Departamento de Informática

PROYECTO FIN DE CARRERA
Titulación: Ingeniería Técnica en Informática de Gestión

E-COMMERCE Y PAGO SEGURO

Autor: Lidia Parrilla Ortega

Tutor: Miguel Ángel Ramos

Leganés, octubre de 2015

Título: E-COMMERCE Y PAGO SEGURO
Autor: Lidia Parrilla Ortega
Director: Miguel Ángel Ramos

EL TRIBUNAL

Presidente: Ana Isabel González-Tablas Ferreres

Vocal: Óscar Pérez Alonso

Secretario: Antonio García Carmona

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 23 de Octubre de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Me gustaría agradecer en primer lugar **a mis padres** ya que por ellos, hoy soy la persona que soy. Siempre han sido el apoyo que necesitaba para seguir adelante en los estudios, en el trabajo y en resto de momentos de mi vida. Gracias por vuestra incondicional fidelidad y por vuestra sabiduría y esfuerzo.

A **mi hermano**, por todos los momentos compartidos en el día a día. Sé que llegarás lejos.

A **mi pareja y amigos**, esas personas que forman parte de tu familia porque tú lo decides. La confianza y ánimos en los momentos duros hicieron que fuera más fácil sobrellevarlos. De los momentos buenos, ni hablamos… No os alejéis nunca.

A **mis compañeros** de estudios y trabajo. Personas extrañas al principio que se van metiendo poco a poco en tu rutina y finalmente se hacen imprescindibles. No olvidaré nunca los momentos en LATAM.

Y, por supuesto, también a **mi tutor**, Miguel Ángel Ramos, por su paciencia y dedicación. No ha sido fácil sacar adelante el proyecto dados los tiempos tan ajustados que manejábamos, pero siempre ha tenido una palabra de apoyo para continuar. Mención especial merece también su alta disponibilidad y sus siempre acertadas indicaciones.

Resumen

El objetivo de este proyecto es acercar el mundo del comercio electrónico y de los pagos electrónicos tanto a los usuarios de los mismos, como a los posibles creadores de tiendas online.

Partiendo de una introducción a la historia y evolución del e-commerce, así como a sus beneficios y posibles riesgos, se profundiza en los tipos de comercio online más importantes hoy en día y su desarrollo en España.

Por otro lado y para complementar todo comercio virtual, es importante tratar los pagos online que completan las compras electrónicas. En el documento se desarrollan los principales sistemas de pago electrónico y la seguridad de los mismos, haciendo hincapié en los protocolos implementados por las grandes marcas de tarjetas de crédito.

Relacionado con la seguridad de Internet, se ha realizado un estudio de los principales riesgos para los usuarios que realizan compras online y cuáles son los mejores métodos para evitarlos. Adicionalmente, se hace un repaso a las leyes y normativas españolas relacionadas con el e-commerce, las cuales se encargan de regular este tipo de transacciones y de fomentar la seguridad de las mismas.

Por último, se han dado una serie de pautas para todo aquel que pueda estar interesado en implementar un comercio online y se ha plasmado cuál es la realidad del comercio electrónico en el continente sudamericano.

Abstract

The aim os this proyect is to get close the world of e-commerce and electronic payments both to the users and to the potencial e-commerce developers or creators.

Starting with an introduction to the history and evolution of e-commerce, as well as its profits and possible risks, I have studied the different types of online commerce today and how these are developed in Spain.

On the other hand and supporting all virtual trades, it's very important to talk about online payments, which make electronic purchases completed. In the document, I develope the more relevant sistems of electronic payments and its security, laying emphasis on the protocols implemented by the main important credit card brands.

Related to Internet security, it has made a study of the principal risks that users take when they are shopping on the Internet and of the best practices to avoid them. Additionally, there is a review of regulations and Spanish laws related to e-commerce, which take care of regulating these kind of transactions and promote the security of them.

At the end, there is a guideline for anyone who could be interensted in implementing a virtual trading and I tried to shape the present situation of e-commerce in Latin America.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1
Introducción y objetivos

1.1 Introducción

El siguiente proyecto está basado en el análisis del comercio online y los pagos seguros que se realizan en él, tanto para los usuarios como para los posibles propietarios de un comercio virtual.

Actualmente no se pueden entender las compras y ventas de bienes o servicios sin tener en cuenta las tiendas online. Se trata de una operativa básica en Internet a la que cada vez más usuarios se están sumando y la que está generando una gran cantidad de mercado nuevo.

El proyecto, por tanto, intenta acercar a todos los usuarios al comercio electrónico, mostrando sus características y beneficios (también sus desventajas). De este modo y con una explicación de los distintos medios de pago utilizados en el comercio online, se espera acabar con ciertos tabúes que giran alrededor de la inseguridad en esta operativa.

Por otra parte, el proyecto también pretende ofrecer una visión general a las personas que plantean verse inmersos en la creación de una tienda virtual, exponiendo una amplia revisión de los pagos online, la seguridad del e-commerce y algunas recomendaciones a seguir durante la implantación del sistema.

Además, se incurre en un pequeño análisis sobre la actualidad de las nuevas tendencias en tecnología de medios de pago, que están impulsando de forma exponencial el volumen de transacciones comerciales realizadas de forma online.

Para finalizar se presenta un estudio del e-commerce en Latinoamérica, mostrando las principales diferencias con esta misma operativa en España.

1.2 Objetivos

El objetivo fundamental del proyecto de fin de carrera es el estudio acerca de los sistemas de comercio electrónico y pago seguro, así como el proceso que se lleva a cabo en las transacciones y un estudio de este tipo de operativa en Latinoamérica.

En base a ese objetivo principal, se proponen los siguientes objetivos parciales:

- Analizar los conceptos básicos relacionados con e-commerce y pago seguro.

- Describir los distintos sistemas de pago en línea, así como sus beneficios y riesgos.

- Analizar los protocolos de seguridad para el pago online y el futuro de estos sistemas.

- Comprobar los principales pasos a realizar para implementar un portal con comercio online con sistema de pago seguro.

- Validar los distintos puntos que componen el comercio electrónico para verificar la seguridad del pago.

- Análisis del comercio electrónico y los pagos seguros en Latinoamérica.

1.3 Estructura de la memoria

Para facilitar la lectura de la memoria, se incluye a continuación un breve resumen de cada capítulo:

1. Conceptos de e-commerce

En este capítulo se realiza una introducción a los conceptos básicos del comercio online y una revisión de los orígenes del mismo.

Se explican los beneficios y riesgos de este tipo de operativa online, tanto para el usuario como para el propietario de una tienda online.

E-commerce y e-business son conceptos similares, pero no iguales, por lo que se detallan sus diferencias.

Por último, se profundiza en los principales tipos de transacciones de e-commerce y su aplicación en el mercado online español.

2. Sistemas de pago electrónico

Este punto ofrece una primera visión de los medios de pago y el detalle de los más utilizados actualmente.

Se profundiza en los medios de pago basados en tarjetas, en el dinero electrónico y en las cuentas pre-pago, ya que son los pilares básicos para realizar compras online. Los proveedores de pagos electrónicos también forman parte importante de las transacciones comerciales online, por lo que se detalla su funcionamiento.

Para terminar el capítulo, se hace una revisión de la banca electrónica y sus riesgos.

3. Seguridad del comercio electrónico

Se detallan las principales consideraciones de seguridad online y sus riesgos más importantes.

Hay una aportación sobre la legislación española al respecto de la seguridad del comercio online y un detalle de los derechos del consumidor así como sobre la privacidad de datos.

A nivel de usuario se puntualizan una serie de buenas prácticas para realizar compras online minimizando el riesgo.

El principal medio de pago online (tarjeta) cuenta con un protocolo de seguridad para proteger tanto a los usuarios como a los vendedores en las transacciones en línea. Se especifican los protocolos de seguridad de MasterCard y Visa.

Por último, se hace un acercamiento al futuro de los medios de pago: tecnologías que están comenzando a utilizarse pero que de momento no están completamente extendidas.

4. Aportaciones personales

En el apartado de aportaciones personales se intenta dar una serie de pautas para implementar un portal de comercio electrónico. Se detallan aspectos técnicos, de marketing, legales, etc.

Adicionalmente se presenta un análisis de la operativa de comercio online y pago seguro en América Latina.

5. Gestión del proyecto

Para llevar a cabo este proyecto, se ha seguido una planificación y se han utilizado una serie de recursos. En este apartado se detallan ambos puntos, sacando las conclusiones oportunas en cuanto a costes económicos y en tiempo.

6. Conclusiones

Resumen del proyecto realizado, sintetizando las principales ideas e incluyendo posibles aportaciones relacionadas con lo aquí desarrollado.

7. Bibliografía

Relación de todos los sitios de los que se ha recogido documentación para la realización del proyecto.

8. Glosario

Pequeño diccionario de términos, siglas y abreviaturas utilizadas a lo largo del proyecto.

Capítulo 2
Conceptos de E-commerce

2.1 ¿Qué es el comercio electrónico?

Se entiende como comercio electrónico la distribución, marketing, compra, venta y suministro de información complementaria para servicios o productos a través de Internet u otras redes informáticas. La industria de la tecnología de la información podría denominarlo como una aplicación informática para realizar operaciones comerciales.

De acuerdo al Centro Global de Mercado Electrónico, se trata de “cualquier forma de transacción o intercambio de información con fines comerciales en la que las partes interactúan utilizando Tecnologías de la Información y la Comunicación (TIC), en lugar de hacerlo por intercambio o contacto físico directo”.

2.2 Orígenes e historia

El significado del término comercio electrónico ha ido variando a lo largo del tiempo. En sus orígenes en los años 70 se relacionó con la facilitación de envíos de manera electrónica de documentos como pedidos de compra o facturas, habitualmente utilizando tecnología como Electronic Data Interchange (EDI).

Más tarde pasó a tratar actividades denominadas *Comercio en la red*, es decir, la compra y venta de bienes y servicios a través de internet. Se utilizaban

servidores seguros con tarjetas de compra electrónicas y servicios de pago electrónico como autorizaciones para tarjetas de crédito.

En los años 90, los países miembros del G7 crearon la iniciativa “A global Marketplace for SMEs” para fomentar el uso del comercio electrónico entre las empresas de todo el mundo. Esto hizo que el e-commerce sufriera un crecimiento explosivo y poco regulado, ya que Internet ofrecía un mercado barato y accesible a todo el mundo. No había códigos o instituciones que regularan la “aventura” del e-commerce. El escaso control propició que multitud de empresas tuvieran problemas de inventario y sufrieran grandes problemas en la adecuación a las nuevas tecnologías. El llamado efecto 2000 también influyó de manera negativa en el comercio electrónico, ya que hubo que invertir grandes cantidades de dinero en la reconstrucción de los sistemas tecnológicos para adaptarse al nuevo milenio.

A partir del año 2001, el comercio electrónico se formalizó y los gobiernos e instituciones comenzaron a regularlo. Apareció la figura del intermediario o distribuidor y el financiamiento e inversiones se comenzaron a realizar de manera estandarizada. Ese es el comercio electrónico que conocemos a día de hoy y sobre el que podemos afirmar que es el mayor medio de compra/venta que existe en la actualidad.

2.3 Beneficios vs Riesgos

2.3.1 Beneficios:

El uso del comercio electrónico aporta beneficios tanto en la empresa que ofrece el servicio como en los consumidores que disfrutan de él.

En la vertiente de la empresa, el principal beneficio es la capacidad de poder dirigirse a un mercado globalizado. Esto se hace posible porque el e-commerce

elimina todas las barreras geográficas del negocio y ofrece una disponibilidad 7x24 los 365 días del año sin necesidad de personal adicional.

Otras ventajas para la empresa pueden dividirse en coste directo, coste indirecto y valor añadido.

Como ventajas en el coste directo se puede decir que se ven reducidos los inventarios y stocks ya que en cada portal de venta electrónica se puede informar la cantidad de productos disponibles en el momento. El presupuesto en publicidad también se ve reducido, debido al coste de realizarlo a través de Internet en lugar de hacerlo en otras plataformas.

En cuanto al coste indirecto, el riesgo de inversión en comercio electrónico hoy en día es mínimo, lo que proporciona estabilidad a las empresas. Además, el comercio electrónico ofrece la posibilidad de facilitar los estudios de mercado con los que orientar su oferta. La automatización de pedidos, gestión de clientes y reclamaciones o sugerencias y consultas, reduce el coste de estos procesos que antes no se realizaban de forma automática.

Los beneficios que aportan valor añadido a la empresa son la venta personalizada de acuerdo a los gustos del consumidor y posibilidad de fidelización de clientes. A este punto se debe añadir la rápida actualización de información de productos/servicios de la empresa y la mayor agilidad de las transacciones entre empresa/proveedor/cliente.

Por la parte del consumidor, su principal beneficio es el de poder tener a su alcance todos los productos y servicios existentes en la red, sobre los cuales podrá tomar la decisión de seleccionar el que más de adecue a sus necesidades.

Del mismo modo, se le ofrece la posibilidad de realizar pedidos inmediatos y a mejor precio al suprimirse los intermediarios. El consumidor tiene a su alcance una cantidad de información mucho mayor e instantánea, lo que permitirá poder

tomar mejores decisiones. A esa toma de decisión sobre la compra, también ayuda la facilidad con que se realizan los pedidos (carrito de compras). Además, en muchos servicios de comercio electrónico ofrecen un gran servicio de preventa y posventa online, los cuales pueden incluir un sistema de seguimiento del pedido.

2.3.2 Riesgos:

El riesgo principal del comercio electrónico y los pagos online, reside en el posible fraude. En este punto, las transacciones de compra y pago online se pueden ver afectadas por ataques para adquirir información confidencial para uso fraudulento.

A parte del posible fraude, también existe riesgo de pharming (suplantación de identidad en correos electrónicos o páginas web). Es decir, no existe la certeza absoluta de que la persona que realiza la transacción es realmente quien dice ser, tanto por parte del vendedor como del comprador.

Actualmente existen multitud de métodos para comprobar la seguridad de un comercio electrónico y es este punto el que las empresas deben reforzar para confirmar a sus clientes que su plataforma de venta online es segura y evitar la desconfianza.

Otra desventaja del comercio online, aunque en menor manera, es la posibilidad de errores técnicos o caídas de red que están fuera del alcance de solución de la empresa. En ese caso, si los errores no se solucionan con prontitud, se puede incurrir en graves pérdidas.

2.4 Diferencias entre e-commerce y e-business

En el mundo de los negocios online, las palabras e-commerce y e-business están fuertemente ligadas, pero no se han de confundir sus significados ni sus alcances, ya que esta diferencia es muy importante para las compañías.

El e-commerce cubre los procesos por los cuales se llega a los consumidores, proveedores y socios de negocios, incluyendo actividades como ventas, marketing, toma de órdenes, entrega, servicios al consumidor, y management de lealtad del consumidor.

El e-business incluye al e-commerce, pero también cubre procesos internos como producción, administración de inventario, desarrollo de productos, administración del riesgo, finanzas, desarrollo de estrategias, administración del conocimiento y recursos humanos.

La estrategia de e-commerce es más estrecha, está más orientada a las ventas y es más simple:

- Sirve para analizar cómo usar Internet para mejorar áreas como ventas, marketing, compras y objetivos de servicio al consumidor.

- Puede hacer foco en las ventas y las órdenes tomadas sobre Internet, y puede servir para realizar mediciones acerca del crecimiento o decrecimiento de la curva de ganancias.

- Necesita estar dirigida sólo a tres direcciones de integración:

    - integración vertical entre las aplicaciones de front-end para la Web y las bases de datos y sistemas transaccionales existentes.

- Integración lateral externa, especialmente en B2B, con consumidores externos, proveedores y socios de distribución.

- Integración funcional entre la tecnología y los procesos de negocios.

Las estrategias de e-business tienen un alcance mayor, son más desafiantes, ofrecen más recompensas y probablemente requieren de fuertes cambios estructurales dentro de la organización:

- Implican el rediseño total de los negocios, cambiando y revisando todos los procesos en la compañía para capturar las eficiencias que pueden proveer el uso de la tecnología en redes.

- Incluyen oportunidades de obtener ganancias, pero el foco principal está en los costos y la eficiencia en las operaciones. Es un camino crítico para las compañías que compiten en economías de baja inflación, donde las oportunidades no pasan por el incremento de precios, y la mejora de ganancias puede ser lograda mediante mejoras productivas.

- Implican una cuarta categoría de integración:
  - a través de la empresa, con una integración funcional profunda entre nuevas aplicaciones y procesos de negocios rediseñados, y horizontalmente a través de una integración mayor de aplicaciones ERP o CRM.

- La estrategia de e-business además conserva el potencial para mejoras mayores en la performance de la compañía, tanto operativa como financieramente.

2.5 Modelo de negocio del comercio electrónico

Un modelo de negocio se puede definir como una serie de actividades planificadas para obtener beneficios en un mercado concreto. En el caso del modelo de negocio de e-commerce, debe tener las siguientes características:

- Modelo de obtención de ganancias: cómo la empresa obtendrá los ingresos necesarios para tener ganancias.

- Valor de la propuesta: cómo el producto o servicio que se oferta va a cubrir las necesidades de los clientes.

- Ambiente competitivo: identificar qué empresas se ofrecen en el mismo mercado.

- Ventaja competitiva: ventajas sobre el resto de competidores.

- Estrategia de mercado: planificación para entrar en un nuevo mercado y/o captar nuevos clientes.

- Oportunidad de mercado: mercado en el que operará la empresa y sus oportunidades financieras.

- Entorno organizacional: estructura organizativa de la compañía.

- Equipo administrativo: responsables de la organización y funcionamiento de la empresa.

El valor de la propuesta y el modelo de obtención de ganancias son los puntos principales a definir dentro del modelo de negocio. Los modelos de obtención de ganancias más importantes son:

- Publicidad: otras empresas pagan por ofertar sus productos a través de publicidad en un espacio de nuestra empresa.

- Suscripción: los usuarios o clientes deben estar suscritos para poder acceder a ofertas.

- Transacción: la empresa recibe un pago por permitir realizar una transacción (subastas).

- Afiliación: la empresa obtiene un porcentaje por las ganancias de otra empresa afiliada.

- Ventas: se obtienen ingresos por la venta de bienes o servicios.

2.6 Tipos de e-commerce

Información obtenida de www.educarm.es, www.slideshare.net, www.prezi.com, www.e-business.com, www.ecomland.com, revista "Contribuciones a la Economía"

Dentro del comercio electrónico, se pueden diferenciar distintos tipos en función a los agentes que participan en él.

2.6.1 Transacciones B2C

Las transacciones B2C (business-to-consumer) son las realizadas entre cualquier web vendedora de bienes o servicios hacia clientes compradores particulares. Es el tipo de e-commerce más común ya que acercan a cualquier consumidor la compra electrónica. Dentro del B2C los principales modelos de negocio son:

- E-tailers: todas las tiendas online. Pueden ser únicamente virtuales o con establecimiento físico. Ejemplos: amazon.com o carrefour.es

- Portales: ofrecen un gran número de servicios de forma integrada. Ejemplo: google.es

- Proveedores de contenido: ofrecen información y entretenimiento. Ejemplo: elpais.es

- Agentes de transacciones: se procesan transacciones que originariamente se realizaban en persona. Ejemplo: booking.com

2.6.2 Transacciones B2B

Las transacciones B2B (business-to-business) hacen referencia a los pagos que se realizan entre fabricante-distribuidor, fabricante-comerciante, comerciante-distribuidor, etc. En este tipo de operaciones nunca se ve involucrado el cliente final del producto.

Buscando ventajas del e-commerce, se han llevado a cabo asociaciones entre vendedores, mediante esquemas electrónicos, a este modelo también se le conoce como e-marketplaces, que también son considerados como un tipo de B2B.

El B2B aumenta la posibilidad de encontrar más proveedores y distribuidores. Esto permite comparar y seleccionar entre varias opciones, en muchos casos entre empresas hasta ese momento desconocidas.

2.6.3 Transacciones C2C

Las operaciones C2C (consumer-to-consumer) son las que se establecen entre cliente-cliente. Se utiliza este término para definir un modelo de negocio en

la red que pretende relacionar comercialmente el usuario final con otro usuario final. Es decir, facilita la comercialización de productos entre particulares, donde las partes de la transacción son las responsables de realizar y confirmar la operación.

El mayor ejemplo de e-commerce C2C es eBay, donde la empresa actúa únicamente como intermediario y cobra por ese servicio.

2.7 Comercio electrónico en España

Los datos mostrados a continuación han sido recogidos de estudios del ONTSI del Ministerio de Industria, Energía y Turismo de España, de la AECE, Cetelem-Nielsen y del portal SoloStocks.

2.7.1 Transacciones B2C en España

En el siguiente gráfico se muestra el incremento de las transacciones B2C en España en los últimos años. Los datos de 2013 casi triplican los ingresos obtenidos 2007. En unos 6 años el volumen de ventas ha crecido de manera muy significativa.

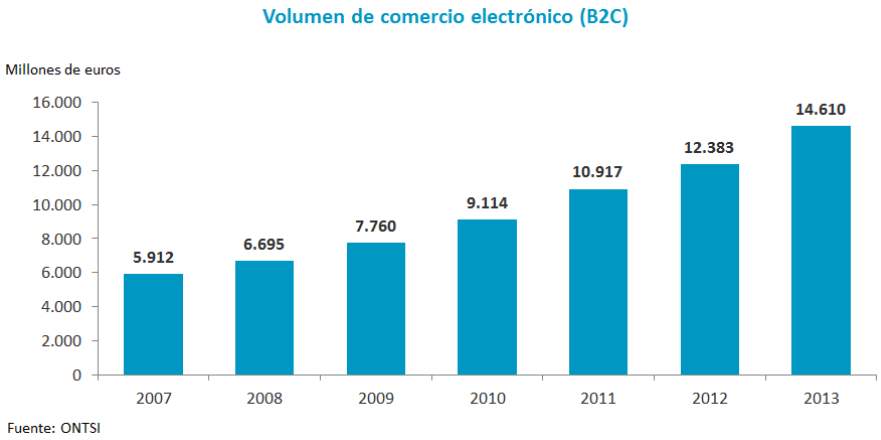


Figura 1. **Volumen de comercio electrónico B2C. Fuente: ONTSI**

La evolución del volumen de compra online declarada por los consumidores españoles se debe al aumento de todas las variables que afectan al comercio online:

- Internautas (estimados en 28,4 millones)
- Número total de compradores online en el año 2013 (que se estiman en 17,2 millones)
- Gasto anual medio por internauta comprador (848€)

El porcentaje total de internautas ha experimentado un incremento de 3,2 puntos porcentuales (p.p.) respecto al año anterior, pasando del 69,9% de 2012 a un 73,1% en 2013. Este aumento es muy similar al observado el año anterior, 3,6 p.p.

Por otro lado, también crece de manera destacable el porcentaje de internautas que han efectuado compras en el último año, representando en 2013 el 60,6% de los internautas totales, frente al 55,7% de 2012. Este incremento de 4,9 p.p. es ligeramente inferior al registrado en 2012, de 5 p.p.

Por consiguiente, el índice de internautas compradores arroja que el número absoluto de internautas compradores ha aumentado en un 14% pasando de los 15,2 millones de 2012 a los 17,2 millones en 2013.

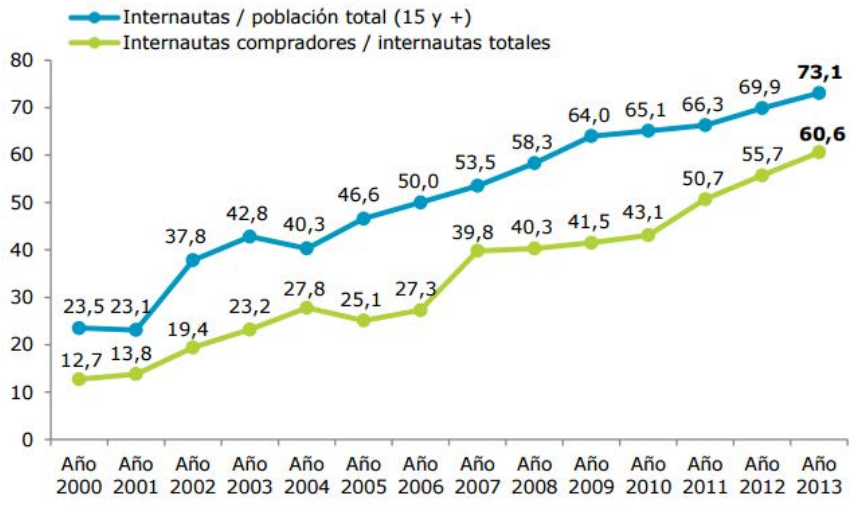


Figura 2. **Evolución del número de internautas vs internautas compradores. Fuente: ONTSI**

Cabe destacar también, que el tercer componente del volumen de compra total, el gasto medio por individuo comprador, ha crecido un 3,9% en 2013, pasando de 816 € en 2012 a 848 €, invirtiendo así la tendencia a la baja de los dos años anteriores.

Año	Importe Total
2008	754
2009	749
2010	831
2011	828
2012	816
2013	848

Figura 3. **Evolución del gasto medio anual por internauta comprador (en millones de euros). Fuente: ONTSI**

Es interesante también revisar los tipos de bienes y servicios que más se adquieren en el comercio B2C. Los productos más solicitados son los billetes de transporte, seguidos de las reservas de alojamiento, ropa y entradas a espectáculos.

Figura 4. **Bienes y servicios adquiridos online en 2013. Fuente: ONTSI**

El mayor motivo por el que se realizan compras online B2C en España es el ahorro de tiempo y la comodidad que ofrece poder adquirir productos sin tener que visitar la tienda física.

También es importante destacar el 23% que indica que el comercio electrónico es el único medio para adquirir los productos. Esto refleja la gran ventaja que ofrece el e-commerce de ser accesible para todo el mundo en cualquier lugar o momento.

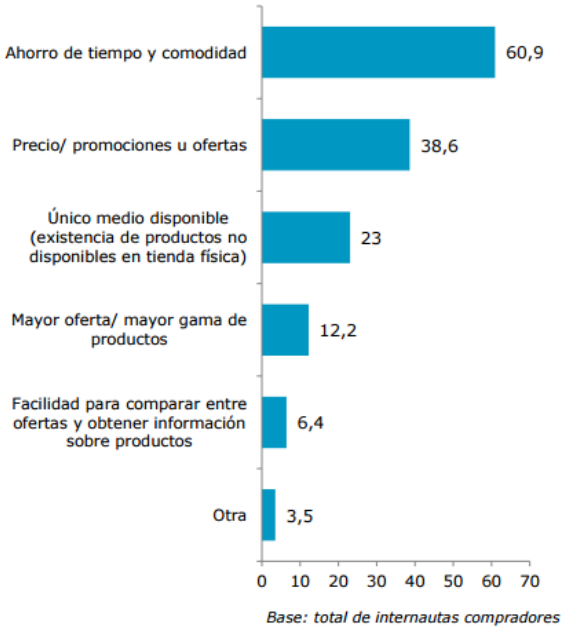


Figura 5. **Razones de la compra online. Fuente: ONTSI**

Si se evalúa la satisfacción de los usuarios con sus compras online, se detecta que casi el 90% de los usuarios nunca ha tenido problemas al realizar compras electrónicas.

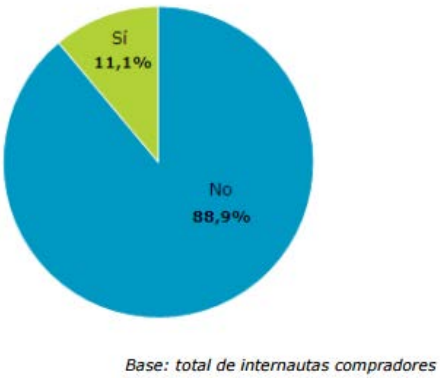


Figura 6. **Usuarios con problemas en las compras B2C alguna vez. Fuente: ONTSI**

Dentro de los problemas más habituales, se concluye que el extravío del producto o los desperfectos en el mismo son las causas más comunes.

Figura 7. **Problemas en las compras online. Fuente: ONTSI**

2.7.2 Transacciones B2B en España

Según el INE, el 68,2% por ciento de las ventas por comercio electrónico en 2013 tuvo como destino otras empresas (B2B) mientras que el porcentaje de ventas a consumidores finales (B2C) fue del 29,9%.

En relación con las transacciones B2B con países extranjeros, la demanda de exportaciones creció un 21,09% en 2014, respecto al ejercicio anterior. Los

principales mercados a los que España exporta producto por B2B son México, Chile, Colombia, Perú, Argentina y Portugal. El mayor crecimiento interanual lo han registrado Australia, Ucrania, EEUU, Chile y Georgia.

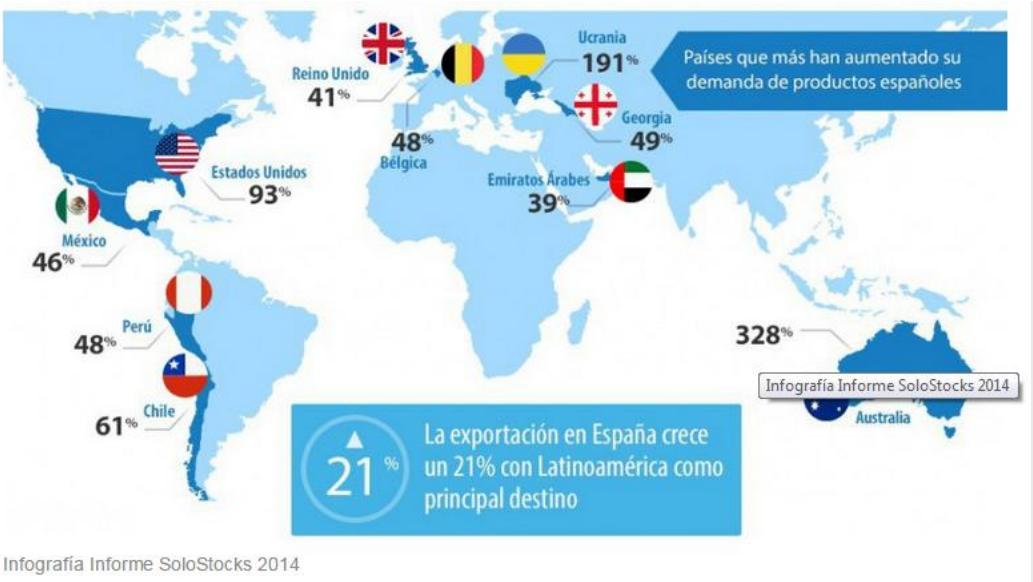


Figura 8. **Tendencias de comercio online B2B internacional. Fuente: SoloStocks**

Por el tipo de empresas, son los autónomos los que han registrado el mayor aumento con un 24,34% a la hora de ofrecer sus productos y servicios en la red, seguido de las Sociedades Limitadas con un 16,86% de crecimiento.

Figura 9. **Tipos de empresas que más aumentaron su actividad online. Fuente: SoloStocks**

2.7.3 Transacciones C2C en España

Según un estudio del ONTSI del 2012, los datos demuestran un incremento de 48,22% de las transacciones comerciales entre particulares (C2C), que en 2011 experimentó un retroceso.

En un estudio realizado por Cetelem el 54% de los encuestados declara haber comprado alguna vez por internet a particulares, frente al 37% que ha realizado ventas C2C. Esto evidencia que el público que utiliza el C2C es más propenso a comprar que a vender productos directamente a particulares.

Figura 10. **Compras online a particulares. Fuente: Cetelem-Nielsen**

Figura 11. **Ventas online a particulares. Fuente: Cetelem-Nielsen**

El top 3 de productos más comprados a un particular en el canal online lo forman en primer lugar los electrodomésticos/tecnología con un 26%. El segundo puesto lo ocupan los libros/música con un 23% de compras a un particular. Las telecomunicaciones con un 13% son el tercer producto más comprado entre particulares.

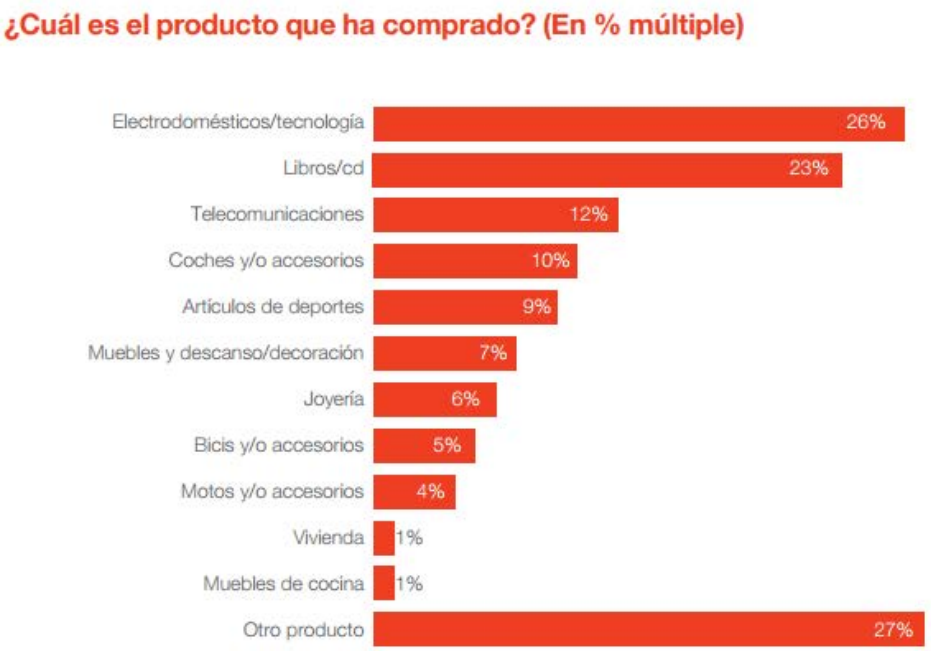


Figura 12. **Productos más comprados a particulares. Fuente: Cetelem-Nielsen**

Los productos más vendidos a un particular en el canal online son prácticamente los mismos que los más comprados. La única excepción es que el tercer puesto de ventas lo ocupan los muebles y objetos de decoración frente al tercer puesto de compras que eran las telecomunicaciones.

Figura 13. **Productos más vendidos a particulares. Fuente: Cetelem-Nielsen**

Capítulo 3
Sistemas de Pago electrónico

3.1 Introducción a los medios de pago

Los medios de pago de una economía son todos los activos que pueden considerarse dinero, es decir, todo activo que sea universalmente reconocido por todos los individuos que formen parte de la zona monetaria facilitando los intercambios. Los principales medios de pago que se utilizan en la actualidad son:

- Dinero físico o efectivo (monedas y billetes). Una importante parte de este dinero efectivo en circulación consiste en depósitos bancarios –cuentas corrientes, de ahorro o a plazo- que no son otra cosa que el papel moneda que cualquier persona deposita en un banco.

- Cheque. Un cheque es una orden de pago que extiende una persona o entidad a favor de otra para ser cancelada por un banco. La parte que extiende el cheque debe poseer una cuenta corriente en algún banco, con fondos suficientes para cubrir el monto emitido; de lo contrario, no será cancelado y el banco procederá a protestar el cheque. Este instrumento de pago se utiliza frecuentemente y, en ciertos sectores de nuestra sociedad, ha desplazado en importancia al dinero en efectivo.

- Pagaré: Documento escrito mediante el cual una persona o empresa se compromete a pagar a otra persona o compañía una determinada cantidad de dinero en una fecha acordada previamente. Los pagarés pueden ser al portador o endosables, es decir, que se pueden transmitir a un tercero.

- Letra bancaria: Título de valor formal y completo que contiene una orden incondicionada y abstracta de hacer pagar a su vencimiento al tomador o a su orden una suma de dinero en un lugar determinado, vinculando solidariamente a todos los que en ella intervienen.

- Tarjeta de crédito. Tarjeta que da derecho a comprar bienes y servicios a crédito en determinados establecimientos. Algunas tarjetas de crédito sólo sirven para una determinada empresa, pero otras tienen un uso genérico, y se pueden utilizar para una gran variedad de actividades comerciales.

3.2 Actualidad de los sistemas de pago electrónico

En sus inicios, los sistemas de pago han sido el mayor obstáculo tanto técnico como psicológico para que se produjera el despegue definitivo del e-commerce. Para que el e-commerce se consiga desarrollar e implantar de manera natural en todo el mundo, es primordial que los usuarios confíen en los sistemas de pago electrónico y no tengan el fraude como el mayor temor. Es importante que se conozcan los sistemas de pago empleados y su fiabilidad.

El dinero físico está actualmente desapareciendo para dejar paso a pagos con tarjetas de crédito o débito, transferencias o pagos con dinero electrónico. Los sistemas de pago electrónicos permiten a los usuarios dar una orden electrónica directa a su entidad bancaria para que realice un pago al beneficiario correspondiente. Es decir, al adquirir un bien o servicio, el cliente transfiere electrónica y directamente el importe de dicho bien o servicio al proveedor del mismo. Al ser un traspaso directo de dinero entre cliente y proveedor, se evita la compensación entre bancos.

Actualmente, el gran foco de los sistemas de pago electrónico se basa en pagos con tarjeta de crédito, pagos por correo electrónico, proveedores de servicios de pago y sistemas de pago mediante teléfonos móviles.

Un sistema óptimo de pago electrónico debería cumplir las siguientes premisas:

- Fácil de usar y universal
- Permitir pagos de cualquier monto
- No tener asociado un costo elevado por transacción
- Ofrecer alto nivel de seguridad
- Brindar garantía de pago
- Dar privacidad a la compra
- Devolver un voucher o comprobante de compra

3.3 Clasificación de los sistemas

Información basada en www.educarm.es, www.mastercard.us, https://usa.visa.com/

3.3.1 Sistemas de pago basado en tarjetas

Se trata del sistema de pago electrónico más actualizado en la sociedad actual. En este bloque se incluyen las tarjetas de crédito, tarjetas de débito y tarjetas prepago.

3.3.1.1 Tarjetas de crédito

La característica principal de una tarjeta de crédito es la posibilidad de realizar transacciones a pesar de no contar en el momento con el cupo suficiente

para cubrir el importe total del pago. Es decir, se aplaza el pago de la transacción a una fecha concreta. A través de cualquier tarjeta de crédito se pueden realizar pagos electrónicos, sólo es necesario tener cupo disponible.

El flujo de un pago electrónico a través de tarjeta de crédito es el siguiente:

- El cliente en la tienda virtual selecciona los productos o servicios que desea adquirir y selecciona como sistema de pago la tarjeta de crédito.

- La tienda virtual, a través de una conexión SSL envía a la entidad emisora de la tarjeta los datos de la transacción: importe, identificación de la tarjeta y método de pago (en cuotas o revolvente).

- A través de la tienda virtual se solicita la conformidad del cliente con relación al pago que se va a realizar.

- El banco valida los datos enviados asociados a la compra y a la tarjeta. Se valida que el cliente tenga cupo suficiente para cubrir el pago de la compra.

- Tras pasar todas las validaciones, el banco, nuevamente a través de una comunicación SSL, comunica a la tienda virtual y por tanto al cliente, la aceptación o denegación de la transacción.

- Si la transacción es aprobada, se realiza el cargo en la cuenta del cliente. Dicho cargo se hará efectivo en un plan de cuotas si el cliente lo solicitó así o de forma revolvente en caso contrario. Al tratarse de una operación de crédito, el cargo no se hará efectivo al momento, si no que se cargará en la cuenta del cliente cuando este haya decidido que factura su cuenta.

Las tarjetas de crédito más utilizadas a nivel mundial son las que proporcionan las entidades bancarias asociadas a las distintas redes (MasterCard, VISA, American Express, Dinners Club, etc.).

A pesar de existir una conexión segura con la entidad bancaria, la transacción puede ser insegura ya que el cliente puede estar utilizando una tarjeta robada o fraudulenta. Por la parte del comercio que ofrece el bien o servicio también se puede caer en un fraude para obtener número de tarjetas de crédito desde una empresa ficticia. Desde las distintas redes que facilitan el pago a través de tarjeta de crédito se han creado protocolos de seguridad para evitar el fraude por ambas partes. VISA ha implementado el servicio Verified by Visa y Mastercard el servicio 3D Secure (ver punto 4.6).

3.3.1.2 Tarjetas de débito

Para poder realizar transacciones con una tarjeta de débito es necesario contar en el mismo momento de la compra con el saldo suficiente para cubrir el pago. En la actualidad, la gran mayoría de e-commerce aceptan la tarjeta de crédito como medio de pago, aunque en un principio estas tarjetas de débito eran usadas en exclusiva para realizar retiros de efectivo en cajeros.

El flujo de un pago electrónico a través de tarjeta de débito sería el mismo que con una tarjeta de crédito, a excepción de:

- El banco debe verificar que el cliente tiene saldo suficiente para cubrir el pago en el día.

- No es posible seleccionar el método de pago en cuotas, siempre son transacciones revolventes.

- El cargo en la cuenta del cliente se realiza al momento de aceptar la compra.

3.3.1.3 Tarjetas prepago.

Las tarjetas prepago también son llamadas monedero, ya que se requiere realizar un abono sobre la tarjeta antes de poder realizar operaciones con ella. Es decir, la tarjeta no nace con un saldo disponible determinado, si no que es el cliente el que tiene que ingresar dinero en ella para poder operar posteriormente. Una vez cargada la tarjeta, se pueden realizar transacciones de e-commerce del mismo modo que con una tarjeta de débito.

El flujo de un pago electrónico a través de tarjeta prepago sería el mismo que con una tarjeta de débito.

3.3.2 Dinero electrónico

El dinero electrónico o e-money es dinero que se emite de forma electrónica y a través de sistemas de valores digitalmente almacenados.

El caso más famoso de e-money es el bitcoin. Este e-money es una criptodivisa (medio digital de intercambio) que usa una base de datos para registrar las transacciones y para proveer funciones de seguridad básica. Estas funciones aseguran que los bitcoins solo puedan ser gastados únicamente por su dueño y nunca más de una vez.

El diseño de los bitcoins permite almacenarlos y ser transferidos de manera anónima. Las monedas pueden ser guardadas en cualquier ordenador o unidad de almacenamiento en forma de archivo. También existen servicios en Internet que ofrecen almacenamiento de estos archivos, lo que llaman monederos. En cualquiera de los casos los bitcoins pueden ser enviados por medio de Internet a cualquiera que tenga una cuenta de bitcoin.

Los bitcoins almacenados están firmados digitalmente con la firma del propietario. Cuando se desea realizar un pago con bitcoins, se firman las monedas a enviar con la firma privada del comprador y la firma pública del

comerciante. De esa forma, únicamente el destinatario puede descifrar el dinero mandado y utilizarlo. Cabe destacar que si el poseedor de los bitcoins pierde el archivo u olvida la contraseña de su firma, pierde el dinero.

Una de las críticas que se le hace al dinero electrónico es que no se pueden rastrear las transacciones, de manera que cualquiera puede hacer un pago a otro usuario sin que ningún organismo o estado pueda detectarlo, lo que afecta a la persecución del crimen y la evasión de impuestos. Pero este punto también afecta a cualquier pago en efectivo que se realice, ya que puede almacenarse en paraísos fiscales difícilmente rastreables.

También hay un riesgo sobre posibles fallos de seguridad del software o de las bases de datos para operar con los bitcoins. Pero al tratarse de software libre cualquiera puede corregir o alertar acerca de errores en el código. Que le software sea libre también evita que el software esté oculto y sólo en manos de unos pocos desarrolladores.

3.3.3 Cuentas pre-pago

En la actualidad, muchos sitios web tienen habilitada la opción de recibir pagos a través de cuentas pre-pago.

El funcionamiento de estas cuentas pre-pago es muy sencillo: el cliente puede ingresar dinero en su cuenta en el momento que quiera y lo puede hacer a través de un pago con tarjeta, en efectivo, por transferencia…

Para los sites que tienen este tipo de pago implantado, les supone la ventaja de no recibir pagos por cada compra que el cliente realiza, si no que lo reciben cada vez que el cliente quiere aumentar su saldo de cuenta.

3.4 Proveedores de pagos electrónicos

Información obtenida de “La Banca en Internet: Riesgos Implícitos” y de las web www.monografias.com, www.cecarm.com

Un proveedor de pagos electrónico, o pasarela de pago, es quien autoriza las transacciones de pago en un comercio electrónico a través del protocolo de cifrado SSL. Es decir, cifra la información sensible entre vendedor y comprador para garantizar la seguridad de la información. Todas las pasarelas de pago cobran una comisión por cada transacción realizada y están preparadas con los sistemas de seguridad habituales en el comercio electrónico para evitar posibles fraudes.

Estos proveedores de pago hacen la función de intermediario entre las partes de la operación en el momento de realizar el pago: trata con la entidad adquirente del vendedor y con la entidad emisora del comprador, evitando que ambas entidades bancarias tengan que conectar entre sí.

Existen un gran número de proveedores de pago electrónicos, pero el que mayor impacto ha tenido es Paypal. A través de Paypal se permite a sus usuarios realizar transacciones monetarias sin compartir su información financiera con el destinatario del pago. Una vez registrado en Paypal, es el propio proveedor de pago el que tiene esa información y el que redirige el pago desde la cuenta Paypal del cliente (a través de su entidad financiera) a la cuenta Paypal del beneficiario (también a través de su entidad bancaria).

3.5 Banca electrónica

Información obtenida de “La Banca en Internet: Riesgos Implícitos” y de la web www.monografias.com

La banca electrónica (o banca en Internet) puede definirse como el conjunto de productos y procesos que permiten, mediante procedimientos informáticos, que el cliente pueda realizar una serie, cada vez más amplia, de transacciones bancarias sin necesidad de ir a la sucursal.

La incorporación de Internet a la banca proporciona una serie de ventajas a las entidades financieras, entre las que destacan:

- La entrada en una nueva unidad estratégica de negocio que ofrece un alto potencial de crecimiento aunque también requiere de fuertes inversiones.

- La reducción de costes de transacción (una transacción realizada vía Internet puede costar a un banco un 1% de lo que vale en la sucursal).

- El acceso a la información general del banco (marketing directo).

- La adecuación de los productos y servicios bancarios a las nuevas necesidades de los clientes, lo cual redunda en su fidelización.

Dos aspectos fundamentales que debemos resaltar en la banca electrónica son, por un lado, la naturaleza del canal a través del cual las actividades se realizan y, por otro, los medios de acceso a dichos canales. Los canales de suministro comunes incluyen tanto a las redes abiertas (Internet) como a las cerradas (redes locales privadas). La diferencia entre ambas estriba en que éstas últimas restringen el acceso a los participantes (instituciones financieras, consumidores, comerciantes y terceros) en los términos recogidos en el acuerdo, mientras que en las abiertas tales requerimientos de participación no existen.

Los productos y servicios ofrecidos a través de la banca electrónica se pueden agrupar en dos tipos:

- De Información:

  La información que podamos transmitir o recibir dependerá de la entidad financiera con la que trabajemos. Así, lo más normal es: consulta de saldos y movimientos de las cuentas, tarjetas, información sobre préstamos y operaciones bancarias, etc.

  Además de este tipo de información particular de cada cliente, las entidades ofrecen otras de tipo genérica, como el acceso a los mercados financieros a tiempo real, productos y servicios ofrecidos por el banco, temas de actualidad, como el euro, etc.; completándose todo ello con la posibilidad de realizar consultas directamente a través del correo electrónico.

- De Órdenes:

  Transferencias y traspasos entre cuentas, solicitud de apertura, domiciliación de recibos, petición de talonarios, suscripción de fondos de inversión, planes de pensiones, petición de tarjetas de crédito, compra - venta de valores, solicitud de moneda extranjera, etc.

3.5.1 Componentes de un sistema de banca electrónica

Los componentes más importantes a la hora de tener en cuenta un sistema de banca electrónica de cualquier entidad financiera son:

- Administración de la seguridad

- Servidor de banca electrónica

- Diseño y hosting del sitio web

- Administración y manejo de firewalls

- Administración de la red interna

- Sistemas de detección de intrusos (IDS)

- Aplicaciones de e-commerce ofertadas (pago de servicios, manejo de préstamos, tarjetas de crédito virtuales…)

- Otros servidores internos de la red (servidor de aplicaciones, servidor de correo electrónico, servidor de base de datos…).

3.5.2 Riesgos de la banca electrónica

Debido a los rápidos cambios en las tecnologías de la información, la lista de riesgos que afectan a la banca electrónica no puede ser exhaustiva. Sin embargo, sí podemos describir un grupo de riesgos, suficientemente significativo, que nos permita diseñar una guía general de apoyo a la gestión de los mismos.

Hay que advertir que los tipos básicos de riesgo generados en la banca electrónica no son nuevos; la novedad estriba en la forma específica bajo la cual estos riesgos surgen, así como la magnitud de su impacto.

En este sentido, las categorías de riesgo más importantes para la banca electrónica, especialmente para la banca internacional diversificada son:

- Riesgo operacional: recoge la pérdida potencial derivada de deficiencias significativas en la integridad o en la confianza del sistema. Este riesgo puede surgir por un mal uso del cliente, un diseño inadecuado del sistema o de un sistema mal planteado.

Algunos ejemplos de riesgo operacional son el acceso no autorizado, el fraude de empleados, la obsolescencia del sistema, el cliente no cumple las pautas de seguridad, ausencia de gestión experta, el cliente niega haber realizado alguna transacción…

- Riesgo reputacional: Es el riesgo de que se forme una opinión pública negativa sobre el servicio bancario prestado. El riesgo reputacional puede derivar en acciones que fomenten la creación de una mala imagen o un posicionamiento negativo en la mente de los clientes, de tal forma que se produzca una migración de fondos hacia otras entidades debido a una pérdida de credibilidad. Este riesgo también aparece vinculado al carácter estratégico de la banca electrónica, es decir, el hecho de no participar en este segmento influye significativamente en la imagen corporativa de la entidad financiera.

  Del mismo modo, un banco podría incurrir en pérdidas por el simple hecho de que otra institución que ofreciese servicios similares de banca electrónica cometiese frecuentemente errores en la prestación de tales servicios. Por esta razón se afirma que el riesgo reputacional no sólo es importante para un banco en particular, sino para el sistema bancario en su conjunto.

- Riesgo legal: El riesgo legal surge de violaciones e incumplimientos con las leyes, reglas y prácticas, o cuando los derechos y obligaciones legales de las partes respecto a una transacción no están bien establecidos. Dada la relativa nueva naturaleza de muchas de las actividades de banca electrónica, los derechos y obligaciones de las partes respecto a estas transacciones son, en algunos casos, inciertas. Por ejemplo, las aplicaciones de algunas reglas de protección del cliente respecto a la banca electrónica en algunos países no son claras.

  Además, el riesgo legal puede derivar de la incertidumbre respecto a la validación de algunos acuerdos relativos a los medios electrónicos.

Otra fuente de riesgo legal es la asociada a la protección de la privacidad. Aquellos clientes que no han sido adecuadamente informados sobre sus derechos y obligaciones pueden acometer contra el banco.

- Riesgo transaccional: La banca electrónica está basada en las tecnologías diseñadas para cubrir amplias áreas geográficas. La expansión del mercado puede extenderse más allá de las fronteras nacionales, aumentando la exposición al riesgo

  Los bancos deben cumplir diferentes requerimientos legales cuando trabajan con clientes más allá de sus fronteras. Por ejemplo, para la banca a través de Internet, existen actualmente lagunas respecto a estos requerimientos en determinados países. Además, hay ambigüedades jurisdiccionales con relación a las responsabilidades de las diferentes autoridades nacionales. Estas consideraciones pueden exponer a los bancos a un riesgo legal asociado con el incumplimiento de las diferentes leyes nacionales, como son las leyes de protección al consumidor, los requerimientos de comunicación, las reglas de privacidad, etc.

- Otros riesgos: Los riesgos tradicionales de la banca, tales como el riesgo de crédito, el riesgo de liquidez, el riesgo de tipo de interés, y el riesgo de mercado, pueden también aparecer en la banca electrónica, aunque sus consecuencias prácticas podrían ser de menor magnitud.

Capítulo 4:
Seguridad del comercio electrónico

4.1 Consideraciones de seguridad

La información ha sido recopilada de fuentes como "*Comercio electrónico*", www.larevistainformatica.com, www.administracionelectronica.ujaen.es

La seguridad en el comercio electrónico es el principal aspecto a tener en cuenta y a mejorar en este tipo de transacciones. La herramienta principal que certifica esta seguridad es un servidor seguro a través del cual se cifra toda la información confidencial antes de realizar el viaje electrónico de forma segura. Es este servidor el que aporta valor y confianza tanto a proveedores como consumidores de e-commerce.

El mayor miedo que todo comprador tiene cuando realiza transacciones a través de e-commerce, es que sus datos personales y sensibles sean interceptados o captados para realizar una suplantación de identidad.

Para evitar todo tipo de captura de información sensible se han creado métodos o sistemas de seguridad para transacciones de comercio online:

- Cifrado: el cifrado es la codificación de la información que se va a enviar a través de la red. Para que le receptor de dicha información pueda descifrarla es necesario el uso de un software de descodificación o una clave que únicamente conocen emisor y receptor de la información.

Por tanto, mediante el cifrado, la información transferida es únicamente accesible por las partes que intervienen en la transacción electrónica (emisor, receptor y las entidades bancarias de ambos).

- Firma digital: La firma digital es el procedimiento por el cual se puede asociar o identificar a una persona o un equipo informático durante la transmisión de mensajes de carácter telemático o en la gestión y tramitación de documentos electrónicos. Todo este proceso se lleva a cabo a través de métodos de cifrado y además, según el método empleado, se puede incluso llegar a asegurar la integridad del documento o el mensaje.

  En España, se definen 3 tipos de firma:
  - Simple: sólo se requieren los datos para autentificar al usuario
  - Avanzada: además de autentificar al usuario en este nivel se comprueba la integridad del mensaje o documento
  - Reconocida: es la firma avanzada y amparada por un certificado reconocido, este se otorga tras verificar presencialmente la identidad del firmante.

  De este modo, la firma digital permite que tanto el receptor como el emisor de un contenido puedan identificarse mutuamente con la certeza de que son ellos los que están interactuando, evita que terceras personas intercepten esos contenidos y que los mismos puedan ser alterados, así como que alguna de las partes pueda "repudiar" la información que recibió de la otra y que inicialmente fue aceptada.

4.2 Principales riesgos de seguridad

Información recopilada de la Oficina de Seguridad del Internauta (www.osi.es) y la Universidad Nacional Autónoma de México.

4.2.1 Phishing

El phishing ("pescar", fishing) consiste en intentar adquirir información confidencial (contraseñas, cuenta bancaria, datos de tarjeta, etc.), de forma anómala, simulando ser una entidad de confianza, vía e-mail o mensajería instantánea utilizando URLs similares.

Características de los correos de phishing

Las principales características de todos los correos electrónicos que intentan captar información personal son:

- El contenido parece real: el correo está diseñado para que parezca que es enviado desde la compañía a la que está suplantando. Se copian logotipos, enlaces de contacto, estilo del sitio web, información de copyright, etc. Incluso pueden incluir algún enlace real al sitio legítimo.

- Solicitan información confidencial de forma no solicitada: ninguna compañía seria debería enviar un correo electrónico no deseado -que no es como consecuencia de una solicitud del cliente-, solicitando que acceda a un enlace que pide información confidencial.

- Saludos genéricos: estos correos electrónicos son enviados de forma masiva y aleatoria a un gran número de personas, por lo que el saludo siempre es muy genérico. Los saludos suelen ser del estilo "Estimado cliente", "A todos nuestros tarjetahabientes".

- Enlaces disfrazados: los enlaces contenidos en el correo electrónico están presentados para que parezcan auténticos.

- Imágenes con enlaces: el correo completo es una imagen que se puede pulsar para acceder al enlace fraudulento.

- Urgencia en la respuesta: la redacción del correo da sentido de urgencia al usuario en la respuesta o envío de datos.

Puntos a verificar ante sospecha de phishing

Ante laguna sospecha de que un correo electrónico recibido pueda ser fraudulento, se recomienda verificar lo siguiente:

- Dominio del correo electrónico: la verificación más básica que se puede hacer es que el dominio del correo electrónico corresponde a la compañía que en teoría está enviando el correo. Debe ser un dominio que no deje lugar a dudas que es legítimo.

- Cuenta equivocada: si el usuario tiene varias cuentas de correo electrónico, debe verificar que la que proporcionó a su compañía es la misma en la que está recibiendo el correo electrónico.

- Archivos adjuntos: los archivos que envían las compañías legítimas suelen tener formato PDF. Es conveniente dudar de archivos en cualquier formato de Microsoft Office o que solicite permisos para ejecutarlo.

- Seguridad SSL: si se accede a alguno de los enlaces que proporciona el e-mail, se debe verificar que la página web a la que se redirige está utilizando una dirección HTTPS (utiliza SSL).

- Direcciones engañosas: antes de hacer clic sobre un enlace, es conveniente pasar el ratón por encima para verificar que la dirección URL que aparece corresponde a la compañía legítima del sitio.

- Formas en el correo: un e-mail con campos para suministrar directamente datos sensibles, es fraudulento.

Argumentaciones para el envío de correos de phishing

Los correos electrónicos suplantadores utilizan todo tipo de argumentos ingeniosos relacionados con la seguridad de la entidad o el adelanto de algún trámite administrativo para justificar la necesidad de facilitar los datos personales del usuario. Entre las excusas frecuentes se pueden encontrar:

- Problemas de carácter técnico.

- Recientes detecciones de fraude y urgente incremento del nivel de seguridad.

- Nuevas recomendaciones de seguridad para prevención del fraude.

- Cambios en la política de seguridad de la entidad.

- Promoción de nuevos productos.

- Premios, regalos o ingresos económicos inesperados.

- Accesos o usos anómalos a tu cuenta.

- Inminente desactivación del servicio.

- Falsas ofertas de empleo.

4.2.2 Pharming

El pharming es una modalidad de ataque que consiste en suplantar el DNS (Sistema de Resolución de Nombres de Dominio) con el propósito de conducir al usuario a una página web falsa. El atacante logra hacer esto al alterar el proceso de traducción entre la URL de una página y su dirección IP.

El DNS es similar a un listín telefónico de Internet. Cada vez que se teclea una dirección web, realmente se está haciendo una llamada una dirección IP (el "número telefónico" en Internet). Como recordar todas las IPs de nuestro interés sería una ardua tarea, los servidores de DNS hacen ese trabajo por nosotros: enviamos el nombre de la página a visitar y ellos miran de forma automática en sus listas para recabar la IP del sitio web al que deseamos acceder.

Comúnmente el atacante realiza el redireccionamiento a las páginas web falsas a través de código malicioso. De esta forma, cuando se introduce un determinado nombre de dominio que haya sido cambiado, el explorador de Internet accederá a la página web que el atacante haya especificado para ese nombre de dominio. Para llevar a cabo redireccionamiento a las páginas web falsas se requiere que el atacante logre instalar en el sistema de la persona afectada alguna aplicación o programa malicioso (malware). La entrada del código malicioso en el sistema puede producirse a través de distintos métodos, siendo la más común a través de un correo electrónico, aunque puede realizarse también a través de descargas por Internet o a través de unidades de almacenamiento como una memoria USB.

La gran diferencia entre phishing y pharming es el nivel de actuación del usuario. En un caso de phishing, el usuario ha tenido que acceder a la dirección que el atacante le ha enviado, mientras que en un caso de pharming basta con que acceda a un DNS modificado.

4.3 Legislación española sobre e-commerce

Basado en “Comercio electrónico: Normativa aplicable” del portal Educadictos.com, el Ministerio de Industria, Energía y Turismo y la Agencia Española de Protección de Datos.

El primer punto a tener en cuenta es que toda empresa de e-commerce tiene las mismas obligaciones legales (civiles, mercantiles, fiscales, laborales, de contratación, sanitarias, de seguridad, etc.) que las que no están en Internet. Sin embargo, el comercio electrónico tiene una serie de particularidades legales, las cuales están recogidas en la Ley 34/2002 o LSSI. La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico regula determinados aspectos jurídicos de los Servicios de la Sociedad de la Información.

El criterio para determinar si un servicio o portal web debe regirse bajo la LSSI es si constituye una actividad económica y/o lucrativa para el prestador. Quedan excluidos los servicios prestados por notarios y registradores de la propiedad y mercantiles en el ejercicio de sus respectivas funciones públicas, y los servicios prestados por abogados y procuradores en el ejercicio de sus funciones de representación y defensa en juicio.

Sin embargo el carácter gratuito de un servicio no determina por sí mismo que no esté sujeto a la Ley. Existen multitud de servicios gratuitos ofrecidos a través de Internet que representan una actividad económica para su prestador (publicidad, ingresos de patrocinadores, etc.) y, por lo tanto, estarían incluidos dentro de su ámbito de aplicación. Ejemplos de estos servicios serían los habituales buscadores, o servicios de enlaces y directorios de páginas web, así como páginas financiadas con publicidad o el envío de comunicaciones comerciales.

Obligaciones y responsabilidades de los prestadores de servicios en la red.

1. Información para la identificación del prestador de servicios.

   Todos los prestadores de servicios en la red deben indicar en su sitio web, siempre de forma clara, gratuita y unívoca, todos sus datos de contacto (nombre, denominación social, NIF, domicilio, teléfono, etc.), su número en el Registro Mercantil, número de colegiado si corresponde, precio de sus servicios (indicando si incluyen impuestos y gastos de envío) y códigos de conducta a los que esté suscrito.

2. Deber de colaboración y responsabilidad de los prestadores de servicios.

   Los prestadores de servicios en la red no son responsables por los contenidos ajenos que transmiten o alojan. Sin embargo, tienen la obligación de colaborar con las autoridades si sospechan de alguna ilegalidad y/o de retirar el contenido de su web.

3. Cookies.

   Las cookies permiten a los prestadores de servicios en Internet almacenar y recuperar datos sobre los usuarios almacenados en sus equipos. Para hacer uso de esas cookies, siempre deben alertarlo en su portal para solicitar el consentimiento de los usuarios. También deben informar los términos de uso y su finalidad (basándose en la LOPD - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal).

4. Información sobre seguridad.

   Por último, se debe ofrecer la información de seguridad frente a spam, virus informáticos, posible software fraudulento, etc.

   Deberán también informar a sus clientes sobre las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos.

Reglamento de la LOPD (RLOPD)

Adicionalmente, se debe tener muy presente también el Reglamento de la LOPD y sus aplicaciones para el tratamiento de datos confidenciales. Este reglamento complementa la LOPD para no dejar sin regulación ningún aspecto. Los principales aspectos que trata son:

- Principios de la protección de datos: complementación de la LOPD en lo referente al principio de calidad de los datos, la obtención del consentimiento del afectado y el deber de información al ciudadano.

- Derechos ARCO (acceso, rectificación, cancelación y oposición): aclaración de los derechos ARCO del ciudadano, es decir, el control que él mismo puede tener sobre sus datos personales.

- Disposiciones aplicables a determinados ficheros de titularidad privada: trata el régimen jurídico aplicable a los ficheros de información sobre solvencia patrimonial y crédito, así como al tratamiento de datos personales para actividades publicitarias y/o comerciales.

- Obligaciones previas: establece el procedimiento para crear, modificar o suprimir los ficheros de titularidad pública.

- Transferencias internacionales de datos: remite las aclaraciones para las transferencias de datos personales fuera del territorio español.

- Códigos tipo: regula la creación, contenido y aplicación de los códigos tipo, que son todos los códigos deontológicos o de buena práctica profesional que se han creado para estandarizar la protección de datos en una empresa.

- Medidas de seguridad al tratar datos de carácter personal: deja constancia de las medidas de seguridad que se deben aplicar en ficheros automatizados y no automatizados.

- Trámites de la AEPD: regula los procedimientos que tramita la AEPD.

Para el caso del comercio electrónico, el punto que aplica de forma significativa es el relacionado con las medidas de seguridad en los ficheros de datos personales, es decir el Título VIII del Reglamento. Se establecen 3 niveles de seguridad aplicables a los ficheros de datos: básico, medio y alto.

- Nivel básico: deben estar claramente definidas y documentadas todas las funciones y obligaciones de cada usuario con acceso al fichero de datos personales. El acceso deberá realizarse de manera autenticada.

  Establece que debe existir un procedimiento de notificación y gestión de las incidencias que puedan afectar a los datos de carácter personal.

  Se deberán realizar copias de respaldo de los ficheros de datos personales, al menos una vez a la semana, siempre que en ese periodo se hayan producido cambios.

  Todos los ficheros de datos personales deberán cumplir al menos el nivel básico de seguridad.

- Nivel medio: en este nivel se mantienen todas las premisas del nivel básico.
  Se deben designar uno o varios responsables de seguridad que controlarán y coordinarán las medidas definidas en el documento de seguridad.

  Al menos cada dos años se debe realizar una auditoría interna o externa que verifique las medidas de seguridad.

  Debe existir un control de acceso físico a los soportes de los ficheros de datos de carácter personal.

- Nivel alto: se mantienen todas las medidas de seguridad de los niveles básico y medio.
  Se debe conservar una copia de respaldo de datos en algún sitio diferente de donde se encuentran los equipos informáticos que los tratan.

  De cada intento de acceso a los ficheros de datos personales se debe llevar un registro que incluya, al menos, la identificación del usuario, la fecha y hora, el fichero al que se deseaba acceder y el tipo de acceso.
  El periodo mínimo de conservación de ese registro de accesos es de, mínimo, 2 años.

  Del mismo modo, cada vez que se transmitan datos de carácter personal a través de redes públicas o inalámbricas de telecomunicaciones, se debe realizar siempre cifrando dichos datos, o en todo caso, haciendo uso de cualquier otro medio que asegure que la información no podrá ser legible ni manipulable por nadie que la intercepte.

4.4 Derechos del consumidor y privacidad

Basado en “El comercio electrónico y usted” del portal Privacy Rigths Clearinghouse, “Derechos del consumidor online” de CECARM y “Derechos del consumidor en el comercio electrónico” de Zaragoza.es

Los derechos de un consumidor de comercio online están basados en los derechos básicos del consumidor, con las particularidades propias de la tecnología empleada y la falta de presencia en las transacciones. Dichos derechos se pueden resumir es:

- Derecho a conocer la identidad de la empresa. Todo consumidor tiene derecho a ser informado de la identidad, localización y datos mercantiles de la empresa con la que está comerciando.

- Derecho a conocer los gastos de envío. El consumidor debe saber con claridad cuáles son los gastos de transporte asociados a la compra. Estos gastos deben ser comunicados siempre en el momento de la compra, no en el momento de la entrega del producto.

- Derecho a obtener una información clara, concisa y actualizada sobre el producto o servicio. La información sobre el bien o servicio a adquirir debe ser clara, unívoca y actualizada para que el consumidor pueda tomar la decisión conociendo todas las características del producto. Se deberá informar además, de las garantías legales.

- Derecho a facilitar únicamente los datos personales necesarios para la transacción. En el momento de hacer efectiva la compra, el consumidor tiene el derecho de no facilitar datos personales que no sean relevantes para la misma. Si el comerciante desea solicitar más datos personales deberá hacer la petición en otro momento y solicitando previamente el consentimiento del consumidor.

- Derecho a la protección de los datos confidenciales. Los consumidores tienen derecho a conocer el fin y la utilización de los datos confidenciales proporcionados a la empresa. Adicionalmente, el consumidor podrá, en cualquier momento, acceder a modificar o cancelar sus datos personales.

- Derecho a utilizar distintos medios de pago y que todos sean seguros. Para realizar el pago del producto adquirido, el consumidor tiene derecho a solicitar el medio de pago que más se adapte a sus necesidades dentro de los ofrecidos por el comerciante. Del mismo modo, tiene derecho a solicitar que dichos medios de pago sean seguros para realizar el pago.

- Derecho ser informado del uso de cookies. El cliente o consumidor tiene derecho a ser informado de la utilización y finalidad de cookies u otros medios de almacenamiento de datos.

- Derecho a recibir atención al cliente por medios distintos al correo electrónico. Además de la información a través del correo electrónico, el consumidor tiene derecho a recibir atención de manera directa e inmediata utilizando un teléfono o presencialmente.

- Derecho a recibir el pedido en un máximo de 30 días salvo que consumidor y comerciante hayan acordado otros plazos. Debe tenerse en cuenta que si no se respeta este plazo, el consumidor puede exigir que se le devuelva el doble de la cantidad adeudada, pudiendo solicitar, además, una indemnización por daños y perjuicios si éstos se producen (Ley 7/1998 de 13 de abril sobre condiciones generales de contratación).

- Derecho a desistir de la compra. El consumidor tiene derecho a devolver el producto adquirido dentro de un plazo de 7 días desde que lo recibe. En ese periodo, el consumidor no tiene obligación de indicar los motivos de la cancelación de la compra ni se le cargará penalización alguna. el que asume los gastos de devolución, siempre que no se hayan acordado otros términos con el comerciante. Si el comerciante decide que ciertos productos no admiten devolución, se deberá informar de forma clara en el momento de la compra.

  Existen ciertos tipos de productos que no están sujetos al derecho de disentimiento:

  - Productos o servicios con un valor fluctuante en el mercado (por ejemplo, en el caso de la adquisición de acciones bursátiles que cotizan en Mercados de Valores, nacionales o internacionales).

  - Productos o servicios generados a demanda (por ejemplo ropa a medida).

- Productos o servicios con fecha de caducidad (productos alimenticios).

- Prensa y revistas.

- Productos fácilmente duplicables (música, películas, software, etc.).

- Derecho a reparación o sustitución del producto adquirido. Los consumidores tiene derecho a solicitar la reparación o sustitución de un producto dañado o que no funcione sin tener que asumir ningún gasto adicional. La reparación o sustitución del producto debe llevarse a cabo en un plazo de tiempo razonable y sin mayores inconvenientes para el consumidor, de acuerdo con la naturaleza de los productos y de la finalidad que tuvieran para el consumidor.

- Derecho a ser informado sobre el envío de información comercial. Si el comerciante envía información comercial a través por correo electrónico, el consumidor tiene derecho a identificar dicha oferta como publicidad, por lo que deberá ser clara e indicar que se trata de publicidad.

4.5 Buenas prácticas del usuario de comercio electrónico

Basado en “La seguridad en internet: reglas de uso y derecho a la privacidad” de Colombia digital y “Derechos del consumidor en el comercio electrónico” de Zaragoza.es.

Existen una serie de normas no escritas o buenas prácticas que todo usuario debería seguir a la hora de navegar por internet y, más concretamente, a la hora de utilizar el comercio electrónico y realizar pagos por internet.

- El primer paso para hacer un pago online seguro es verificar que el dispositivo desde el que se realiza es seguro y no está afectado por ningún virus o spyware que pueda recoger la información confidencial que se va a enviar.

- Para acceder al sitio web de comercio electrónico, se recomienda teclear la dirección web, no acceder mediante ningún enlace externo o recibido por correo electrónico.

- Se debe verificar que en el navegador, la URL donde la web visitada tiene el prefijo HTTPS (o un símbolo de candado), lo cual indica que el sitio ofrece seguridad para transacciones electrónicas.

- Es importante cerciorarse de que el sitio web es fiable y de que proporciona de manera clara toda la información relacionada con la entidad comercial y mercantil.

- Es recomendable verificar que la web donde se realiza la transacción ofrece con claridad su Política de Privacidad (o Aviso Legal) donde detalla el uso de los datos personales proporcionados por los consumidores.

- También es una buena práctica buscar opiniones de otros consumidores sobre el proceso de compra y el servicio recibido. Existen guías de compra que reúnen opiniones imparciales de los consumidores sobre multitud de comerciales. Algunos ejemplos son Ciao (www.ciao.es), Kelkoo (www.kelkoo.es), Twenga (www.twenga.es) o Dooyoo (www.dooyoo.es).

- Nunca se debe enviar información personal o financiera de carácter confidencial a no ser que esté cifrada en un sitio web seguro.

- Gran cantidad de sitio web cuentan con un sello de calidad. Estos sellos de confianza son voluntarios y se constituyen como una garantía de fiabilidad y transparencia de las empresas que los ostenta y están regulados por la Ley 34/2002 (LSSICE).

  El Instituto Nacional de Consumo ha promovido el "Distintivo Público de Confianza en Línea". Con la finalidad de identificar aquellos prestadores de servicios de comercio electrónico que voluntariamente se adhieren y respetan unos determinados códigos de conducta de ámbito nacional fijados por el Estado.

  Actualmente hay tres códigos de Conducta o sellos de confianza que cuentan con el "Distintivo Público de Confianza en Línea" reconocido por el Instituto Nacional del Consumo y son:

  - Sello de Confianza Online. Promovido por la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL) y la Asociación Española de Comercio Electrónico y Marketing Relacional (AECEM). www.confianzaonline.es

  - Sello de Calidad AGACE. Promovido por la Asociación para la promoción de las tecnologías de la Información y el Comercio Electrónico (APTICE). www.agace.org

  - Sello OPTIMAWEB. Promovido por la Asociación para el fomento del Comercio Electrónico Empresarial (ANETCOM) www.optimaweb.anetcom.es

- Antes de confirmar la compra online es importante tener claro que el producto o servicio contratado cumple con las expectativas que se desean cubrir y que el coste final no conlleva sorpresas de sobrecostes adicionales.

- También se deben leer con detenimiento las Condiciones de Venta del sitio web para saber con claridad los medios de pago de los que se

dispone, los plazos de entrega, los gastos de envío y devolución del producto, etc.

4.6 Protocolos de seguridad 3DSecure

Basado en documentación de Visaeurope.com y MasterCard.com y manuales de usuario de ambas marcas, apoyado sobre el portal www.ccm.net

A la hora de realizar pagos seguros por internet, el medio de pago más habitual es la tarjeta de crédito. Dentro de este medio de pago, existes protocolos estándar de seguridad que certifican que el pago se realizad de manera segura para el comprador y para el comercio.

La tecnología 3DSecure añade al pago en línea un paso de autenticación y pretende evitar estafas en tiendas en línea, tales como fraudes de tipo CNP (Card No Present), además de dar seguridad a los clientes en sus pagos digitales.

Para realizar un pago online con tarjeta se requiere que el comprador facilite los datos de su tarjeta (PAN, fecha de caducidad y criptograma visual). Esta información es fácil de obtener de una tarjeta para posteriormente utilizarla sin que la tarjeta esté presente, por lo que resulta fácil cometer fraude.

Con 3DSecure, se solicita información suplementaria para validar el pago. Si alguien obtiene la información contenida en una tarjeta de crédito/debito o incluso si la roba, no podrá efectuar ninguna compra en las tiendas en línea que utilizan 3DSecure, ya que la persona que intenta cometer el fraude no conoce la información suplementaria que le será solicitada por el protocolo de seguridad.

Para que un pago sea en modo 3DSecure, es necesario que la tarjeta sea 3DSecure y que la tienda online soporte el protocolo 3DSecure. Si una de las

dos partes, la tarjeta o la tienda, no soporta la tecnología 3DSecure, las compras no se verán protegidas por el protocolo de seguridad.

Cuando se realiza el pago online, se sigue le procedimiento habitual de facilitar los datos de la tarjeta. Tras ello, la tienda online redirige la operación hacia un sitio web de la entidad bancaria emisora de la tarjeta donde se solicita información adicional para confirmar la autenticidad del propietario de la tarjeta. Tras ingresar esa información, se dirige nuevamente la transacción a la tienda online para confirmar el pago. De este modo, la entidad bancaria ha asegurado a la tienda online que la persona que realiza el pago es realmente el propietario de la tarjeta.

La información que se solicita para autenticar al propietario depende de cada entidad bancaria, pero las más comunes son:

- Contraseña clásica (que puede modificarse cuando el usuario desee).

- Sistema de dispositivo electrónico o token (se debe ingresar un código que varía en el tiempo, el cual expira si no se utiliza).

- Tarjeta de coordenadas (se introduce un número asignado según una fila y columna de una tarjeta que la entidad ha proporcionado).

En casi todos los sitios de compras o ventas online, se hace uso de los teclados virtuales para el ingreso de las claves personales de autenticación. La utilización de este tipo de teclados previene el fraude por keyloggers (el inglés Key = Tecla y Log = Registro).

Un keylogger es una aplicación que almacena las teclas presionadas en un archivo. Generalmente este archivo es enviado a su autor a través de Internet. No es difícil implementar un keylogger, por lo tanto muchos programas dañinos los utilizan para obtener la información que tecleamos y así poder conocer nuestras contraseñas de acceso a diversos sitios, la cuenta bancaria o la tarjeta de crédito.

Al hacer uso de un teclado virtual no es necesario pulsar ninguna tecla para introducir las claves, si no que se realiza haciendo clic sobre el teclado mostrado en pantalla. Así, los datos “se escriben” con el ratón en vez de con el teclado y no pueden ser obtenidos por el keylogger.

Legalmente, al realizar un pago con 3DSecure, la responsabilidad de dicha transacción recae sobre la entidad bancaria del consumidor, ya que ha sido el que ha confirmado la autenticidad de la persona que realiza la compra. Esa responsabilidad se transfiere directamente al consumidor, ya que debe ser el único conocedor de la información sensible para trabajar con 3DSecure.

Para identificar que un comercio participa en 3DSecure, en el portal online se exhibirá los logotipos de los distintos protocolos a los que está acogido.

Figura 14. **3D Secure**

Las marcas que antes han desarrollado este protocolo y los cuales son más usados en todos los portales online son Visa con su programa *Verified by Visa* y Mastercard con el programa *MasterCard SecureCode*.

4.6.1 MasterCard SecureCode:

Según los datos manejados por MasterCard, más del 70% de los contracargos realizados en transacciones online están asociados a las razones “Sin autorización del titular” o “Titular de la tarjeta no reconocido” y están estimados en un coste de unos 34$ por contracargo para el comercio. MasterCard SecureCode es un servicio de seguridad para proteger al usuario

contra el uso no autorizado de su tarjeta MasterCard mientras compra por Internet en los comercios participantes. Del mismo modo, reduce el número de disputas generadas, al ofrecer la posibilidad de autenticar al titular de la tarjeta en el momento de la compra, lo que minimiza los costes asociados a esos contracargos.

Para hacer uso de este programa, no es necesario obtener una tarjeta nueva, ni descargar ninguna aplicación, por lo que no hay que pagar costo alguno. Una vez inscrito en este servicio, se tendrá más confianza sabiendo que MasterCard SecureCode realiza un paso adicional de autenticación para proteger la tarjeta de los usuarios no autorizados por Internet.

Para registrar una tarjeta en MasterCard SecureCode y obtener los códigos privados a utilizar en la autenticación, se puede hacer solicitándolo a la entidad emisora de la tarjeta de forma previa a la realización de la compra, o se puede solicitar en el mismo momento de realizar el pago online. Si en el momento de realizar un pago online, se ha olvidado el Secure Code (en caso de ser una contraseña clásica), MasterCard proporcionará una pregunta secreta para confirmar el pago. Si la respuesta es correcta y el pago termina correctamente, el usuario deberá dirigirse al sitio web de inscripción y volver a generar el código seguro.

MasterCard.com ofrece una lista de todas las entidades financieras participantes en este protocolo. También ofrece un listado de todos los comercios que participan en el servicio SecureCode para que todos los usuarios tengan claridad de qué comercios trabajan con pagos seguros.

Dentro de los datos a verificar por el titular de la tarjeta se encuentra el “saludo personal”. Este dato es un mensaje que el usuario crea en el momento que se inscribe en el servicio MasterCard SecureCode. Cada vez que se realiza un pago online en un comercio participante, MasterCard SecureCode muestra el saludo personal y otros detalles de la compra. El saludo personal es su garantía que tiene el tarjetahabiente de que se está comunicando con la institución financiera que emitió su tarjeta.

MasterCard SecureCode asegura al usuario que nunca comparte los códigos privados con el comercio. El proceso es similar a ingresar el PIN en un cajero automático o ATM. Del mismo modo, todos los comercios adheridos a MasterCard SecureCode reconocen automáticamente las tarjetas inscritas también en el protocolo de seguridad para realizar así todo el tratamiento de pago seguro.

En la figura 15 se muestra el desplegable que MasterCard proporciona para obtener el SecureCode antes de verificar un pago online. Los datos que se muestran son:

- Logo del emisor de la tarjeta
- Logo del banco
- Nombre del comercio donde se realiza el pago
- Importe del pago
- Fecha de la transacción
- Número de tarjeta de crédito (sólo aparecen en claro las últimas 4 posiciones del PAN)
- Saludo personal
- SecureCode

El usuario de SecureCode debe verificar y aprobar que todos los datos suministrados sean correctos y a continuación ingresar su código de seguridad.

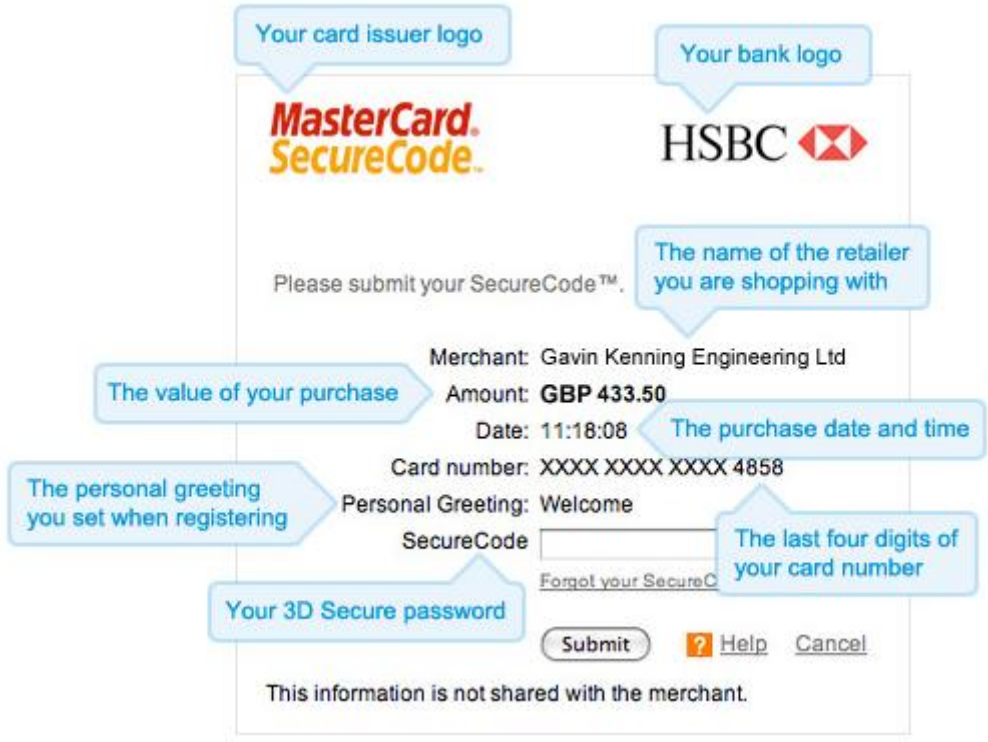


Figura 15. **MasterCard SecureCode**

4.6.2 Verified by Visa (VbV):

Verified by Visa es un programa que ayuda a verificar la identidad de un comprador online, en tiempo real, a través del uso de una clave personal. Este programa proporciona a los clientes un nivel de seguridad extra para que puedan formalizar sus compras electrónicas con mayor confianza. Los beneficios de utilizar este sistema recaen tanto en el consumidor como en el comerciante. El comerciante verá reducidos los contracargos que recibe por operaciones no reconocidas y los intentos de fraude en su comercio web.

Como consumidor, para enrolarse en el programa de pago seguro de Visa no es necesario solicitar una tarjeta nueva. El tarjetahabiente tiene la posibilidad de solicitar a su entidad financiera que vincule la tarjeta a Verified by Visa y le proporcione los códigos seguros, o puede adherirse al programa en el mismo momento que realiza la compra, ya que Verified by Visa le redirigirá a una web propia para generar sus claves personales. Una vez el consumidor tenga posesión de las claves seguras, podrá realizar los pagos con la seguridad del

programa de Visa. En el momento de adherirse al programa, se solicitará crear un “mensaje personal” que será mostrado siempre que realice un pago con Verified by Visa. El mensaje personal sólo es conocido por el tarjetahabiente y su entidad bancaria, por lo que es el método de confirmar al consumidor que se está comunicando con el emisor de su tarjeta al realizar el pago.

Desde Visa facilitan una lista de todos los comercios que están participando en su programa, para que los usuarios de Visa tengan al alcance los sitios seguros de compra con su tarjeta.

En la figura 16 se muestra el pop-up que Visa muestra para obtener el código de seguridad antes de confirmar un pago seguro. Los datos que se facilitan son:

- Logo de Verified by Visa
- Logo del banco
- Nombre del comercio donde se realiza el pago
- Importe del pago
- Fecha de la transacción
- Número de tarjeta de crédito (sólo aparecen en claro las últimas 4 posiciones del PAN)
- Mensaje personal
- Contraseña

El usuario de Verified by Visa comprobar que todos los datos mostrados son correctos antes de ingresar su código seguro.

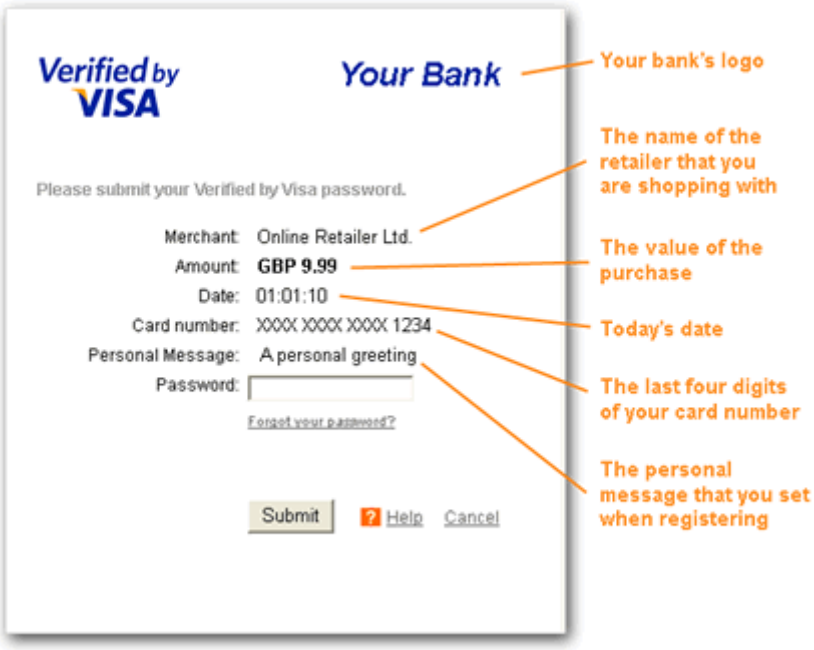


Figura 16. **Verified by Visa**

4.7 Futuro de los medios de pago

4.7.1 M-payment

Información obtenida de artículos publicados en los portales www.cnet.com, www.finanzasparamortales.es, www.mobilepaymentstoday.com, www.movilion.com, www.fayerwayer.com, www.visaeurope.com, MasterCard.com, www.isaca.org

Partiendo como base de los pagos con tarjeta, de crédito, débito o prepago, se ha desarrollado un nuevo medio de pago utilizando la tecnología NFC (Near field communication). Se trata de los mobile payments o pagos móviles.

Este nuevo medio de pago consiste en utilizar el terminal móvil como "cartera" móvil y realizar de pagos a través del teléfono móvil. Esto ofrece al comprador la posibilidad de omitir la tarjeta física y al comerciante le agiliza todo el proceso de pago electrónico.

Para que el pago se pueda realizar, el dispositivo móvil y el terminal de pago deben estar equipados con tecnología NFC. El teléfono móvil podrá contar con un chip instalado o almacenar la información de seguridad en la nube.

Después de iniciar la aplicación de pagos en el teléfono, se debe acercar al terminal de tarjetas y se realiza una conexión a través de NFC. En este tipo de pago la credencial de pago (elemento seguro) se almacena en el chip del dispositivo móvil o en la nube y se transmite de forma inalámbrica, mediante el empleo de tecnología NFC, al terminal de pago compatible. Es decir, el dispositivo móvil actúa como una tarjeta de pago sin contacto.

El usuario sólo necesita acercar el dispositivo móvil al terminal de pago y la transacción queda confirmada. Por motivos de seguridad, se ha establecido que para operaciones superiores a 20 euros se solicita el ingreso del código PIN en el terminal.

El componente más crítico en la transacción de un pago móvil es el elemento de seguridad, que contiene todo el poder de autorización. Ya sea un chip en el teléfono, o funcione desde la nube, el elemento de seguridad es a prueba de manipulaciones y está protegido por una firma digital única.

Desde PayPal se implementó un sistema que mejora aún más los pagos móviles: Beacon. Se trata de un pequeño adaptador USB que usa tecnología BLE (*Bluetooth de Baja Energía*) para saber cuando el comprador está listo para pagar sin tener que iniciar la aplicación de PayPal. El adaptador USB es para las tiendas, que se conecta directamente a un ordenador o a un adaptador de corriente.

Cuando un cliente con la aplicación de PayPal Beacon instalada en su teléfono accede a un comercio que tenga el terminal activo, éste le avisa que el establecimiento proporciona el servicio de pagos a través de Beacon. Además, realiza un registro automático en el comercio.

Al comercio, en su sistema le aparecerá el nombre y fotografía del comprador registrado. Después, si el cliente quiere, otorgará permisos al establecimiento para que le pueda cobrar productos de manera automática. Al pasar por caja, el personal del comercio identifica al comprador por la fotografía y sólo es necesaria una confirmación verbal para pagar. Automáticamente, Paypal transfiere el importe de la compra de la cuenta del cliente a la del vendedor y el primero recibirá un recibo de la transacción en su correo electrónico.

Este sistema sólo funciona cuando el móvil y Beacon están cerca, por lo que al contrario del pago con NFC, tan sólo es necesario estar más o menos cerca del punto de venta para confirmar la compra. La tecnología BLE integra cifrado AES para proteger las conexiones entre dispositivos.

4.7.2 Wearable payments

Basado en la información recogida de portales como www.paymentssource.com, www.mobilepaymentstoday.com y www.cincodias.com

La última tendencia en medios de pago puede decirse que son los pagos wearable, es decir, a través de dispositivos que el usuario lleva puestos tales como pulseras, anillos y relojes inteligentes o las google glass.

Estos dispositivos basan su actividad en el contactless, pero tienen la particularidad de ofrecer al usuario la confirmación de pagos sin utilizar su tarjeta o teléfono móvil. En un dispositivo que el cliente ya porta, se introduce la tecnología necesaria para complementarlo y que realice pagos a través de cualquier terminal de pago sin contacto.

Las primeras pulseras inteligentes con capacidad de pago online fueron creadas para festivales de música (como la creada por Barclays para el festival

British Summer Time) o parques temáticos (MagicBand implementada por Walt Disney Co.).

En España, Visa ha lanzado una pulsera inteligente en colaboración con Caixabank para realizar pagos wearables. Han puesto en circulación más de 15.000 pulseras contactless entre sus clientes, entre los que ya hayan mostrado un uso habitual de este tipo de tecnología con sus tarjetas de crédito y débito. De hecho, la pulsera es una tarjeta adicional, con los mismos datos que la principal, y como tal se registrarán sus transacciones en la cuenta del cliente.

Realmente, la pulsera, no es más que la tarjeta de crédito en forma de wearable que dentro lleva una microtag con la información cifrada de los datos para el pago del cliente y que cuenta con las mismas garantías de seguridad que los actuales medios de pago en este sentido. El cliente sólo tiene que acercar la pulsera al terminal de pago sin contacto para realizar la transacción. Esta pulsera es compatible con cualquier datáfono provisto de la tecnología contactless en todo el mundo. Para operaciones superiores a 20 euros hay que seguir tecleando el PIN de la tarjeta para confirmar la operación.

La pulsera de CaixaBank-Visa también puede utilizarse en los cajeros que cuentes con la tecnología contactless. El terminal al identificar la pulsera, solicita el PIN del mismo modo que lo solicita con una tarjeta o con un teléfono móvil.

Adicionalmente, CaixaBank ha lanzando una aplicación para el móvil con el que se pueden tener controladas en todo momento las transacciones realizadas con la pulsera.

Actualmente, los anillos y las gafas de Google no pueden ser utilizados como una tarjeta emitida por una entidad bancaria, pero pueden usarse como monedero bitcoin para realizar los pagos.

Como conclusión se puede indicar que es un medio de pago poco explotado ahora mismo, ya que los usuarios estamos completamente adaptados a los

pagos online, pero aún nos estamos adaptando a los pagos contactless con tarjeta o smartphone. Los pagos wearable son un paso más allá, que aún está pendiente de aceptación.

Capítulo 5
Aportaciones personales

5.1 Pasos a seguir para implementar un comercio electrónico

La actual situación económica está empujando a muchas personas al auto-empleo, y las tiendas virtuales se ven como una muy buena opción debido a su relativo bajo coste de lanzamiento.

A continuación, se ofrecen una serie de pautas a seguir si se desea tomar el camino del comercio electrónico como negocio, desde que surge la idea hasta confirmar la implementación del portal online:

1. **Realizar un estudio de mercado**

   El primer paso cuando se piensa en implementar cualquier tipo de comercio, es hacer un estudio amplio para determinar:

   - Producto o servicio a ofertar: hay que identificar un producto que necesite mucha gente y que además lo necesite con frecuencia. Además, se deberá conocer al detalle todo lo relacionado con el producto ofertado; no se puede crear un comercio online sin una base de conocimiento clara de lo que desea vender.

   - Nicho de mercado: una vez hay claridad sobre el producto/servicio, hay que analizar el mercado relacionado con él. Es decir, hay que ver que el nicho de mercado no esté ya saturado. Crear un sitio web de comercio electrónico en un mercado demasiado explotado y subestimar la cantidad de recursos necesarios para

comercializar y vender productos específicos online son causas de fracaso. El sector elegido debe ser estudiado y comprendido en profundidad para aumentar posibilidades de éxito.

2. Seleccionar la plataforma de comercio electrónico

A la hora de elegir la plataforma sobre la que implementar el e-commerce, hay que analizar las necesidades de la propia tienda. No hay una plataforma estándar, si no que cada tienda virtual tendrá unas necesidades distintas.

Actualmente existen plataformas “paquetizadas” que a modo de alquiler, ofrecen todo lo necesario para iniciar un e-commerce: su propia plataforma, hosting, servicios SEO, reserva de dominio, etc. Son recomendables para una primera aproximación al e-commerce, pero también tienen sus limitaciones a la hora de personalizar la experiencia, integrar sistemas internos de la compañía o migrar hacia otra plataforma si el negocio fructifica.

Figura 17. **Ejemplos de plataformas de e-commerce**

3. Costes de la implementación

Evaluar los costes de poner en funcionamiento un comercio electrónico es una tarea compleja y que no puede quedarse únicamente en la parte económica. Para hacer un análisis completo de los costes asociados, se debe evaluar tanto el coste económico como el coste en tiempo.

En relación con el tiempo, se deben evaluar los conocimientos de programación e Internet que se tienen para implementar una tienda virtual. Si no se tienen los conocimientos adecuados, los costes en tiempo pueden ser enormes, ya que son procesos muy específicos que no se aprenden rápidamente. Por tanto, si no se cuenta con esos conocimientos informáticos, es mejor ahorrar tiempo y emplear el dinero en contratar a alguna empresa experta al respecto.

El coste económico de montar una tienda online debe ser proporcional al volumen de negocio que se espera obtener. Si se emplea un presupuesto mínimo, no se puede esperar que la tienda virtual sea de la misma calidad que si se destina un presupuesto mayor. La idea de poner en funcionamiento un e-commerce de forma gratuita es algo que se debe descartar, ya que las posibilidades que ofrecerá serán mínimas y por tanto, no generará negocio.

Normalmente, los sitios web tienen estructuras muy pobres y poco profesionales y esto puede afectar las posibilidades de éxito. Por esta razón, una tienda online debe ser creada y diseñada profesionalmente para obtener mejores resultados. Los diseñadores experimentados saben lo que funciona y lo que no. Contratar profesionales para gestionar la estructura del sitio web es la clave para el éxito online.

4. Funcionalidades

Las funcionalidades de una tienda online son algo muy específico en función del mercado que se esté copando. De forma general y para una

tienda online al uso, las funcionalidades principales que se deberían cubrir son:

Diseño: el diseño de un e-commerce no es una funcionalidad del mismo, pero la apariencia y el diseño de la tienda es un aspecto importante a tener en cuenta.

No sólo ha de ser un portal atractivo y elegante, sino que debe ser usable para el usuario. Es decir, el cliente se debe sentir cómodo en la tienda y debe poder realizar las compras de la manera más sencilla posible.
Uno de los motivos por los que las personas compran en tiendas virtuales es porque quieren comprar con rapidez, fácilmente y desde la comodidad de sus casas. Cualquier tienda online que no ofrezca todo eso a sus visitantes tendrá muy pocas visitas y por tanto, pocas ventas. Habitualmente se comete el error de poner obstáculos en el proceso de compra, obligando a los clientes a efectuar acciones innecesarias, creando más pasos de los mínimos necesarios antes de llegar a la compra.

Figura 18. **Diseño en e-commerce**

Catálogo de productos: es importante incluir un catálogo de todos los productos o servicios que se ofrecen, así como fotos en vuestras fichas de producto y que esas fotos sean en alta resolución. Si se vende algo que requiera de un manual de usuario o una hoja de datos, es conveniente adjuntar un PDF descargable.

Plantear un árbol de categorías navegables y que esas categorías se reflejan en las URLs por el tema del posicionamiento web, ayudará a que los clientes naveguen con más facilidad por el portal e-commerce.

Carrito de compra: es el software utilizado para recoger los pedidos de los clientes de la tienda online. La función principal es poder almacenar todos los productos que el usuario desea adquirir, y una vez están todos seleccionados, proceder a realizar la confirmación de la compra completa y el pago de la misma. Se trata de una funcionalidad básica a día de hoy, ya que ofrece mucha comodidad a los usuarios y hace que las compras se asemejen mucho a las compras en tiendas físicas, a las que los clientes están habituados.

El carrito de la compra ha de ser eficiente, visible, rápido y sencillo de manejar para todos los posibles clientes potenciales. Además de todas estas características este carrito debe ser atractivo para incitar a la compra y para que los usuarios no se vayan a otra tienda online.

Figura 19. **Carrito de compra online**

Herramientas: una buena tienda online debe contar con herramientas de marketing y reglas de negocio, optimización para motores de búsqueda, valoraciones de visitantes, programa de afiliados (para que otros ayuden

a vender), control de inventario e incluso herramientas de cupones descuento y control de abandono de carritos.

Atención al cliente: se debe ofrecer algún medio por el que poder ayudar a los clientes en el proceso de compra o en las devoluciones. La ayuda puede ser a través de correo electrónico, pero siempre se debe ofrecer algún medio de asistencia inmediata, ya sea un teléfono o una chat instantáneo.

Seguridad: para favorecer la confianza de los usuarios y aumentar el número de ventas, el portal de e-commerce debe contar con medios de pagos seguros, conexión SSL y sellos de confianza.

Redes sociales: actualmente, es imprescindible disponer de redes sociales que apoyen la venta de productos o servicios. Además, este "social e-commerce" ayuda a evaluar el mercado en el que está inmersa la tienda online, ya que permiten, de un modo rápido, conocer las opiniones que los clientes tienen acerca de la imagen de la tienda, de la marca, de los productos, de la calidad del servicio, de la conformidad de los tiempos de envíos y devoluciones, etc.

5. Nombre de dominio y alojamiento

Una vez seleccionado la plataforma a usar y haber diseñado el presupuesto global de la tienda online, se debe decidir el nombre de dominio y el alojamiento web.

Nombre de dominio: no es más que un conjunto de caracteres alfanuméricos, que cumple un formato y normas establecidos, en la que se traduce una dirección IP de una máquina. Es decir, es la forma de referenciar la marca a vender en Internet.

Lo ideal es registrar la marca a vender como nombre de dominio, ya que es la forma más fácil de identificar los productos y la tienda online por

parte de los clientes. Un nombre de dominio ambiguo o que no referencie claramente la marca asociada, puede dar lugar a dudas a los consumidores, haciendo busquen los productos que necesitan en sitio web más claros.

También es conveniente registrar la marca como nombre de dominio no sólo a nivel regional (.com, .es, .cl, etc.), sino también el resto de dominios del tipo .net, .org, etc. Al comprar y registrar todos estos nombres de dominio, se asegura que ningún competidor va a utilizar esos dominios para robar tráfico a la tienda online.

En caso de no poder registrar la marca como dominio, se recomienda utilizar algún nombre que referencie de forma clara a los productos o servicio que se ofrecen en el e-commerce.

Alojamiento web: es un espacio virtual a donde apuntará el dominio (www.) y en el que se puede instalar y hacer visible el negocio en Internet, almacenar los correos electrónicos, foros, blog, base de datos, etc.

Elegir un alojamiento web es un asunto complicado pues, está intrínsecamente ligado a las peculiaridades propias de cada negocio. En el caso de un e-commerce, se necesitará bastante espacio para almacenar las fotos de los productos, bases de datos para almacenar la información de productos y clientes y una cierta velocidad para poder atender los picos de carga.

La recomendación es no destinar un presupuesto pequeño a este punto. Un buen servicio de alojamiento web es crítico para ofrecer una buena experiencia de usuario (velocidad de carga de la web, etc.…) a vuestros clientes. Si la tienda recibe muchas visitas y el alojamiento web no puede soportarlo, la navegación por la misma será lenta y hará que algunos clientes abandonen la compra.

Existen infinidad de compañías que ofrecen esta clase de servicios de forma individual o en pack (dominio, dominio+alojamiento,…).

Figura 20. **Alojamiento web**

6. Medios de pago

El medio de pago que se ofrezca en una tienda online puede determinar el número de ventas que se realicen. Una vez el cliente está seguro de realizar la compra, no puede cambiar de opinión porque los medios de pago que se ofrecen no son seguros o no le inspiran confianza.

Para ello, se deben ofrecer al menos dos medios de pago distintos: el terminal de pago virtual y un proveedor de pago electrónico (tipo Paypal).

Conseguir un terminal de pago virtual es algo complejo, ya que lo tiene que proporcionar una entidad bancaria y los plazos que manejan para ello son bastante amplios. Sin embargo, para comenzar, la opción de incluir como medio de pago Paypal es mucho más rápido y los clientes están ya muy familiarizados con este proveedor. Hay que tener en cuenta que Paypal cobra una comisión por cada transacción que efectúa, por lo que no se debe perder de vista la opción de incluir un terminal de pago virtual.

7. Aspectos legales

Quizá este sea el punto más importante a la hora de levantar cualquier tipo de negocio. Hay que estar completamente al día y bien informado sobre las leyes que se deben cumplir, los artículos que aplican a cada tipo de comercio y las posibles medidas sancionadoras en caso de incumplimiento.

En el caso del comercio online, se deben contemplar y tener en cuenta las siguientes leyes y normas:

- LOPD: es la ley que regula la protección de los datos personales y confidenciales de todo individuo. Si la tienda virtual registra personas físicas, datos personales, etc.… se deberá dar de alta la tienda en la AEPD (Agencia Española de Protección de Datos).

- RLOPD: es el Reglamento de la LOPD y sus aplicaciones para el tratamiento de datos confidenciales. Se debe prestar atención al punto relacionado con las medidas de seguridad en los ficheros de datos personales.

  Al manejar datos personales dentro de la gestión de clientes del comercio electrónico, se debe establecer el nivel de seguridad que se va a aplicar sobre los ficheros que contienen esa información confidencial. En función a ese nivel de seguridad se deberán seguir unas pautas de seguridad más o menos restrictivas (detalladas en el punto 4.3). Como mínimo, en el documento de seguridad que exige este reglamento, se deben dejar claras las normas, reglas y estándares que garantizan la seguridad de los ficheros. Adicionalmente, hay que crear unos procedimientos de notificación, gestión y actuación ante las incidencias, así como de realización de copias de respaldo y recuperación de datos. También hay que reflejar las medidas para el transporte y/o destrucción de los documentos y soportes.

- LSSI: como comentamos anteriormente, es la ley que regula todos los servicios de la sociedad de la información y del comercio electrónico. Si la tienda online dispone de publicidad y se cobra por ello, ha de ser transparente en cuanto a información de contacto, spam, …

- Ley de Ordenación del Comercio Minorista: esta ley cubre la venta de productos a través de Internet y ayuda a informar al comprador sobre el vendedor, las formas de pago, el precio, los impuestos, etc.

- Propiedad intelectual: Los derechos de propiedad intelectual protegen los intereses de los creadores de cualquier creación del intelecto humano. Por tanto, toda creación propia debe ser registrada para evitar plagios; así como se debe tener contemplado no violar los derechos de propiedad intelectual de cualquier otra persona.

- Normas de uso de la web: no es una norma establecida legalmente, pero toda tienda online debe dejar claras sus normas de uso y hacerlas llegar a todos los usuarios de forma clara y concisa. De este modo, el cliente ante cualquier compra estará perfectamente informado sobre el uso

- Condiciones de envío y devolución: tampoco se trata de ningún requisito legal, pero para evitar confusiones con los usuarios, es muy importante tener unas condiciones de envío y devolución estipuladas y publicadas en la tienda virtual. Los clientes las tendrán a su disposición siempre para cualquier consulta que deseen realizar, previa o posterior a la compra.

8. Registro de caídas del sistema y protocolos de actuación

A nivel técnico se debe tener un control de las caídas del sistema y unos protocolos o planes de contingencia definidos para tales casos. De este modo, se tendrán planificadas ciertas tareas para minimizar siempre las consecuencias y ofrecer el mejor servicio posible.

La mayoría de estas coberturas las ofrecen las plataformas de hosting, por lo que si se contrata una de ellas, se debe confirmar qué puntos cubren y qué garantías ofrecen.

- Acciones proactivas: consistirán en introducir medios para evitar caídas de las comunicaciones, de los servidores de internet, de las aplicaciones propias de la tienda virtual y de las bases de datos implicadas. Para ello es importante:

    - Contar con la instalación de un buen firewall.

    - Administrar correctamente los perfiles y permisos de los usuarios.

    - Tener la configuración adecuada de los servicios.

    - Tener al día el software implicado, instalando todos los parches y actualizaciones necesarias.

    - Mantener una réplica del sitio web como contingencia.

- Acciones reactivas: son las acciones que se llevarán a cabo durante una caída del sistema para restablecerlo cuanto antes o para ofrecer la mejor alternativa hasta que se restablezca el servicio. Algunas de estas acciones a tomar son:

    - Registrar todas las transacciones, almacenando los distintos estados por los que va pasando. Así, ante una caída se sabrá en qué punto estaba cada venta.

    - Activar la réplica del sitio web de contingencia con prontitud.

    - Disponibilizar un teléfono o soporte online para los clientes.

- Análisis de causas y consecuencias: ante una caída esporádica o recurrente del sistema, debe haber algún tipo de análisis para evaluar las causas y consecuencias de las caídas y así evitar futuros problemas similares.

Es importante tener un historial de todos los problemas acontecidos con el mayor detalle posible. Pero no sirve con tener el registro, sino que se debe dedicar algún recurso a analizarlo para sacar las conclusiones pertinentes. Tras ese análisis se decidirán las mejores medidas a implementar en el sistema (formarán parte desde ese momento de las acciones proactivas antes detalladas).

Otra tarea a realizar es la gestión de la información almacenada. Se debe evaluar qué información mantener en base de datos y cual es susceptible de eliminar, así como los plazos de almacenamiento.

9. Otros aspectos

- Marketing: el marketing es también un aspecto a considerar para que la tienda online tenga el impacto deseado. Por tanto, hay que familiarizarse con conceptos como:

    - SEO (Search Engine Optimization): optimización de los motores de búsqueda. Son un conjunto de técnicas utilizadas para aumentar el tráfico de calidad hacia un sitio web mediante la mejora del posicionamiento de un site páginas de resultados de un motor de búsqueda.

    - SEM (Search Engine Marketing): Es una forma de marketing que busca promover los sitios web mediante el aumento de su visibilidad en el motor de búsqueda de páginas de resultados.

    - Afiliación: se trata de acuerdos con otras páginas online para que pongan a la venta tus productos a cambio de una comisión.

  - Blog y creación de contenido: contar con un blog integrado en la tienda virtual y mantenerlo activo, puede hacer que le número de visitas y ventas crezca.

- Logística y envíos: es importante saber si la tienda online va a trabajar con stock o sin stock. En función a esa decisión, se deberán evaluar otras variables:

  - Sí hay stock, se debe contar con el dinero suficiente para el aprovisionamiento de cierta cantidad de artículos y su almacenaje. Por el contrario, se garantiza un mayor control en los envíos.

  - No hay stock, se puede prescindir del dinero de aprovisionamiento y almacenaje, pero hay que invertir en un buen proveedor de envíos para garantizar unos tiempos de entrega adecuados.

5.2 Estudio del comercio electrónico en Latinoamérica

El comercio electrónico en Latinoamérica todavía no está al mismo nivel de desarrollo e influencia que en España o Europa, pero se encuentra en plena expansión. A continuación se exponen algunas de las causas por las que el e-commerce en LATAM está menos avanzado y las acciones que se están llevando a cabo para dar reconducirlas.

- Diferencias sociales. En Latinoamérica, las diferencias sociales han sido siempre muy grandes, lo que hace que haya habido un gran descalabro económico entre la clase media-alta y alta y el resto de latinoamericanos. Los salarios altos se pueden asemejar a los que se reciben en España, pero los salarios medios y bajos están muy alejados de la realidad

española, lo que hace que una gran cantidad de la población no se pueda permitir un gran volumen de compras. Por este motivo, hay una gran parte de la población de LATAM que está poco familiarizada con los medios digitales. La adopción de las nuevas tecnologías en muy lenta en el continente sudamericano. Por ejemplo, el porcentaje medio de usuarios con conexión a Internet es de aproximadamente el 43%, frente al 75% de España.

Acciones emprendidas → a nivel global, Latinoamérica está sufriendo una expansión social y económica bastante importante. Mercados como el brasileño, el mexicano y el chileno están creciendo a pasos agigantados. Este crecimiento está afectando de manera significativa a casi todos los sectores, por lo que la creación de puestos de empleo cualificados está en alza. Así, al elevarse el poder adquisitivo de los países, se fomenta mucho más el comercio.
De todos modos, este es quizá el punto más complicado de corregir, ya que las diferencias económicas son las más difíciles de salvar.

- Infraestructura. Las infraestructuras que soportan los medios digitales son en general muy básicas y quedan lejos de ofrecer un servicio amplio y seguro. Brasil es el país que mejor ancho de banda posee y de todos modos, no puede cubrir el país completo. En el resto de países, suelen ser sólo las zonas metropolitanas las que cuentan con una infraestructura tecnológica bien planteada y accesible.
  En relación con los medios de pago, el uso de plataformas seguras y confiables, está poco trabajado. Hay gran cantidad de compras online que se siguen pagando contra reembolso porque los usuarios se sienten más cómodos con esa forma de pago.

  Acciones emprendidas → desde la mayoría de los gobiernos se está promoviendo la mejora de las redes móviles e infraestructuras, ya sea a nivel público o privado. Las empresas de telecomunicaciones han mejorado y ampliado la cobertura de sus redes. Al mejorar las infraestructuras, los usuarios se han animado a adquirir más dispositivos

electrónicos y móviles, ya que cuentan con un mejor servicio de acceso a Internet. Por ejemplo, la posesión de teléfonos inteligentes y tabletas por hogar en Chile creció de 12.2% en 2011 a 107.8% por ciento en 2013.
En cuanto a las plataformas de pago seguro también se ha hecho una gran inversión para mejorar la seguridad de los pagos online y para inculcar a los consumidores esta "nueva" forma de pagar.

- Logística. La logística encargada del transporte de los objetos que se compran a través de internet era escasa y no abarcaba grandes zonas, lo que hace que la entrega de los productos se dificulte y los plazos de entrega sean muy amplios.

  Acciones emprendidas → en los últimos años se han creado una importante cantidad de empresas encargadas de hacer llegar los productos a los consumidores. Además, estas compañías cubren una zona geográfica mucho más amplia, lo que es primordial en las compras online.

- Legislación. Las legislaciones latinoamericanas no contemplaban muchos de los aspectos relacionados con el comercio electrónico, o lo que es peor aún, algunas de las normativas estipuladas iban contra otras. El tema de la protección de datos y los documentos electrónicos también tardó bastante en formalizarse. Al no existir un comercio virtual desarrollado, no se dio mucha importancia a cómo regularlo.

  Acciones emprendidas → a medida que el e-commerce ha crecido, los gobiernos latinos han tenido que adaptar sus legislaciones para contemplar este tipo de comercio. La base ha sido la ley de comercio tradicional y sobre eso han realizado las acotaciones necesarias para los puntos propios de la tecnología y seguridad que forma parte del comercio online. Adicionalmente, y para fomentar el comercio electrónico, han promovido ciertas leyes que rebajan los impuestos e intereses que gravan estas transacciones. Del mismo modo, han establecido reglas de

envío y devolución de los bienes o servicios adquiridos, protegiendo así al consumidor digital y también a quien oferta los productos.

El e-commerce en números en LATAM.

El desarrollo del comercio electrónico, por las acciones llevadas a cabo que hemos detallado antes, ha dado un impulso enorme en los últimos años. De este modo, el gasto que han realizado los latinoamericanos en el año 2013 ha sido de cerca de 70 millones de dólares, por lo que se sitúan en índices muy altos dado el poco tiempo que lleva desarrollado este comercio en el continente latino.

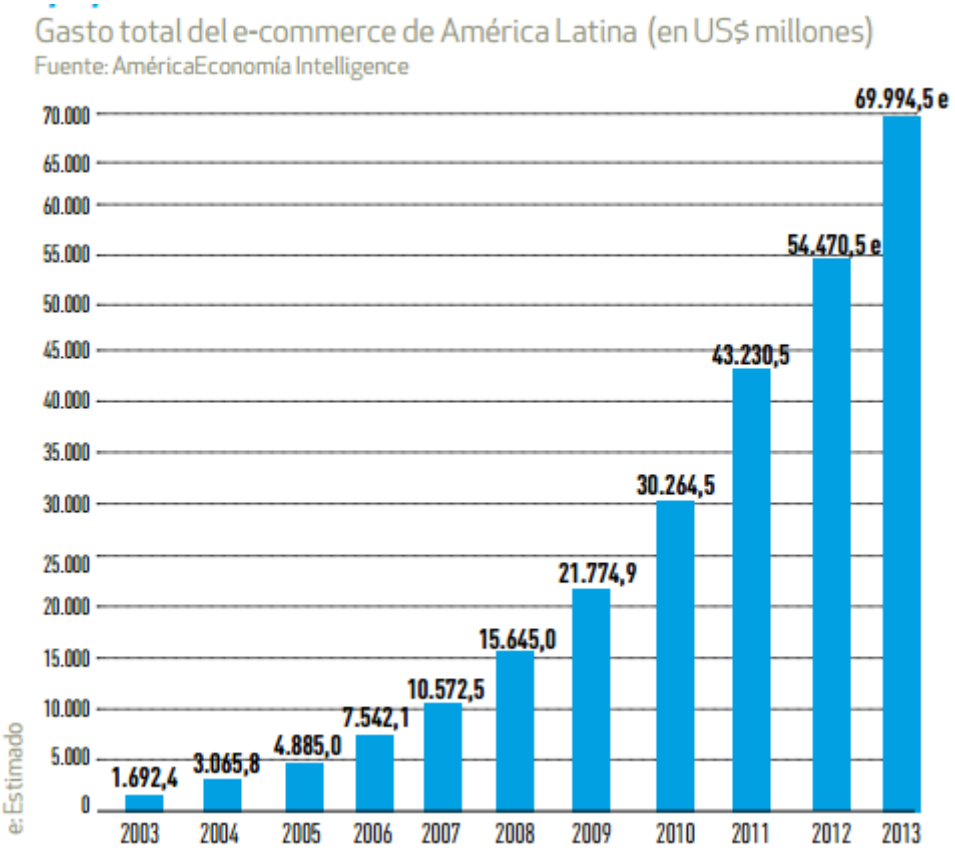


Figura 21. **Evolución del gasto online en LATAM**

Sin embargo, hablar de números en cualquier sector económico de Latinoamérica hace que siempre sea Brasil la punta del iceberg. Y por tanto, en el comercio electrónico también es así. De este modo, es Brasil el que aporta más del 59% del consumo online total de Latinoamérica.

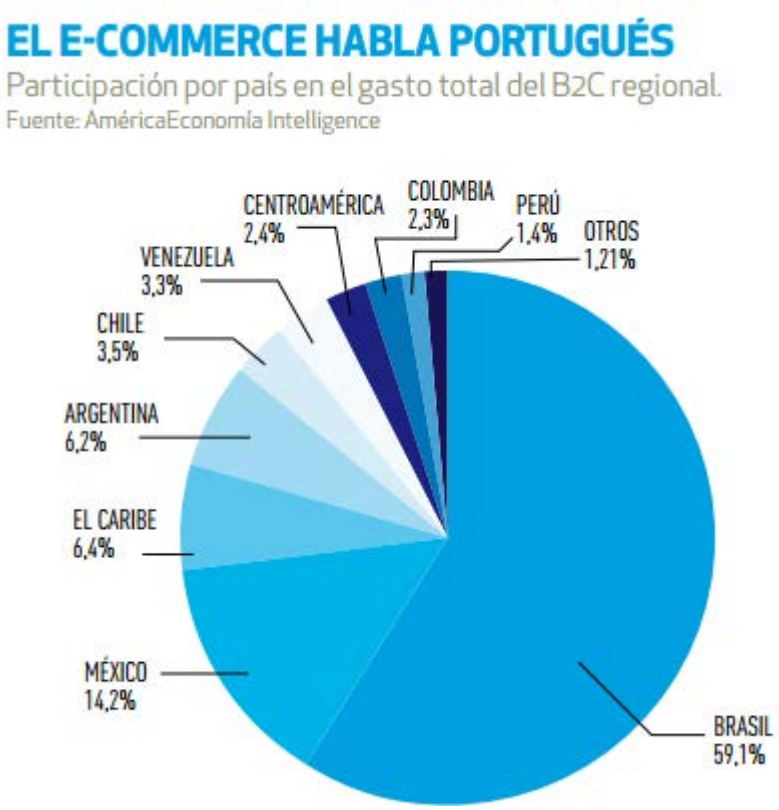


Figura 22. **Participación por país**

En cuanto a volumen de ventas B2C, Brasil se coloca a la cabeza todos los años desde 2010, abarcando siempre cerca del 50% del total de compras del subcontinente.

B2C Ecommerce Sales in Latin America, by Country, 2010-2016
billions

	2010	2011	2012	2013	2014	2015	2016
Brazil	$12.23	$16.25	$19.81	$23.07	$27.47	$29.82	$31.88
Mexico	$3.02	$3.99	$5.02	$5.88	$6.78	$7.74	$8.69
Argentina	$1.73	$2.57	$3.39	$4.34	$5.38	$6.35	$7.11
Other	$5.25	$6.89	$8.60	$10.05	$11.58	$13.20	$14.75
Latin America	**$22.23**	**$29.70**	**$36.82**	**$43.34**	**$51.21**	**$57.10**	**$62.42**

Note: includes travel, digital downloads and event tickets; excludes online gaming; numbers may not add up to total due to rounding

Figura 23. **Ventas online por país**

Si hablamos del tipo de productos que más se consumen en Sudamérica de forma online, se aprecia que difiere un poco frente a lo que se compra online en

España. En el caso de los latinos, en primer lugar compran ropa, seguido por electrónica (software y hardware, música, electrodomésticos, etc.). Los billetes de transporte o para eventos de entretenimiento están por detrás, mientras que en España era lo más demandado.

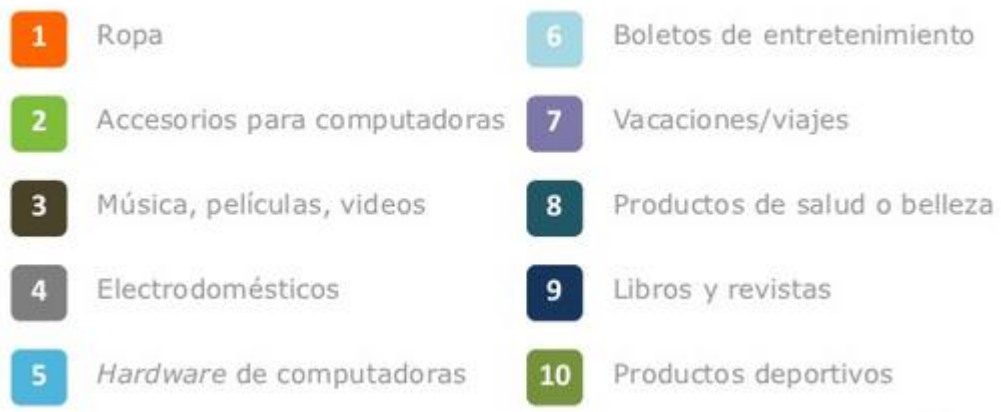


Figura 24. **Productos más comprados**

En cuanto a los medios de pago utilizados, claramente gana la partida la tarjeta de crédito. Los proveedores de medios de pago tales como Paypal o las nuevas tecnologías wearables que en España y Europa están creciendo mucho, aún no han tenido gran aceptación entre los latinos, los cuales se encuentran muy cómodos con el pago con tarjeta.

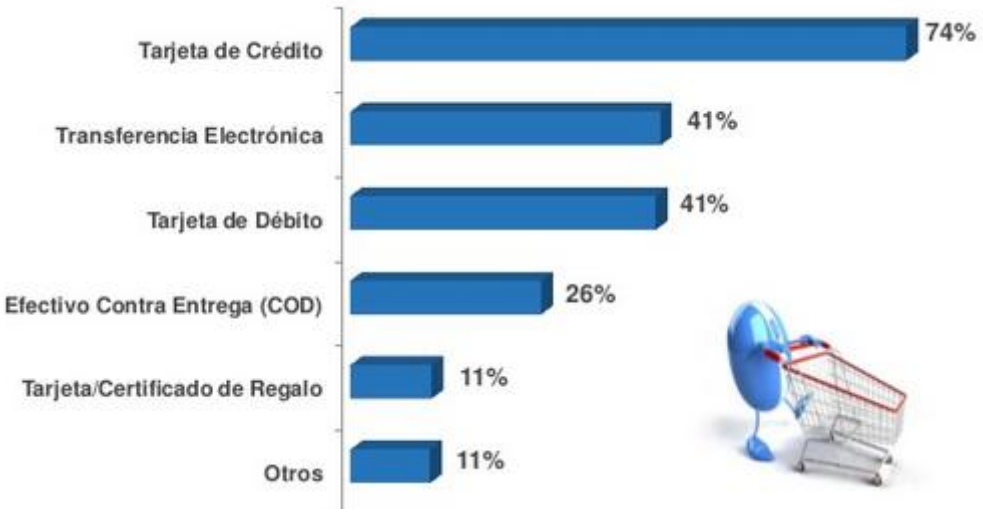


Figura 25. **Medios de pago más utilizados**

Capítulo 6
Gestión del Proyecto

En este apartado se hará un análisis de la planificación general del proyecto, del coste económico del mismo y de los recursos utilizados para llevarlo a cabo.

6.1 Planificación del proyecto

A continuación se realiza un resumen de la planificación de las distintas fases del proyecto.

1. **Fase de Planteamiento y Análisis**

   Planteamiento idea inicial PFC: determinar el tema a tratar en el proyecto.

   Identificación puntos principales: determinar el alcance del proyecto y los puntos más importantes a tratar.

   Identificación puntos secundarios: determinar qué puntos toman menos interés dentro del proyecto.

   Identificación aportes personales: determinar los puntos que aportan el toque personal al proyecto.

2. **Fase de Planificación**

   Actividades a realizar: identificar todas las tareas a realizar para la finalización del proyecto.

Recursos y tiempos disponibles: asociar a las tareas identificadas los recursos y el tiempo disponible para cada una de ellas.

3. Fase de Documentación

Recopilación de información: recopilar toda la información necesaria para cubrir todos los puntos del proyecto.

Análisis de documentación para los distintos puntos a desarrollar: identificar dentro de la documentación recopilada, la información que se manejará para los puntos del PFC, así como desechar la información no válida.

4. Fase de Desarrollo

Estructuración del documento: formatear el documento de PFC en función a los puntos a tratar.

Desarrollo Conceptos E-commerce: desarrollo de los puntos relacionados con los conceptos principales del comercio electrónico.

Desarrollo Sistemas de Pago Electrónico: desarrollo de los puntos que forman parte de los Sistemas de Pago Electrónico.

Desarrollo Seguridad Comercio Electrónico: desarrollo de los puntos necesario para complementar todo lo relacionado con la Seguridad en el comercio online.

Desarrollo aportación personal: desarrollo de la aportación personal al proyecto.

Revisión de contenidos: una vez configurados y desarrollados todos los puntos, se revisan para dar la completa conformidad.

5. <u>Fase de Entrega</u>

Una vez acabado y revisado el proyecto, y tras la aprobación del tutor, se procede a la presentación y entrega del proyecto.

6.1.1 Estimación inicial

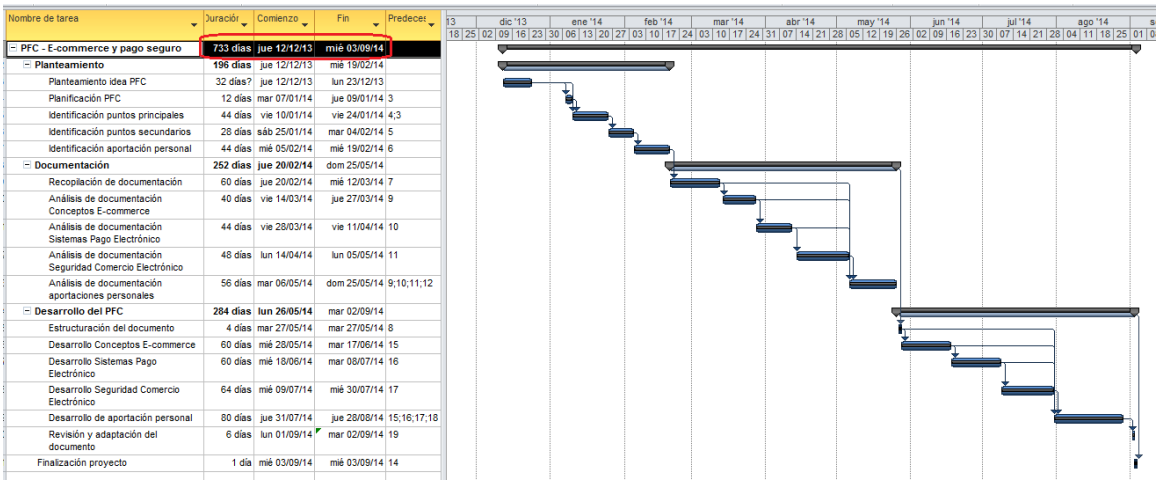
Una vez planteado el tema del proyecto e identificados grosso modo los distintos puntos a desarrollar, se realizó una estimación en tiempo y coste de la realización del mismo.

Como fecha inicial se planteó el día 12-12-2013 como comienzo del proyecto, con una dedicación de 10 horas semanales y un coste de 4€/hora. La dedicación en todas las tareas es del 100% por un único recurso.

Figura 26. **Definición de horario laboral estimado**

A partir de ahí se estimó el tiempo de cada una de las tareas a implementar, lo que derivó en un total de 733 días para finalizar el proyecto, resultando como fecha final el 03-09-2014. Los 733 días no son días naturales, si no los calculados con la estimación de 10 horas semanales de trabajo.

Esta planificación se refleja en la siguiente carta Gantt:



Nombre de tarea	Duración	Comienzo	Fin	Predeces
PFC - E-commerce y pago seguro	733 días	jue 12/12/13	mié 03/09/14	
Planteamiento	196 días	jue 12/12/13	mié 19/02/14	
Planteamiento idea PFC	32 días?	jue 12/12/13	lun 23/12/13	
Planificación PFC	12 días	mar 07/01/14	jue 09/01/14	3
Identificación puntos principales	44 días	vie 10/01/14	vie 24/01/14	4;3
Identificación puntos secundarios	28 días	sáb 25/01/14	mar 04/02/14	5
Identificación aportación personal	44 días	mié 05/02/14	mié 19/02/14	6
Documentación	252 días	jue 20/02/14	dom 25/05/14	
Recopilación de documentación	60 días	jue 20/02/14	mié 12/03/14	7
Análisis de documentación Conceptos E-commerce	40 días	vie 14/03/14	jue 27/03/14	9
Análisis de documentación Sistemas Pago Electrónico	44 días	vie 28/03/14	vie 11/04/14	10
Análisis de documentación Seguridad Comercio Electrónico	48 días	lun 14/04/14	lun 05/05/14	11
Análisis de documentación aportaciones personales	56 días	mar 06/05/14	dom 25/05/14	9;10;11;12
Desarrollo del PFC	284 días	lun 26/05/14	mar 02/09/14	
Estructuración del documento	4 días	mar 27/05/14	mar 27/05/14	8
Desarrollo Conceptos E-commerce	60 días	mié 28/05/14	mar 17/06/14	15
Desarrollo Sistemas Pago Electrónico	60 días	mié 18/06/14	mar 08/07/14	16
Desarrollo Seguridad Comercio Electrónico	64 días	mié 09/07/14	mié 30/07/14	17
Desarrollo de aportación personal	80 días	jue 31/07/14	jue 28/08/14	15;16;17;18
Revisión y adaptación del documento	6 días	lun 01/09/14	mar 02/09/14	19
Finalización proyecto	1 día	mié 03/09/14	mié 03/09/14	14

Figura 27. **Planificación inicial del proyecto**

En relación con la cantidad de horas estimadas en la realización completa del proyecto, serían unas 1.366 horas.

Nombre del recurso	Trabajo	gregar nueva column
Lidia	1.366 horas	
Planteamiento idea PFC	*64 horas*	
Planificación PFC	*24 horas*	
Identificación puntos principales	*88 horas*	
Identificación puntos secundarios	*56 horas*	
Identificación aportación personal	*88 horas*	
Recopilación de documentación	*120 horas*	
Análisis de documentación Conceptos E-commerce	*80 horas*	
Análisis de documentación Sistemas Pago Electrónico	*88 horas*	
Análisis de documentación Seguridad Comercio Electrónico	*96 horas*	
Análisis de documentación aportaciones personales	*112 horas*	
Estructuración del documento	*8 horas*	
Desarrollo Conceptos E-commerce	*120 horas*	
Desarrollo Sistemas Pago Electrónico	*120 horas*	
Desarrollo Seguridad Comercio Electrónico	*128 horas*	
Desarrollo de aportación personal	*160 horas*	
Revisión y adaptación del documento	*12 horas*	
Finalización proyecto	*2 horas*	

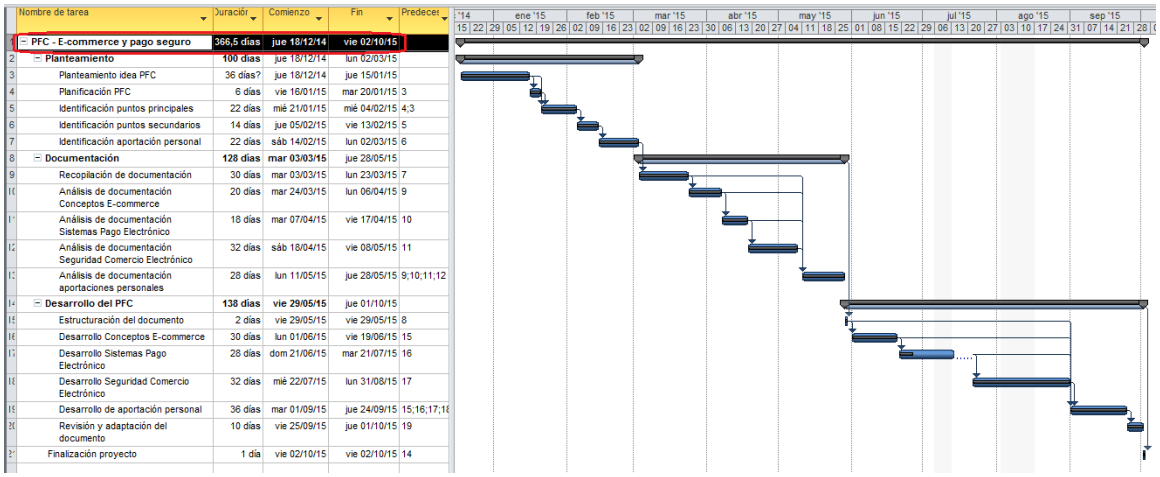
Figura 28. **Estimación inicial en horas**

Por tanto, calculando a 4€/hora, el coste estimado del proyecto sería de **5.464€.**

6.1.2 Planificación real

Como en todos los proyectos reales, la planificación inicial suele diferir con respecto al resultado final.

En este apartado se reflejan las fechas reales de cada una de las tareas. El inicio del proyecto realmente se llevó a cabo el 18-12-2014, lo que hizo que la finalización del proyecto se retrasara y llegara a fecha de 02-10-2015.



	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	PFC - E-commerce y pago seguro	366,5 días	jue 18/12/14	vie 02/10/15	
2	Planteamiento	100 días	jue 18/12/14	lun 02/03/15	
3	Planteamiento idea PFC	36 días?	jue 18/12/14	jue 15/01/15	
4	Planificación PFC	6 días	vie 16/01/15	mar 20/01/15	3
5	Identificación puntos principales	22 días	mié 21/01/15	mié 04/02/15	4;3
6	Identificación puntos secundarios	14 días	jue 05/02/15	vie 13/02/15	5
7	Identificación aportación personal	22 días	sáb 14/02/15	lun 02/03/15	6
8	Documentación	128 días	mar 03/03/15	jue 28/05/15	
9	Recopilación de documentación	30 días	mar 03/03/15	lun 23/03/15	7
10	Análisis de documentación Conceptos E-commerce	20 días	mar 24/03/15	lun 06/04/15	9
11	Análisis de documentación Sistemas Pago Electrónico	18 días	mar 07/04/15	vie 17/04/15	10
12	Análisis de documentación Seguridad Comercio Electrónico	32 días	sáb 18/04/15	vie 08/05/15	11
13	Análisis de documentación aportaciones personales	28 días	lun 11/05/15	jue 28/05/15	9;10;11;12
14	Desarrollo del PFC	138 días	vie 29/05/15	jue 01/10/15	
15	Estructuración del documento	2 días	vie 29/05/15	vie 29/05/15	8
16	Desarrollo Conceptos E-commerce	30 días	lun 01/06/15	vie 19/06/15	15
17	Desarrollo Sistemas Pago Electrónico	28 días	dom 21/06/15	mar 21/07/15	16
18	Desarrollo Seguridad Comercio Electrónico	32 días	mié 22/07/15	lun 31/08/15	17
19	Desarrollo de aportación personal	36 días	mar 01/09/15	jue 24/09/15	15;16;17;18
20	Revisión y adaptación del documento	10 días	vie 25/09/15	jue 01/10/15	19
21	Finalización proyecto	1 día	vie 02/10/15	vie 02/10/15	14

Figura 29. **Planificación final del proyecto**

El primer punto que se vio modificado en la planificación real del proyecto han sido la cantidad de horas semanales que se han dedicado. Se tuvieron que aumentar a 16 horas semanales para poder finalizar a tiempo.

Figura 30. **Definición de horario laboral final**

Adicionalmente, se comprueba que el esfuerzo en días del proyecto ha resultado finalmente de 366,5 días. Esto es por el cambio de horas semanales empleadas.

Las horas empleadas realmente en esos 366,5 días han sido 1.466.

Nombre del recurso	Trabajo	Agregar nueva columna
Lidia	1.466 horas	
Planteamiento idea PFC	*144 horas*	
Planificación PFC	*24 horas*	
Identificación puntos principales	*88 horas*	
Identificación puntos secundarios	*56 horas*	
Identificación aportación personal	*88 horas*	
Recopilación de documentación	*120 horas*	
Análisis de documentación Conceptos E-commerce	*80 horas*	
Análisis de documentación Sistemas Pago Electrónico	*72 horas*	
Análisis de documentación Seguridad Comercio Electrónico	*128 horas*	
Análisis de documentación aportaciones personales	*112 horas*	
Estructuración del documento	*8 horas*	
Desarrollo Conceptos E-commerce	*120 horas*	
Desarrollo Sistemas Pago Electrónico	*112 horas*	
Desarrollo Seguridad Comercio Electrónico	*128 horas*	
Desarrollo de aportación personal	*144 horas*	
Revisión y adaptación del documento	*40 horas*	
Finalización proyecto	*2 horas*	

Figura 31. **Horas empleadas finales**

Por tanto, calculando a 4€/hora, el coste real del proyecto ha sido de **5.864€.**

6.1.3 Análisis de la planificación

Una vez revisadas las planificaciones iniciales y reales se pueden sacar las siguientes conclusiones con respecto a la gestión del proyecto:

- Cambio en la fecha inicial.

  Debido a motivos personales y profesionales, la fecha de inicio del proyecto se vio claramente afectada. En un principio estaba planificado para el 12-12-2013, pero finalmente se comenzó el 18-12-2014.
  Esto hizo que el proyecto completo se viera desplazado prácticamente un año.

- Nuevo planteamiento de horas empleadas a la semana.

  Al comenzar el proyecto con un año de retraso, tuve que plantearme nuevamente las horas semanales que debía dedicarle para poder entregarlo en las fechas estimadas.

  De este modo, en lugar de plantear 10 horas semanales, se tuvo que subir a 16 horas a la semana. Es decir, se tuvo que aumentar el esfuerzo para no comprometer el plazo.

- Replanificación de tareas.

  La duración real de la gran mayoría de las tareas ha sido similar a lo planificado originalmente. Sin embargo, ha habido algunos puntos que han variado:

  - la tarea inicial de planteamiento del proyecto fue bastante más costosa en tiempo de lo esperado: 144 horas reales frente a 64 estimada, lo que supone un aumento de hasta el 225% de la tarea.

  - El análisis de la documentación recopilada para la Seguridad del Comercio Electrónico varió desde las 96 horas planificadas a las 128 horas reales. Es decir, un tercio más de lo planificado.

  - La revisión y adaptación final del proyecto estaba planificada en 12 horas y finalmente se dedicaron 40. Por tanto, la estimación se quedó en menos de la tercera parte del tiempo que realmente se necesitó.

- La tarea relacionada con el desarrollo de las aportaciones personales también sufrió una desviación entre lo planificado y lo real. En este caso, la desviación fue positiva, ya que se emplearon 144 horas frente a las 160 estimadas. Esto supone una mejora del 10% de la tarea.

- Plazo real empleado en días naturales.

  La duración en días naturales del proyecto también se ha visto modificada entre la estimación inicial y la finalización real del mismo.

  En la estimación inicial, comenzando el proyecto el 12-12-2013, se esperaba finalizarlo el día 03-09-2014, lo que suponía 265 días.

  Por el contrario, en la planificación real del proyecto, comenzando el 8-12-2014 y finalizando el 02-10-2015, han transcurrido 288 días naturales.

  De este modo, en días naturales ha habido una desviación de 23 días.

- Esfuerzo realizado en horas.

  Tras la revisión de horas semanales empleadas y la replanificación de algunas tareas, el esfuerzo en horas ha variado de las 1.366 horas estimadas a las 1.466 horas reales empleadas.

  Por tanto, estos cambios en la planificación del proyecto han tenido un impacto negativo de 100 horas.

- Coste en importe.

  Finalmente, la variación en horas empleadas se puede traducir en dinero. El coste planificado era de 5.464€, pero al aumentar las horas dedicadas, el coste subió hasta los 5.864€.

  Esto hace que todas las deviaciones de planificación y gestión hayan provocado unas pérdidas de **400€.**

6.2 Recursos empleados

6.2.1 Recursos hardware

Detalle de los recursos hardware utilizados para realizar el proyecto:

RECURSO	NOMBRE
Ordenador portátil	Ordenador HP Probook 6460b
Impresora	Impresora HP Universal Printing PCL

Tabla 1. **Recursos hardware**

6.2.2 Recursos software

Detalle de los recursos software de los que se ha hecho uso:

RECURSO	NOMBRE
Sistema Operativo	Windows 7
Navegador Internet	Google Chrome
Procesador de Texto	Microsoft Word 2007
Gestor de proyectos	Microsoft Project 2010
Gestor hojas de cálculo	Microsoft Excel 2007
Gestor de diapositivas	Microsoft Power Point 2007

Tabla 2. **Recursos software**

6.3 Balance económico

En el siguiente punto se hace un resumen de los costes económicos derivados de la realización del proyecto. Los distintos costes se han diferenciado en:

- **Costes humanos**: aplicados por la dedicación de las personas involucradas en el proyecto.

PUESTO	COSTE/HORA	TOTAL HORAS	COSTE TOTAL
Lidia Parrilla	4€	1.366	5.464€
TOTAL			**5.464€**

Tabla 3. **Costes humanos iniciales**

PUESTO	COSTE/HORA	TOTAL HORAS	COSTE TOTAL
Lidia Parrilla	4€	1.466	5.864€
TOTAL			**5.864€**

Tabla 4. **Costes humanos reales**

- **Costes materiales**: recursos materiales utilizados en la realización del proyecto.

RECURSO	COSTE	% DEDICADO PROYECTO	USO (MESES)	PERIODO DEPRECIACIÓN	COSTE TOTAL
Ordenador portátil	906€	100	8,33	48	157,23€
Microsoft 2007	130€	100	8,33	48	22,56€
TOTAL					**179,79€**

Tabla 5. **Costes materiales iniciales**

RECURSO	COSTE	% DEDICADO PROYECTO	USO (MESES)	PERIODO DEPRECIACIÓN	COSTE TOTAL
Ordenador portátil	906€	100	9,6	48	181,2€
Microsoft 2007	130€	100	9,6	48	26€
TOTAL					**207,2€**

Tabla 6. **Costes materiales reales**

- **Otros costes**: Otros costes asociados a la finalización del proyecto.

TIPO	EMPRESA	COSTE TOTAL
Material de oficina		50€
TOTAL		**50€**

Tabla 7. **Otros costes iniciales**

TIPO	EMPRESA	COSTE TOTAL
Material de oficina		75€
TOTAL		**75€**

Tabla 8. **Otros costes reales**

A los costes ya calculados se le debe añadir un 20% de costes indirectos, es decir, unos 1.138,76€ para la estimación inicial y 1.229,24€ para el presupuesto real.

Por tanto el resultado de los costes calculados en la planificación inicial sería:

PRESUPUESTO GENERAL DEL PROYECTO INICIAL	
Costes humanos	5.464€
Costes materiales	179,79€
Otros costes	50€
Costes indirectos	1.138,76€
TOTAL	**6832,55€**

Tabla 9. **Presupuesto inicial**

Debido a los cambios de planificación sufridos en la realización del proyecto, el resumen presupuestario real es:

PRESUPUESTO GENERAL DEL PROYECTO REAL	
Costes humanos	5.864€
Costes materiales	207,2€
Otros costes	75€
Costes indirectos	1.229,24€
TOTAL	**7375,44€**

Tabla 10. **Presupuesto real**

Analizando estos resultados distintos, se verifica que la replanificación del proyecto se ha visto reflejado en un sobrecoste de **542,89€**.

Capítulo 7
Conclusiones

El objetivo de estudiar el comercio electrónico y los pagos seguros por Internet se ha llevado a cabo de forma exitosa debido a lo siguiente:

El proyecto aporta ciertas claves para que los usuarios de Internet pierdan el miedo a realizar compras online, ya que muestra que los riesgos de hacerlo son mucho menores que los beneficios. Del mismo modo, han quedado patentes los principales peligros y las mejores formas de evitarlos o solventarlos, haciendo que las transacciones comerciales electrónicas resulten más accesibles para los consumidores.

La aportación legal incorpora gran valor tanto para los usuarios de e-commerce como para cualquier persona que tenga o piense tener un portal de venta online. Es muy importante estar al tanto de los aspectos legales que nos protegen y también cuales debemos cumplir. En el ámbito de Internet y del comercio virtual hay todavía un gran desconocimiento legal, la gran mayoría de nosotros perdemos el hilo de hasta dónde estamos cubiertos como usuarios y cuáles son nuestras obligaciones.

El estudio de los distintos medios de pago utilizados a día de hoy deja claro que la seguridad en todos ellos está verificada y se han realizado muchos avances en protocolos y metodologías para proteger la seguridad de los pagos realizados y de la confidencialidad de los datos que se transfieren en las transacciones.

De cara a la posible implementación de un comercio electrónico, el proyecto podría servir como guía inicial para llevarlo a cabo. Se especifican de modo teórico todos los aspectos a tener en cuenta, tanto tecnológicos, legales, de negocio o a nivel de marketing y diseño.

El acercamiento al e-commerce en Latinoamérica muestra un poco más de cerca los motivos por los que la explosión de estas transacciones electrónicas se ha dado más tarde que en Europa y también qué han tenido que hacer para poder retomar el ritmo perdido.

En cuanto a futuros proyectos que puedan partir de este, creo que sería interesante seguir investigando en las nuevas tecnologías de medios de pago "para llevar". Aunque todavía están en pleno desarrollo y aún no están introducidas en el día a día de todos los usuarios, parece que los pagos wearables van a estar muy en auge en un periodo corto de tiempo. Por tanto, sería interesante hacer un seguimiento a la tecnología utilizada y a la seguridad que se le aplique.

También sería un buen punto de partida para hacer un mayor estudio del comercio online en LATAM y del desarrollo de herramientas para su desarrollo. El avance de estas transacciones están dando un salto exponencial en los últimos años y con el desarrollo económico tan grande que están experimentando, es digno de estudio qué van a desarrollar en este ámbito, cómo los usuarios se van a adaptar a las nuevas tecnologías y también cómo los gobiernos van a fomentarlo.

Capítulo 8
Referencias y bibliografía

A continuación se detallan los libros, sitios web y demás documentos que han sido utilizados para la realización del proyecto (ordenados alfabéticamente por el nombre del libro o referencia tomada):

- Oficina de Seguridad del Internauta. *"Aprendiendo a identificar los phishing".* Septiembre 2015.

- Magento Infographics. *"Buying on the Internet".* Septiembre 2015.

- Revista Contribuciones a la Economía. *"Comercio electrónico".* Julio 2012.

- UPM. *"Cómo construir aplicaciones seguras en el Negocio Electrónico. El caso de los ERPs".* XI Edición, Septiembre 2012.

- Kalakota, Robinson, Addison, Robinson, Wesley, Pearson Educación. *"Del E-Commerce al e-business".*

- Oficina Municipal de Información al Consumidor Zaragoza. *"Derechos del consumidor en el comercio electrónico"* http://www.zaragoza.es/contenidos/. Diciembre 2013.

- Negocio electrónico de la Región de Murcia. *"Derechos del consumidor online"* http://www.cecarm.com. Septiembre 2015.

- Real Academia de la Lengua Española. "*Diccionario de la Lengua Española"* (http://www.rae.es). Edición 2015.

- *"Diferencias entre e-commerce y e-business"* http://www.internetnegocios.com/. Septiembre 2015.

- Cetelem-Nielsen. *"El comercio electrónico en España".* Edición 2014.

- Privacy Rights Clearinghouse. *"El comercio electrónico y usted".* Septiembre 2015.

- ONTSI. *"Estudio B2C 2013".* Edición 2014.
- Kalakota, Robinson. *"E-business 2.0: Roadmap for Success".* Edición 2000.
- AECE. *"Firma electrónica".* Septiembre 2015.
- Portal Administración Electrónica (gobierno de España). *"Firma electrónica".* Septiembre 2015.
- Universidad de Jaén. *"Firma electrónica".* Septiembre 2015.
- Invesp Infographics. *"How big is e-commerce industry".* Julio 2011.
- Merchant Accounts. *"How online credit card processing works".* Septiembre 2012.
- Mastercard. *"SecureCode: Issuer Implementation Guide".* Diciembre 2011.
- Naranjo, Laura. *"La Banca electrónica abarata los costes y fideliza las pymes".* Septiembre 1998.
- Feria Domínguez, José Manuel. *"La banca en Internet: riesgos implícitos".* Octubre 2000.
- Charro Pastor, Alberto Manuel. *"La Función de Tesorería en la Empresa, Banca Electrónica y Cash Management".* Boletín de Estudios Económicos, Vol. 1.1, nº. 157, Abril 1996
- Colombia digital. *"La seguridad en internet: reglas de uso y derecho a la privacidad".* Octubre 2014.
- Adigital. "*Libro blanco del comercio electrónico*". 2ª edición, 2012.
- Guillen, Imanol.*"Los tecnicismos de 1992".* 1988.
- Ministerio de Industria, Energía y Turismo. "*LSSI".* Julio 2002.
- Steinhardt, Ricardo J.M. *"Marketelematica, La Nueva Estrategia de la Banca Electrónica".* 1986.

- Mastercard. *"MasterCard SecureCode Cardholder Interface Requirements".* Febrero 2008.

- ISACA. *"Mobile payments: Risk, Security and Assurence Issues".* Noviembre 2009.

- Payments Source. *"New wereable payment innovations"* http://www.paymentssource.com/. Septiembre 2015.

- Montoya, Andrés. *"Nuevos Servicios Bancarios. La Banca electrónica".* 1994.

- Visa. *"Protocolo Verified by Visa"* https://usa.visa.com/. Septiembre 2015.

- CCM – Comunidad informática. *"Protocolos 3D Secure".* Septiembre 2015.

- Universidad Nacional Autónoma de México. *"Phishing – la nueva amenaza".* Septiembre 2012.

- La revista informática *"Qué es la encriptación de la informática".* http://www.larevistainformatica.com/ . Septiembre 2015.

- Pérez-Ocerin, Javier. *"Realidad y Futuro de Internet en los Servicios Electrónicos Bancarios".* Noviembre 1998.

- Basle Committee on Banking Supervision.*"Risk management for electronic banking and electronic money activities".* 1998.

- Mastercard. *"SecureCode ACS Security Requirements".* Octubre 2011.

- Mastercard. *"SecureCode Member Enrollment and Implementation Guide".* Noviembre 2007.

- Guy Kawasaki. *"The Art os Social Media: Power Tips for Power Users".* Diciembre 2014.

- Volusion Infographics. *"The blueprint of a successful online shopping cart".* Septiembre 2015.

- Ecommcerce News. *"Wereable tech & Internet os Things"* http://ecommerce-news.es/. Junio 2015.

Capítulo 9
Glosario de términos y abreviaturas

AECE: *Asociación Española de Comercio Electrónico.*

AEPD: *Agencia Española de Protección de Datos.*

AES: *Advanced Encryption Standard (Estándar de cifrado avanzado).*

ATM: *Automated Teller Machine. Cajero automático.*

B2B: *Business to Business (negocio a negocio). Tipo de e-commerce en el que una empresa vende sus servicios o productos a otra empresa.*

B2C: *Business to Consumer (negocio a cliente). Tipo de e-commerce más tradicional, en el que una empresa vende sus servicios o productos a clientes individuales.*

BLE: *Bluetooth de Baja Energía*.

C2C: *Consumer to Consumer (cliente a cliente). Tipo de e-commerce que permite que las personas vendan productos a otras personas.*

CMR: *Customer Relationship Management (Manejo de las Relaciones con el Cliente).*

DNS*: Domain Name System (Sistema de Resolución de Nombres de Dominio).*

EDI: *Electronic Data Interchange.*

ERP: *Enterprise Resource Planning (Planeamiento de los Recursos de la Empresa).*

HTTPS*: Hypertext Transfer Protocol Secure (Protocolo seguro de transferencia de hipertextos).*

IDS: *Intrusion Detection System (Sistema de detección de intrusos).*

ISP: *Internet Server Provider.*

LATAM: *América Latina.*

LSSI: *Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico.*

LOPD: *Ley Orgánica de Protección de Datos de Carácter Personal.*

NFC*: Near field communication* (*comunicación de campo cercano). Tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos.*

ONTSI: *Observatorio Nacional de las Telecomunicaciones y de la SI.*

P2P: *Point to Point. Tipo de e-commerce que se da cuando dos usuarios intercambian bienes, servicios o algún valor de forma directa, sin ningún intermediario.*

PAN: *Personal Account Number. Número de tarjeta de crédito o débito.*

PIN*: Personal Identification Number. Número de identificación personal utilizado en ciertos sistemas, como el teléfono móvil o el cajero automático,*

para identificarse y obtener acceso al sistema.

PKI: *Public Key Infrastructure. Infraestructura necesaria para poder utilizar sistemas que utilizan criptografía asimétrica. Incluye: usuarios con certificados digitales, entidades de confianza, protocolos estándar para el intercambio de mensajes, formatos estándar, etc.*

POS: *Point of Service (Punto de servicio). Sistema que controla las ventas e inventarios de un negocio.*

RLOPD: *Reglamento de la Ley Orgánica de Protección de Datos de Carácter Personal*

SCM: *Supply Chain Management (Gerencia de la cadena de Suministro)*

SEM: *Search Engine Marketing (Mercadotécnia en buscadores web).*

SEO: *Search Engine Optimization (Optimización en buscadores web).*

SET: *Secure electronic transactions. Protocolo, apoyado en la infraestructura de clave pública (PKI) y requiere la autenticación de todas las partes implicadas en los pagos con tarjeta de crédito.*

SI: *Sistemas de Información.*

SSL: *Secure Sockets Layer. Permite establecer conexiones seguras a través de Internet, de forma sencilla y transparente. Consiste en interponer una fase de codificación de los mensajes antes de enviarlos por la red mediante un canal seguro.*

TIC: *Tecnologías de la Información y la Comunicación*

VbV: *Verified by Visa. Es un protocolo de seguridad para los pagos con tarjeta*

por internet.

WPKI: *Wireless Public Key Infrastructure. Es una extensión de PKI que permite ofrecer estas mismas características de seguridad en redes móviles.*

WTLS: *Wireless Transport Layer Security. Basado en el estándar SSL, se encarga de establecer conexiones seguras en redes inalámbricas al asegurar la integridad de los datos, cifrar la información y autenticar.*

Leganés a 23 de octubre de 2015

El ingeniero proyectista

Fdo. Lidia Parrilla Ortega