Arquitecturas de comercio electrónico

Josep Lluís Ferrer Gomila
Llorenç Huguet Rotger
M. Magdalena Payeras Capellà

PID_00199786

Universitat Oberta de Catalunya

Índice

Introducción

La generalización del comercio electrónico ha supuesto una revolución en la manera de llevar a cabo las transacciones comerciales, sobre todo desde el momento en el que todas las etapas de determinadas operaciones se pueden efectuar a distancia. La compra, la contratación y el pago son algunas de las operaciones que se pueden realizar electrónicamente gracias a la aparición de protocolos que implementan la versión electrónica de los servicios comerciales tradicionales. Las primeras relaciones de los usuarios consumidores con el comercio electrónico se limitaban a la obtención de información y a la selección de productos, únicas etapas de la cadena comercial que un usuario estaba dispuesto a realizar electrónicamente, puede ser porque estas etapas se caracterizan por el anonimato del usuario y la ausencia de datos personales o bancarios. De manera general, los usuarios no se muestran dispuestos a continuar el proceso si el servicio no ofrece garantías de seguridad y de protección del consumidor. Actualmente, todas las etapas comerciales se pueden realizar electrónicamente, incluso la contratación y el pago, utilizando protocolos que satisfacen conjuntos importantes de propiedades deseables. Algunas de estas propiedades derivan de las propiedades de los servicios análogos del mundo físico, mientras que otras provienen de las características propias del mundo electrónico. Algunas propuestas se descartan por su falta de seguridad, privacidad o viabilidad.

En este primer capítulo de la asignatura de *Comercio electrónico* se enumerarán los modelos de negocio habituales en las arquitecturas de comercio electrónico. Estos modelos de negocio serán el punto de partida de las aplicaciones que requieren protocolos seguros y que se irán describiendo en los diferentes módulos de la asignatura. En el segundo apartado se describirán las bases de seguridad utilizadas en el comercio electrónico y en la tercera se hará un repaso de la situación actual, partiendo de datos y cifras relativas al comercio electrónico.

1. Arquitecturas, actores y modelos de negocio

En este primer capítulo de la asignatura de *Comercio electrónico* definiremos el término *comercio electrónico* basándonos en la descripción de los actores y los modelos de negocio.

La definición de comercio electrónico engloba la compartición de información comercial, el mantenimiento de relaciones comerciales y la ejecución de transacciones comerciales mediante ordenadores u otros dispositivos conectados a redes de telecomunicaciones.

Dentro de las relaciones comerciales englobadas en el comercio electrónico se pueden identificar diferentes tipos de actores, los consumidores, a los que denominaremos C, las entidades comerciales, B, y la Administración, A. En función de cuáles sean los actores involucrados en una transacción comercial aparecen los modelos clasificados como *business to business, B2B*, *business to costumer, B2C*, *costumer to costumer, C2C* o *costumer to administration, B2A*.

Durante los últimos años se ha podido constatar un aumento en el interés por los sistemas distribuidos que involucran relaciones comerciales. Existe un número elevado de modelos que las empresas pueden adoptar a la hora de establecer sus comercios virtuales. Probablemente el modelo más conocido es aquel en el que el comerciante pone a la venta determinados productos, ya sean productos que requerirán un envío físico o productos digitales que se pueden ofrecer a través de la red.

Los modelos de negocio han sido utilizados para crear aplicaciones en Internet. Un modelo de negocio es una descripción de alto nivel de un tipo de aplicación que contiene las características comunes que se pueden encontrar en ejemplos específicos del modelo. A continuación se enuncian otros modelos de negocio propios del comercio electrónico:

- **Tienda electrónica**. Es la forma más habitual de establecimiento comercial en la Red. Se basa en una empresa que presenta un catálogo de productos a sus clientes potenciales a través de Internet, proporcionando mecanismos para facilitar que los consumidores puedan adquirir sus productos. Por tanto, estos establecimientos deberán incluir un mecanismo para permitir la realización de la solicitud y el pago de los productos. Los sistemas de pago habitualmente son varios, desde pagos de tipo tradicional, como el pago contra reembolso, hasta pagos basados en tarjeta de crédito o sistemas de pago totalmente específicos de las compras electrónicas. En esta asignatura

se describirán ampliamente los sistemas de pago electrónicos que mejor se adaptan al comercio electrónico y que satisfacen los requisitos de seguridad y privacidad.

La sofisticación de estos establecimientos varía desde una presentación simple de un catálogo estático a catálogos interactivos con contenidos multimedia y mantenimiento de espacio para incluir los comentarios de los clientes. El modelo de tienda electrónica proporciona una presencia global, una manera barata de presentar los productos a la audiencia y reducir los costes de promoción y marketing.

- **Subastas en línea**. Se trata de sitios donde se subastan objetos aceptando las licitaciones de los usuarios dentro de un periodo. Dependiendo del sistema utilizado se puede permitir la participación anónima de los usuarios. Solo el usuario que haya conseguido el objeto subastado será identificado. La empresa en línea obtiene beneficios cobrando comisión a todas las partes participantes o a algún subconjunto de estas.

- **Centros comerciales**. Un centro comercial es una colección de tiendas electrónicas normalmente relacionadas con un mismo servicio o producto. Habitualmente los centros comerciales son gestionados por una empresa, que cobra a las tiendas por el hecho de administrar su presencia: mantenimiento de la página web, marketing y gestión de transacciones y pagos.

- **Portales**. Un portal es una página web que contiene catálogos y gestiona grandes volúmenes de información. Por el hecho de contener un gran número de enlaces estas páginas representan un lugar de entrada a la Red. Los portales pueden ser horizontales o verticales. Un portal vertical ofrece la entrada a un conjunto de información relacionada con un mismo tema. Un portal horizontal proporciona información sobre un área grande. Se pueden incluir enlaces a los establecimientos que venden productos o servicios. El portal puede cobrar por visita realizada al establecimiento electrónico o puede recibir una tarifa por incluir el establecimiento en el portal.

- **Ajuste dinámico de precios**. En determinadas implementaciones se permite hacer el ajuste dinámico de precios. El precio se convierten en una variable abierta a negociación. En algunos casos el precio lo propone un cliente individual; la propuesta se valora y se decide la posible aceptación. En otros casos se requiere el agrupamiento de los clientes para negociar un precio conjunto. Su éxito vendrá determinado tanto por el precio solicitado como por el número de usuarios interesados.

- **Proveimiento electrónico**. Es el término utilizado para describir la licitación de bienes y servicios. Si una empresa decide que requiere algunos productos para llevar a cabo la compra, primero debe anunciar públicamente sus necesidades e invitar a un número de empresas a presentar ofertas para el negocio.

Existe un número de ventajas en la realización del proceso de contratación electrónica. Para los proveedores significa que a menudo hay más oportunidades de licitación y que se reduce el coste de presentación de ofertas de licitación y de colaboración con otras empresas. Para las ofertas de la empresa anunciadora hay una reducción importante en los costes.

- **Comunidades virtuales**. Una comunidad virtual es una página web que vende algún producto o servicio. En este sentido, no hay diferencia con una tienda electrónica. La característica que distingue una comunidad virtual es que el operador de la página web facilita que los clientes de un producto o un servicio interactúen entre sí, por ejemplo, indicando maneras de mejorar un producto. Las tecnologías utilizadas para esta interacción incluyen listas de correo, tablones de anuncios y listas de preguntas frecuentes. El objetivo de las comunidades virtuales es fidelizar a los clientes y permitir a la empresa que gestiona la página web recibir una gran cantidad de comentarios sobre el producto o servicio que vende. Los clientes se sienten atraídos por las empresas asociadas a las comunidades virtuales. Una empresa puede obtener beneficios de las comunidades virtuales de numerosas maneras: se puede cobrar por la participación en la comunidad o se puede beneficiar de mayores ventas a clientes atraídos por la base de conocimientos en poder de la empresa y de la reducción de costes de soporte.

- **Suministro de información**. Las páginas web descritas en este modelo de negocio ofrecen acceso a información, en general información empresarial. Por ejemplo, una página web que ofrece los resultados de encuestas de satisfacción del cliente para un producto podría ser utilizada por las empresas que ofrezcan este producto, así como por organizaciones de consumidores. Las empresas que encajan en este modelo suelen obtener ingresos por suscripción o mediante un cargo por cada transacción de información.

- **Suministro de confianza**. En este módulo se tratarán varias aplicaciones seguras de comercio electrónico que requerirán la intervención de terceras partes que proporcionen confianza a las distintas partes involucradas.

  Este modelo de negocio describe aquellas empresas u organizaciones que prestan algún servicio relacionado con la seguridad o la confianza. Un ejemplo de las funciones de los suministradores de confianza es la función de certificación de que una página web asociada a una empresa es, realmente, el sitio de esta compañía.

- **Productos y servicios gratuitos**. Puede parecer paradójico incluir los productos o servicios gratuitos en la categoría de modelos de negocio. Estas páginas no ingresan nada por los productos o servicios que ofrecen; obtienen los ingresos indirectamente, por ejemplo a través de publicidad o mediante la recepción de los ingresos procedentes de las páginas que hay que visitar antes de poder acceder al servicio o producto.

2. Bases de seguridad para el comercio electrónico

Para desarrollar un sistema de comercio electrónico seguro son necesarios servicios de seguridad avanzados, como veremos en esta asignatura. Pero también son servicios de seguridad que han sido objeto de otras asignaturas, e incluso forman parte de los conocimientos básicos necesarios para poder cursar este máster.

En general, se supone que nos enfrentamos a dos posibles tipos de atacantes: pasivos y activos. Los atacantes pasivos son los que pueden tener acceso a la información intercambiada entre un remitente y un destinatario, pero no la pueden manipular. Por el contrario, el atacante activo, además de tener acceso al contenido de la información, también la puede manipular: modificar, introducir nueva información, etc.

Los servicios de seguridad generalmente previstos son los siguientes: confidencialidad, integridad, autenticidad, no-rechazo y disponibilidad. El último servicio de seguridad, muy vinculado a los ataques de denegación de servicio (DoS, *denial of service*), no los repasaremos aquí, dado que las técnicas para protegernos de ellos no suelen basarse en técnicas criptográficas.

El servicio de confidencialidad tiene por objeto proteger las comunicaciones ante escuchas no autorizadas, es decir, que solo los extremos autorizados de la comunicación pueden tener acceso al contenido de la información. Proteger la información cuando esté en tránsito no significa garantizar al cien por cien la confidencialidad de la información intercambiada. Los ataques de análisis de tránsito permiten recuperar una información determinada del intercambio sin necesidad de acceder al contenido de la información. Por ejemplo, podemos deducir que dos empresas están negociando algún tipo de contracto, fusión, etc. del hecho de que intercambian un elevado número de correos en un periodo de tiempo de manera anómala. Pese a no tener acceso al contenido de los correos, podemos deducir información simplemente observando los extremos de la comunicación.

El objetivo del servicio de integridad es que el destinatario de una información podrá determinar si la información ha sido manipulada mientras estaba en tránsito. Observad que el objetivo fijado no es que no se pueda manipular la información, que sería deseable pero generaría un coste muy elevado (incluso rozaría lo imposible), sino que no sea dada por buena una información que no es exactamente la que envió el remitente. Una vez detectada la manipulación (que la información no es íntegra), el destinatario debería des-

cartar esta información y, de manera opcional, solicitar de ella (implícita o explícitamente) la retransmisión.

El servicio de autenticidad tiene por objeto que los extremos de una comunicación puedan verificar que están dialogando con quien creen estar dialogando, es decir, que no se produce una impersonación. De nuevo, la definición no pretende hacer que sea imposible esta impersonación, sino que se pueda detectar para poder actuar una vez detectada.

Finalmente, tenemos el servicio de no-rechazo, que de manera genérica tiene por objetivo no permitir que una entidad que ha participado en una comunicación lo pueda negar *a posteriori*. El servicio de no-rechazo se puede clasificar en diferentes subtipos, los más importantes de los cuales son el no-rechazo en origen y el no-rechazo en destino. El primero no permite negar al remitente de un mensaje haberlo enviado, y el segundo no permitirá al destinatario de un mensaje haberlo recibido. El segundo servicio será objeto de un tema de esta asignatura.

Hay que remarcar que si logramos proporcionar el servicio de no-rechazo en origen estamos proporcionando también los servicios de integridad y autenticidad. Si una entidad no puede negar haber emitido un mensaje determinado, significa que este mensaje no ha sido manipulado (integridad) y que sabemos quién ha sido el originador (autenticidad). En caso contrario, si el mensaje hubiese podido ser manipulado, o hubiese dudas sobre el origen del mensaje, el emisor del mensaje podría (y con motivo) negar haber generado este mensaje. Veremos que lo contrario no es cierto, es decir, que si conseguimos los servicios de integridad y autenticidad no necesariamente cubrimos el servicio de no-rechazo en origen.

Mecanismos

Repasaremos brevemente los mecanismos utilizados para conseguir los servicios definidos anteriormente. Se trata de la criptografía de clave secreta, la criptografía de clave pública (con la infraestructura de clave pública que normalmente implica) y las funciones resumen (o funciones *hash*).

La criptografía de clave secreta consiste en la aplicación de algoritmos sobre la información que queremos proteger utilizando una clave secreta que debe ser compartida entre el remitente y el destinatario de la información. El remitente lleva a cabo la operación de encriptación con la clave k sobre el mensaje M y obtiene un criptograma C:

$$C = E_k(M)$$

El destinatario debe realizar la operación de desencriptación con la misma clave para recuperar el mensaje original:

$$D_k(C) = M$$

Con este tipo de criptografía claramente obtenemos el servicio de confidencialidad, teniendo en cuenta que solo quien conoce la clave secreta (remitente y destinatario) puede realizar las operaciones de encriptación y desencriptación. Los algoritmos de encriptación y desencriptación pueden ser (y en realidad deben ser) conocidos por toda la comunidad, ya que el único requisito que pedimos es que sean seguros (que no tengan debilidades).

No es tan obvio, pero bien utilizados (si introducimos códigos de redundancia) también obtenemos los servicios de integridad y autenticidad. Un espia puede manipular la información mientras esté en tránsito, pero dado que desconoce la clave utilizada no puede producir una información encriptada (la que circula por el canal de comunicaciones) que sea dada por buena por el destinatario. Por tanto, obtenemos el servicio de integridad. Por otro lado, solo remitente y destinatario pueden realizar las operaciones de encriptación con la clave secreta *k* (solo ellos dos la conocen). Si el destinatario recibe una información encriptada correctamente con la clave secreta *k*, sabe que esta información debe proceder del remitente. Por tanto, obtenemos el servicio de autenticidad.

Aun habiendo obtenido los servicios de integridad y autenticidad, no hemos obtenido el servicio de no-rechazo en origen. Esta aparente contradicción se resuelve pensando que el servicio de no-rechazo se invoca ante terceros, es decir, con el servicio de no-rechazo en origen queremos convencer a terceros de que el remitente ha enviado un determinado mensaje. Mediante la criptografía de clave secreta no lo podemos conseguir, ya que el remitente siempre podrá negar haber enviado un mensaje, y aunque el destinatario disponga de un mensaje encriptado con la clave secreta *k* y esté seguro de que la ha enviado el remitente, este podrá alegar que la encriptación ha sido llevada a cabo por el destinatario porque también conoce el algoritmo y la clave secreta *k*.

La criptografía de clave secreta, además de no proporcionar no-rechazo en origen, nos plantea un segundo problema, que es el de la distribución de claves. Hemos indicado que el remitente y el destinatario deben compartir una clave secreta *k*, pero la cuestión es cómo comparten esta clave secreta. Además, para dotar de mayor seguridad al sistema, esta clave se debe cambiar periódicamente (cada sesión, cada mensaje, etc.).

Para resolver los dos problemas surge la criptografía de clave pública, en la que cada usuario dispone de un par de claves. Una de las claves se emplea para llevar a cabo las operaciones de encriptación y desencriptación. Una de las claves debe ser conocida por los interlocutores del propietario del par de claves, que denominaremos clave pública, y la otra solo debe ser conocida por el propietario del par de claves, que denominaremos clave privada. Para simplificar la explicación, supondremos que se pueden utilizar en cualquier orden (como es el caso del algoritmo de encriptación asimétrica RSA).

De esta manera, si un remitente quiere enviar una información confidencial a un destinatario, debe cifrar el mensaje M con la clave pública del destinario PU_B:

$$C = PU_B(M)$$

Solo quien conozca el par de la clave pública utilizada podrá llevar a cabo la operación de desencriptación (continuemos suponiendo que los algoritmos son públicos y seguros). En este caso solo el destinatario conoce la clave secreta PR_B, con la que puede realizar la operación de desencriptación:

$$PR_B(C) = M$$

De esta manera hemos conseguido proporcionar el servicio de confidencialidad, ya que solo el destinatario puede recuperar el mensaje M enviado por el remitente. Observad, sin embargo, que no se proporciona el servicio de integridad y el de autenticidad, ya que cualquier espía que conozca la clave pública del destinatario puede producir un criptograma C', que será dado por bueno. De hecho, la criptografía asimétrica o de clave pública no se suele emplear para el servicio de confidencialidad (porque es muy costosa computacionalmente), pero la podremos utilizar para resolver uno de los dos problemas que teníamos planteados: el intercambio de claves de criptografía simétrica. Si cambiamos el mensaje genérico M del ejemplo anterior por una clave secreta k, ya disponemos del mecanismo para que remitente y destinatario puedan intercambiar tantas claves secretas como quieran:

$$K = PU_B(k)$$
$$PR_B(K) = k$$

Quedaría por resolver el problema de cómo conoce de manera segura la clave pública del destinatario el remitente de la información. La respuesta es lo que se conoce con el nombre de *certificados de clave pública*.

Aunque hemos resuelto el problema de distribución de claves de la criptografía simétrica, y conseguimos el servicio de confidencialidad con la criptografía asimétrica, parece que conseguimos menos servicios de los que ya teníamos con la criptografía anterior. Pero veamos cómo la criptografía de clave pública nos permite conseguir el servicio de no-rechazo en origen. Para hacerlo, en lugar de utilizar la clave pública del destinatario, haremos una encriptación con la clave privada del remitente sobre el mensaje M:

$$C = PR_A(M)$$

El destinatario (y, de hecho, cualquier usuario que conozca la clave pública del remitente) puede llevar a cabo la operación de desencriptación:

$$PU_A(C) = M$$

Y si el resultado de esta operación es adecuado, significa que el mensaje procede del remitente, y además no lo podrá negar *a posteriori*, ya que es el único usuario que conoce la clave privada PR_A que permite hacer la operación de encriptación. Por tanto, conseguimos el servicio de no-rechazo en origen (recordemos que también conseguimos el de integridad y el de autenticidad), y por ello este uso de la criptografía asimétrica se suele denominar *servicio de firma digital* (porque permite cumplir funciones análogas a la firma manuscrita).

Si combinamos los dos posibles usos de la criptografía asimétrica, vemos que podemos conseguir los cuatro servicios de seguridad que queríamos proporcionar a los usuarios del sistema.

Otra vez queda por resolver cómo sabe el destinatario de manera segura si PU_A es la clave pública de A o si es de un impostor. Hemos comentado que la solución son los certificados de clave pública, es decir, unos documentos electrónicos firmados digitalmente por una entidad, denominada *autoridad de certificación*, que acredita que un determinado usuario es el propietario de una determinada clave pública (y por tanto de su par, la clave privada correspondiente).

Ya hemos indicado que la criptografía de clave pública es muy costosa computacionalmente, y por este motivo no se suele utilizar para cifrar los mensajes y conseguir el servicio de confidencialidad. Por esta razón, no sería eficiente tener que cifrar todo el mensaje para conseguir el servicio de no-rechazo en origen y se emplean las funciones resumen (o funciones *hash*, del inglés). Las funciones *hash* son funciones unidireccionales que realizan un resumen de medida fija de un mensaje de medida arbitraria:

$$h = H(M)$$

La condición que se impone a estas funciones para que sean útiles es que sea computacionalmente imposible encontrar dos mensajes que produzcan el mismo resumen, pero que sea computacionalmente poco costoso hacer una operación de resumen.

Con la introducción de estas funciones *hash*, las operaciones que se deben realizar para conseguir el servicio de no-rechazo en origen cambiarán. Ahora el primer paso que debe hacer el remitente es un resumen de la información que debe proteger, y sobre este resumen se realiza la operación de encriptación con su clave privada:

$$f = PR_A[H(M)]$$

Ahora el remitente debe transmitir el mensaje M y la firma f para que el destinario pueda verificar la corrección de la firma digital realizada por el remitente. Por un lado, el destinatario volverá a realizar un resumen del mensaje recibido:

$$H(M) = h'$$

Y por otro, descifrará la firma recibida con la clave pública del remitente:

$$PU_A(f) = PU_A[PR_A[H(M)]] = H(M) = h$$

Si los dos resúmenes coinciden, significa que la firma digital es correcta. Si difieren en uno o más bits, significa que el mensaje o la firma, o ambos, han sido manipulados mientras estaban en tránsito, o en cualquier caso, que la firma no es correcta y que, por tanto, no se podrá imputar este mensaje al remitente que supuestamente lo ha enviado.

El carácter unidireccional de las funciones *hash*, además de servir para las firmas digitales, es útil para las aplicaciones que requieren servicios de seguridad.

Para acabar este breve repaso de conceptos básicos de seguridad, pondremos un ejemplo de uso combinado de criptografía simétrica y asimétrica para los cuatro servicios de seguridad planteados. Supongamos una versión simplificada de certificado de clave pública:

$$Cert_A = A,PU_A,PR_T[H(A,PU_A)]$$

Es decir, un documento electrónico firmado por una autoridad de certificación T, que vincula la clave pública PU_A con la identidad del remitente A, y con la suposición de que el destinatario de la información conoce la clave pública de T de manera segura.

El remitente quiere enviar el mensaje M de manera confidencial y con el servicio de no-rechazo en origen. Para hacerlo, enviará al destinatario la información siguiente:

$$C = E_k(M),K = PU_B(k),f = PR_A[H(M)],Cert_A$$

Ahora el destinatario debe realizar las operaciones siguientes. En primer lugar, debe recuperar la clave que se ha empleado para cifrar el mensaje, para lo que debe aplicar su clave privada sobre K:

$$PR_B(K) = k$$

Una vez que dispone de la clave utilizada por el remitente para cifrar el mensaje, puede descifrar el criptograma recibido C:

$$D_k(C) = M$$

Por otro lado, debe verificar que el certificado de clave pública del remitente es correcto, utilizando la clave pública conocida de la autoridad de certificación:

$$PU_T(PR_T[H(A,PU_A)]) = H(A,PU_A)$$

Si el resumen anterior coincide con lo que el remitente debe hacer sobre el par A y PU_A, seguro que PU_A es la clave pública del remitente A. Ahora puede verificar la firma realizada por el remitente:

$$PU_A(f) = h'$$
$$H(M) = h$$

Si los dos resúmenes coinciden, el destinatario dará por buena la firma digital realizada por el remitente y podrá verificar que se han proporcionado adecuadamente los servicios de seguridad requeridos: confidencialidad (solo él y el remitente tienen acceso al mensaje M) y no-rechazo en origen (el remitente no podrá negar haber enviado el mensaje M).

3. Datos y cifras relativas al comercio electrónico

En este apartado se reflejan algunos datos y cifras relativas al comercio electrónico en España que se han extraído de las páginas del Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información (ONTSI) y del estudio de Market Service (*El comercio electrónico en España 2011)*.

Webs de consulta

En este apartado utilizaremos datos publicados en diferentes encuestas, aunque las de referencia son las publicadas por el ONTSI, que podréis ir actualizando a través de la página web www.ontsi.red.es. También podéis consultar los estudios de Market Service, que podréis encontrar y actualizar en www.emarketservices.es. Para los datos relativos a Cataluña, podéis consultar la página web del Institut d'Estadística de Catalunya (IDESCAT): www.idescat.cat.

La evolución de los datos del comercio electrónico en los últimos años es importante y esperanzadora, tanto respecto a las ventas en línea, que crecen a buen ritmo, llegando a facturar casi 10.000 millones de euros, en el año 2011, como en el número de internautas compradores, que llega casi a los 11 millones y en el de empresas que se incorporan a la Red, que superan las 14.000.

A grandes rasgos, la radiografía de la evolución del estado del comercio electrónico en España está determinada por estos cinco indicadores que muestran su crecimiento. No obstante, la oferta española todavía puede considerarse escasa y por esta razón, como veremos más adelante, se compran más de la mitad de los bienes y servicios en línea en el exterior, mientras que es muy poco significativo lo que los extranjeros compran en España.

Comercio electrónico	2008	2009	2010	2011	Característica
Empresas: compras	20,3	24,1	23,3	22,5	% sobre el total
Empresas: ventas	11,1	13,1	12,2	14,2	% sobre el total
Particulares: compras	13,3	15,7	17,4	18,9	% sobre población total
Volumen de negocio	6.695	7.760	9.114	10.000	Millones de euros
Facturación total	9,6	11,5	11,5	13,7	% sobre el total

A pesar de estos datos, todavía deben superarse muchos retos para igualarnos a nuestros vecinos europeos, tal como marca la Agenda digital europea, que fija, entre otros, los objetivos siguientes para el año 2015:

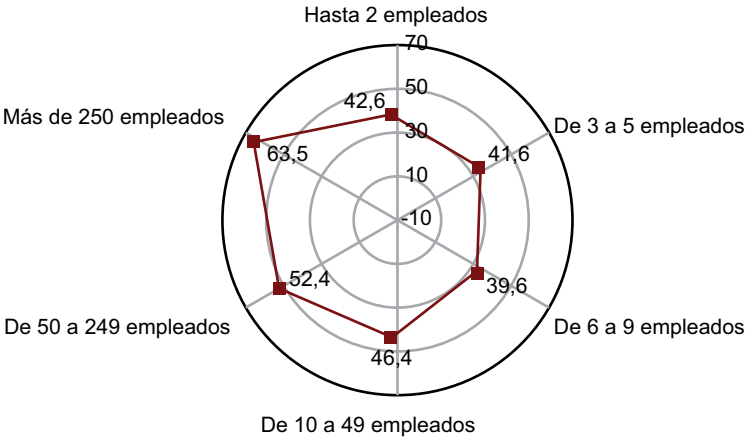
1) Comercio electrónico para las empresas: un 33% de las pymes debería efectuar compras y ventas en línea (en el año 2011, el 20% han sido compradores y un 11% vendedores).

2) Promoción del comercio electrónico: un 50% de la población debería efectuar compras en línea (en el año 2011 se ha computado un 27% de la población, mientras que en la UE-27 fue de un 47%).

3) Comercio electrónico transfronterizo: un 20% de la población debería efectuar compras transfronterizas en línea (en el año 2011 ha experimentado una disminución respecto al año 2010 y se ha computado solo un 9%).

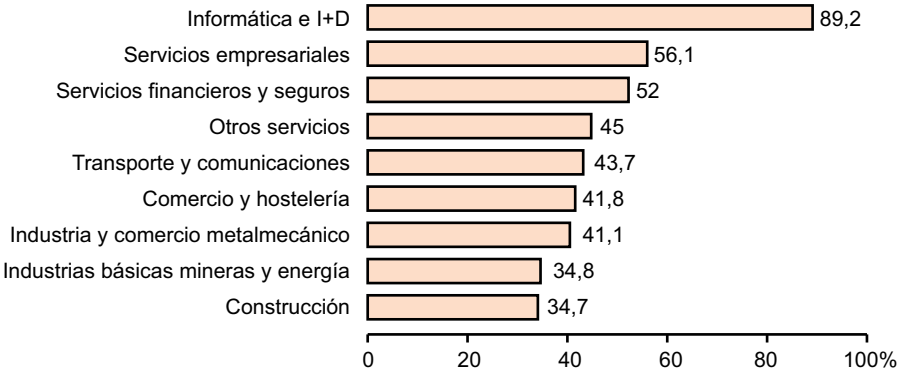
Los dos gráficos siguientes muestran, respectivamente, el porcentaje de empresas usuarias de comercio electrónico, según su extensión, y el sector de actividad al que pertenecen:

Empresas que utilizan comercio electrónico según tamaño



Fuente: AMETIC/Everis/Red.es

Empresas que utilizan comercio electrónico por sectores de actividad (Porcentaje/total de empresas)



Fuente: AMETIC/Everis/Red.es

En cualquier caso, y según la encuesta sobre el uso de las TIC y el comercio electrónico en las empresas 2010/2011 del Instituto Nacional de Estadística (INE), el 97,4% de las empresas españolas de 10 o más asalariados dispone de conexión a Internet, y de estas un 99,4% lo hacen mediante conexiones de banda ancha.

Estos datos pueden facilitar la consecución de los retos de la Agenda digital. Con vista al futuro, hay que destacar el papel que desarrollarán las redes sociales en el comercio electrónico, ya que el comprador en línea se deja influenciar por las opiniones que circulan por la Red, dándole más crédito incluso que a las especificaciones técnicas.

Por ello las empresas deberán utilizar todos los medios tecnológicos disponibles para hacer llegar al consumidor sus ofertas, teniendo en cuenta que los compradores conectados pueden ser la clave del éxito o del fracaso del producto.

3.1. B2C: Comercio electrónico entre empresas y consumidores

Como datos estadísticos, hay que destacar que más de la mitad de las investigaciones previas a la compra se realizan a través de Internet, ya sea mediante fuentes generadas por la marca, como las webs de fabricantes y tiendas, o mediante comparadores de precio o buscadores, o mediante fuentes generadas por el propio usuario, como los blogs o las propias redes sociales. Por otro lado, los productos que más se buscan a través de Internet son los relacionados con los viajes (78%) y los relacionados con la telefonía móvil (71%).

Los hombres destacan sobre las mujeres en el uso de comercio electrónico; aunque la brecha entre ambos sexos tiende a reducirse. En todos los grupos de edad va aumentando el porcentaje de personas que realizan comercio electrónico, pero quienes lo lideran son las personas del grupo de 25 a 34 años.

En el periodo 2010-2011, las transacciones de comercio electrónico desde España con el exterior supusieron un 52,4% del volumen de negocio total (7,6% de crecimiento), mientras que las transacciones desde el exterior con España supusieron un 9,2% (30,1% de crecimiento) y dentro de España han representado un 38,4% (0,8% de decrecimiento) del volumen de negocio total. De las operaciones transfronterizas, respecto a las cantidades gastadas en el comercio electrónico interior en España se ha generado un incremento del valor medio monetario de cada transacción, mientras que en el comercio electrónico exterior se ha producido una caída de este valor medio.

En cuanto a las ramas de actividad más favorables en términos de volumen de negocio, el sector turístico (que comprende transporte aéreo, las agencias de viaje, los operadores turísticos, los hoteles, los apartamentos, los campings, y el transporte terrestre de viajeros) supuso el 55,6% de los ingresos. En orden de importancia por ingresos, le siguieron la educación (10,3%) y las prendas de vestir (4,9%). La Administración pública, impuestos y seguridad social supusieron un 3%.

3.2. B2B: Comercio electrónico entre las empresas

El comercio electrónico entre empresas continúa acaparando, con gran diferencia, las ventas en Internet, con casi un 90%. Durante el 2011 estas ventas representaron el 13,7% del total de ventas efectuadas por las empresas españolas, con lo que se superó el porcentaje del año 2010, que fue del 11,5%, lo

que refleja que las empresas españolas todavía muestran ciertas debilidades a la hora de apostar por las ventas a través de Internet.

La Unión Europea y América Latina fueron las áreas geográficas que compraron más bienes de España. En particular, los países de la Unión Europea (UE-27) gastaron un total de 255,5 millones de euros a través del comercio electrónico, lo que representó un 81,9% del total. América Latina ostentó el segundo lugar por gasto total realizado por vía electrónica, con 14,8 millones de euros, un 4,7% del total.

La facturación que generan las empresas deriva principalmente de diez ramas de actividad:

Rama de actividad	% sobre el volumen total
Agencias de viajes y operadores turísticos	12,4
Transporte aéreo	12,2
Marketing directo	6,3
Transporte terrestre de viajeros	6,1
Juegos de azar y apuestas	4,9
Espectáculos artísticos, deportivos y recreativos	4,1
Software educativo	3,7
Prendas de vestir	3,5
Publicidad	3
Ordenadores y software	2,4

Respecto a las comunidades autónomas en las que más se usa el comercio electrónico, en primera posición se sitúa Cataluña, donde el 45,6% de las empresas lo utilizan. Le siguen el País Vasco, con un 44,9% y Andalucía, con un 44,3%.

Se puede afirmar que se va incrementando el comercio electrónico mediante el teléfono móvil, aunque el uso no está generalizado en las empresas; se sitúa actualmente en el 2,5%.

Respecto a los medios electrónicos de pago, un 30,1% de las empresas los utiliza, de las que un 28,5% realiza pagos a través de Internet, mientras que el 4,4% de estas ejecuta el cobro en línea. Los pagos a través de los móviles todavía son poco frecuentes: un 0,1%; por ello es importante el desarrollo de sistemas de pago en línea, ágiles y seguros, para facilitar las compras en el comercio electrónico, en especial en los micropagos.

Más de la mitad de las empresas que comercializan sus productos a través de la Red utilizan como medio de cobro electrónico giros, letras, talones o transferencias (55,8%), seguido del uso de la tarjeta de crédito o débito (43,4%). Otras alternativas, como PayPal o cobros a través del teléfono móvil, son menos utilizadas (11,6 y 1,2%, respectivamente).

Las principales webs de comercio electrónico españolas son:

web	Contenido
e-bay	El más amplio mercado de segunda mano, compraventa y subastas
El Corte Inglés	Centro comercial más visitado
Amazon	Una de las primeras compañías en vender bienes (libros)
BuyVip	Club de ventas privadas perteneciente a Amazon
Privalia	Venta privada de tipo generalista, pero focalizado en moda

Entre las razones del porqué se debe vender por Internet, encontramos en primer lugar la posibilidad de captar nuevos clientes (37,8%) y, a continuación, el hecho de que proporciona más agilidad (35,4%), la comodidad (30,7%) y la posibilidad de llegar a nuevos mercados (26,9%).

Las empresas que compran en Internet y no venden mediante esta herramienta lo hacen sobre todo por comodidad (51,5%), mientras que para un 40,9% el principal valor es la mayor agilidad en la gestión y para un 31% lo es el hecho de que los precios son mejores. Evitar desplazamientos y encontrar productos innovadores o nuevos proveedores también son mencionados por las empresas que adquieren productos a través de Internet, aunque con menor frecuencia.

Sobre el principal freno mostrado por las empresas para no usar el comercio electrónico, hay que destacar el temor a ser objeto de robos y estafas, cifra refrendada por el 61% de las entidades que aceden a Internet. También se alega, en un 26,8% de los casos, que no todos los productos son adecuados para el comercio electrónico y un 11,6% cree que necesitaría formar específicamente a su personal para este tipo de mercados.

El tema de la seguridad computacional es cada vez más importante para generar confianza en el mundo del comercio electrónico, en particular, y en Internet en general, incluyendo la nueva versión del trabajo en la nube (*cloud computing*).

No deja de ser preocupante lo que revela un estudio reciente del *Ponemon Institute*: que menos del 30% de los proveedores de servicios en la nube opina que sus servicios protegen y aseguran sustancialmente la información del cliente, pero menos del 50% de los usuarios consideran que la seguridad deba ser una prioridad.

3.3. B2A: La relación electrónica con las administraciones públicas

El informe del ONTSI (*La Sociedad en Red 2010*) señala que los particulares que han utilizado Internet para tratar con las administraciones públicas se encuentran a dos puntos porcentuales de la convergencia europea (España

39,2% y UE27 41,2%, siendo el 50% la meta de la Agenda digital europea para el 2015).

España se encuentra en novena posición en el ranquin mundial de desarrollo de la administración electrónica entre los 184 países analizados, de Naciones Unidas, en esta clasificación. Y es que a finales del 2010, el 99% de los procedimientos de alto impacto de la Administración General del Estado eran totalmente accesibles en Internet.

Un hecho de especial relevancia es que las empresas utilizan más la firma electrónica para contactar con la Administración pública (93,5%) que con proveedores y clientes (20%).

En cuanto a la relación con las empresas, continúa creciendo el porcentaje que interacciona con la Administración pública por Internet, que se sitúa, de media, en un 70,1% entre las empresas que tienen acceso a Internet. El detalle por extensión de las empresas refleja que entre las grandes y las medianas compañías no existe mucha diferencia y en ambos estratos se contabiliza más de un 90% de medianas y grandes empresas que interactúan con la Administración pública a través de Internet. En las pequeñas, aunque el contacto telemático no es tan habitual, tiene lugar casi en un 67% de los casos.

El hecho de que sean las administraciones públicas las que promueven el impulso de la sociedad de la información en España, y que también ofrecen la posibilidad de realizar gestiones administrativas, provoca que se hayan constituido en las promotoras del uso de Internet en sus relaciones. Entre las más visitadas por las empresas españolas encontramos la página de la Agencia Tributaria, en la que el 41,2% de las empresas con conexión en Internet han interaccionado, las páginas web de las comunidades autónomas (16,3%), de la Seguridad Social (13,8%) y las páginas propias de los ayuntamientos (9,4%).

En la distribución geográfica del uso del B2A, por comunidades autónomas, la Rioja se coloca en primer lugar, con un 76,1% de pymes y grandes empresas que tienen relación con la Administración a través de Internet. Después se sitúan Cataluña, Navarra, Madrid y Castilla-León, en las que se supera el 73%.

3.4. Retos y tendencias

La evolución del comercio electrónico en España está siendo desigual. Por un lado, se llegan a nuevas cifras récord de facturación y aumenta cada día el número de consumidores en línea, al mismo tiempo que aumenta la penetración de Internet entre los particulares, tanto en dispositivos fijos como móviles.

Sin embargo, el principal reto es implicar a las empresas en este canal de compraventa, en el que los objetivos más importantes son los precios competiti-

vos y la capacidad de entregar los bienes y servicios en menos de 24 horas. Alcanzar este reto supone educar a las empresas para atraer y retener a los potenciales consumidores en línea. En particular, la optimización de contenidos, tanto para buscadores como para redes sociales, y la usabilidad de las páginas de compra son todavía asignaturas pendientes para muchas empresas del sector.

En cuanto a las tendencias que se observan en el mercado, parece claro que los dispositivos móviles serán grandes aliados de las compras en línea. No solo crecen las compras a través de teléfonos móviles, sino que las tabletas comienzan a despuntar como medio para comprar en línea. De hecho los propietarios de una tableta están más ligados a las marcas minoristas, realizan más compras en línea y visitan más páginas web que los usuarios de teléfonos inteligentes. Por ello se va haciendo indispensable disponer de aplicaciones para los diferentes dispositivos móviles y abrir el abanico de posibilidades para el consumidor y ampliar así las posibles ventas.

Por otro lado, las redes sociales siguen al alza. En Twitter y Facebook comienzan a surgir soluciones de comercio electrónico y tiendas virtuales, al mismo tiempo que se van creando redes específicamente enfocadas al comercio electrónico, como Xopers.com, donde los usuarios comparten artículos y productos de venta en la Red.

La nube (*the cloud*) es otra de las tendencias que se pueden apreciar en el sector. La facilidad de implantación, la despreocupación por el almacenamiento de datos, la escalabilidad que permite y el poder acceder desde cualquier lugar hacen de estas soluciones una gran ayuda al comercio electrónico (pero hay que tener cuidado con los riesgos inherentes a la seguridad, respecto a la confidencialidad y la autenticación).

En cuanto a los mercados electrónicos, la tendencia es claramente la introducción de herramientas sociales: bien creando soluciones híbridas a caballo entre un mercado web (puntos de encuentro de empresas compradoras y/o vendedores de productos y servicios) y una red social, como www.grera.net, bien adaptando las nuevas funcionalidades que aportan al modelo tradicional, como hizo www.acambiode.com.

Como conclusión, y por cuanto hemos comentado, es interesante tomar posiciones de manera activa en estos nuevos canales y aprovechar las ventajas que ofrecen.