vocabularios comunes tratado en el apartado anterior, existen otras formas de facilitar al usuario hacer búsquedas más precisas, que le permitan ajustar mejor el conjunto de resultados que obtiene (es decir, ni los resultados incluyen ítems en los que no se tiene interés, ni aquellos que podrían interesar han quedado fuera del conjunto de resultados). Entre estos mecanismos merece la pena mencionar las búsquedas combinadas mediante el uso de operadores, las búsquedas por campos o metadatos, las búsquedas semánticas, la posibilidad de afinar las búsquedas, o el uso de filtros.

Un *operador* es un comando que indica cómo combinar los términos de la consulta. Uno de estos operadores, bastante conocido, es el uso de comillas para indicar que el texto entre ellas debe aparecer literalmente como se introduce, sin otras palabras en el medio. Otros operadores básicos son el AND (Y), que indica que se buscan registros donde aparezcan todos los términos introducidos en la consulta, y el OR (O), cuyo significado es que se buscan registros donde aparezca alguno de los términos introducidos (pueden aparecer todos ellos, pero no se requiere que sea así). No obstante, una consulta típica contiene un pequeño número de términos o palabras, sin ningún operador. Esto será interpretado por el buscador como la presencia implícita de un operador, normalmente, AND u OR.

Las búsquedas por campos son aquellas donde se puede indicar *dónde* buscar un valor. Por ejemplo, sólo en el nombre de la empresa, o en la ciudad. Estas búsquedas se

pueden ofrecer cuando se almacena información que describe los productos ofertados usando campos, cuyo valor se rellena en cada caso. Estas descripciones son metadatos (por ejemplo, los metadatos sobre la categoría CPV, país... que describen un concurso). Las búsquedas por estos metadatos o campos permiten hacer múltiples combinaciones a los usuarios (buscar sólo en un campo, en varios de ellos, con distinto valor en cada uno, etc.) y, en consecuencia, especificar búsquedas precisas. Además suelen presentarse bajo el aspecto de formularios de búsqueda, cuyo uso resulta intuitivo a los usuarios.

Las búsquedas semánticas son más desconocidas. Se pueden considerar muchos tipos de búsquedas semánticas (Yu, 2011). Sin embargo, para los efectos que aquí interesan, es suficiente con indicar que suelen construirse sobre las búsquedas por campos y el uso de vocabularios u ontologías conocidos.

5. Soporte para contextualizar las búsquedas

La posibilidad de contextualizar las búsquedas está recibiendo mucha atención en los últimos tiempos (Kessler, 2010). Los avances en el tratamiento de información geográfica, combinado con la expansión de la presencia de GPS en los dispositivos ligeros como móviles y tabletas, ha motivado un creciente interés en la capacidad de restringir las búsquedas de los usuarios a áreas geográficas concretas. En particular, para el caso de transacciones comerciales la posibilidad de localizar potenciales clientes o proveedores en áreas concretas, por ejemplo, en áreas cercanas, tiene un interés evidente.

Además de la posibilidad de combinar las búsquedas usando información sobre la posición geográfica existen otros métodos más sencillos que ya están siendo utilizados en varias plataformas, tales como el uso de los códigos postales, que se solicitan al usuario para, una vez se han obtenido los resultados de la consulta, *filtrar* para seleccionar únicamente aquellos cuyo código postal responde al criterio del usuario.

III. SEGURIDAD

La seguridad en una plataforma de mercados electrónicos responde a unos requisitos básicos de seguridad comunes al comercio electrónico[4]. Estos requisitos son cuatro: *confidencialidad*, *integridad*, *autenticación* y *no repudio*. Se verá cómo se resuelve cada uno de ellos, particularizando el análisis para el caso de plataformas dedicadas a mercados electrónicos, si bien en varios de ellos las soluciones tecnológicas son comunes a los de cualquier plataforma con requisitos similares o en la Web. Además de estos cuatro requisitos se debe tomar en consideración un quinto y un sexto, no incluidos tradicionalmente como requisitos de seguridad en el comercio electrónico: la *privacidad* y la *fiabilidad* de la información.

[4]En Martínez-González (2009) se puede encontrar una revisión detallada de estos requisitos.

Con el auge de las comunicaciones por la web y otras redes, la posibilidad de distribuir masivamente información privada ha aumentado de forma llamativa. Prueba de ello es la sensibilidad existente en España y países de su entorno respecto a estas cuestiones. Las plataformas de mercados electrónicos no son una excepción, y el cumplimiento de las normativas protectoras de la privacidad, tales como la Ley de Protección de Datos, forma parte de sus requisitos funcionales. Es también, lógicamente, una preocupación de sus usuarios (es fácil entender que una empresa no desee compartir todos los datos que proporciona a una plataforma con cualquier otro usuario de la misma). Por eso la privacidad supondrá que estos sistemas deberán proveer los mecanismos necesarios para que los datos privados que recaban se almacenan de forma segura, a salvo de accesos no autorizados.

La fiabilidad de la información, o la garantía de que la información es fiable, no se consideró como un requisito de seguridad en los inicios del comercio electrónico. El uso masivo de la Web como soporte para gran número de las transacciones relacionadas con el comercio electrónico influyó en ello: siendo la Web por su propia naturaleza un medio donde no se garantizaba la fiabilidad de las fuentes de información, era lógico que este mismo principio tuviese vigencia cuando se utilizaba para transacciones de comercio electrónico. La fiabilidad de la información era algo que el propio usuario debía comprobar, porque confiaba en el sitio web que visitaba (la empresa era de su confianza, y en consecuencia también podía suponer que había tomado las precauciones necesarias para que la información de su portal fuese correcta), o por otros medios que tuviese a su disposición. Sin embargo, aunque los mecanismos utilizados sean sencillos, cuando se utiliza una plataforma proporcionada por un tercer agente, éste se ocupa de garantizar, en la medida en que esto le resulta posible, que la información que en ella se publica sea fiable. En resumen, procurará que sólo usuarios autorizados para ello (usuarios registrados) puedan introducir la información.

1. Requisitos de seguridad

Confidencialidad

La confidencialidad en una comunicación consiste en transmitir un mensaje por un canal no seguro garantizado que terceros no pueden acceder al mensaje.

Integridad

En este caso se trata de garantizar que un mensaje, documento o fichero no ha sido modificado de modo intencionado. Es decir, que se recibe tal como fue enviado por el emisor.

Autenticación

Autenticarse es probar de modo interactivo la identidad ante un interlocutor.

No repudio

Si un cliente niega haber realizado una compra, o un emisor haber enviado un mensaje, está repudiando la compra o el mensaje.

2. Aspectos de seguridad

En este apartado se introducen los mecanismos que se utilizan para garantizar la seguridad a través de la presentación de los aspectos de seguridad que pueden inquietar a un usuario de una de estas plataformas[5]. Un usuario que se plantea por primera vez la utilización de una de estas plataformas debería preguntarse acerca del modo y nivel en que se garantizan las siguientes cuestiones: pago seguro, garantía de la información, identificación (autenticación) y la integridad de la información. La tabla 2 resume los mecanismos usados para satisfacer cada una de ellas.

A) **Pago seguro**

El pago seguro es probablemente la primera cuestión que se plantea un potencial usuario. En general estas plataformas requieren un registro y el abono de algún tipo de cuota por el uso de sus servicios. Además sus usuarios acceden a ellas con la intención de llevar a término transacciones comerciales, lo cual significa que en algún momento deberá producirse el pago del producto o productos objeto de la transacción. Se puede plantear la cuestión desde dos puntos de vista: ¿Cómo se garantiza la seguridad en el caso de que la plataforma desvíe el pago a otro agente, esto es, si el pago se realiza de modo externo a la plataforma? ¿Cómo se garantiza la seguridad de los pagos que se realizan a través de la plataforma?

En el primer caso el agente externo suele ser una pasarela de pago, sistema especializado en ofrecer pagos seguros. Actualmente esto es muy habitual y prácticamente todas las entidades financieras ofrecen algún tipo de pasarela de pago. También existen pasarelas que no están directamente vinculadas a una entidad concreta, pero que son muy conocidas, como es el caso de PayPal.

Las pasarelas de pago tienen la ventaja de garantizar la seguridad en los pagos y de que, una vez la plataforma ha desviado la interacción hacia ellas, los datos se transfieren entre el cliente y la pasarela. Esto significa que la plataforma no interviene directamente en la comunicación (se descarga así de esta función) y, lo que es aún más importante, no accede a los datos que se intercambian, lo cual significa que no accede ni almacena los datos privados necesarios para el pago. Estos datos se gestionarán en los servidores de la pasarela, que se encarga de su seguridad.

En el caso de que la plataforma asuma la gestión de algún pago (cuotas, otros) debe hacerse cargo de su seguridad. El mecanismo más utilizado es el protocolo SSL

[5] Algunas de estas cuestiones están reflejadas en las preguntas recogidas en las "*checklist*" que recoge el portal *e-Market services* del ICEX.

(*Secure Socket Layer*). SSL es un protocolo que garantiza la seguridad en las comunicaciones web, y por ello el más utilizado actualmente en las transacciones que se realizan a través de la web. Es también el protocolo que garantiza la seguridad en las comunicaciones entre los clientes y las pasarelas de pago. Este protocolo se ocupa de garantizar cuestiones como la autenticación, para lo cual hace uso de certificados digitales. En el apartado III.4 se ofrece una breve introducción.

B) **Garantía de la información**

El aspecto que ahora se trata es el de garantizar que la información que se consulta es correcta, esto es, que ha sido introducida por una fuente fidedigna, no ha sido manipulada posteriormente, y ha sido validada cuando se introdujo para asegurar en la medida de lo posible su validez.

La confianza en la información que se consulta depende en gran medida de la confianza que se tiene en que ha sido introducida por el agente correcto. Es decir, que nadie ha suplantado a su supuesto autor para introducir información incorrecta. En las plataformas de mercado electrónico esta preocupación se resuelve de varios modos. En primer lugar, tratándose de plataformas donde es necesario registrarse como usuario para introducir datos, sólo los usuarios registrados podrán hacerlo. Por ello, es necesario conocer el usuario asignado en el sistema (login) y sus claves de acceso para poder introducir información. Esta seguridad viene condicionada por dos factores: en primer lugar, que el usuario no desvele esta información a otros individuos (lo cual no depende de la plataforma); en segundo lugar, del nivel de bondad (o fortaleza) de las claves de acceso elegidas. Para medir este nivel de bondad existen softwares validadores que avisan la primera vez que se selecciona una contraseña de lo segura que es. Estas herramientas suelen estar incluidas en las plataformas. Aunque van surgiendo mecanismos adicionales para reforzar esta seguridad, basados en el uso de certificados o de otros dispositivos, el comentado es el más habitual –en gran medida porque al ser sencillo suele ser también el preferido por los usuarios--.

Pero además de garantizar que únicamente los usuarios autorizados para ello introducen información en el sistema, es necesario que ésta no sea manipulada posteriormente. Esto significa garantizar la seguridad del servidor que alberga la plataforma frente a ataques externos, y la seguridad de las bases de datos donde se almacenan los datos frente a accesos no autorizados. Los sistemas gestores de bases de datos ofrecen mecanismos depurados por una amplia experiencia para garantizar el acceso a sus datos, tales como el uso de roles, vistas, y control de permisos (Connolly, Begg y Holowczak, 2008). La seguridad de los servidores web frente a ataques externos es un tema con muchos aspectos que considerar, que por su amplitud no se abordará en este capítulo. Sin embargo, es conveniente recordar que existen compañías que supervisan y certifican la seguridad de sitios web. Haber obtenido una de estas certificaciones es una garantía para los clientes de una plataforma.

Por último está la confianza que se tiene en la corrección de los datos introducidos por los usuarios. Aunque los usuarios actúen legítimamente pueden cometer errores al introducir los datos, o las herramientas de transformación e importación al sistema pueden resolver un conflicto de modo que el resultado final

contenga errores. Para minimizar en la medida de lo posible estas situaciones existen herramientas que validan automáticamente los datos que se van a almacenar. Un supuesto muy conocido es la validación de los números de teléfono y códigos postales, que en este caso es simple: deben contener sólo números y una determinada cantidad de dígitos.

Existen otros supuestos más complejos, donde se plantea validar la información que se introduce contra ontologías y otras herramientas. En estos supuestos debemos remitirnos a lo comentado en el apartado primero sobre la recuperación de información, ya que las técnicas utilizadas reposan sobre los mismos principios. Finalmente, un modo también sencillo de garantizar la corrección de la información introducida es limitar las posibles entradas o valores que introduce un usuario a los desplegados en un menú de valores posibles. Esto es de interés en casos donde el valor introducido debe ser uno entre el conjunto de una clasificación, como en el ejemplo de la clasificación CPV del portal TED de la Unión Europea.

C) **Identificación o autenticación**

Como se indicó en el apartado III.1, la autenticación consiste en probar la propia identidad ante un interlocutor. En el caso de mercados electrónicos, se trata de autenticarse cuando se accede a la plataforma, o de probar la identidad durante las distintas transacciones que posteriormente se realizan. Esto afecta tanto a sus usuarios como a la propia plataforma y las pasarelas de pago.

El acceso a plataformas por parte de usuarios suele utilizar como método de autenticación la inserción de contraseñas o palabras de paso. Este método, que ya se comentó en el epígrafe anterior cuando se trató la garantía de la información, tiene la ventaja de ser sencillo y bien aceptado por los usuarios. Sin embargo, no es aplicable a la autenticación de la propia plataforma o de las pasarelas de pago. En estos últimos casos se trata de servidores, que deben autenticarse para que el usuario pueda estar seguro de que se está conectando con la auténtica plataforma y no con otro sitio creado con fines fraudulentos para suplantarla.

La autenticación de servidores se realiza con certificados digitales. El servidor presenta a la aplicación cliente, que será un navegador web si la plataforma está accesible a través de la web, un certificado con el que se autentica. La aplicación cliente comprobará el certificado e informará al usuario sobre la validez (o no) de éste. En el supuesto de plataformas web este proceso está incluido dentro de los pasos del protocolo *Secure Socket Layer* (SSL), que regula comunicaciones seguras en la web. También es posible utilizar certificados para que los usuarios se autentiquen (piénsese por ejemplo, que el DNI electrónico contiene certificados que sirven para autenticarse[6]), aunque actualmente esto no está tan extendido. En el apartado III.3 se introducen los certificados digitales.

[6] Sobre el DNI electrónico puede encontrarse información en la página web de INTECO (www.inteco.es) y en la página web donde la Policía Nacional detalla sus componentes (http://www.dnielectronico.es/Guia_Basica/descrip_fisica.html).

D) **Integridad de la información**

Que la información no haya sido manipulada por terceros desde que el autor la introdujo o la envió se conoce como integridad de la información. Este es uno de los requisitos clásicos en seguridad de las comunicaciones y también, como es lógico, en comercio electrónico. Es importante que la información que se proporciona no sufra alteraciones por parte de terceros, y tener la garantía de que la que se recibe es la misma que el emisor envió. Existen distintas variantes para el modo de garantizar la integridad, en función de que se trate de un mensaje que se envía a través de una red, o que se trate de un documento. Pero todas ellas reposan sobre el mismo principio: el uso de la criptografía.

En el caso de documentos, mensajes de correo, etc. es posible firmarlos digitalmente. La firma digital es en realidad un criptograma que se obtiene aplicando una serie de funciones de encriptación a los datos de entrada. La validación de una firma requiere conocer el algoritmo de firma que se utilizó y disponer del certificado del firmante. Las firmas digitales y ambos procesos, firma y verificación, se abordan con detalle en Martínez-González (2014).

Una segunda forma de garantizar la integridad de unos datos son las funciones resumen (también llamadas funciones hash o funciones de dispersión). Esta opción es muy utilizada en el caso de software, pero también puede acompañar los procesos de firma electrónica. En este caso se genera un *resumen* o *huella digital* (una cadena de caracteres) a partir de los datos o archivos cuya integridad se quiere garantizar. Para generar esta cadena se utilizan las funciones resumen, que son procesos capaces de generar una cadena única a partir de los datos de entrada. Su propiedad relevante es que no generan el mismo resumen para dos conjuntos de datos (léase archivos o mensajes) diferentes. La comprobación de la integridad consiste en generar también la función resumen utilizando la función hash que indica el proveedor (esto es, el software correspondiente) y verificar si el resultado es el mismo resumen que obtuvo el proveedor. En la figura 3 se puede ver la huella digital que se obtiene para el certificado cuyos datos se muestran aplicando dos de los algoritmos más habituales, el SHA1 y el MD5.

Por último, en las comunicaciones de mensajes se utiliza la encriptación de los mensajes. Para ello existen varios algoritmos criptográficos. Estos algoritmos utilizan unas claves para encriptar. Como indicación general, cuanto mayor es la longitud de la clave más seguro es el método de encriptación. Esta encriptación tiene lugar, entre otros, en el proceso de intercambio de información del protocolo SSL, que ofrece la posibilidad de utilizar distintos algoritmos de encriptación. Por eso es interesante fijarse en qué longitud de clave (128 bits, otros) utilizan las plataformas de comercio electrónico.

Además de la integridad durante la comunicación es posible preguntarse si ésta puede ser modificada en algún otro momento. Por ejemplo, porque alguien consigue suplantar al proveedor y sustituirla por otra, o porque una vez almacenada en los servidores consigue modificarla. En el primer caso el problema que se plantea es el de la *suplantación* de usuarios, que se abordó en el apartado sobre la garantía de información. En el segundo supuesto se trata de la seguridad de la información almacenada, que también se abordó en ese mismo apartado. No obstante, dado el auge que ha tomado

recientemente el uso de servidores en la nube (*cloud computing*) las preguntas acerca de la seguridad de un servidor deben extenderse a los servidores o servicios que en su caso pueda estar utilizando la plataforma de comercio electrónico.

E) Riesgos para los sistemas de los usuarios

El uso de *cookies* en los portales y plataformas web se ha extendido a medida que las empresas han visto el potencial interés que tiene la información que pueden extraer a partir de los datos recogidos con estas cookies sobre sus usuarios. Es prácticamente imposible encontrar un portal web que no use cookies para recabar datos sobre el comportamiento de sus clientes.

Las cookies son pequeños archivos creados por los sitios web que se almacenan en los equipos de los usuarios. El servidor web pide al navegador web que almacene este archivo en el equipo. Su función, como ya indicamos, es la de recabar información sobre los hábitos de navegación, información que identifica al usuario[7]... que el navegador web enviará al servidor web en la siguiente visita.

Esta recogida de datos puede entrar en conflicto con la privacidad de los usuarios. Por ello los navegadores ofrecen la posibilidad de inhabilitar el uso de cookies . Para hacerlo deben seguirse las instrucciones del navegador que se está utilizando, Firefox[8], Google Chrome[9], Internet Explorer[10], etc. A su vez las plataformas deben avisar a sus usuarios del uso de cookies y la finalidad de éstas.

[7] Sólo si el usuario la introduce expresamente. Las cookies no pueden acceder a cualquier dato almacenado en archivos del disco duro de un ordenador.

[8] https://support.mozilla.org/es/kb/cookies-informacion-que-los-sitios-web-guardan-en-

[9] https://support.google.com/chrome/answer/95647?hl=es

[10] http://windows.microsoft.com/es-es/windows7/how-to-manage-cookies-in-internet-explorer-9

CRITERIO	MECANISMO: VENTAJA
Pago seguro	Pasarela de pago: la plataforma no accede a, ni almacena, datos del pago Protocolo SSL: comunicación web segura, autenticación con certificados
Garantía de la información	Autenticación: no suplantación Seguridad de los servidores y de las bases de datos: evita los accesos no autorizados Validación: minimiza errores
Identificación (autenticación)	Usuarios registrados: identificación de los usuarios Certificados digitales: identificación de los servidores y de las pasarelas de pago
Integridad de la información	Firma digital: sólo el poseedor de la clave privada asociada puede firmar con su identidad Resumen o huella digital: si el documento ha sido modificado no se obtendrá la misma huella Encriptación: es necesario conocer la clave de encriptación

Tabla 2. Aspectos de seguridad, mecanismos para satisfacerlos y ventajas que proporcionan.

3. Certificados digitales

Un certificado digital es un documento, esto es, un archivo, que permite autenticarse. Un certificado está firmado digitalmente por una Autoridad de Certificación (AC) –una autoridad de certificación cumple una función equivalente a un notario: certifica con su firma que los datos que figuran en el documento que firma son ciertos--. En el certificado se vinculan los datos que identifican al propietario con su firma, de modo que también puede utilizarse para comprobar los documentos firmados por el propietario del certificado. Cuando un navegador web se conecta con un servidor web, éste último le envía su certificado para autenticarse. Opcionalmente también puede pedir al navegador web que envíe el suyo (éste sería el caso si los usuarios utilizan certificados para identificarse, como pueden ser los asociados al DNI electrónico).

Un certificado contiene los datos de identidad del propietario (nombre, otros), su período de validez (cuándo se emitió y hasta cuándo es válido), los datos de la autoridad de certificación que emite el certificado y su firma, y la clave pública del propietario, que es la que utilizará un software para comprobar su firma. Contiene además otros datos necesarios para el software que lo manipula, como algoritmo de firma utilizado, etc. La figura 3 corresponde a la visualización de los datos de uno de estos certificados en el navegador Firefox.

La confianza en un certificado reposa en la confianza en la entidad que lo emite (la autoridad de certificación). Esta confianza se garantiza comprobando la firma de la autoridad de certificación. Para ello el navegador web utilizará el certificado de la autoridad de certificación. Pero, ¿de dónde obtiene el navegador este certificado? En el caso de las más conocidas estos certificados vienen instalados por defecto en los navegadores, de modo que cuando se instala el navegador también se están obteniendo (aunque no se sea consciente de ello) los certificados de estas agencias. Cuando se trata de una autoridad de certificación menos conocida, cuyo certificado no se distribuye por defecto con los navegadores web, es posible "instalarlo", para que en el futuro esté disponible.

4. El protocolo SSL

El protocolo *Secure Socket Layer (SSL)* regula las comunicaciones seguras entre servidores web y clientes web (un cliente web es un navegador web). Este protocolo es el más utilizado actualmente en la web y, por consiguiente, el utilizado por las plataformas web. Cuando entra en funcionamiento suele reconocerse por dos signos: 1) la URL pasa a empezar por *https* en vez de *http*; 2) el navegador muestra en algún sitio de la ventana un candado, una llave, u otro icono que se asocia a seguridad. La figura 4 muestra una de estas ventanas.

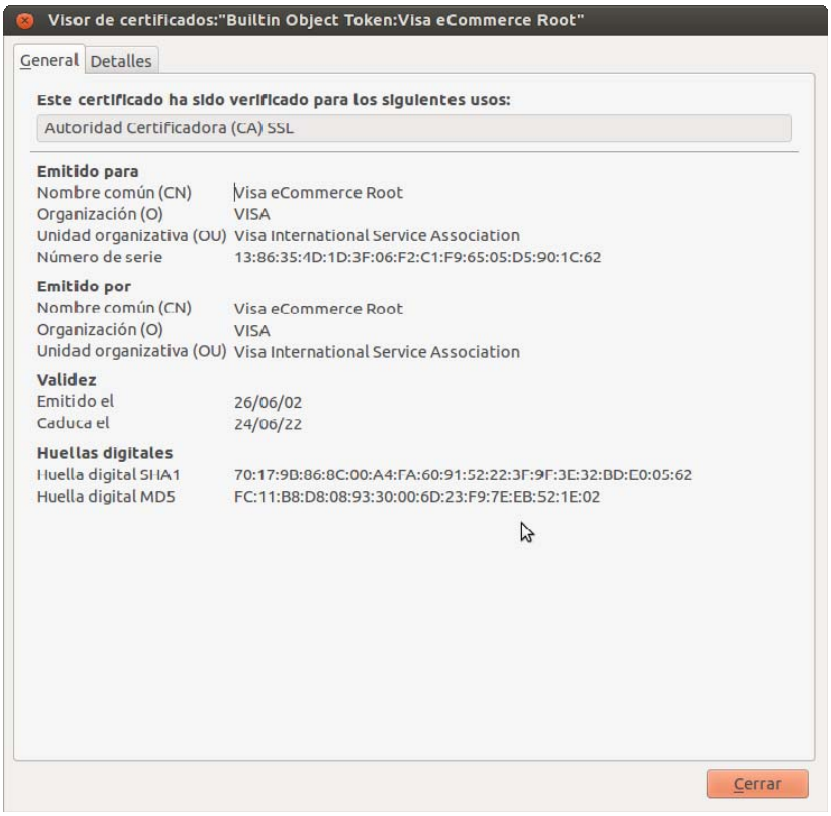

Figura 3. Visualización de los datos de un certificado digital en Firefox.

Figura 4. Uso del protocolo SSL en un navegador web.

Su funcionamiento se organiza en dos fases: una primera fase, de autenticación, y una segunda, en la que se intercambia la información. En la primera fase el servidor web se autentica (lo cual, como se ha visto al hablar de certificados, hace enviando su certificado). Opcionalmente puede autenticarse también el cliente, si bien esto no es lo habitual en procesos de pago –ocurre así, por ejemplo, en procesos de administración electrónica en los cuales es importante asegurarse de que el usuario que usa el servicio web es la persona jurídica cuya identidad se está asociando a los trámites--. Una vez se ha terminado la autenticación satisfactoriamente se negocian los algoritmos de encriptación, y las claves, que se utilizarán en la segunda fase. Esta negociación ocurre entre el servidor web y el navegador web, y es aquí donde uno de ellos propone al otro el uso de uno u otro algoritmo de encriptación; por eso qué algoritmos de encriptación soporta una plataforma es importante, ya que cuanto más seguros sean éstos más segura será la interacción con ella.

En la segunda fase se produce el intercambio de información. Si se trata de un pago, la información que se intercambia son los datos necesarios para realizarlo. Si se trata de otra información, como datos privados o confidenciales que se deban rellenar en algún formulario, otros, serán estos mensajes. Para los efectos del protocolo todos ellos son mensajes que se intercambian entre el servidor web y el navegador web, y que se encriptarán utilizando el algoritmo de encriptación y la clave que se han negociado en la fase anterior. El emisor (cliente o servidor) los encripta utilizando el software adecuado y el receptor los desencripta utilizando también el software adecuado. Sólo quienes disponen de la clave de sesión que han negociado en la fase anterior (deberían ser únicamente ellos) podrán desencriptar estos mensajes.

IV. OTRAS CONSIDERACIONES

Además de los relacionados con el acceso a la información y la seguridad existen otros aspectos que se pueden considerar a la hora de seleccionar una plataforma de mercado electrónico. Se mencionan cuatro categorías que resumen algunas de estas cuestiones.

A) Facilidad de uso

La facilidad de uso de una herramienta es importante para sus usuarios. Además de lo sencillo que resulte hacer búsquedas de información o navegar por ella, se pueden plantear algunas cuestiones adiciones. En primer lugar, la facilidad para darse de alta en el mercado. ¿Qué hay que hacer para empezar a usarlo, hay que darse de alta como usuario en una web, hay que instalar algún software adicional, es necesario que la plataforma acceda a algún dato de los propios servidores? En general este proceso suele facilitarse con mecanismos sencillos, como rellenar formularios web, ya que una dificultad en esta etapa puede suponer el rechazo definitivo de un potencial usuario.

En segundo lugar se plantea qué capacidades tecnológicas son necesarias para usar la plataforma. Aquí es necesario tener en cuenta que, en función del perfil de los destinatarios del mercado electrónico, se adaptará la interacción de la plataforma con sus usuarios. Por un lado, usuarios con habilidades de búsqueda y buen conocimiento de los vocabularios del sector, podrán utilizar con mayor ventaja las posibilidades de búsquedas por metadatos usando estos vocabularios. Por otro lado, se procurará facilitar una inserción sencilla de información, o se podrá requerir la utilización de software adicional para hacerlo (esto es más fácil cuando los usuarios son empresas que disponen de personal con habilidades tecnológicas que puede asistir en estas tareas).

B) Integración de información

En relación con la inserción de información en una plataforma debe tenerse en cuenta que en muchos casos la información que una empresa desea ofrecer ya está almacenada en sus propios sistemas de información. Se plantea pues la posibilidad de importar esta información desde sus propios sistemas a los de la plataforma. Para ello se usan las herramientas ETL que se comentaron en la sección I.2. Estas herramientas sirven para extraer la información necesaria de las bases de datos locales, transformarla y normalizarla para que se adapte a los esquemas y formatos que se usan en la plataforma. Una vez se ha conseguido, se procede a su inserción.

Cuestiones que es posible plantearse en estos supuestos son si debe asumirse el desarrollo de estas herramientas o si la plataforma facilita herramientas para ello (aunque no cubran la totalidad de la tarea). Es normal que haya que asumir una parte de esta tarea, ya que los esquemas locales son específicos de cada usuario y estas herramientas deben trabajar sobre ellos, además de acceder a las propias bases de datos.

No obstante, esta tarea se ve facilitada cuando en el destino se usan formatos, esquemas y vocabularios bien conocidos, y cuando se facilita el uso de herramientas de construcción de filtros diseñadas expresamente para facilitar esta tarea –en (Doan, Alon y Zachari, 2012) pueden encontrase referencias a estas herramientas--.

C) Características de red social

Las características de red social son una de las cuestiones pendientes en los mercados electrónicos en la cual se esperan importantes desarrollos en un futuro próximo (Holland, Diehl y Herrmann, 2013). El uso de correos, chats, foros, la publicidad personalizada, la capacidad para gestionar foros públicos o abiertos y foros privados donde sólo los usuarios autorizados por el moderador pueden acceder, y en definitiva, la posibilidad de adaptar todos los avances que se introducen en las redes sociales al supuesto de los mercados electrónicos se está produciendo ya (algunas plataformas acogen foros y otras herramientas de red social para sus usuarios), pero es claro que aún quedan muchos avances por llegar que se producirán en los próximos años.

D) Geolocalización

La geolocalización ha adquirido protagonismo con la expansión de dispositivos móviles dotados de GPS. Su integración con sistemas de búsqueda y sistemas de información para complementar las búsquedas, permitiendo filtrar los resultados en función del área geógrafica en la que se encuentran, es ya una realidad. Desde soluciones sofisticadas basadas en la posición actual del usuario hasta soluciones más sencillas, pero no por ello menos útiles, como la selección manual de un área geógrafica (por provincia, municipio, código postal...) se pueden encontrar disponibles. También se utiliza la posición geográfica del usuario para adaptarle la publicidad, u ofrecerle información que se estima le puede resultar de interés.

V. CONCLUSIONES

La selección de un mercado electrónico, y por consiguiente de una plataforma de mercado electrónico, está condicionada por múltiples factores, de los cuales sólo algunos tienen que ver con las capacidades tecnológicas. En este capítulo se han abordado estos últimos. Se han presentado de forma sencilla, adaptada al perfil de los destinatarios del libro en que se inserta, procurando no entrar en consideraciones técnicas complejas que requieran conocimientos técnicos para comprenderlas.

La presentación se ha organizado en tres grandes categorías: acceso a la información, seguridad y otros. En todos ellos se verán avances en el futuro próximo, que vendrán determinados por dos cuestiones. En primer lugar, por los propios avances tecnológicos en cada uno de esos campos, que se irán trasladando, como es lógico, al supuesto de los mercados electrónicos. En segundo lugar, por los cambios en los modelos de funcionamiento de estos mercados, que son los que en rigor condicionan qué capacidades tecnológicas se requieren para satisfacerlos.

REFERENCIAS

Baeza-Yates, Ricardo; Ribeiro-Neto. Berthier (2011). "Modern Information Retrieval. The concepts and technology behind search". 2ª edición. Addison Wesley. 2011.

Connolly, Thomas; Begg, Carolyn; Holowczak, Richard (2008). "Business Database Systems". Pearson. 2008.

Croft, W. Bruce; Metzler, Donald; Strohman, Trevor (2010). "Search Engines. Information Retrieval in practice". Pearson. 2010.

Diffie, W.; Hellman, M.E. (1976) New Directions in Cryptography. // IEEE Transactions on Information Theory. IT-22. 644-654.

Doan, Anhai; Halevy, Alon; Ives, Zachary (2012). "Principles of Data Integration". Morgan Kaufmann. 2012.

Federal Information Processing Standard. (1995). Secure Hash Standard. FIPS Publication 180-1. Disponible en http://wwww.itl.nist.gov/fipspubs/fip180-1.htm.

Garfinkel, Simson; Spafford, Gene. (2002). Web Security, Privacy & Commerce. 2ª edición. O'Reilly. 2002.

Hegarty, Tony; Verheul, Eric; Steuperaert, Dick; Skouma, Georgia. (2003). Study on the Security of Payment Products and Systems in the 15 Member States. Contract No. ETD/2002/B5-3001/C/11. Internal Market DG. Final Report. Disponible en http://www.europa.eu.int/comm/internal_market/payments/fraud/index_en.htm

Holland, Christopher P.; Diehl, Kristin; Herrmann, Andreas (2013). Introduction to the special theme on "Internet marketing" and General Research// Electronic Markets (2013) 23:3, 175-176. DOI 10.1007/s12525-013-0139-1.

Kessler, C. (2010). "Context-aware Semantics-based Information Retrieval (Dissertations in Geographic Information Science)". IOS Press. 2010.

López San Miguel, Alberto (2004). Los mercados electrónicos: un nuevo canal para la internacionalización de la empresa. // Información comercial española, ICE. Revista de economía. ISSN 0019-977X. 813 (Febrero 2004) 115-140.

Manning, Christopher D.; Raghavan, Prabhakar; Schütze, Hinrich (2008). "Introduction to Information Retrieval". Cambridge University Press. 2008.

Martínez-González, M. Mercedes (2009). "Mecanismos de seguridad en el pago electrónico". En Mata y Martín, R y Javato Martín, A. M. (2009). *Los medios electrónicos de pago: Problemas jurídicos.* Editorial Comares. pp. 5-65.

Martínez-González, M. Mercedes (2014). Informática jurídica para estudiantes de Derecho. Introducción a los sistemas de información y seguridad. TECNOS. 2014.

Wichmann, Thorsten. Mercados electrónicos y directorios online – Manual para pequeñas empresas. Accesible en http://www.pymesonline.com/noticias/articulos-y-documentos/detalle/po/mercados-electronicos-y-directorios-online-manual-para-pequenas-empresas/poac/show/Content/ (último acceso: 4 de marzo de 2014)

Yu, Liyang (2011). A Developer's Guide to the Semantic Web. Springer. 2011.