Universidad Nacional Autónoma De Nicaragua

UNAN-LEÓN

Tesis para optar al título de Ingeniería en Telemática.

PROPUESTAS DE PRÁCTICAS DE LABORATORIO PARA LA ASIGNATURA DE COMERCIO ELECTRÓNICO.

Autor:

- ***Br. Elving David González Olivas.***
- ***Br. Gabriel Ramón Rodríguez Jirón.***
- ***Br. Kenia del Carmen Miranda Ruiz.***

Tutor: MSC. Aldo Rene Martínez Delgadillo.

04/03/2016

LEÓN, NICARAGUA

"A Libertad por la Universidad"

Dedicatoria

Dedicamos este trabajo investigativo:

Primordialmente a nuestros padres que siempre nos han apoyado en cada momento de nuestras vidas.

A los docentes que nos brindaron su apoyo tiempo y dedicación.

También dedicamos nuestra investigación a las generaciones futuras quienes continuaran realizando investigaciones científicas en pro del desarrollo de nuestro país.

Agradecimiento.

Primero y, antes que nada, dar gracias a Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

Agradecer hoy y siempre a mi familia por el esfuerzo realizado por ellos. El apoyo en mis estudios, de ser así no hubiese sido posible. A mis padres y demás familiares ya que me brindan el apoyo, la alegría y me dan la fortaleza necesaria para seguir adelante.

Simplemente Gracias

Br: Elving David González Olivas.

Agradecimiento.

Primeramente, a Dios por haberme permitido llegar hasta este punto y haberme dado salud, ser manantial de mi vida y darme lo necesario para seguir adelante día a día para lograr mis objetivos, además de su infinita bondad y amor.

A mi madre por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada por su amor. A mi hermana y a todos aquellos que me ayudaron directa e indirectamente realizar este documento.

A mis profesores por su apoyo y motivación para la culminación de nuestros estudios profesionales, por su apoyo ofrecido en este trabajo monográfico y por haberme transmitido los conocimientos obtenidos y haberme llevado paso a paso en aprendizaje.

Br: Gabriel Ramón Rodríguez Jirón.

Agradecimiento.

A Dios porque a pesar de que muchas veces puse mis intereses por encima de ti nunca me faltaste y en ti confío. Siempre me ha ayudado a seguir adelante y por ti aún no pierdo la esperanza, sé que todos pueden decepcionarme menos tú y reconozco que sin ti no hubiese podido estar donde estoy hoy. Muchas Gracias.

A mi familia, papa tú has sido sin duda uno de los principales precursores de este logro, nunca te desesperaste e hiciste lo imposible para que yo pudiera seguir con mis estudios, creíste que podía y siempre te preocupaste por lo que estaba haciendo, eso me mantuvo firme las veces que pude tambalearme; sé que muchas veces tenemos desacuerdos pero quién no los tiene, salimos adelante y así será siempre .Mami, tú también te mantuviste ahí, tú creatividad y dedicación me sacaron a camino muchas veces y tú incondicional comprensión siempre se impuso, a pesar de todo siempre me apoyaste; muchas veces no me doy cuenta y paso por alto tus esfuerzos, pero es que si te agradeciera todo lo que haces por mí no terminaría nunca.

A mi esposo. Gracias por todo tu amor tu apoyo y paciencia conmigo te amo muchas gracias.

A nuestros profesores quienes con sus enseñanzas y sabiduría supieron guiarnos en cumplir la meta de ser profesionales en especial MSC Aldo Rene Martínez Delgadillo. Gracias.

Br: Kenia del Carmen Miranda Ruiz.

Contenido

Ilustración.

Tablas.

RESUMEN.

El comercio electrónico se está convirtiendo en unas de las formas más habituales de realizar las compras. Los usuarios de Internet están más familiarizados con los procesos de alta en foros, portales y tiendas. Se está perdiendo el miedo a Internet.

Hoy en día existen numerosos sistemas de pago que son 100% fiables, como son los TPVs virtuales de los distintos bancos o el sistema PayPal (altamente extendido). Si la tienda online muestra claramente datos fiscales, información sobre el proceso de compra/ventas, tablas de gastos de envío, conseguiremos ganar la confianza del usuario.

Su mercado se abre a millones de usuarios de Internet y da la posibilidad a aquellos compradores que no tienen acceso a productos como el suyo en sus zonas de residencia.

Tener una tienda online puede ser de gran ayuda para un negocio. En la actualidad, existe un gran número de plataformas de E-Commerce que facilitan las transacciones entre empresa y cliente.

Una plataforma de comercio electrónico es un software que sirve para crear una tienda online y vender tus productos a través de Internet. En algunos casos, para implantarla, ni siquiera es necesario tener conocimientos de programación o diseño. La mayoría son de código abierto y tienen una versión gratuita, así que no se necesita grandes cantidades de dinero para crear una tienda online, es suficiente con pagar el hosting y quizá algún módulo adicional para habilitar alguna funcionalidad especial.

El gran desarrollo que han alcanzado las plataformas de E-Commerce, permiten estandarizar esta labor mediante una interfaz visualmente agradable y muy funcional para los clientes, además de una fácil administración y gestión para las empresas. De esta manera, una plataforma cuenta con dos vistas: una para la administración de contenidos y otra para la visualización de la tienda de parte de los usuarios, ambas conocidas como: Back-end y Front-end, respectivamente.

El Back-end: Corresponde al módulo de administración de la tienda virtual, también llamado vista del administrador. En esta vista, el administrador del comercio puede dar de alta los productos, definir precios, promociones, administrar niveles de usuarios, ver estadísticas, tendencias, etcétera.

El Front-end: Corresponde a la tienda virtual que se despliega en el sitio, la que también es llamada vista de usuario. En esta vista, los clientes interactúan y realizan compras en el comercio a través de la tienda virtual. Aquí, se pueden desplegar los productos, precios y promociones.

En nuestro trabajo monográfico implementaremos una serie de prácticas con el uso de plataformas de comercio electrónico (Magento, OpenCart, OsCommerce) donde crearemos una tienda virtual desde cero la cual le agregaremos las categorías que necesitaremos para nuestro negocio, sus productos, sus clientes, métodos de pago, compras etc. Con lo cual queremos que quede demostrado cómo funciona el comercio electrónico, como se lleva a cabo la compra y venta del producto deseado. Todo esto lo hicimos con el fin de darle una actualización al componente curricular de comercio electrónico de la carrera de Ingeniería en Telemática.

1 INTRODUCCIÓN.

1.1 Antecedentes.

El presente trabajo monográfico tiene como primer antecedente un Trabajo de Fin de Carrera, titulado **"Comercio Electrónico"**, elaborado por los Br. Luis Salvador Matamoros Cáceres; Br. Lester Israel Gutiérrez Vílchez y Br. William José Osejo Palma. El documento contiene un total de 70 páginas y se crea una página web para poder vender en internet. Esta página permite que la empresa que adquiera esta aplicación pueda promover y vender sus productos. En la creación de estas aplicaciones hicieron uso de ASP (Pages Active Server) la cual es una tecnología diseñada para la creación de páginas dinámicas. El trabajo fue dirigido por el Msc. Martin Ibarra Padilla, en el año 2003.

Como segundo antecedente se crea el componente curricular de Comercio Electrónico en el Plan de Estudios 2006, en ese entonces se encontraba en el décimo semestre (2do semestre de 5to año).

Como tercer y último antecedente se mantiene el componente curricular de Comercio Electrónico en la asignatura de ELECTIVA VI: Comercio Electrónico perteneciente al ciclo 8 del pensum 2011.

Teniendo como punto de referencia los trabajos antes mencionados, desarrollamos un nuevo documento en donde se proponen nuevas prácticas de laboratorios enfocado a la carrera de Ingeniería en Telemática de la UNAN-León, que cumpla con las necesidades educativas actuales para los estudiantes.

1.2 Definición del problema.

El componente curricular de comercio electrónico de la carrera de Ingeniería en Telemática de la Unan-León, juega un papel importante para el estudiantado ya q se ha vuelto una tendencia en el área de tecnología de la información (TIC's). Este componente no cuenta con documentos teóricos y prácticos actualizados.

En los años previos los docentes programaban paso a paso la creación de un sitio web, esto incluía la creación de una plantilla web hasta la creación de un carrito de compras. En la parte teórica presentaban muy poca documentación haciendo que el estudiante no posea muchos conocimientos para la solución de las prácticas de laboratorio. Otra forma en que solucionaban la problemática era la realización improvisadas de proyectos de laboratorio poco convencionales a las tecnologías actuales.

Como con secuencia hace que en dicho componente curricular no se aplique el uso de tecnologías más actuales y esto causa que los estudiantes queden estancados en desarrollar las prácticas de la misma manera, es por esta razón que decidimos realizar propuestas de laboratorios haciendo uso de tecnologías más actuales, que serían plataformas web y realizar un documento con conceptos más actuales y extendidos del comercio electrónico.

Frente a los hechos nos surgen las siguientes interrogantes.

Pregunta general:
¿Sería necesaria la realización de un nuevo documento donde quede expuesta la actualización tanto teórica como práctica de dicho componente curricular?

Preguntas específicas:
¿Será necesario desarrollar un plan de prácticas de laboratorio relacionadas con la utilización de plataformas del comercio electrónico para la carrera de Ingeniería en Telemática del Departamento de Computación de la UNAN-León?

¿Qué secuencia deben de llevar la realización de estas prácticas de manera que le permita al estudiante un orden para la implementación de una tienda virtual para llevarlo a una mejor compresión de los conocimientos que ha adquirido a lo largo del curso?

1.3 Justificación.

En base a los problemas antes planteados se hace necesaria la creación de un nuevo documento donde se plasme información teórica y práctica del componente curricular de comercio electrónico que les permita a los estudiantes tener una visión más actual de las tecnologías usadas en el comercio electrónico.

Nuestro trabajo monográfico está basado en propuestas de prácticas de laboratorio del comercio electrónico. Primeramente, realizaremos una serie de guías prácticas de laboratorio haciendo uso de tecnologías más actuales (plataformas web), de forma más sencilla, segura y fiable donde quede plasmado la implementación actual del comercio electrónico.

Demostraremos:
¿Cuál plataforma es la más ideal a utilizar? ¿Cómo realizar una compra segura en el comercio electrónico? ¿Cómo se realiza las transacciones en ambos lados (compra/venta)? Son una de las tantas dudas que pretendemos dar solución en la realización de las guías prácticas de laboratorio que desarrollaremos.

1.3.1 Originalidad.

Anteriormente no se ha desarrollado ningunas prácticas de laboratorios haciendo uso de plataforma de comercio electrónico, con el fin de fomentar una implementación actualizada del comercio electrónico, demostrando así una simulación de cómo se realiza la compra y venta de productos online en la tienda virtual creada en las prácticas de laboratorio.

1.3.2 Alcance.

El uso de plataformas web permitirá tanto a los estudiantes como docentes:

- Llegar a tener un documento lo más completo para el componente curricular de comercio electrónico.
- Que el alumno quede claro cómo trabaja el comercio electrónico, como funciona, como se realiza la compra y venta, como hacer reclamos, etc.
- Creación de una tienda virtual en el cual se hará uso de una plataforma web.

1.3.3 Producto.

El resultado de este proyecto es mostrar una forma sencilla y actualizada donde el estudiante y docente hagan uso de una plataforma de comercio electrónico dejándole claro su función e implementación. Para ello tenemos que tomar en cuenta los siguientes aspectos:

- **Integridad:** Porque es necesario que la información se mantenga inalterable a menos que sea modificado por el usuario autorizado previamente.

- **Escalabilidad:** Dejar siempre abierta la posibilidad de agregar más funcionalidad sin afectar a lo que ya estará desarrollado.
- **Estabilidad:** Porque el usuario debe poder realizar sus peticiones de la información de manera eficaz y con eficiencia.

1.3.4 Impacto.

El desarrollo de estas prácticas de laboratorio les permitirá a estudiantes como docente hacer uso de una manera más sencilla, eficaz, fiable de implementar las nuevas tecnologías del comercio electrónico basado en las plataformas web dando una nueva experiencia más allá de lo que ha brindado en este componente curricular ya que podrá realizar todo lo que conlleva administrar una tienda virtual.

1.4 Objetivos.

1.4.1 Objetivos Generales.

- Crear propuestas de prácticas de laboratorio correspondiente a la asignatura de Comercio Electrónico para la carrera de Ingeniería en Telemática, Departamento de Computación de la UNAN – León.

1.4.2 Objetivos Específicos.

- Implementar como medio de pago en las plataformas del comercio electrónico el servicio de PayPal.
- Simular una tienda virtual haciendo uso de las plataformas de Comercio Electrónico, para implementación de las prácticas que se desarrollan.
- Realizar una comparativa en cuanto a velocidad de respuesta, interfaz gráfica, simplicidad y requerimiento básicos de las plataformas de comercio electrónico utilizadas en guías prácticas de laboratorio.
- Elaborar un documento con información teórica y práctica sobre el componente curricular de Comercio Electrónico.

2 MARCO TEÓRICO.

2.1 Comercio electrónico.

2.1.1 Origen y evolución.

2.1.1.1 ***Origen.***

En líneas generales, y con un sentido amplio, el comercio implica la investigación de mercado con el fin de interpretar los deseos del consumidor, la publicidad que anuncia la existencia del producto, la posibilidad de adquirirlo, y en qué lugar, a la vez que se utilizan los métodos de persuasión, la venta al por menor y finalmente, la adquisición por parte del público.

Según lo expuesto, a través de los años han aparecido diferentes formas o tipos de comercio.

A principio de los años 1960 en Los Estados Unidos apareció la venta por catálogo, impulsado por las grandes tiendas de mayoreo. Este sistema de venta, revolucionario para la época, consiste en un catálogo con fotos ilustrativas de los productos a vender. Este permite tener mejor llegada a las personas, ya que no hay necesidad de tener que atraer a los clientes hasta los locales de venta. Esto posibilitó a las tiendas poder llegar a tener clientes en zonas rurales, que para la época que se desarrolló dicha modalidad existía una gran masa de personas afectadas al campo. Además, otro punto importante de esto es que los potenciales compradores pueden escoger los productos en la tranquilidad de sus hogares, sin la asistencia o presión, según sea el caso, de un vendedor. La venta por catálogo tomó mayor impulso con la aparición de las tarjetas de crédito; además de determinar un tipo de relación de mayor anonimato entre el cliente y el vendedor.

A principio de los años 1970, aparecieron las primeras relaciones comerciales que utilizaban una computadora para transmitir datos. Este tipo de intercambio de información, sin ningún tipo de estándar, trajo aparejado mejoras de los procesos de fabricación en el ámbito privado, entre empresas de un mismo sector. Es por eso que se trataron de fijar estándares para realizar este intercambio, el cual era distinto con relación a cada industria. Un ejemplo conocido de esto es el caso del Supermercado mayorista Amigazo.

A mediados de los años 1970 esta empresa desarrolló un sistema para procesar órdenes de pedido electrónicas, por el cual los clientes de esta empresa emitían ordenes de pedido desde sus empresas y esta era enviada en forma electrónica. Esta implementación trajo importantes beneficios a Amigazo, ya que se eliminaron gran parte de errores de entregas y se redujeron los tiempos de procesamiento de dichas órdenes. El beneficio fue suficiente como para que la empresa Amigazo, instale un equipo a sus clientes habituales.

Por otra parte, en el sector público el uso de estas tecnologías para el intercambio de datos tuvo su origen en las actividades militares.

A fines de los años 1970 el Ministerio de Defensa de Estados Unidos inicio un programa de investigación destinado a desarrollar técnicas y tecnologías que permitiesen intercambiar de manera transparente paquetes de información entre diferentes redes de computadoras, el proyecto encargado de diseñar esos protocolos de comunicación se llamó "Internetting

Project" (de este proyecto de investigación proviene el nombre del popular sistema de redes), del que surgieron el TCP/IP (Transmission Control Protocol)/(Internet Protocol) que fueron desarrollados conjuntamente por Vinton Cerf y Robert Kahn y son los que actualmente se emplean en Internet. A través de este proyecto se logró estandarizar las comunicaciones entre computadoras.

A mediados de 1980, con la ayuda de la televisión, surgió una nueva forma de venta por catálogo, también llamada venta directa. De esta manera, los productos son mostrados con mayor realismo, y con la dinámica de que pueden ser exhibidos resaltando sus características. La venta directa es concretada mediante un teléfono y usualmente con pagos de tarjetas de crédito.

En 1989 aparece un nuevo servicio, la WWW (World Wide Web, Telaraña Global), cuando un grupo de investigadores en Ginebra, Suiza, ideo un método a través del cual empleando la tecnología de Internet enlazaban documentos científicos provenientes de diferentes computadoras, a los que podían integrarse recursos multimedia (texto, gráficos, música, entre otros). Lo más importante de la WWW es su alto nivel de accesibilidad, que se traduce en los escasos conocimientos de informática que exige de sus usuarios.

El desarrollo de estas tecnologías y de las telecomunicaciones ha hecho que los intercambios de datos crezcan a niveles extraordinarios, simplificándose cada vez más y creando nuevas formas de comercio, y en este marco se desarrolla el Comercio Electrónico.

A finales de los años 90 el comercio electrónico era una forma emergente de hacer negocios que no era muy utilizado por las empresas en las compras o ventas de productos on-line.

Como compañías pioneras del comercio electrónico de aquel entonces cabe destacar:

- Amazon, como tienda de libros.
- eBay, como tienda de subastas electrónicas.

Negocios que proporcionaban herramientas de búsqueda: AltaVista, HotBot, Lycos y Yahoo!.

La popularidad creciente de los portales de búsqueda permitió a Google cobrar tasas cada vez más altas para los espacios publicitarios en sus páginas Web. Google adoptó el modelo de oferta de palabras clave en el año 2000 y lo utilizó para vender anuncios pequeños de texto que aparecen en las páginas de los resultados de las búsquedas realizadas a través de su portal.

Ejemplo:
Un concesionario de automóviles podría hacer una oferta en el precio de la palabra clave "coche" para las búsquedas a través del portal. Supongamos que el concesionario de automóviles era el mejor postor con 10 céntimos de euro de coste para cada clic en los anuncios. Esto significa que el concesionario pagaría por el anuncio a una razón de 12 céntimos de euro por cada visitante del sitio que clica en el anuncio.

Podemos situar el inicio del comercio electrónico a mediados de los años de 1990 cuyas fases podían quedar establecidas en la siguiente cronología:

- Primera ola del comercio electrónico. Creció rápidamente hasta el año 2000.

Descenso importante. Del año 2000-2003 se pasó del "dot-com boom" al "dot-com bust".

- Segunda ola del comercio electrónico. Recesión económica general en 2008: el comercio electrónico resultó herido, pero menos que la mayoría de los comercios tradicionales.
- Tercera ola del comercio electrónico. La aparición de los dispositivos portátiles (teléfonos móviles inteligentes, tabletas...) ofrecen la posibilidad de una nueva evolución de los negocios online.

2.1.1.2 *Evolución del internet y el comercio electrónico.*

Desde sus orígenes hasta nuestros días Internet ha revolucionado el mundo de las comunicaciones, brindando la posibilidad de interactuar desde cualquier lugar del planeta y, a un costo mínimo, la red ha ofrecido y sigue ofreciendo infinitas posibilidades. Todos estos logros se dieron a través de un proceso de evolución que se desarrolló a lo largo de distintas etapas.

A continuación, se desarrollará cada una de ellas, pero no con la finalidad de realizar un simple análisis histórico. Dado que en la actualidad tanto agentes de gobierno como empresas y particulares tienen ya una actitud tomada frente a la temática del comercio electrónico, lo que se busca es movilizarlos hacia una reflexión a los efectos que cada uno de ellos evalúe en qué etapa se encuentra y, de acuerdo a ello, se plantee sus propios desafíos para poder enfrentar exitosamente los cambios producidos por el desarrollo y desenvolvimiento del comercio electrónico.

2.1.1.2.1 Primera etapa.

La primera parte del desarrollo de Internet abarca desde su creación hasta el momento en que diversas empresas comienzan a utilizarla con fines de lucro. A partir de principios de los años sesenta, diversas universidades y el gobierno de EE.UU. buscan la forma de crear una red que transporte información digitalizada y fraccionada desde un punto a otro, a través de un sistema descentralizado.

Hacia fines de los años sesenta se puso en funcionamiento Arpanet, una red que unía a cuatro universidades dentro de EE.UU. Con el paso del tiempo se fueron integrando a dicha red nuevas instituciones y paralelamente se fueron desarrollando aplicaciones específicas con el fin de optimizar su uso. De esta manera, en 1972 se presenta por primera vez el e-mail (correo electrónico).

Como culminación de la etapa se logra la estandarización de formatos y protocolos destinados a la interconexión de diversas redes.

2.1.1.2.2 Segunda etapa.

Esta etapa se caracteriza por la ausencia de herramientas de trabajo efectivas. Si bien existían numerosas aplicaciones, no había un software confiable y estandarizado. Fuera

del ámbito gubernamental o académico se encontraban pocos medios para interactuar comercialmente en la red, los sistemas de seguridad eran simples y la infraestructura de acceso a la red estaba poco desarrollada.

Por estos motivos, grandes y pequeñas empresas se encontraban en una relativa igualdad de condiciones por lo que esta etapa pueda ser caracterizada como etapa "democrática". Al no existir herramientas para el desarrollo de páginas o de motores de búsqueda cuando se realiza una búsqueda activa sobre un tema determinado, pequeñas y grandes empresas aparecen en un mismo plano de participación.

Así, la voluntad para actuar en nuevos campos y el ingenio pasaba a ser los requisitos esenciales para incursionar en el ámbito de la red.

En esta etapa, el uso de Internet no era visto como un recurso comercial atractivo. El modo de operar estaba dado por la transferencia que las empresas hacían de su material disponible (brochures, folletería, reportes anuales, etc.) a la red. Eventualmente algunas de ellas ofertaban sus productos, pero para realizar cualquier operación comercial se debía, o bien acudir a un lugar físico o bien hacer uso del teléfono, fax u otro medio de comunicación. El alcance de Internet se limitaba, principalmente, a instituciones educativas y al gobierno. Secundariamente, algunos proveedores de servicios de acceso a la red contaban con suscriptores (personas o empresas) que la utilizaban para la publicación de determinada información o como medio de comunicación mediante la utilización de servicios como el email.

Las limitaciones del medio para ser utilizado como un vehículo eficaz del comercio, se hacían presentes con claridad.

2.1.1.2.3 Tercera etapa.

Recién a partir de mediados de los años noventa, ya dentro de una nueva etapa, tanto el hardware como el software alcanzan un mayor grado de desarrollo, haciendo posible la utilización de interfaces gráficas y ofreciendo mayor seguridad y velocidad. Esto permitió, por primera vez, una interacción real y fluida a través de la red.

Los motores de búsqueda se perfeccionaron y existe una mayor oferta de servicios on-line (América online, Compuserve, por mencionar algunos) que posibilitan que el público masivo comience a acercarse a Internet. La red deja de ser patrimonio exclusivo de científicos, gobiernos o instituciones educativas, abriéndose al público en general y a las empresas que comienzan a hacer uso de este medio publicando, viendo y comparando información.

De todas maneras, más allá de los logros que se experimentaban, Internet no dejaba de ser utilizada solamente como canal mediático adicional. No se verificaba comercio real puesto que no se percibía, dadas las dudas acerca de la seguridad en la transmisión de información, la rentabilidad o utilidad del medio.

Para comenzar a dar respuesta a esta problemática hay que abordar una nueva etapa.

2.1.1.2.4 Cuarta etapa.

Esta nueva etapa se hace presente a partir de 1995 (la fecha podría resultar arbitraria) momento a partir del cual comienza el crecimiento "exponencial" de la red. Se produce un aumento de la infraestructura disponible, contándose con mayor cantidad de recursos y mayor velocidad de acceso, a lo que hay que agregar las ventajas dadas por el software que permiten sumar sonido y movimiento, mejorando simultáneamente la seguridad de las transacciones.

En este período comienzan a utilizar agresivamente la red empresas que hoy son emblemas del comercio electrónico tales como Yahoo! (inicialmente motor de búsqueda) y Amazon.com (inicialmente venta de libros), Dell o Cisco (OCDE [1999]).

Durante 1997, Inter-Nic (compañía responsable de registrar las direcciones de los sitios en la red) reportó que se incorporaban nuevos sitios a un promedio de uno por minuto. Librerías, publicistas, firmas de servicios financieros, compradores y vendedores de todo tipo estaban inundando el espacio con sus archivos de información.

En esta etapa el comercio electrónico se desarrolla, principalmente, a través de tres vertientes que incluyen a:

- Empresas que ya mantenían lazos comerciales y que deciden utilizar la red para realizar sus operaciones comerciales y hacer uso de los medios tecnológicos disponibles para mejorar la eficiencia y fluidez de una relación comercial preexistente.
- Empresas y personas innovadoras que comienzan a realizar operaciones comerciales percibidas como no "riesgosas".
- Empresas y personas que utilizan la red para obtener información sobre bienes y servicios ofrecidos y, eventualmente, para iniciar una operación comercial.

2.1.1.2.5 Quinta etapa.

Hacia el futuro.

La adopción definitiva del medio marca la etapa final en la cual ya no existen mayores problemas de capacidad, velocidad o seguridad (a pesar de no ser percibido este hecho por el público masivo). Internet, Intranet o Extranet son usadas, según convenga, para interconectar proveedores, distribuidores y socios. El público en general utiliza el medio con regularidad.

En lo que respecta al uso de Internet como herramienta de comercio, ya no se encuentra con facilidad el antiguo espíritu "democrático". De alguna manera, la mayor o menor disponibilidad de recursos condiciona la participación de la empresa en el comercio electrónico. Para crear una Extranet que conecte empresas como las automotrices, las grandes cadenas de supermercados o de venta minorista con sus miles de proveedores, se hace necesario dedicar -a tales efectos- una gran cantidad de recursos (tiempo, dinero, recursos humanos).

Así, son diversas las maneras de poder acceder al comercio electrónico. Existen formas extremadamente sencillas como, por ejemplo, ofrecer bienes y servicios a través de

empresas preestablecidas como Yahoo!, donde por unos US$ 150 se puede ocupar un lugar en los shoppings virtuales o, a través de la creación de páginas web propias. Si bien esta última opción otorga mayor libertad e independencia, puede resultar extremadamente costosa, no sólo en lo relativo a su diseño sino también en lo concerniente a su mantenimiento y administración cotidiana.

En esta etapa son principalmente las grandes empresas las que, al decidir recuperar el espacio perdido, hacen su irrupción en el medio invirtiendo grandes sumas de dinero a través de canales publicitarios tradicionales e Internet.

Empresas como Amazon.com o CDNOW.com, por ejemplo, lograron situarse en lo más alto del podio en términos de ventas dentro de sus categorías. Ahora deben enfrentar la competencia de empresas con una mayor trayectoria en el campo del comercio tradicional. En EE.UU., cadenas de librerías (como Barnes & Noble) no sólo cuentan con sus tradicionales locales, sino que, además, disponen de un servicio de ventas en Internet en un esfuerzo por detener la erosión de su cuota de mercado producida por la aparición de tiendas de libros que sólo operan a través de la red.

Otro ejemplo del uso de medios publicitarios masivos con el fin de atraer público hacia la red ha sido dado por la marca inglesa de ropa femenina Victorias Secret que, a principios de este año, invirtió varios millones de dólares promocionando un desfile de moda transmitido en vivo a través de su página en Internet. Como resultado, diversos servidores de la red colapsaron debido a la congestión provocada por la gran cantidad de usuarios que buscaban acceder a la página de la marca (Napoli [1999]). Esto ha demostrado que sí es posible una combinación efectiva de medios de publicidad tradicionales y el comercio electrónico y que la red ya no es un ámbito totalmente democrático como lo fue en sus inicios. Ahora, a mayores recursos invertidos, mayor exposición y, normalmente, mayores ventas.

De todos modos, lo verdaderamente alentador es que la red continúa manteniendo sus características esenciales de accesibilidad e interconectividad. Cualquier empresa o persona puede, potencialmente, acceder a ella y contar con un espacio donde ofrecer sus bienes y servicios. La capacidad de poseer una página en la red, participando así de las ventajas del comercio electrónico, es básicamente la misma para una empresa cuya facturación se mide en millones de dólares que para una empresa que inicia sus operaciones y cuenta con un presupuesto limitado.

2.1.2 Definición.

Pondremos a continuación tres definiciones que nos parecen apropiadas al término Comercio Electrónico:

- "Es la aplicación de la avanzada tecnología de información para incrementar la eficacia de las relaciones empresariales entre socios comerciales". (Automotive Action Group in North America).
- "La disponibilidad de una visión empresarial apoyada por la avanzada tecnología de información para mejorar la eficiencia y la eficacia dentro del proceso comercial." (EC Innovation Centre).

- "Es el uso de las tecnologías computacional y de telecomunicaciones que se realiza entre empresas o bien entre vendedores y compradores, para apoyar el comercio de bienes y servicios."

Conjugando estas definiciones podemos decir que el comercio electrónico es una metodología moderna para hacer negocios que detecta la necesidad de las empresas, comerciantes y consumidores de reducir costos, así como mejorar la calidad de los bienes y servicios, además de mejorar el tiempo de entrega de los bienes o servicios.

Por lo tanto, no debe seguirse contemplando el comercio electrónico como una tecnología, sino que es el uso de la tecnología para mejorar la forma de llevar a cabo las actividades empresariales. Ahora bien, el comercio electrónico se puede entender como cualquier forma de transacción comercial en la cual las partes involucradas interactúan de manera electrónica en lugar de hacerlo de la manera tradicional con intercambios físicos o trato físico directo.

Actualmente la manera de comerciar se caracteriza por el mejoramiento constante en los procesos de abastecimiento, y como respuesta a ello los negocios a nivel mundial están cambiando tanto su organización como sus operaciones.

El comercio electrónico es el medio de llevar a cabo dichos cambios dentro de una escala global, permitiendo a las compañías ser más eficientes y flexibles en sus operaciones internas, para así trabajar de una manera más cercana con sus proveedores y estar más pendiente de las necesidades y expectativas de sus clientes. Además, permiten seleccionar a los mejores proveedores sin importar su localización geográfica para que de esa forma se pueda vender a un mercado global.

2.1.3 Ventajas y Desventajas del comercio electrónico.

A través del comercio electrónico se posibilita que los usuarios accedan a un mercado lleno de oportunidades desde su ordenador personal. Estas oportunidades llevan consigo tanto una serie de ventajas como de inconvenientes.

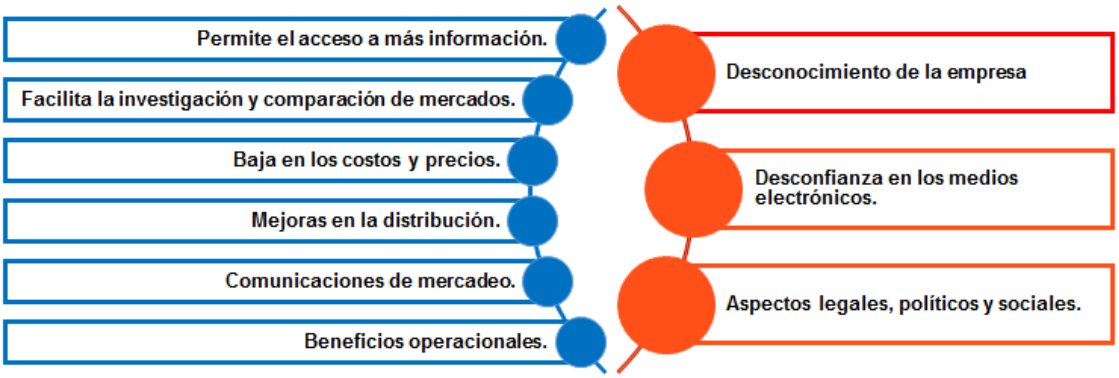


Ilustración 1: Ventajas e inconvenientes del comercio electrónico.

2.1.3.1 *Ventajas.*

Permite el acceso a más información. Al tratarse de un entorno Web permiten búsquedas profundas que son iniciadas y controladas por los clientes, por lo tanto, las actividades de mercadeo mediante el Web están más impulsadas por los clientes que aquellas proporcionadas por los medios tradicionales.

Facilita la investigación y comparación de mercados. La capacidad del Web para acumular, analizar y controlar grandes cantidades de datos especializados permite la compra por comparación y acelera el proceso de encontrar los artículos.

Baja en los costos y precios. Conforme aumenta la capacidad de los proveedores para competir en un mercado electrónico abierto se produce una baja en los costos y precios, de hecho, tal incremento en la competencia mejora la calidad y variedad de los productos y servicios.

Mejoras en la distribución. El Web ofrece a ciertos tipos de proveedores (industria del libro, servicios de información, productos digitales) la posibilidad de participar en un mercado interactivo, en el que los costos de distribución o ventas tienden a cero. Por poner un ejemplo, los productos digitales (software) pueden entregarse de inmediato, dando fin de manera progresiva a la intermediación. De igual forma se puede disminuir el tiempo que se tardan en realizar las transacciones comerciales, incrementando la eficiencia de las empresas.

Comunicaciones de mercadeo. La naturaleza interactiva del Web ofrece beneficios conducentes a desarrollar las relaciones con los clientes. Este potencial para la interacción facilita las relaciones de mercadeo, así como el soporte al cliente, hasta un punto que nunca hubiera sido posible con los medios tradicionales. Un sitio Web se encuentra disponible las 24 horas del día bajo demanda de los clientes. Las personas que realizan el mercadeo pueden usar el Web para retener a los clientes mediante un diálogo asincrónico que sucede a la conveniencia de ambas partes. Esta capacidad ofrece oportunidades sin precedentes para ajustar con precisión las comunicaciones a los clientes individuales, facilitando que éstos soliciten tanta información como deseen. Además, esto permite que los responsables del área de mercadeo obtengan información relevante de los clientes con el propósito de servirles de manera eficaz en las futuras relaciones comerciales.

Beneficios operacionales. El uso empresarial del Web permite mayor facilidad para entrar en mercados nuevos, especialmente en los geográficamente remotos, y alcanzarlos con mayor rapidez. Todo esto se debe a la capacidad de contactar de manera sencilla y a un costo menor a los clientes potenciales, eliminando demoras entre las diferentes etapas de los subprocesos empresariales.

2.1.3.2 *Desventajas.*

Desconocimiento de la empresa. No conocer la empresa o persona que vende es un riesgo del comercio electrónico, ya que muchas veces ni siquiera están constituidas legalmente en su país y no se trata más que de gente que esta "probando suerte en Internet" o tratando de estafar.

Desconfianza en los medios electrónicos. La mayoría de los usuarios no confía en la Web como canal de pago ya que desconocen que existen mecanismos y protocolos que proveen seguridad en la transmisión, autenticación, privacidad e integridad de los datos.

Aspectos legales, políticos y sociales. Existen algunos aspectos abiertos en torno al comercio electrónico: validez de la firma electrónica, no repudio, legalidad de un contrato electrónico, violaciones de marcas y derechos de autor, pérdida de derechos sobre las marcas, pérdida de derechos sobre secretos comerciales y responsabilidades. Por otra parte, deben considerarse las leyes, políticas económicas y censura gubernamentales.

2.1.4 Características.

2.1.4.1 *Transacción de bienes y/o servicios.*

El comercio electrónico por Internet, es una clase de comercio electrónico, diría el principal y de mayor importancia y, a su vez, está involucrado dentro del comercio genérico, y como abarca la comercialización de productos (tanto bienes de consumo como bienes de capital) y servicios de información, financieros y jurídicos, hasta actividades tradicionales (como asistencia sanitaria, educación) y otras actividades.

2.1.4.2 *Utilización de medios electrónicos.*

La característica principal de esta clase de comercio, es que se realiza por medio electrónico, o sistema telemático, o por algún medio de comunicación. Si esto no fuera así estaríamos ante un comercio convencional.

La contratación más frecuente es la vía Internet, debido a sus múltiples aplicaciones como son: el correo electrónico, el chat, la web (World Wide Web), etc.

2.1.4.3 *Reducción de costes de transacción.*

Los costes de transacción son los costos en los que tenemos que incurrir para celebrar un contrato. Estos incluyen los costos de negociación, los costos para encontrar información relevante, los costos de hacer cumplir los contratos, los costos de encontrar opciones adecuadas y de elegir entre ellas, entre otros.

La existencia de costes de transacción es determinante en el desarrollo de los mercados; se puede decir que los países que han desarrollado mercados dinámicos y eficientes son aquellos que han logrado reducir sustancialmente los costes de transacciones, de manera que contratar se torna menos costoso, más rápido y eficiente.

Por el contrario, si los costes de transacción son demasiado elevados entonces habrá menos contratos y con ello menor desarrollo del mercado y perdida de los beneficios que su operación podría generar a los consumidores y a las empresas.

Los costes de transacción en el comercio electrónico, se explican en el uso de la tecnología cada vez más común y al mismo tiempo más barata y asimismo por las ventajas que traen

el uso de estas tecnologías aplicadas al comercio: oferta de una variedad de servicios y productos, flexibilidad en los horarios, eliminación de desplazamientos etc.

Sin embargo, esta reducción de los costes de transacción se ve contrarrestada por la elevación de los costes de cumplimiento o "Enforcement" (seguridad en los pagos, recepción puntual de la mercancía, entrega en buen estado de la misma, etc.).

2.1.4.4 *Apertura de un nuevo mercado: "el mercado Virtual"*

En la actualidad podemos distinguir dos tipos de mercado que conviven y en algunos casos se complementan entre sí, cada uno de estos goza de características diferentes tanto en lo que se refiere a su funcionamiento como al papel de los agentes que lo componen; éstos son: el mercado tradicional o convencional y el mercado electrónico o virtual.

El mercado convencional se basa en la interacción física entre un vendedor y un comprador, también en un lugar físicamente determinado. El contacto entre ambos permite que el vendedor tenga un mayor conocimiento de las necesidades del cliente y por lo tanto pueda utilizar las herramientas necesarias para atraerlo hacia su o sus establecimientos.

Por su parte, el mercado virtual o electrónico se fundamenta en las nuevas tecnologías y, contrariamente al mercado convencional, permite que las transacciones comerciales se realicen sin importar el lugar físico donde se encuentre el comprador y el vendedor e incluso que la transacción se lleve a cabo en distintos momentos en el tiempo.

En este mercado se produce el fenómeno de la desgeografización, no existen las fronteras entre los países, todos podemos contratar, el mercado se amplía, lo cual genera una mayor demanda de los bienes o servicios y la reducción de los precios, de los mismos. En otras palabras, se puede decir que el mercado se convierte en un mercado virtual, donde la distancia geográfica de las partes, no interesa para poder contratar.

Es indudable que la globalización de los mercados y la rápida expansión de las tecnologías de la información y de la comunicación, proporcionan claros beneficios y ventajas en el comercio, pero asimismo se crean algunos riesgos, ya que dan lugar a nuevos contextos comerciales con los que las personas no están completamente familiarizadas. Los negocios de hoy dependen cada vez más de los sistemas informáticos, por lo que se han hecho particularmente vulnerable, por falta de seguridad jurídica en estas transacciones.

2.1.5 Tecnologías empleadas en comercio electrónico.

Existe un amplio rango de tecnologías que utiliza el comercio electrónico, entre ellas son:

- Intercambio Electrónico de datos (EDI- Electronic Data Interchange).
- Transferencia Electrónica de Fondos (EFT- Electronic Funds Transfer).
- Aplicaciones Internet: Web.
- Aplicaciones de Voz: Buzones, Servidores.
- Transferencia de Archivos.
- Multimedia.
- Videoconferencia.

- Tableros Electrónicos de Publicidad.

Para este proyecto nos centraremos en la tecnología de Aplicaciones de Internet, particularmente el Web, ya que éste puede utilizarse como un medio comercial ofreciendo ventajas importantes tanto para los clientes como para las empresas.

2.1.6 Algunos estándares de comercio electrónico.

El primer estándar de comercio electrónico ampliamente adoptado fue el anteriormente citado EDI, que estaba orientado a facilitar el intercambio de información entre empresas sin intervención humana, siempre que los participantes se hubieran puesto de acuerdo sobre el formato de los datos. Esto puede ocurrir entre dos empresas específicas o para un sector completo, por ejemplo, SWIFT en la banca o DAKOSY en la industria transporte.

Desarrollar estándares para sectores específicos tiene la ventaja de que se reduce sustancialmente la necesidad de implementaciones a medida, pero estos estándares realizados de forma independiente no son compatibles entre sí. Por esa razón surgió el estándar EDIFACT (EDI for Administration, Commerce and Transport), que pretende establecer reglas y un vocabulario en los que basar la descripción de los objetos de negocio, para mantener así compatibilidad entre diferentes sectores. Aunque supone un gran paso adelante, acusa un inconveniente muy importante: el coste de las comunicaciones de la red a la que todas las empresas necesitaban estar conectadas, con lo cual, el uso de estas tecnologías ha sido un lujo solamente al alcance de las grandes compañías. Con la introducción de XML se desarrolla a finales de los años noventa la fusión entre XML y EDI, que convenientemente lleva el nombre de ieXML/EDIle, un área de trabajo compatible con las infraestructuras EDI existentes que sustituye los mensajes EDI por mensajes XML, más una serie de elementos de infraestructura. Las ventajas se deben fundamentalmente al carácter auto descriptivo de XML.

La estructura del lenguaje y procesos de negocio ya existentes bajo EDI se aprovechan y al poder expresarlas en XML, y se añaden posibilidades derivadas de este hecho, como poder buscar en estos documentos, introducir referencias, auto descripción de servicios, etc. En este momento las iniciativas en el comercio electrónico se multiplican y nacen tanto líneas desvinculadas de fabricantes concretos, como ebXML o RosettaNet, e iniciativas propietarias, empujadas por empresas como Comerse One o Ariba. Éstas empujan a su vez estándares propietarios con el fin de acelerar la realización del comercio electrónico a gran escala, y de paso, tomar una posición dominante en el mercado. En esta línea se encuentran las iniciativas como xCBL (Comerse One) y cXML.

2.1.7 Principales métricas del comercio electrónico.

- **CR o Tasa de Conversión**: porcentaje de visitas a la tienda online convertidas en ventas.
- **CTR o Clic Through Rate** o porcentaje de clics o visitas que recibe una acción o campaña.
- **Coste de adquisición por lead:** presupuesto de marketing anual o coste de una campaña/número de leads conseguidos

- **Coste de adquisición por cliente:** presupuesto de marketing anual o coste de una campaña/número de clientes conseguidos.
- **Rentabilidad por cliente:** Ingreso medio por cliente.
- **Rentabilidad por canal:** análisis de la rentabilidad obtenida por canales adicionales a la tienda online. Ejemplo, campañas en BuyVip, Amazon, eBay, etc. Incluye la medición de campañas de afiliación en redes conocidas y/o campañas adhoc con afiliados seleccionados.
- **ROI:** análisis comparativo de los resultados obtenidos en los distintos esquemas de contratación: CPM / CPC / CPL / CPA.
- **Tasa de devoluciones:** porcentaje de pedidos completados y enviados que son objeto de devolución, por distintas causas (comercial, mercancía defectuosa, mercancía errónea, etc.). En el sector moda y complementos, es una métrica importante, al ser una decisión comercial en la mayoría de los casos. En el Reino Unido se manejan datos del 33%.
- **Tasa de fraude:** porcentaje del total de las transacciones o facturación de la compañía que ha supuesto una pérdida para la compañía debido a operaciones fraudulentas
- **Porcentaje de pedidos no completados.**
- **Número de reclamaciones por semana/mes/año:** número de llamadas / emails / chats recibidos relativos a reclamaciones por defectos en el producto y/o proceso de compra.

2.1.8 Factores del comercio electrónico.

2.1.8.1 *Comodidad.*

Uno de los principales factores que influyen en el auge del comercio en Internet, es la comodidad que este implica.

Imaginemos que queremos comprar o que tenemos la necesidad de hacer una compra, pero no tenemos ganas de salir a la calle o no contamos con un automóvil, el hecho del gasto del trasporte público y las incomodidades que esto implica, etc.

¿Qué pasaría si pudiéramos ir de compras desde nuestro hogar?
La comodidad de llevar esta actividad a cabo sin duda parece sumamente importante y determinante, podemos comprar artículos desde nuestra casa, contando con la información de sus características, precio etc. Es más, podemos contar con el servicio que llegue directamente a nuestras casas, y pagarlo en ese mismo instante. Es por todo ello que este es un factor que influye dentro del comercio electrónico, y por ello cada día tiene más auge.

2.1.8.2 *Seguridad.*

En el comercio cotidiano se dan factores que han permitido la transición de este, lo que lleva a algunas etapas que podemos distinguir:

- En el inicio del comercio cotidiano lo que importaba y preocupaba al vendedor era tan sólo vender en el instante y contar con un capital inmediato.

- Tiempo después parecía más importante comprometer al cliente a pagar a plazos, pues con ello resultaba más fácil vender más, aunque después se tuviera que cobrar.
- Hoy en día, la mayoría de las misiones de empresas grandes y pequeñas, es hacer que el cliente prefiera nuestro producto por sobre otros y que el cliente sea siempre fiel al producto. Pero en este proceso han aparecido varios temas que hoy por hoy aún tienen que vencer muchos obstáculos que no se han superado, como el temor de los "cyberconsumidores" hacia ellos. Como, por ejemplo:
    - Desconocimiento de la empresa: En muchos casos las "empresas" que ofrecen sus productos o servicios por Internet no están constituidas legalmente en su país y no se trata más que de gente que esta "probando suerte en Internet". Esto no quiere decir que tengan necesariamente que ser negocios fraudulentos, pero, a todos nos gusta saber y conocer a quien compramos.

2.1.8.3 *Auge y Motivos.*

Tener un sitio de comercio electrónico, bien manejado, te puede traer grandes rendimientos con muy baja inversión. Conoce algunos de los principales motivos para iniciar o complementar tu tienda con la venta online:

Disminución de costos: La mayoría de los negocios poseen costos fijos que deben ser pagados con puntualidad cada mes. Muchas veces éstos son muy altos y no se equiparán con las ventas mensuales obtenidas, por lo que comienzan las cifras negativas. Tener una empresa que venda vía online ahorra gran parte de los gastos.

Visibilidad: Para que una tienda física sea conocida por muchas personas, debe contar con una buena estrategia de marketing y una excelente ubicación, así como contar con productos de calidad y comentarios positivos transmitidos de boca en boca. De lo contrario, le costará mucho salir adelante y que la gente la tome en cuenta.

Internet se caracteriza por ser un canal de comunicación donde las personas masifican productos o marcas. Por lo tanto, tener una plataforma online ayudará a **aumentar los clientes potenciales** que irán a visitar el negocio. Además, con esta modalidad puedes llegar a públicos que no se encuentren en tu misma ciudad e incluso de tu país, y cuentas con un servicio abierto las 24 horas del día, los siete días de la semana.

Comunicación directa: Las empresas deben tener siempre presente qué es lo que sus consumidores quieren. Para esto, tienen que compartir los canales de comunicación donde ellos exponen sus opiniones.
Las marcas deben estar presentes en cada lugar donde sus clientes estén para responder inmediatamente a las preguntas, dudas o reclamos, o bien, para saber de sus gustos e intereses, y las redes sociales son los canales ideales para hacerlo, de una manera efectiva y oportuna. Un 53% de los consumidores buscan información de compra en la Web. Aprovecha esta tendencia para conquistarlos desde la búsqueda y lograr una venta directa en ese mismo instante.

Redes sociales: El comercio online adquiere herramientas que le ayudan a su masificación entre los propios consumidores, como por ejemplo las redes sociales. Facebook, Twitter,

Pinterest o blogs son los canales de comunicación que reúne a mucha gente que está dispuesta a compartir y enterarse de las opiniones de los demás. Sin duda, éstas serán tu mejor herramienta de marketing y promoción.

La competencia: Las empresas grandes o pequeñas tienen mucha competencia en el mercado, la cual puede ser determinada por los usuarios de internet. Ahí radica la importancia de tener una plataforma online, ya que hay mucha competencia que fácilmente puede llamar la atención de tus clientes, por tener mayor facilidad y comodidad de compras y pagos. Adelántate y ofrece este servicio, es un valor agregado que te ayudará a que muchos clientes te prefieran.

La tecnología avanzada: La tecnología crece a pasos agigantados. Actualmente son muchas las tiendas que cuentan con ventas online y le han implementado sistemas de probador online, perfecto para definir la compra de consumidores indecisos.

Para 2015 se espera que la mayoría de la gente navegue en Internet mediante dispositivos móviles, por lo tanto asegúrate que tu sitio cuente con una versión móvil y para tablets, así como con aplicaciones que motiven y faciliten las compras.

El auge del actual Internet se podría afirmar que en lo relativo a Comercio Electrónico, está motivado por el hecho de que en Internet podemos encontrar todo aquello que, en circunstancias normales, (en la zona / sociedad donde vivimos), no podemos encontrar. Podemos hacer una lista más o menos larga de cuáles son las cosas, en este caso: información, productos, servicios, etc... Que podemos obtener en Internet. Sin embargo, de dicha lista podríamos destacar algunos temas que habitualmente no tenemos acceso, o llegar hasta ellos nos resulta un poco difícil, tales como: armamento, sexo, drogas...

2.1.8.4 *Factor Psicológico y Costumbres.*

La sociedad actual aún tiene unos valores claramente arraigados, llamados "costumbres", los cuales determinan e influyen en su manera de pensar, de actuar o de comportarse. Dichas costumbres y en lo relativo al comercio están claramente marcadas por el hecho de poder tocar el producto, (en el caso de que se tratase de un servicio serio de recibir información sobre el mismo).

Si bien es cierto que gracias a la venta por catálogo o por Correo dichas costumbres han ido cambiando también lo es que dicho tipo de venta ha arraigado en aquellos sitios donde la "venta tradicional" no conseguía llegar ya fuera por la distancia (estar muy apartado de algún centro urbano) o por limitaciones de apertura de los comercios (en muchos países la ley impide que un comercio esté las 24 h. del día abierto e incluso regulan los horarios). Es en estos casos o lugares donde este tipo de Comercio ha arraigado.

También han influido negativamente factores tales como un mal arranque o mal servicio de este tipo de comercio, por ejemplo, en España este tipo de empresas comenzaron vendiendo entre otras cosas los "Prismáticos de la Marina", en los folletos decían maravillas sobre ellos y luego a la hora de la verdad eran simples juguetes de plástico que no aumentaban nada. Todo ello dificultó el arranque y consolidación de éste tipo de ventas en España.

Estas costumbres o factores psicológicos influyen sobre el comercio electrónico de una forma negativa, pues todo esto en Internet no se puede hacer.

2.1.9 Claves de evolución del comercio electrónico.

El crecimiento del comercio electrónico es una realidad incontestable actualmente, se trata de una de las más recientes revoluciones económicas y culturales que han sido propiciadas por el despliegue masivo de Internet.

Las tres claves de evolución del comercio electrónico son:

1º) La relativa madurez que ha alcanzado el comercio electrónico en el mercado de consumo. En apenas una década el comercio electrónico ha pasado de ser una actividad de alto riesgo, en la cual había pocas garantías de siquiera recibir el producto solicitado, a ser una alternativa real y frecuente a los medios tradicionales en gran cantidad de sectores (transportes, reservas turísticas o libros especializados, entre otros muchos). Aunque quede un gran camino por recorrer para alcanzar unos índices de aceptación elevados en la totalidad de la población (especialmente aquella de mayor edad y menos familiarizada con las nuevas tecnologías), cabe destacar la satisfacción de los clientes con los servicios de comercio online y su confianza en los mismos, que se ha elevado de forma notable y continúa creciendo.

2º) Parte de este gran incremento en la confianza por parte de los consumidores en las empresas que ofrecen comercio electrónico se debe a otro factor que ha sido de vital importancia para el desarrollo del mismo: La evolución regulatoria y auto-regulatoria que ha sufrido el medio. Aunque en muchos aspectos el mundo digital disfruta de una legislación más laxa que los comercios tradicionales equivalentes. La presencia de una mayor vigilancia y un mejor marco jurídico (como la LSSICE y la LOPD y sus reglamentos de desarrollo) han terminado con gran cantidad de abusos y malas prácticas que minaban la confianza del usuario en Internet como medio para realizar compras. De igual forma, los actores involucrados en el comercio electrónico han tomado conciencia en gran medida de la necesidad de dar confianza al usuario y han realizado grandes esfuerzos por mejorar la transparencia de sus procesos mediante la implantación de mecanismos de buenas prácticas o sellos de calidad que dan fe de que se cumplen unos mecanismos adecuados seguridad. La presencia del logotipo de una entidad bancaria de prestigio o del sello de adhesión a una asociación de autorregulación y mediación que defiende al consumidor puede ser el factor que haga decidir a miles de consumidores a confiar en una transacción de comercio electrónico.

3º) La importancia de la llegada de nuevos paradigmas de comercio, inexistentes anteriormente, que han sido propiciados por las características de Internet. Originalmente y de forma comprensible, el comercio electrónico se limitaba a ser una extensión del modelo de comercio tradicional en la que la tecnología se utilizaba como mero escaparate virtual para llegar a un mayor número de personas. Sin embargo, y paralelamente a este comercio electrónico tradicional, han florecido nuevas y originales formas de hacer negocio en la red. Fenómenos como YouTube, MySpace o Facebook (todos se pueden englobar como “redes sociales”) han

surgido en pocos años y se han convertido en gigantes económicos con una base comercial novedosa: La empresa únicamente ofrece una plataforma software y gran capacidad de almacenamiento (que carecen de un gran valor económico en sí mismas), mientras que los contenidos y el valor añadido lo producen voluntariamente los usuarios. Esta mecánica crea una sinergia de red, basada en la Ley de Metcalfe, mediante la cual la llegada de nuevos usuarios aumenta exponencialmente el valor de la propia red (y por tanto su atractivo para nuevos usuarios). La clave del éxito económico de estas redes sociales está en encontrar la forma de capitalizar la afluencia masiva de usuarios, que en general pasa por combinar los ingresos generados por la publicidad online con alguna forma ingeniosa de aplicación del modelo "freemium" (en el cual una gran mayoría de usuarios disfruta de servicios gratuitos – usuarios free – mientras que una minoría está dispuesta a pagar por algún servicio exclusivo – usuarios Premium.) Facebook, por ejemplo, utiliza varios canales de publicidad online (algunos evidentes, otros más sutiles como grupos patrocinados por empresas) y decenas de formas de obtener dinero mediante el modelo freemium (por ejemplo, cuando un usuario decide pagar por hacer un regalo virtual a otro usuario por su cumpleaños, se trata de una transacción con unos beneficios del 100% para la empresa dado que el regalo virtual tiene un coste nulo).

2.1.10 Internet como herramienta vital.

El comercio electrónico por Internet es visto por las personas solo como un medio de compras fáciles y rápidas pero como todos sabemos esto no es tan simple por que varias personas creen que al poner cierto tipo de seguridad en sus computadoras con eso basta la seguridad a la que nos referimos son los firewalls estos los cuales tienen cierta utilidad pero que pasa cuando los usuarios al comprar algo dan o entregan los que son los números de las tarjetas de crédito no hay seguridad de ninguna forma lo cual nos ha llevado a que se realicen varios actos fraudulentos, los cuales les han afectado a millones de usuarios y varios bancos pero lo más importante es la economía, la cual ha resentido en mayor parte estos actos.

Varias personas han encontrado en Internet la esperanza de crecer como negocio un ejemplo de esto lo podemos ver en las empresas que se dedican a vender la conexión a Internet, pero eso no solo son todos los motivos o razones por lo cual las personas utilizan esta herramienta a continuación les mostraremos otras razones para poner su negocio en Internet.

20 RAZONES PARA PONER SU NEGOCIO EN INTERNET.

1) Por el nuevo mercado que se abre.
2) Para hacer contactos.
3) Para anunciar interactivamente su negocio.
4) Para dar servicio a sus clientes.
5) Para atraer el interés público.
6) Para publicar información estratégica.
7) Para vender productos o servicios.
8) Para difundir fotografías, sonido y películas.
9) Para alcanzar un perfil de mercado altamente deseable.
10) Para responder a las preguntas más frecuentes.

11) Para estar en contacto directo con los comerciales.
12) Para penetrar en mercados internacionales.
13) Para ofrecer servicios las 24 horas al día.
14) Para publicar al instante la información que cambia.
15) Para fomentar el intercambio con los clientes.
16) Para probar nuevos productos y servicios.
17) Para impactar en los medios de comunicación.
18) Para alcanzar al mercado educativo y juvenil.
19) Para atacar mercados especializados.
20) Para cubrir su mercado local.

¿Quién puede vender por Internet?
Todo el mundo puede realizar negocios por Internet, este no se encuentra monopolizado por una empresa sino se podría decir que Internet es para todo el mundo, si todos podemos vender en Internet sin tener una ley que controle este tipo de compra venta se pueden realizar varias transacciones y no tenemos que pagar algún tipo de impuesto se podría decir que esto está bien porque son negocios en donde la ganancia es 100% neta pero que me dicen cómo afecta esto al país, obviamente en estos momentos no nos damos cuenta pero en un futuro no muy lejano es muy posible que casi todos los tipos de compra venta se tengan que hacer vía Internet lo cual se verá afectada la economía del país en un número que no nos podemos imaginar en estos momentos pero de lo que estamos seguros es que ve hacer muy grande.

¿Quién puede administrar un comercio electrónico por Internet?
La administración del comercio por Internet no es cosa del otro mundo está la puede realizar toda persona que tenga conocimientos de la utilización de internet, no nos referimos a conocimientos muy particulares sino todo lo contrario deben ser conocimientos muy generales los cual le permite a casi cualquier persona administrar un comercio electrónico, pero un consejo o tips que les damos es que si pueden obtener ciertos conocimientos en la programación de datos les beneficiaría para poder entender mejor lo que es el funcionamiento de Internet.

¿Qué organismo controla el comercio electrónico por Internet?
Existen varias empresas la cuales se dedican a estudiar este nuevo fenómeno que se encuentra en Internet pero la verdad no existe ningún organismo que controle el comercio electrónico por lo cual le da la libertad al comerciante de realizar cualquier cosa en este medio nos referimos a cualquier cosa es el aceptar las tarjetas de crédito que el comerciante quiera solamente, la formas de solución a cualquier problema y sobre todo poder realizar actos ilícitos sin preocupación a que se la aplique una sanción.

2.1.11 Infraestructura y fundamentos del comercio electrónico.

Las aplicaciones del comercio en línea se basan principalmente en esta infraestructura:

1) **Infraestructura de servicios comerciales comunes:** directorios, catálogos, tarjetas inteligentes de seguridad/autentificación, instituciones intermediarias para el pago electrónico.
2) **Infraestructura de red:** Internet (VAN, LAN, WAN), Intranet, Extranet, televisión por cable y satelital, dispositivos electrónicos, Internet.

3) **Infraestructura de los mensajes y de distribución de información:** intercambio electrónico de datos, correo electrónico, protocolo de transferencia de hipertexto.
4) **Infraestructura de interfaces:** está asentado en bases de datos, agenda de clientes y aplicaciones, y sus interrelaciones.
5) **Plataformas y lenguajes multimedia para la infraestructura pública de red:** VRML, HTML, XHTML, JAVA Script.

2.1.12 Sujetos intervinientes en el comercio electrónico.

El comercio electrónico constituye un acto jurídico con contenido patrimonial, es decir un contrato, con la peculiaridad que la comunicación entre las partes contratantes: aceptante y oferente se da por medios electrónicos.

Entonces como en toda contratación en el comercio electrónico, intervienen dos o más sujetos, los cuales se dividen en: empresario (business), consumidores (consumer) y administración (goverment). Esta clasificación, nos servirá de base al hablar de los tipos de comercio electrónico, ya que ésta, se determina mediante la interacción de estos sujetos entre sí.

2.1.12.1 ***Empresario.***

Son las personas que ofertan bienes o servicios en un mercado determinado. Generalmente son personas jurídicas; sin embargo, las personas naturales pueden estar incluidas dentro de esta categoría.

Desde un punto de vista estrictamente jurídico patrimonial, la empresa se habrá de concebir , a nuestro juicio , como una específica modalidad de riqueza productiva constitutiva de un bien o valor patrimonial de explotación, resultante de la materialización de la iniciativa creadora del empresario de la proyección patrimonial de su labor organizadora de los distintos factores productivos, facultades, poderes y técnicas jurídicas y de la actividad de producción e intermediación de bienes y servicios para el mercado a través del establecimiento mercantil. Este valor patrimonial de explotación se sustenta en aportes fundamentales: el empresario (sujeto organizador), el establecimiento (objeto organizado) y la organización. La empresa en sentido jurídico patrimonial, será la resultante patrimonial (valor de explotación) o suma de conjuntos (y subconjuntos) factoriales conexas a esos soportes.

2.1.12.2 ***Consumidores.***

Son las personas que tienen posición de demandantes en un mercado determinado. Pueden ser personas naturales o jurídicas. Existen ciertas dudas de considerar a las personas jurídicas como consumidores, puesto que por su propia naturaleza todas las actividades que realicen dentro de su objeto social son consideradas actos empresariales, características que las incluirán en la categoría business. Sin embargo, pensamos que ciertos actos de comercio realizados por las personas jurídicas pueden ser considerados actos de consumidores".

El consumidor es aquel adquiere los bienes o servicios para consumirlos o utilizarlos (en un ámbito personal, familiar o doméstico). No se considera destinatario final y tampoco consumidor, aquel que adquiere los bienes para introducirlo al mercado para su venta o para ceder a terceros en propiedad o uso.

2.1.12.3 *Administración.*

La administración está conformada por todos los órganos e instituciones del Estado. Con respecto a este sujeto, la denominación no queda muy clara, ya que se suele usar indistintamente otras denominaciones, tales como: Gobierno (government).

Entendemos que el término administración es más adecuado pues engloba a otros organismos, además del poder ejecutivo, que pueden tener presencia en el entorno electrónico, como la administración de justicia o el parlamento, por ejemplo.

2.1.13 Impacto económico del comercio electrónico.

La práctica intensiva del comercio electrónico causa y causará un impacto profundo tanto en la economía global como en las economías locales. Diversas industrias o sectores se verán afectados con mayor o menor rapidez dependiendo de la naturaleza de los bienes y servicios ofrecidos en sus áreas.

Estos cambios tendrán aspectos positivos y negativos siendo necesario reconocerlos a fin de tomar las medidas adecuadas para moderar los aspectos negativos y crear las condiciones óptimas para el pleno desarrollo de los aspectos positivos.

2.1.13.1 *Impacto sobre la industria informática.*

Como ya se ha explicado, aquellas industrias cuyos bienes y servicios son digitalizables no sólo serán las primeras en acusar dicho impacto, sino que sufrirán procesos profundos de transformación.

La industria de las aplicaciones y servicios informáticos tal vez sea uno de los sectores donde el impacto será más visible. La posibilidad de transferir aplicaciones a través de la red permite que dichas industrias puedan y tengan que competir a escala global. Esto no sólo beneficia a las grandes corporaciones que comercializan los títulos más conocidos, sino que también crea posibilidades para que pequeñas y medianas empresas puedan comercializar aplicaciones, soluciones y servicios informáticos. Un claro ejemplo lo brindan las empresas dedicadas al diseño y mantenimiento de páginas de Internet. Sin lugar a dudas, el diseño de estructuras capaces de realizar operaciones de comercio electrónico es uno de los sectores que está experimentando mayor crecimiento y donde, hasta la fecha, son las Pymes las que canalizan la mayor parte.

Mientras amplios sectores relacionados con la industria informática crearán empleo, como contrapartida, aquellos que tengan como función la venta de aplicaciones a través de tiendas minoristas, verán reducida su cuota de participación.

Finalmente, otro aspecto negativo está dado por la llamada "piratería" que provoca que copias ilegales de aplicaciones (una situación análoga se vive en la industria de la música) puedan viajar libremente a través de la red sin ningún tipo de control o límite.

2.1.13.2 *Impacto sobre el sector turístico.*

El comercio electrónico a través del internet brinda a cada destino y proveedor turístico, independientemente de cual sea su tamaño o volumen de negocio, la oportunidad de desplegar una actividad comercial de un modo más eficaz basándose en los costes. El marketing en la red y el comercio electrónico como herramienta de comunicación resultan en la actualidad fundamentales para este tipo de empresas.

El comercio electrónico permite que los mismos consumidores preparar sus paquetes vacacionales comparando, reservando y contratando directamente a las aerolíneas, cadenas de hoteles, empresas de alquiler de autos, líneas de cruceros, etc. También crea para las empresas mayoristas o consolidadoras localizadas en cualquier lugar del mundo la posibilidad de organizar viajes pre armados (paquetes) y venderlos directamente a consumidores de cualquier país.

2.1.13.3 *Impacto en los servicios bancarios.*

Bancos y entidades financieras han operado a través de redes de comunicación desde hace cientos de años (haciendo uso, por ejemplo, del sistema de clearing bancario que data de épocas medievales y del denominado giro cablegráfico que permite la transferencia de dinero de un lugar a otro). Aprovechando las tecnologías que hicieron posible desarrollar operaciones más rápidas y eficientes, los bancos incorporaron los cajeros automáticos que, al estar conectados entre sí mediante redes de telecomunicaciones cerradas (EDI), permiten realizar diversas operaciones a cualquier hora y desde diversos lugares. Para mantener los niveles de seguridad requeridos en este tipo de operaciones, sólo se puede acceder a las redes ya sea desde una terminal ubicada en una oficina bancaria, o bien desde un cajero automático.

La utilización de los cajeros permitió a los bancos automatizar operaciones, siendo el cliente quien provee el recurso humano necesario. De esta manera se logró un nivel superior de eficiencia y un mayor alcance geográfico.

Al ofrecer Internet la posibilidad de llegar potencialmente a cualquier lugar del planeta, una vez solucionado el problema de la seguridad mediante el uso simultáneo de diversas tecnologías, algunos bancos aceptaron integrar sus redes cerradas con Internet. Así es como un tercio de los bancos en EE.UU. y al menos un 15% en el resto del mundo ofrecen servicios a través de la red. Según las capacidades tecnológicas de cada institución bancaria, sus clientes podrán realizar a través de Internet operaciones más o menos complejas como revisar balances de cuenta, transferir dinero de una cuenta a otra, realizar pagos e incluso obtener préstamos e hipotecas. Cuanto más se automaticen dichas transacciones más se reducirá la necesidad de contar con activos físicos y empleados para atender las necesidades de los clientes.

Los servicios bancarios y financieros son digitalizables en su gran mayoría, por lo que la capacidad de prescindir de activos físicos destinados a la atención del público es total. Esto ha causado dos fenómenos:

1) El alcance ilimitado de las entidades bancarias. Un determinado banco puede mantener clientes activos aún donde no tiene una presencia física. Este hecho beneficiaría a aquellas instituciones cuya reputación o renombre trasciende el área geográfica donde operan en la actualidad.

   En la medida en que continúen las condiciones actuales (que permiten movimientos financieros con gran libertad y fluidez) este fenómeno se irá acentuando.

2) La aparición de bancos virtuales. Como se mencionó anteriormente, un banco puede operar aún en aquellos lugares donde carece de presencia física. Llevado este principio al extremo mediante el establecimiento de bancos virtuales, la institución pasa a operar con una prescindencia total de oficinas. Una de las razones que ha llevado a considerar esta opción es el costo comparativo existente entre operar una sucursal "real" y un banco "virtual". Cuesta tanto abrir y poner en funcionamiento un banco virtual con su consiguiente alcance global que una sucursal de un banco tradicional.

Más allá de lo expuesto, si bien en un futuro la mayor parte de las operaciones tradicionales podrán ser realizadas desde una PC con acceso a Internet, no parece probable que los bancos de "cemento y ladrillo" vayan a desaparecer o sean suplantados por bancos virtuales.

El mayor peligro derivado del uso de herramientas de comercio electrónico aplicadas a los servicios bancarios, es su utilización por entidades no bancarias (como cadenas de venta minorista o empresas del sector automotor) que ya ofrecen en ciertos países toda una gama de servicios bancarios que van desde la emisión de tarjetas de crédito hasta servicios de financiación y préstamos.

2.1.13.4 ***Impacto sobre los servicios de correo.***

Debido al crecimiento experimentado por el comercio electrónico, el servicio de correo sufrirá grandes cambios.

Tanto el e-mail como el uso de servicios bancarios a través de Internet harán que la función del correo como medio de comunicación se vea notoriamente reducida.

El costo de utilización del e-mail y la velocidad que ofrece hace que las limitaciones dadas por la necesidad de tener que acceder a la red y desarrollar habilidades a fin de poder operar en ella, se vean compensadas. De todos modos, aún estas mismas limitaciones están siendo superadas. En la India, por ejemplo, campesinos analfabetos o semianalfabetos que se ven obligados a migrar durante meses y que carecen de acceso a un teléfono, ya son capaces de utilizar un servicio que envía, a un costo menor que el que insume el envío de una carta tradicional o una llamada telefónica, un video mensaje de tres minutos de duración a través de Internet.

En lo que respecta al sistema de envío y pago de cuentas, representa un alto volumen del total manejado por los correos nacionales. En EE.UU., por ejemplo, constituye casi el 50% del total de correspondencia distribuida por el correo público.

El uso de servicios bancarios a través de la red permite el pago directo. Una vez más, el límite para el desarrollo de este tipo de pagos está dado por el tema de la seguridad. En la mayoría de los países todavía se exige una prueba escrita (impresa por la empresa o gobierno correspondiente) como constancia de pago.

Finalmente, el desarrollo de tecnologías como la firma digital ayudará a que los documentos enviados por medios electrónicos ofrezcan las garantías necesarias de legitimidad e integridad, irrefutabilidad e irrepudiabilidad. Una vez que esto se logre es lógico deducir que los volúmenes de documentos enviados a través del correo se verán reducidos.

Como contrapartida, el desarrollo del comercio electrónico dirigido a consumidores finales ha de incrementar los envíos de encomiendas y paquetes a través de servicios de correo regulares.

2.1.13.5 *Impacto sobre la industria de entretenimiento.*

Radio y televisión.

La radio y la televisión son unas de las industrias más controladas por los gobiernos. Tanto el acceso a las frecuencias de transmisión como los contenidos son estrictamente regulados por distintas agencias gubernamentales.

Nuevas posibilidades surgen con la transmisión de programas televisivos o radiales efectuada a través de Internet. Este modo de operar, llamado Webcast, puede alterar significativamente el funcionamiento de la industria de la televisión y la radio.

Específicamente en el campo de las transmisiones radiales es donde se ha dado el mayor desarrollo, puesto que pueden llevarse a cabo por medio de la red logrando un producto similar al ofrecido a través de las ondas radiales.

En la actualidad hay 7.500 estaciones radiales alrededor del mundo que transmiten al menos una parte de su programación en la red, de las cuales casi 2.000 transmiten en vivo.

En lo relativo a la TV. en Internet, todavía se presentan limitaciones. Si bien canales de TV. muestran parte de su material en la red, la calidad de sonido y principalmente de imagen, no alcanza niveles óptimos como para sustituir a las transmisiones regulares. De todas maneras, a medida que se superen las limitaciones en la capacidad de transmitir, se espera poder lograr niveles de calidad e imagen superiores y similares a los de la TV. actual.

Lo destacable es que, para ambas industrias, los requisitos y cualidades de las transmisiones realizadas a través de la red, presentarían las siguientes particularidades:

1) Mientras que obtener una licencia o permiso para operar una estación de radio o un canal de televisión puede ser extremadamente complicado y costoso (sin considerar que haya frecuencias disponibles), no existen prerrequisitos ni controles especiales si se quiere transmitir voz, sonido o imágenes a través de la red.

2) Tanto una estación de radio como un canal de televisión tradicional tiene un alcance geográfico limitado, y sólo por medio de acuerdos y contratos con otros canales y estaciones su programación trasciende esas limitaciones geográficas.

De hacerse la transmisión a través de la red, una estación de radio puede llegar, a cualquier lugar del planeta.

3) Cada canal de TV y estación de radio es responsable por los contenidos que emite. Como tal, está sujeto a una jurisdicción, y violar cualquier regulación podría significarle desde sanciones y multas hasta la pérdida de licencias o permisos ya que el marco regulatorio está claramente definido.

Por el contrario, todavía no hay un marco que regule claramente las transmisiones a través de la red. Además, ante la inexistencia de tratados internacionales sobre el tema, dichas transmisiones podrían ser realizadas desde países que tuvieran marcos regulatorios permisivos en relación a los contenidos.

4) Toda actividad comercial (comprar o vender, exportar o importar material, vender espacios o publicidad, etc.) realizada por canales o estaciones está sujeta a la legislación impositiva y aduanera del lugar donde es efectuada.

La transmisión digitalizada a través de la red atraviesa fronteras y jurisdicciones, y la capacidad de los gobiernos para controlarlas e imponerles impuestos es básicamente nula o extremadamente limitada.

Cine.
En octubre de 1999 se realizará en EE.UU. la primera distribución de un film a través de Internet. El mediometraje en cuestión será enviado a cinco salas de cine, las cuales contarán con los equipos informáticos necesarios para recibir y procesar la transmisión. Este sistema creará para las compañías de cine la posibilidad de ahorrar las grandes cifras de dinero que cada año son gastadas en la producción y distribución de copias en celuloide. También evitará las múltiples copias que deben hacerse a fin de incorporar bandas de sonido o subtítulos en otros idiomas para los films exhibidos en el extranjero puesto que el formato digital permite que sean agregados a cada copia con un esfuerzo menor.

A la fecha, el principal factor limitativo para este tipo de distribución está dado por la calidad de imagen, que será similar a la ofrecida por la TV, pero muy inferior a la lograda por medio de las copias de celuloide.

2.1.13.6 ***Impacto sobre el empleo.***

Aunque cuantitativamente hablar del comercio electrónico constituya una pequeña parte del comercio en general, su impacto a diversos niveles es innegable.

Dentro del contexto del ámbito laboral, el comercio electrónico contrariamente a lo que se piensa a corto plazo creará nuevos empleos a través de la red. Los efectos más fuertes se harán sentir a largo plazo mientras que a mediano plazo sólo se registrarán pérdidas en ciertos sectores.

Lo importante es reconocer cuáles serán las industrias en las que el comercio electrónico generará nuevas demandas y crecimiento; identificar qué tipo de trabajos serán destruidos y cuáles será creado y, finalmente, visualizar las nuevas exigencias que serán requeridas a fin de poder insertarse en el mercado laboral.

Reestructuración del empleo a corto plazo.
Como se ha dicho con anterioridad, las ventas a través del comercio electrónico todavía representan un valor mínimo dentro del total de la economía.

Por consiguiente, no pareciera razonable argumentar que algunas compañías hayan tenido que cesar sus operaciones a causa de la competencia generada por compañías virtuales. Por el contrario, las creaciones de empresas destinadas a la venta en el marco del comercio electrónico continúan demandando personal y consumiendo bienes y servicios de modo tal que, a corto plazo, habrá creación neta de empleo mientras estas firmas continúen operando bajo ambos modelos de comercio.

Mediano plazo.
En este lapso ambos tipos de comercio acusarán el impacto de la competencia. Las continuas guerras de precios que se observan en la actualidad aumentan la presión para reducir costos operativos. Sumado esto a la implementación de sistemas de mayor eficiencia, las empresas podrían optar por adoptar políticas que implicarían una reducción del personal.

En el marco de esta competencia, habrá, seguramente, empresas que se verán forzadas a cerrar sus puertas.

A largo plazo.
La combinación de nuevos productos, mayores mercados y la optimización del uso del ingreso disponible generará mayor volumen de comercio teniendo esto efectos positivos sobre distintas industrias, destacándose el aumento de las ventas de software, de los servicios on-line, audio, música, publicidad y productos novedosos.

También los efectos positivos se reflejarían en la generación de empleos relacionados con la construcción y el mantenimiento de infraestructura. El comercio electrónico en sí mismo demandará el desarrollo de todo un sistema capaz de sostener su crecimiento. Aún en los países más desarrollados, la infraestructura actual tiene limitaciones para manejar eficientemente grandes volúmenes de comercio de modo que se darán nuevas posibilidades en este sentido.

No obstante, estos efectos variarán de acuerdo a los países y a la estructura y el tamaño que el comercio electrónico tenga en cada uno de ellos.

2.1.14 Arquitecturas de Comercio Electrónico.

A continuación, se describen brevemente algunas arquitecturas de comercio electrónico definidas hasta el momento por una variedad de organismos: la asociación CommerceNet, consorcios industriales y proyectos financiados por la Comisión Europea.

2.1.14.1 *Arquitectura eCo.*

CommerceNet promueve proyectos piloto de investigación tecnológica (prototipos y demostraciones) con empresas líderes del mercado. Uno de estos proyectos es el desarrollo de la arquitectura eCo, lanzado en respuesta al creciente número de especificaciones de comercio electrónico incompatibles entre sí.

El grupo de trabajo eCo, que incluye expertos de compañías como Hewlett-Packard, IBM, Intel, Sun Microsystems, RosettaNet y VeoSystems, tiene como objetivo desarrollar un entorno común que permita la interoperabilidad de diversas especificaciones de entornos de comercio electrónico tales como EDI, OBI, OTP y otras. El enfoque de eCo no es esperar hasta que se resuelvan todos los problemas de normalización, sino mejorar la traducción entre los diferentes protocolos y normas existentes.

La arquitectura eCo está basada en el lenguaje XML. En eCo las interfaces de servicio se definen en términos de documentos comerciales, por ejemplo, una oferta de precios, un pedido, etc. y de los procedimientos asociados a cada uno de ellos. Una interfaz así definida se denomina en la terminología de eCo Business Interface Definition (BID). Un elemento clave de eCo es una biblioteca de documentos genéricos denominada Common Business Library. CBL facilita la definición de documentos y la reutilización de partes comunes a varios documentos.

CBL no es una especificación más, sino más bien un "común denominador" de los documentos definidos en otras especificaciones propuestas por diversos sectores industriales, tales como OBI, OTP, o RosettaNet (un estándar de la industria de ordenadores). Si cada una de estas especificaciones se aplica sobre CBL, puede resolverse el problema de la interoperabilidad entre especificaciones con un mínimo de traducciones.

En este caso CommerceNet, al igual que otros consorcios como el W3C, define una especificación y ofrece un software genérico que la cumple. El disponer de software asequible ayuda a crear una norma "de facto", mientras que la existencia de una especificación da una vía evolutiva para sustituir este software por otro de mejor calidad si es necesario. Actualmente existe una primera versión pública de CBL.

Las directrices elaboradas por los firmantes del Memorándum de Acuerdo sobre libre acceso de las Pymes europeas al comercio electrónico con el respaldo de la Comisión Europea recomiendan el uso del sistema eCo utilizarse como punto de partida para el desarrollo de una arquitectura de comercio electrónico interoperable.

Otras ventajas de la arquitectura eCo, citadas en las directrices, son:

- Tiene una arquitectura de bloques flexible
- Evita el problema de interoperabilidad mediante un tipo avanzado de traducción de protocolos, que se basa en un análisis semántico de procesos empresariales
- Es una plataforma neutral en el sentido de que se beneficia de la aportación de la mayoría de las principales empresas implicadas en el comercio electrónico en Estados Unidos sin que ninguna de ellas sea dominante

Las directrices del Memorándum de Acuerdo recomiendan el establecimiento de un pequeño número de puntos focales europeos; por ejemplo, ECE, CommerceNet, W3C, CEN/ISSS o ICC para promover el desarrollo de bloques constitutivos de software interoperables, tomando como punto de partida la arquitectura eCo. La misión de estos

centros consistiría en seleccionar aquellas partes de la infraestructura del comercio electrónico que sean vitales para su aplicación, determinar qué organizaciones pueden elaborar las especificaciones necesarias y promover el desarrollo de software que cumpla estas especificaciones.

2.1.14.2 ***Open Buying on the Internet (OBI).***

OBI es una especificación para comercio electrónico entre empresas, en particular para el caso de compras numerosas de productos de bajo precio unitario, por ejemplo, como las realizadas por el departamento de compras de una organización grande. La especificación ha sido desarrollada por el consorcio OBI, que desde junio de 1998 está gestionado por CommerceNet. OBI tiene actualmente más de 60 miembros.

La versión 1.0 de la especificación OBI se publicó en marzo de 1997 y la versión 1.1 en junio de 1998. La arquitectura OBI incluye cuatro entidades: la persona que hace un pedido, la empresa vendedora, la compradora y la autoridad de pago. Omitiendo algunas interacciones complementarias u opcionales, las entidades citadas interactúan en cuatro pasos:

1) Una persona, perteneciente a la organización compradora, hace un pedido de un producto seleccionado del catálogo de un vendedor.
2) El vendedor reenvía el pedido a la organización compradora que le devuelve el pedido autorizado.
3) El vendedor comprueba el crédito del comprador con la autoridad de pago y procesa el pedido.
4) La autoridad de pago emite una factura y recibe el pago.

La versión 1.1 de OBI especifica los procedimientos de acceso a los catálogos, el formato de los mensajes intercambiados entre las entidades anteriores (basado en el estándar EDI ANSI X12, aunque en el futuro pueden incluirse EDIFACT y XML), los procedimientos de transmisión de estos mensajes a través de Internet (HTTP) y los mecanismos de seguridad necesarios para la autenticación de las partes, confidencialidad y no repudio de los mensajes (uso de SSL, mensajes formato PKCS 7 y certificados digitales X.509 versión 3).

La inclusión del lenguaje XML es una de las mejoras previstas por el consorcio para futuras versiones de OBI.

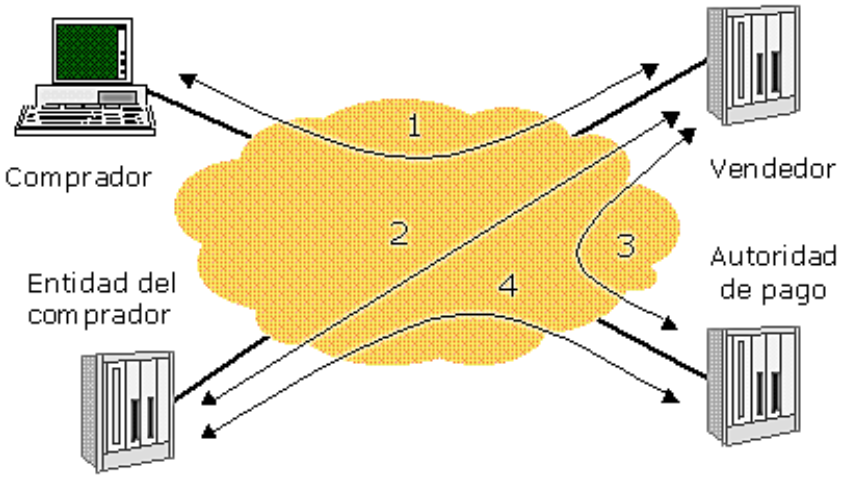


Ilustración 2: Modelo OBI.

2.1.14.3 ***Open Trading Protocol (OTP).***

OTP es una especificación para comercio electrónico sobre Internet desarrollada por el consorcio OTP, que cuenta actualmente con más de 30 miembros. OTP pretende reproducir en un escenario electrónico la secuencia de interacciones que tienen lugar en las transacciones tradicionales, incluyendo los documentos que ahora nos son familiares: recibos, facturas, etc.

Como en el caso de OBI, el modelo caracteriza una serie de entidades o "roles" y de transacciones que pueden tener lugar entre ellas (aunque tanto las entidades como las transacciones de OTP son diferentes a las de OBI). Los roles definidos por OTP son el comprador, el vendedor, el receptor del pago (que actúa en representación del vendedor), la entidad que entrega el producto y la entidad que se encarga de la atención al cliente y la resolución de posibles conflictos.

OTP especifica el formato y contenido de los mensajes intercambiados entre entidades, así como las posibles formas de transmitir los mensajes OTP de una entidad a otra. OTP hace uso del estándar XML por lo que sus mensajes pueden procesarse directamente con analizadores de este lenguaje.

En general, una transacción se compone de una serie de "pasos" que pueden estar presentes o no y ordenarse de diferentes maneras según el tipo concreto de transacción a modelar, por ejemplo, una compra, una devolución, un depósito de fondos, etc... Los pasos de una transacción encapsulan procedimientos básicos como, por ejemplo:

- Oferta.
- Acuerdo de compra.
- Pago (usando alguno de los mecanismos de pago existentes).
- Entrega.
- Recibo de compra.
- Resolución de problemas en la transacción.

OTP sigue el criterio de definir una especificación base sencilla y añadir funciones en respuesta a demandas del mercado. Por ejemplo, el uso de firmas digitales es opcional y

no se requieren certificados de cliente. La primera versión de la especificación se publicó en 1998.

2.1.14.4 *Building Blocks for Electronic Commerce.*

Esta propuesta se elaboró en 1997 en el marco del grupo de comercio electrónico del EBES (European Board for EDIFACT Standardization), origen del actual grupo de comercio electrónico del CEN/ISSS (Information Society Standardization System del Comité Europeo de Normalización CEN). El proyecto fue patrocinado por la Comisión Europea DGIII/B2.

Los componentes (building blocks) de comercio electrónico se definen a partir del análisis de los procesos comerciales de interés, clasificándolos en tres grupos según el ámbito donde actúan: componentes del comprador, del vendedor y de terceras partes. En la terminología del modelo, se denomina "solución" a la implementación de un componente en forma de un producto o servicio específico de comercio electrónico. Un "conjunto de soluciones" es la implementación de varios componentes en forma de conjunto integrado de productos y servicios que constituyen un sistema de comercio electrónico completo.

El modelo identifica los siguientes componentes:

1) **De marketing:**
- Creación / consulta de catálogos.
- Publicación de información / análisis de información.
- Ofertar un precio / pedir una oferta de precio.
- Reservar un producto para un comprador / añadir un producto a la cesta de la compra.

2) **De contratación:**
- Confirmar un pedido / hacer un pedido.
- Reponer existencias de un producto / registrar la confirmación de un pedido.
- Aceptar la cancelación / cancelar un pedido.

3) **De logística:**
- Recibir / generar una notificación de entrega.
- Recibir /entregar un producto.

4) **De cierre de una operación:**
- Confirmar / seleccionar un método de pago.
- Procesar / entregar una tarjeta de crédito o monedero electrónico.
- Efectuar el pago.

5) **De interfaz con la Administración**
- Declaración de impuestos.
- Notificaciones de exportación.

2.1.14.5 ***Secure Electronic Market Place for Europe (SEMPER).***

SEMPER, abreviatura de Secure Electronic Market Place for Europe, es un proyecto del programa ACTS que ha desarrollado una arquitectura de comercio electrónico con un avanzado sistema de seguridad. El proyecto se planteó como objetivos estudiar los requisitos e implicaciones técnicas, legales, comerciales y sociales del comercio electrónico, definir una arquitectura de comercio electrónico abierta e independiente de plataformas hardware/software o arquitecturas de red específicas y, por último, implementar y evaluar un prototipo.

La arquitectura SEMPER soporta transacciones seguras entre comprador y vendedor, así como con terceras partes como autoridades de certificación, bróker, notarios, etc. SEMPER ofrece dos grupos de servicios de seguridad:

1) Básicos.

- Autenticación.
- Integridad.
- Firma digital.
- Pago.
- Confidencialidad.

2) avanzados, por ejemplo.

- Anonimidad.
- Resolución de conflictos.
- Sellos de tiempo.
- Firma de contratos por varias partes.

La arquitectura propuesta por SEMPER comprende cuatro niveles o capas, de arriba a abajo:

1) Comercio.
2) Intercambios.
3) Transferencia.
4) Servicios de soporte.

El nivel de comercio ofrece el conjunto de servicios de seguridad a las aplicaciones de negocio a través de una API definida por SEMPER. Además, este nivel ofrece un conjunto de bloques de propósito general que pueden reutilizarse en el diseño de nuevas aplicaciones.

El nivel de intercambios se encarga de controlar "intercambios justos" entre las partes. Por intercambio justo se entiende aquí aquel en el que las partes acuerdan los términos del intercambio de antemano de forma que cuando éste se lleva a cabo tienen garantía de recibir la información acordada.

El nivel de transferencia ofrece servicios para transmitir y recibir información estructurada en "contenedores" con unos determinados atributos de seguridad asociados. Por ejemplo, un contenedor con el atributo de no repudio de origen requiere que la entidad origen firme digitalmente el contenido del contenedor y que la entidad destinataria verifique la firma. Existen tres tipos de contenidos que puede transportar un contenedor: documentos

firmados, información y pagos. Cada tipo de contenido se extrae del contenedor y es procesado por bloques diferentes a su paso por el nivel de transferencia, antes de re ensamblar el contenedor y entregarlo de nuevo al nivel de intercambio del destinatario. El nivel de transferencia se encarga también de otras tareas como la gestión de monederos electrónicos, el establecimiento y liberación de conexiones, etc.

El nivel más bajo proporciona al resto de niveles servicios básicos, por ejemplo:

- **Criptográficos:** cifrado, hash, firma digital y generación de claves
- **De comunicación:** ocultan los detalles de la tecnología de red subyacente
- **De archivo:** almacenamiento seguro de certificados, documentos firmados, claves y registros de transacciones.

La integridad del sistema SEMPER es responsabilidad de un núcleo que, de forma similar a un sistema operativo, controla los derechos de acceso a recursos críticos de todos los módulos del sistema, incluidos los módulos de aplicación.

2.1.15 Clasificación.

Actualmente el Comercio Electrónico presenta múltiples categorías, entre las que podemos destacar dos: por la forma de relacionarse, o según los agentes implicados.

2.1.15.1 *Por la forma de relacionarse.*

En esta modalidad tenemos a su vez dos subcategorías: el Comercio Electrónico Indirecto y el Comercio Electrónico Directo.

2.1.15.1.1 Comercio Electrónico Directo o comercio electrónico on-line.

Es el cual las transacciones son netamente on-line desde el pedido hasta el pago y envío.

Respecto de este tipo de comercio, concurren distintas formas de canalizar dicha información, como vimos, respecto de las transacciones comerciales no físicas (correo, teléfono, fax, televisión, radio, medios análogos, medios electrónicos), sin embargo, la forma más globalizada es sin lugar a dudas la Internet, mediante todas las herramientas que ofrece, lo que ha traído consigo la dación de nuevos principios en materia de negociaciones.

Otra definición sostiene que: “Es aquel que se lleva a cabo exclusivamente a través de un medio electrónico, típicamente Internet, por los que nos estamos refiriendo al comercio de bienes y/o servicios digitalizados.

2.1.15.1.2 Comercio Electrónico Indirecto o comercio electrónico off-line.

Es aquel utilizado para la adquisición de bienes tangibles, es decir aquellos contenidos en un soporte material. Si bien las transacciones se realizan electrónicamente, al ser cosas y objetos tangibles deben ser enviados usando canales de distribución tradicionales. “…por

lo que la ejecución de esa obligación coincide con la que tendría lugar de haberse concluido la transacción por medio del comercio tradicional".

El comercio electrónico indirecto comprende las transacciones realizadas por medios electrónicos relativas a bienes tangibles, que no pueden descargarse u obtenerse directamente a través de Internet. El contrato puede perfeccionarse en línea con todos sus elementos, pero su ejecución precisa de medios materiales que exceden al mundo virtual.

Cabe precisar que si bien la contratación electrónica presupone la transmisión inmaterial a través de las redes informáticos de la declaración negóciales y la marginación de documentos en papel, el objeto de estos contratos puede caer tranquilamente sobre el bien material cuya entrega física es necesaria para el cumplimiento, "pues sólo en ocasiones se trata de prestaciones susceptibles de ser ejecutadas por medio de la transmisión a través de la propia red de información digitalizada.

2.1.15.2 *Según los agentes implicados.*

La proliferación de empresas y consumidores ha diversificado esta nueva realidad, creándose diferentes tipos de comercio electrónico para adaptarse a las necesidades del mercado.

En virtud de esta clasificación podemos agrupar al Comercio Electrónico en las categorías presentadas a continuación:

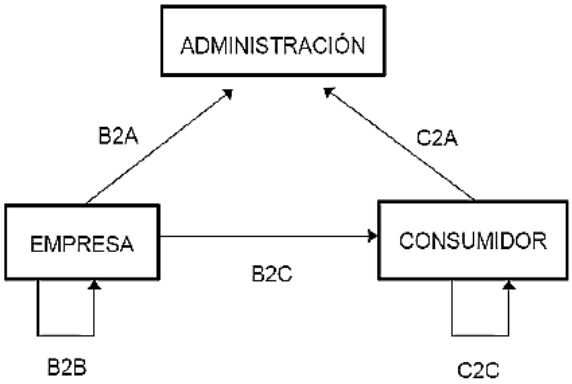


Ilustración 3: Clasificación según agentes implicados.

2.1.15.2.1 Comercio electrónico B2B (empresa a empresa).

Ilustración 4: Empresa a empresa.

B2B es la abreviación de business to business (negocio a negocio), y es aquel en donde la transacción comercial únicamente se realiza entre empresas que operan en Internet, lo que quiere decir que no intervienen consumidores. Existen tres modalidades:

- El mercado controlado que únicamente acepta vendedores en busca de compradores.
- El mercado en el que el comprador busca proveedores.
- El mercado en el que los intermediarios buscan que se genere un acuerdo comercial entre los vendedores y los compradores.

El comercio electrónico B2B ha supuesto un gran avance tecnológico, pero se requieren una serie de características para sacar el rendimiento óptimo:

- Experiencia en el mercado concreto.
- La oferta debe ser un valor añadido.
- Evitar fallos de producción, logística y distribución.

Las ventajas y características han convertido al comercio B2B en una opción que cada vez tiene más adeptos:

- Reducción de costes.
- Ampliación de mercado.
- Aumento de la velocidad.
- Centralización de oferta y demanda.
- Información de compradores, vendedores, productos y precios en un lugar común.
- Mayor control de las compras.

2.1.15.2.2 Comercio electrónico B2C (empresa a consumidor).

Ilustración 5: Empresa a consumidor.

Este es el tipo de comercio electrónico, también conocido como business to consumer (negocio a consumidor), es el más conocido y el que seguramente tú empleas. Es aquel que se lleva a cabo entre el negocio o, en este caso tienda virtual, y una persona interesada en comprar un producto o adquirir un servicio. Así que si tú tienes tu tienda online y clientes fieles que adquieren tus productos, perteneces a este tipo. Las ventajas más destacables son:

- El cliente puede acceder a la tienda virtual desde cualquier lugar a través de un dispositivo electrónico, lo que le facilita una compra cómoda y rápida.
- Se tienen actualizadas las ofertas y los precios de manera constante para la comodidad del cliente.
- El soporte al cliente se puede proporcionar de manera directa por diferentes medios, como chat en vivo, redes sociales, correo electrónico o Skype.

Los inconvenientes, como sucede en toda transacción, también existen. El consumidor debe prestar especial atención a la seguridad en las compras.

Existen diferentes tipos de comercio electrónico B2C:

- **Intermediarios on-line:** Se trata de compañías que facilitan las transacciones entre compradores y vendedores a cambio de una contraprestación económica a modo de porcentaje.
- **Modelos basados en la publicidad:** Publicidad basada en el sistema, donde las empresas tienen sitios web de un inventario, que venden a las partes interesadas.
- **Modelos basados en la comunidad:** Las empresas facultan a los usuarios para interactuar, en todo el mundo, en áreas similares de interés.
- **Modelos basados en tarifas:** En un sistema de pago basado en el sistema. En este caso la empresa cobra una tarifa de suscripción para ver su contenido.

2.1.15.2.3 Comercio electrónico E-Tailing.

Ilustración 6: E-Tail.

Es una variante del B2C que consiste en una plataforma de E-Commerce gestionada por un negocio retail. Las características de este tipo de negocio son las mismas que el B2C, pero el e-tailing ha provocado el nacimiento de multitud de herramientas e-tailware, todo un conjunto de software especialmente diseñado para la creación de catálogos virtuales y gestión del producto ligado al retail. El crecimiento de estas pequeñas empresas retail que se lanzan al comercio electrónico ha supuesto la aparición de multitud de webs que permiten comparar precios de un mismo producto ofrecido por diversos e-tailers. Ejemplo: www.librerianorma.com

2.1.15.2.4 Comercio electrónico B2B2C (empresa a empresa a consumidor).

Ilustración 7: Empresa a empresa a consumidor.

Es una modalidad de comercio electrónico que agrupa el B2B (business to business) y el B2C ('business to consumer'). Se trata de una versión más sofisticada de lo que podría ser la simple superposición de los dos negocios. Con la misma plataforma online y la misma plataforma de distribución se trata de crear la cadena de valor completa desde que un producto o servicio se fabrica hasta que llega al consumidor final.

El B2B2C, también se emplea en algunos casos para definir a los mercados llamados "mercados diagonales" en Internet, plataformas en línea (online) que atienden tanto a transacciones comerciales entre negocios como entre negocios y consumidores finales. Por lo general estos mercados diagonales suelen ser proporcionados por fabricantes o

mayoristas que proporcionan una diferenciación de precios y condiciones comerciales según se trate de una compra hacia un distribuidor o minorista (otra empresa) o un consumidor final o ciudadano. Ejemplo: Un Call Center.

2.1.15.2.5 Comercio electrónico C2B (consumidor a empresa).

Ilustración 8: Consumidor a empresa.

Se basa en una transacción de negocio originada por el usuario final, siendo éste quien fija las condiciones de venta a las empresas.

El modelo es muy interesante, existen páginas que los usuarios ofrecen sus casas como alquiler y las compañías de viajes pugnan por dichas ofertas, aquí podemos ver muchas páginas web que se dedican a dicho negocio como pagar noches de hotel, billetes de avión, una cena romántica en una casa rural. Ejemplo: www.priceline.com

Las ventajas de este modelo son:

- El consumidor puede establecer una relación directa con la empresa eso hace que las transacciones entre ambos sean más rápidas y más segura.
- Además, los costos de dichas transacciones se reducen.
- Hace posible que muchos usuarios o consumidores se pongan de acuerdo.

2.1.15.2.6 Comercio electrónico B2A (empresa a administración).

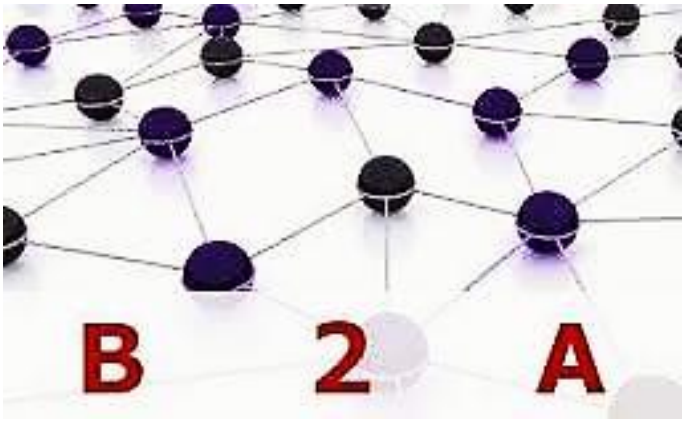


Ilustración 9: Empres a administración.

El comercio electrónico B2A (Business to Administration) es un servicio que ofrece la administración a las empresas –y también a los ciudadanos– para que se puedan realizar los trámites administrativos a través de Internet. Ejemplo: www.iess.gob.ec

Las ventajas para las empresas son evidentes:

- Ahorro considerable de tiempo y esfuerzo.
- La posibilidad de descargarse formularios y modelos de los procedimientos administrativos.
- Disponibilidad las 24 horas del día.
- Información siempre actualizada.

2.1.15.2.7 Comercio electrónico B2E (empresa ha empleado).

Ilustración 10: Empresa ha empleado.

La relación comercial *business to employee* (negocio a empleado) se centra principalmente entre una empresa y sus empleados. Es decir, son las ofertas que la propia empresa puede ofrecer a sus empleados directamente desde su tienda online o portal de Internet, con ofertas atractivas que servirán de impulso para una mejora en el desempeño laboral. Este tipo de comercio electrónico se ha convertido en un tema novedoso entre empresas para generar competencia entre sus empleados.
Más allá de una opción, es un portal en donde los empleados pueden utilizar algunos recursos de la empresa. El empleado tendrá la posibilidad de hacer trámites internos en este micro sitio empresarial, que una vez en la red, llegará a manos del encargado.

Algunas de sus ventajas son:

- Reducción de costos y tiempos en actividades internas.
- Comercio electrónico interno, con oportunidades únicas para los empleados.
- Motiva y fideliza al empleado con la empresa.
- Informa, en el momento y en línea para consultar en cualquier momento.
- Equipos de colaboración en el entorno web.
- Integración más ágil del profesional en la empresa.
- Soporte para la gestión.
- Comercio electrónico interno.
- Fidelización del empleado.

2.1.15.2.8 Comercio electrónico C2C (consumidor a consumidor).

Ilustración 11: Consumidor a consumidor.

Una persona puede ofrecer en venta un producto que ya no necesita a través del comercio electrónico como medio para realizar esta transacción con otro consumidor. Esto es una evolución de las tradicionales y ya conocidas ventas de garaje que está tomando fuerza en Internet. El consumidor final le adquiere al consumidor primario los productos que él ya no quiere o necesita y a los que les podrá dar una nueva utilidad a precios muy accesibles. Se sigue el mismo proceso de compra del comercio electrónico tradicional Este tipo se conoce como *consumer to consumer (consumidor a consumidor).*,

Una de las estrategias más comunes del comercio C2C para Internet viene definida por aquel tipo de negocio cuyo objetivo es facilitar la comercialización de productos y/o servicios

entre particulares. También puede hacer referencia a las transacciones privadas entre consumidores que pueden tener lugar mediante el intercambio de correos electrónicos. Ejemplo: www.ebay.com

Las principales razones de este éxito creciente de C2C son las siguientes:

- La posibilidad de ingresos adicionales para los que venden.
- Ofertas a precios bajos para los que compran.

Las operaciones se realizan con 3 modalidades principales.

- **Subasta:** es la transacción más común en el sitio. El vendedor pone un precio de salida y una duración determinada para el anuncio y mientras dure ese período de tiempo, los compradores pujarán por ella. El pujador más alto se lleva el artículo, bajo las condiciones de entrega y devoluciones impuestas por el vendedor.
  ¡Cómpralo ya!: el vendedor establece un precio fijo y, si el demandante está dispuesto a pagarlo, será suyo.
- **Anuncio clasificado:** venta de artículos bajo esta forma de anuncio, en el que se exponen las características del artículo en cuestión y su precio.

2.1.15.2.9 Comercio electrónico C2G (consumidor a gobierno).

Ilustración 12: Consumidor a gobierno.

Cuando un gobierno municipal, estatal o federal permite que los ciudadanos realicen sus trámites en línea a través de un portal, se realiza el conocido comercio goverment to consumer (gobierno a consumidor), y se considera un tipo de comercio ya que se paga un trámite y se puede acceder a la información en línea en cualquier momento.

Algunas de las ventajas son:

- Ahorro en tiempo.
- Trámites más rápidos y seguros.
- Respaldo electrónico.
- Costos más bajos.

Aunque estos tipos de comercio electrónico no son los únicos, son los más utilizados de manera cotidiana. Así que ya sabes, el comercio electrónico no solo son compras en tiendas online, va más allá y se adentra a situaciones más complejas, como el proceso interno de una empresa o las acciones por parte de gobierno. Si conoces algún otro tipo de comercio electrónico, esperamos tus comentarios a continuación.

2.1.15.2.10 Comercio electrónico B2G.

Ilustración 13: Empresa a gobierno.

El comercio electrónico B2G (Business to Government) busca una mejor optimización de los procesos de negociación entre empresas y el gobierno. Su aplicación se destina a los sitios o portales especializados en la administración pública. En ellos las instituciones oficiales tienen la posibilidad de contactar con sus proveedores, pudiendo estos agrupar ofertas o servicios.

Importancia:

- Permite a las empresas establecer relaciones comerciales o legales con las Entidades Gubernamentales, suministrar productos y servicios a los gobiernos.

Características:

- Transparencia en el desarrollo de convocatorias y licitaciones.
- Mayor rapidez en el desarrollo de los trámites.
- El gobierno puede encontrar los mejores precios y condiciones de pago.

Ventajas.

- Ayuda a las Administraciones Públicas a ahorrar tiempo y dinero.
- Mayor transparencia de mercado, accediendo eficientemente a la oferta de los proveedores, comparando productos y realizando pedidos.
- Proceso simple y estandarizado.

Aplicaciones.
Se aplica a sitios o portales especializados en la relación con la administración pública. En ellos las instituciones oficiales, (hacienda, contrataciones públicas, etc.) pueden ponerse en contacto con sus proveedores, y estos pueden agrupar ofertas o servicios.

Normas e implicaciones.

- Ventas únicamente a gobiernos locales, municipales y estatales.
- Aplica reglas muy particulares para la licitación de contratos o la enajenación de bienes y servicios.
- El volumen y monto de ventas es el principal atractivo.

2.1.15.2.11 Comercio electrónico P2P (punto a punto).

Ilustración 14: P2P.

La arquitectura P2P se puede definir como un modelo de red en el que los integrantes, denominados peers, actúan tanto de clientes como de servidores. Estos peers pueden ser dispositivos muy heterogéneos, y pueden por tanto diferir mucho en capacidad de proceso, de almacenamiento, ancho de banda, sistema operativo, etc. Una red P2P destaca principalmente por su gran dinamismo, fuerte descentralización y alta escalabilidad. Ejemplo: www.kazaa.com

En el modelo P2P se introduce el concepto de igualdad en las redes: los peers son, en principio, iguales en derechos y obligaciones. Sin embargo, la arquitectura P2P es lo suficientemente flexible para permitir la existencia de grupos o usuarios más privilegiados, e incluso combinar modelos cliente/ servidores puros con modelos P2P.

Negocio que no tiene clientes fijos. Se trata de la comunicación directa entre dos clientes a través de e-mail o internet. Se utiliza para el intercambio de información y/o archivos.

Existen dos tipos de modelos de p2p que son: p2p centralizado y p2p descentralizado.

2.1.15.2.11.1 P2P centralizado.

Ilustración 15: P2P centralizado.

Un intermediario “supervisa” en la compartición de un archivo o recurso. Los usuarios registran sus archivos en un agente central para compartirlos, y utilizan el intermediario para encontrar otros ficheros. Este modelo puede ser aplicable a relaciones comerciales en las que no exista ninguna compañía que esté por encima de las otras, pero sí que sea necesaria una cierta coordinación central

Ejemplo:

- Napster.

Ilustración 16: Napster.

Se desarrolló una aplicación revolucionaria basada en este principio. Napster facilitaba que los usuarios pudieran descargarse archivos musicales en formato MP3 en su ordenador, sin ningún tipo de autoridad central que almacenara estos archivos.

2.1.15.2.11.2 P2P descentralizado.

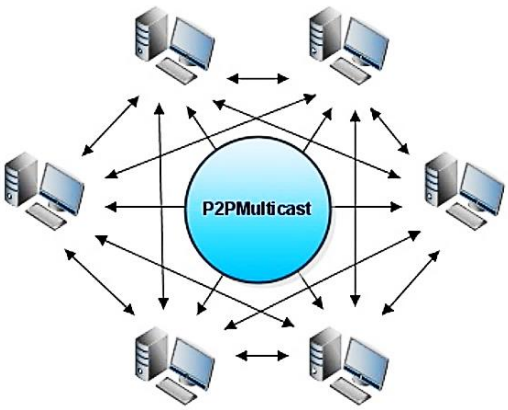


Ilustración 17: P2P descentralizado.

El usuario registra sus ficheros en un ordenador cercano dentro de la red de ordenadores de un intermediario. Cuando un usuario solicita un fichero, éste se busca a lo largo de todos los ordenadores de la red del intermediario, y cuando lo encuentra, se produce una transmisión directa del ordenador de la red donde se encuentra al del usuario que la había pedido.

Ejemplo: Los más conocidos de este tipo de modelo son Gnutella, Emule o Kazaa ya que su filosofía se deduce que no es necesario un intermediario centralizado.

Características.

- **Escalabilidad.** Las redes P2P tienen un alcance mundial con cientos de millones de usuarios potenciales.
- **Robustez.** Las Redes P2P permiten a los peers encontrar la información sin hacer peticiones a ningún servidor centralizado de indexado.
- **Descentralización.** Estas redes por definición son descentralizadas y todos los nodos son iguales.
- **Distribución de costes entre los usuarios.** Se comparten o donan recursos a cambio de recursos.
- **Seguridad.**

2.1.15.2.12 Comercio electrónico M-Commerce (comercio móvil).

Ilustración 18: Comercio Móvil.

Todas las transacciones pueden ser ejecutadas desde un teléfono móvil u otro dispositivo inalámbrico móvil. Ejemplo: Banca Móvil.

2.1.15.2.13 Comercio electrónico L-Commerce (comercio basado en la localización).

Ilustración 19: Comercio Basado en la Localización.

Comercio basado en la localización (L-Commerce) se refiere a la localización de productos y servicios a través de comercio móvil y tecnologías de computación sensibles al contexto. Ejemplo: Marketing a través de Blueetooth.

Comercio L gira en torno a 5 áreas de servicio clave:

- **Ubicación:** la determinación de la posición básica de una persona o de una cosa.
- **Navegación:** el trazado de una ruta desde una ubicación a otra.
- **Seguimiento:** el seguimiento del movimiento de una persona o de una cosa.
- **Cartografía:** la creación de mapas de ubicaciones geográficas específicas.
- **Timing:** determinar el momento preciso en un lugar específico.

2.1.15.2.14 Comercio electrónico Intrabusiness.

Ilustración 20: Intrabusiness.

Categoría de E-Commerce que incluye todas las actividades internas de la organización, que envuelve el intercambio de artículos, servicios o información de las unidades e individuos dentro de ella. Ejemplo: El portal de una universidad, a través del cual los docentes realizan actividades propias de su trabajo.

2.1.15.2.15 Comercio electrónico C-Commerce (comercio colaborativo).

Ilustración 21: Comercio Colaborativo.

Es considerado como el reemplazo de comercio electrónico y, por tanto, la siguiente etapa en el desarrollo de negocios electrónicos soluciones. Se define como ("una aplicación de un sistema de información interorganismos para la colaboración electrónica entre socios comerciales y empleados de la organización"). Entre todas las partes que son participantes de la Value_chain (clientes, proveedores y socios comerciales), una solución de C-Commerce forma una plataforma conjunta para diseñar, crear, gestionar y administrar los datos en tiempo real. Ejemplo: www.portalpsicologia.org

Ventajas y desventajas:
Las empresas que están dispuestas a implementar C-Commerce experimentará procesos de negocio optimizados, nuevas eficiencias de costes, una mayor satisfacción del cliente y la lealtad, y el potencial de ingresos muy ampliados.

Por otro lado, esto significa que las empresas tienen la obligación de compartir bases de datos, Intellectual_capital y Core_competencies. Un resultado deseado es la total transparencia que permite mejorar los procesos de negocio y el desarrollo y aplicación de medidas de ahorro de costes. Sin embargo, esto requiere un Paradigm_change en la cultura empresa.

2.1.15.2.16 Comercio electrónico E-learning.

Ilustración 22: E-Learning.

Es el proceso de enseñanza que se lleva a cabo o se desarrolla en internet y mediante la utilización de medios electrónicos. También se le denomina entre otras acepciones formación on-line, enseñanza virtual, tele formación o aprendizaje electrónico. En este sentido hay que hacer una distinción importante entre lo que se entiende por e-learning (el conocimiento se adquiere a través de internet) y el b-learning o blended learning (el conocimiento se adquiere combinando el aprendizaje a distancia y el aprendizaje presencial). En este artículo me centraré exclusivamente en el e-learning y cuáles son las múltiples ventajas que presenta una enseñanza exclusivamente en red. No se debe confundir la educación a distancia con el e-learning. Ejemplo: www.moodle.org

Entre las características más destacadas del e-Learning están:

- **Desaparecen las barreras espacio-temporales.** Los estudiantes pueden realizar un curso en su casa o lugar de trabajo, estando accesibles los contenidos cualquier día a cualquier hora. Pudiendo de esta forma optimizar al máximo el tiempo dedicado a la formación.
- **Formación flexible.** La diversidad de métodos y recursos empleados, facilita el que nos podamos adaptar a las características y necesidades de los estudiantes.
- **El alumno es el centro** de los procesos de enseñanza-aprendizaje y participa de manera activa en la construcción de sus conocimientos, teniendo capacidad para decidir el itinerario formativo más acorde con sus intereses.
- **El profesor,** pasa de ser un mero transmisor de contenidos a un tutor que orienta, guía, ayuda y facilita los procesos formativos.
- **Contenidos actualizados.** Las novedades y recursos relacionados con el tema de estudio se pueden introducir de manera rápida en los contenidos, de forma que las enseñanzas estén totalmente actualizadas.
- **Comunicación constante entre los participantes,** gracias a las herramientas que incorporan las plataformas e-Learning (foros, chat, correo-e, etc.).

2.1.15.2.17 Comercio electrónico Exchange (electronic).
Mercado electrónico público con muchos vendedores y compradores. Ejemplo: www.forex.com

2.1.15.2.18 Comercio electrónico E2E (Exchange to Exchange).
Modelo de E-Commerce en el cual hay interconexión electrónica para intercambio de información. Ejemplo: Bolsa de Valores

2.1.15.2.19 Comercio electrónico batering (trueque).

Ilustración 23: Trueque.

Bajo este modelo las compañías intercambian los excedentes que no necesitan por productos que necesitan. Ejemplo: www.bookcrossing-spain.com

2.1.15.2.20 Sistemas electrónicos de ofertas (bajastas).
Modelo de E-Commerce en el cual los vendedores ofrecen sus productos a los compradores y estos a su vez compran el producto a quien lo vende al precio más bajo. Ejemplo: www.labajasta.com

2.1.15.2.21 Modelo name-your-own-price.
Modelo de E-Commerce en el cual los compradores colocan el precio el cual están dispuestos a pagar por un producto o servicio e invitan a los vendedores a hacer su oferta. Ejemplo: www.priceline.com

2.1.15.2.22 Bróker de información (Infomediaries).
Modelo de E-Commerce que ofrece información especializada en nombre de los productores de bienes y servicios y sus clientes potenciales. Ejemplo: www.alibaba.com

2.1.15.2.23 Offshoring.
Modelo de E-Commerce en el que se subcontratan procesos de negocios de un país a otro. Ejemplo: Servicios de CRM y Call Center http://www.callfasst.com/Docs/CRM-Campanas-Offshore-y-Atencion-al-Cliente-Via-Call-Center.htm

2.1.15.2.24 Vending.
Modelo de E-Commerce por medio de máquinas auto expendedoras accionadas por diversos medios de pago. Ejemplo: http://vendingcolombia.com.co

2.1.15.2.25 E-trading.
Modelo de E-Commerce que utiliza tecnología de la información para reunir a compradores y vendedores a través de medios electrónicos, para crear un mercado virtual. (NASDAQ, NYSE Arca y Globex, son ejemplos de lugares mercado electrónico (E-Marquet places). Ejemplo: www.correval.com/etrading/

2.1.15.3 ***Atendiendo al entorno tecnológico.***
En esta modalidad tenemos a su vez dos subcategorías: Comercio electrónico abierto y Comercio electrónico cerrado.

- **Comercio electrónico abierto:** Cuando los contratos se perfeccionan y eventualmente se ejecutan en redes abiertas de telecomunicación (Internet).
- **Comercio electrónico cerrado:** Cuando la contratación tiene lugar en redes cerradas, en las que sólo pueden operar quienes cuentan con la pertinente habilitación contractual, sin la cual el acceso a dichas redes resulta velado (EDI).

2.2 Aspectos de seguridad.

2.2.1 Amenazas al Comercio Electrónico.

Se entiende por amenaza a una acción o condición del entorno de redes (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación en la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo).

Las amenazas a la seguridad de los sistemas de comercio electrónico pueden ser clasificadas como internas y externas. La amenaza interna es la que tiene más probabilidad de ocurrir, es la más difícil de combatir o controlar y sin embargo es la que más se pasa por alto. Este tipo de amenazas es difícil de combatir ya que muy pocos sistemas brindan protección contra acciones maliciosas ejecutadas por usuarios que estén autorizados en el sistema. Es por esto que la mejor manera de combatir esta amenaza es con una combinación de políticas de seguridad estrictas y un esquema de acceso a información privilegiada que solo les permita el acceso a aquellas personas que deban tenerlo.

Sin embargo, las amenazas a la seguridad a las que más se les da importancia son a las externas. Tanto los ejecutivos de las compañías como los administradores de los sistemas sienten un temor especial a los intrusos desconocidos que estando fuera de las barreras de la organización puedan tener acceso a información privilegiada. Parte de esta preocupación está bien fundada, ya que la Internet les da a los comerciantes la posibilidad de llegar a los consumidores potenciales en cualquier parte del mundo, pero al mismo tiempo permite que todos los usuarios mal intencionados, hackers y espías corporativos en todo el mundo puedan tener acceso a la información de la compañía.

Las categorías generales de amenazas o ataques al comercio electrónico son las siguientes:

2.2.1.1 *Vandalismo y sabotaje en Internet.*

Ilustración 24: Vandalismo y sabotaje.

El vandalismo o sabotaje en la web es tal vez el ataque que ha recibido más atención de los medios de comunicación. Este ataque consiste en rescribir la página web de alguien más, generalmente de forma ilegal, para cambiar el contenido de esa página dejando un mensaje propio del saboteador. Este ataque generalmente está motivado por razones

políticas o por el ego del saboteador que muestra que pudo romper las medidas de seguridad de un sitio web.

Aunque este ataque está dirigido al servidor web, el resto de los programas o información contenidas en la máquina que fue blanco del ataque también pueden estar comprometidas, como también otros recursos de red que estuvieran conectados a esa máquina, ya que el atacante pudo tener acceso a ellas tan fácilmente como lo hizo con los archivos de las páginas web.

Este tipo de ataques es muy perjudicial para la imagen de la compañía que sufre el ataque. La página web es la imagen de la compañía ante el mundo, y si esta es saboteada, la organización completa se verá vulnerable.

2.2.1.2 *Violación a la seguridad o privacidad.*

Ilustración 25: Violación de la seguridad o privacidad.

En la Internet, los mensajes son transmitidos a través de un número de intermediarios antes de llegar a su destino, los intermediarios son generalmente Routers, cualquiera de los cuales puede copiar, modificar o borrar los mensajes. Es por esta razón que no se debe asumir que las comunicaciones de datos son privadas a menos que se utilice un mecanismo de encriptación para protegerlas. El mayor temor de los consumidores en la Internet es el de revelar sus números de tarjetas de crédito, actualmente se han desarrollado un número de sistemas de transacciones de pago seguras para proteger la privacidad de las transacciones.

El “romper” las claves de los sistemas de encriptación actuales es muy difícil, por lo que es poco probable que se pueda comprometer la seguridad de las transacciones que utilizan estos sistemas. Sin embargo, los componentes web activos pueden presentar riesgos a la seguridad en el client-side. Los componentes activos son programas que se descargan y ejecutan automáticamente desde el navegador web cuando un usuario entra en un sitio web que los tiene como parte de su código. Ejemplo de estos componentes son los controles ActiveX, Applets de Java, Java Scripts, VBScript y ciertos archivos multimedia que se ejecutan vía plugins. Los plugins son aplicaciones que se ejecutan automáticamente cuando el navegador descarga archivos de un determinado formato.

2.2.1.3 *Robo y fraude en Internet.*

Ilustración 26: Robo y fraude.

El robo y fraude en la Internet tienen lugar cuando las personas son engañadas para que confíen en sitios web (y sus operadores), con los que no han tenido relaciones previas. La mayoría de los fraudes son resultado de realizar transacciones comerciales con sitios web establecidos por criminales que se hacen pasar por sitios que llevan a cabo negocios legítimos, cuando en realidad son una fachada para actividades criminales. Los consumidores son engañados para entregar sus números de tarjetas de crédito para pagar por productos o servicios que nunca son entregados.

2.2.1.4 *Violación a la integridad de los datos.*

Ilustración 27: Violación a la integridad de los datos.

Los ataques a la integridad de los datos casi no se discuten en el contexto de sesiones de Internet, sin embargo, son un problema en las transacciones de comercio electrónico. Las fallas en la integridad de los datos que se envían a través de las redes son casi siempre accidentales, pero existe la posibilidad de que los datos sean alterados intencionalmente para hacer algún daño. Un ataque que modifique datos, como por ejemplo precio de las acciones de la bolsa de valores puede tener gran impacto.

Existen mecanismos para detectar si los datos han sido modificados, pero al igual que con los métodos de encriptación, no se han implantado tan ampliamente como deberían.

2.2.1.5 *Denegación de servicio.*

Ilustración 28: Denegación de servicio.

Los ataques de denegación de servicio han sido denominados como las peores amenazas a la seguridad en Internet. Un ataque de denegación de servicio tiene como objetivo imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. Por lo general, este tipo de ataques está dirigido a los servidores de una compañía, para que no puedan utilizarse ni consultarse. El potencial que tiene este tipo de ataques para causar daños o pérdidas aumenta cada día, mientras se automatizan más servicios y se conducen cada vez más negocios de manera electrónica.

Generalmente, estos ataques se dividen en dos clases:

- Las denegaciones de servicio por saturación, que saturan un equipo con solicitudes para que no pueda responder a las solicitudes reales.
- Las denegaciones de servicio por explotación de vulnerabilidades, que aprovechan una vulnerabilidad en el sistema para volverlo inestable.

Los ataques por denegación de servicio envían paquetes IP o datos de tamaños o formatos atípicos que saturan los equipos de destino o los vuelven inestables y, por lo tanto, impiden el funcionamiento normal de los servicios de red que brindan.

Cuando varios equipos activan una denegación de servicio, el proceso se conoce como "sistema distribuido de denegación de servicio" (DDOS, Distributed Denial of Service). Los más conocidos son Tribal Flood Network (TFN) y Trinoo.

Cómo protegerse contra una denegación de servicio

Para protegerse contra este tipo de ataques, es importante mantenerse informado de los nuevos ataques y las vulnerabilidades, además de descargar las revisiones (patches) de Internet diseñadas por editores de software y algunos grupos especializados:

- http://windowsupdate.microsoft.com/
- http://www.securityfocus.com/

2.2.2 Amenazas y riesgos en las transacciones.

Ilustración 29: Amenazas y riesgos en las transacciones.

Cuando se hacen transacciones por medio de internet, las partes involucradas se pueden enfrentar a los siguientes problemas:

Falta de contacto físico con el producto: Las transacciones que se realizan a través de Internet son de carácter no presencial, lo que genera un cierto grado de incertidumbre. A su vez se omite tanto la atención personal como el contacto físico con el artículo, factores que pueden influir de forma determinante en la elección de un producto u otro. En el caso del comercio electrónico, a fin de eliminar dicha desventaja se está produciendo la incorporación de chats en directo o asistentes virtuales que ayudan a resolver dudas durante el proceso de compra.

Falta de seguridad y fiabilidad: Es un punto clave a la hora de decidir la compra a través de Internet que la empresa esté bien identificada y sobre todo que ofrezca la posibilidad de contactar directamente con ella. También es vital que disponga de información clara, completa y concisa tanto sobre temas contractuales como sobre el producto/servicio y el precio, clarificando los gastos que van o no incluidos en la transacción.

Problemas de distribución: Las incidencias logísticas (retrasos en la recepción, recepción del pedido con desperfectos, no recibir el producto) son otro de los principales inconvenientes del comercio electrónico.

Problema de reclamaciones y devoluciones: La principal problemática en las compras a través de la Red es que el producto o servicio adquirido no responda a lo que se ofrecía en Internet. La inseguridad de a quién dirigirse en caso de reclamación es otro de los problemas que conlleva el comercio electrónico.

Problemas de pago: En la mayoría de los casos, las compras a través de Internet se realizan utilizando el número de la tarjeta de crédito del comprador, pero aún no es 100% seguro introducirlo en la Red sin conocimiento alguno.

Perdida de integridad de los datos: un intruso crea, modifica o borra información.

Perdida de privacidad en los datos: se brinda acceso a la información a personas no autorizadas.

Pérdida de servicio: el servicio se interrumpe como consecuencia de las acciones de un hacker.

Pérdida de control: personas o usuarios externos sin ningún control.

2.2.3 Componentes de la Seguridad del Comercio Electrónico.

El modelo de seguridad en el comercio electrónico se puede dividir en cuatro componentes principales que hay que proteger; el software del client-side, el transporte de los datos, el software del servidor Web y el sistema operativo del servidor. Es importante hacer un esfuerzo para que la seguridad de estos componentes sea consistente, ya que, si uno de ellos presentara una debilidad obvia, sería blanco de la mayoría de los ataques, y debido a su debilidad muchos de esos ataques serían exitosos.

2.2.3.1 *Seguridad del software cliente.*

La seguridad del software cliente se refiere a la seguridad que presenta el software cliente de web, es decir, el software que se utiliza para navegar en Internet. Los dos grandes riesgos de este componente son las vulnerabilidades de los navegadores y los componentes Web activos.

Los navegadores presentan riesgos debido a que su código fuente no está disponible para revisión y los usuarios deben confiar en que el navegador no sea vulnerable a ataques, no habrá hoyos en la seguridad ni ejecute código malicioso en segundo plano.

El contenido web activo presenta el riesgo de que ejecute código malicioso en segundo plano sin que el usuario se entere. El contenido web activo es cada vez más común y puede presentarse en forma de Applets de Java, controles ActiveX, macros de Word, JavaScript, VBScript, y al descargar o ver archivos de formato PostScript, GIF o JPEG.

2.2.3.2 *Seguridad en el transporte de los datos.*

El transporte de los datos a través de las redes es el aspecto del comercio electrónico que ha recibido la mayor concentración de recursos para asegurar su seguridad. El brindar seguridad a los datos en tránsito implica garantizar la integridad y confidencialidad de los datos, y la autenticidad tanto del emisor como del receptor. La integridad de los datos se refiere a asegurar que los datos no son modificados mientras son transportados a través de la Internet, La confidencialidad se refiere a que los datos no puedan ser leídos por una entidad diferente al receptor y la autenticidad del emisor y receptor se refiere a garantizar que las partes involucradas en la transmisión sean quienes dicen ser, es decir, que no sean suplantados por terceros.

La necesidad de desarrollar mecanismos de seguridad para el transporte de los datos surge de la naturaleza insegura de la Internet ya que la información en tránsito se puede leer, copiar, modificar o eliminar mientras se transmite por las diferentes redes. Para brindar la seguridad necesaria en el transporte de los datos se han desarrollado diferentes mecanismos como la encriptación de datos, las firmas digitales y los certificados de autenticidad, también se han desarrollado protocolos de comunicación seguros como el

SSL (Secure Socket Layer, que es el estándar de facto para la transmisión segura de datos a través de la Internet) o el S-HTTP y protocolos para garantizar la seguridad de las transacciones de pago electrónico como el SET (Secure Electronic Transaction).

2.2.3.3 *Seguridad del servidor Web.*

Los servidores web se componen de tres elementos básicos: el software servidor que se encarga de responder a todas las peticiones de información provenientes de los navegadores, bases de datos donde están almacenados los datos acerca de los productos, servicios o información acerca de los usuarios, y los programas de interfaz entre el software servidor web y las bases de datos, esta interfaz puede hacerse a través de CGI (Common Gateway Interface) que son programas invocados por el servidor web para extraer la información de las bases de datos o a través de ASP o JSP que son programas incluidos en el código HTML y que son ejecutados por módulos del mismo servidor web. Las fallas de seguridad en el server-side se presentan generalmente en el software servidor y en los programas de interfaz con las bases de datos.

Es importante hacer notar que mientras más servicios prestan el servidor mayor será la probabilidad de que brinde oportunidades que los atacantes puedan aprovechar. Por eso es necesario escoger entre un servidor con una amplia gama de servicios y que sea inseguro, o un servidor extremadamente seguro pero que no preste muchos servicios. Además de las brechas de seguridad que presentan algunos de los servicios, los programas también tienen fallas en la seguridad que son producto de errores de programación. Este tipo de errores hace que los programas se comporten de manera anormal y son bien conocidos y aprovechados por los atacantes. La única manera de corregir este tipo de problemas es conseguir las actualizaciones de software que corrigen esos errores o conseguir versiones actualizadas del software que no presenten el error.

El software del servidor generalmente lo instala el “súper usuario” o “root”, que tiene todos los derechos y puede acceder a cualquier archivo del sistema. Como los programas del servidor son propiedad del “súper usuario” estos se ejecutan con sus privilegios. Esto es necesario debido a que solo los programas con este nivel de privilegio pueden abrir el puerto 80 (http) o el puerto 443 (SSL) y escribir en los archivos de log. Sin embargo, es recomendable configurar el software servidor para reducir sus privilegios de ejecución.

Cuando hay una conexión entrante al puerto 80, se crea un proceso hijo para manejar la solicitud y el proceso servidor (proceso padre) regresa al modo de escucha de peticiones. Se puede configurar el servidor de manera que los procesos hijos se ejecuten sin privilegios especiales al procesar las peticiones remotas. Si no se configura el software servidor de esta manera se puede presentar el problema de “escalamiento de privilegios”. El escalamiento de privilegios ocurre cuando un usuario o entidad no autorizados o no confiables obtiene privilegios de acceso, creación, modificación o eliminación de archivos más elevados de los que tendría normalmente. El peligro de este problema está en que, si un atacante logra explotar una vulnerabilidad del servidor o algún script CGI, podría ejecutar comandos en el servidor con privilegios de súper usuario. Esto significa que el atacante podría tener acceso privilegiado a cualquier archivo en esa máquina y en las máquinas del mismo dominio de confianza, incluyendo las bases de datos de la compañía, o ejecutar programas maliciosos en esas máquinas.

Además de las opciones de privilegios de ejecución existen otras opciones que tienen impacto en la seguridad de los servidores. Algunas de ellas son:

- **Listado automático de directorios:** Esta opción hace que si un navegador apunta a un directorio en el servidor donde no existe un archivo Index.htm, entonces la respuesta por defecto del servidor será un listado de los archivos de dicho directorio. El peligro está en que un atacante puede tener acceso a un directorio donde están los log o existan enlaces simbólicos o peor aún, los códigos fuente de los CGI o los archivos de configuración del servidor, los cuales pueden ser descargados y examinados minuciosamente para encontrar fallas que puedan ser explotadas. Para evitar este problema se debe deshabilitar esta característica del software, y de no ser posible, crear archivos Index.html en todos los directorios del servidor web.

- **Server Side Include (SSIs):** Esta característica permite incluir comandos en el código HTML de una página web. Cuando se recibe una petición para mostrar la página que tiene los comandos incluidos, estos son ejecutados por el servidor web con su privilegio de ejecución. El comando más peligroso es el "EXEC", el cual permite ejecutar cualquier programa en el sistema. Esta opción debe ser deshabilitada para prevenir problemas de ejecución de programas maliciosos o escalamiento de privilegios.

- **Seguimiento de enlaces simbólicos:** Esta característica permite extender el árbol de directorios. Un enlace simbólico es una referencia a un archivo que se encuentra en otro directorio, cuando se accede al enlace simbólico es como si se accediera al archivo al cual hace referencia. Los enlaces simbólicos pueden apuntar a archivos fuera del árbol de directorios especificado para el servidor web. El peligro es que los enlaces simbólicos pueden apuntar a directorios sobre los cuales el administrador web no tenga control y que contengan archivos como scripts CGI maliciosos que puedan ser ejecutados vía web. Esta opción también debe ser deshabilitada.

Los archivos que son parte del web Site solo deben ser accesibles a los administradores del sitio web o a usuarios autorizados para publicar información en el web y no deben poder ser accedidos vía web por usuarios internos o externos, esto para evitar que los atacantes tengan acceso a los archivos de configuración o log que pueden revelar información que los atacantes pueden utilizar contra el servidor.

Si se presta el servicio de FTP, los directorios donde residen los archivos del sitio web y el directorio ftp deben estar separados para evitar que usuarios no autorizados o atacantes coloquen archivos en el servidor (páginas web o CGI) vía ftp y luego estos archivos sean mostrados o ejecutados por el servidor web.

En las aplicaciones de venta de contenido es necesario poder controlar el acceso a los documentos que están a la venta. Esto permite dar acceso a los documentos a ciertos clientes y restringir el acceso a otros. Los tres tipos de mecanismos de control de acceso que están presentes en la mayoría de los servidores web son:

2.2.3.3.1 Restricciones por direcciones IP o nombre de host.

Es uno de los mecanismos de control de acceso más básicos. Consiste en restringir el acceso a las páginas web basándose en la dirección IP o nombre del host que hace la solicitud de información. Una solicitud web incluye el nombre del host y la dirección IP del

cliente, el servidor web puede utilizar esta información para determinar si la solicitud proviene de un equipo autorizado a ver el contenido del documento.

Para determinar si la solicitud proviene de una dirección autorizada el servidor web utiliza las Listas de Control de Acceso (ACLs). Las ACLs son una serie de reglas de acceso que se evalúan en secuencia para determinar si una solicitud proviene de una dirección autorizada. Se aconseja que los ACLs primero restrinjan el acceso a todos y luego se autorice a determinadas direcciones a acceder a la información. Esto es debido a que si existe algún error en el ACL esto resultará en inconveniencia para algunos usuarios y no en fallas a la seguridad.

Este método de control de acceso no se considera especialmente seguro, puede mantener alejados a los usuarios curiosos, pero no a los atacantes determinados. El problema de este método de control de acceso es que es vulnerable al “spoofing”. El spoofing se presenta cuando un atacante enmascara la dirección IP o nombre de host de su máquina para que aparezca como la de otra máquina en la cual se confía. Además, aunque la solicitud provenga realmente de una máquina autorizada, no se tiene la seguridad de que el usuario de esa máquina sea el usuario autorizado a ver la información que solicita.

2.2.3.3.2 Autenticación basada en contraseñas.

En este mecanismo el servidor web verifica la identidad del usuario basándose en un identificador de usuario y una contraseña. Para establecer el control de acceso utilizando este mecanismo el administrador del sistema debe crear una base de datos de usuarios autorizados, que contenga los identificadores de los usuarios y sus respectivas contraseñas (encriptadas). Luego el administrador debe declarar explícitamente que partes del sistema de archivos serán protegidos por este mecanismo.

Cuando un usuario quiera acceder a un documento protegido el servidor le mostrará un cuadro de dialogo donde el usuario debe ingresar su identificador y contraseña. El identificador de usuario se compara con los que están almacenados en la base de datos y la contraseña se encripta y compara con la contraseña que acompaña al identificador en la base de datos, si existe una correspondencia se da acceso al documento.

Este mecanismo presenta varios problemas de seguridad. Primero, como el identificador de usuario y la contraseña viajan a través de la red en “texto plano” cuando son enviados al servidor cualquier atacante con las herramientas adecuadas puede obtenerlos a través de la red.

Otro problema es la escogencia de contraseñas por parte de los usuarios representa un problema. Los usuarios tienden a escoger como contraseñas su mismo identificador de usuario, su nombre o apellido, fecha de nacimiento u otro dato que es fácil de averiguar por parte de los atacantes. Además, muchos sistemas no encriptan las contraseñas en la base de datos, sino que las codifican, por esta razón si un atacante logra obtener el archivo de la base de datos podría recuperar todos los identificadores de usuario y sus respectivas contraseñas con una herramienta de fuerza bruta. Esto se conoce como autenticación débil.

Para evitar molestias a los usuarios muchos servidores web no solicitan una re-autenticación del usuario durante la misma sesión web si este solicita documentos que estén en la misma “región de autenticación”. Una región de autenticación es un área del sistema de archivos protegida por el mismo ACL. Para evitar la re-autenticación el servidor

envía al cliente una cookie y el cliente presenta esta cookie cada vez que solicita información de la misma región de autenticación. El problema es que cada vez que el cliente envía la cookie al servidor este puede ser interceptado por un atacante y luego tener acceso a los archivos de esa región de autenticación. Para minimizar este problema se puede encriptar la cookie y vincularlo a la dirección IP del cliente al cual se le envió, así solo es válido si proviene de la dirección IP a la cual fue enviado. Sin embargo, esto no evita el spoofing.

2.2.3.3.3 Autenticación basada en Certificados Digitales.

El control de acceso mediante certificados digitales se hace utilizando el protocolo SSL, el cual en su versión 3.0 soporta la autenticación tanto del servidor como del cliente de una sesión web. Para poder implantar este mecanismo es necesario que los clientes posean certificados digitales emitidos por alguna Autoridad Certificadora. Los certificados digitales contienen los datos del cliente, así como su clave pública para poder realizar la encriptación asimétrica.

Este mecanismo presenta un nivel de seguridad más alto que el que presentan los mecanismos explicados anteriormente. Además, este mecanismo se implementa de forma transparente al usuario porque el intercambio de la información de identificación lo realiza el software cliente al momento de establecer la comunicación con el servidor.

Este mecanismo no sufre de los problemas de spoofing, de contraseñas débiles o de la captura de contraseñas cuando son transmitidas. El único problema es que se le impone al usuario la responsabilidad de conseguir un certificado personal emitido por una Autoridad Certificadora. Lo difícil es convencer al usuario a que se someta al proceso de obtención del certificado.

Los scripts CGI también son de interés para la seguridad de los servidores web. Una de las preocupaciones con los scripts CGI es que estos pueden actuar maliciosamente en respuesta a peticiones web de posibles atacantes. Esto se debe a que los CGI se ejecutan en el servidor respondiendo a las entradas de usuarios en los cuales no se tiene confianza. Los riesgos que presentan los CGI incluyen la habilidad de que clientes web ejecuten comandos del sistema que realicen alguna de estas tareas:

- Leer, remplazar, modificar o remover archivos.
- Enviar archivos al atacante vía mail a través de Internet.
- Ejecutar programas previamente cargados en el servidor, como colectores de contraseñas o un servidor para brindar acceso no autorizado vía telnet.
- Lanzar un ataque de negación de servicio sobrecargando el CPU con trabajos de cómputo intensivo.

Debido a que los CGI realizan muchas de las funciones de negocios de los sitios web dedicados al comercio electrónico es imposible eliminarlos para resolver los problemas de seguridad, pero se pueden seguir las siguientes recomendaciones para minimizar la posibilidad de que sean aprovechados por atacantes:

- Analizar cuidadosamente los scripts antes de ponerlos en producción para asegurarse de que no contengan vulnerabilidades que sean aprovechadas por los atacantes.
- Configurar el servidor web para reducir sus privilegios de ejecución. Debido a que los CGI son ejecutados por el servidor con su nivel de privilegios, el reducir los

privilegios de ejecución del servidor minimiza el daño que pueda causar un CGI defectuoso.

- Configurar el servidor para que solamente ejecute los CGI que se encuentren en un directorio específico. Todos los CGI que sean aprobados para estar en el ambiente de producción deben estar en ese directorio, este directorio generalmente se llama CGI-bin.
- Se deben establecer restricciones de acceso al directorio donde residen los códigos fuente de los scripts CGI, generalmente es el directorio CGI-src. Si un atacante tiene acceso a los códigos fuente de los CGI los puede examinar para determinar las fallas que puedan tener.
- Se deben realizar revisiones periódicas para determinar el origen, propósito y modificaciones hechas a cada CGI en el sistema. Los CGI que no tengan ninguna función en el sistema o cuyo origen no sea confiable deben removidos del sistema, así como su código fuente y versiones de respaldo.
- Se puede generar periódicamente un hash del contenido del directorio CGI-bin para comprobar que los scripts que están en ese directorio no sean modificados sin autorización.
- No incluir interpretadores de comandos (shell interpreters) en el directorio CGI-bin debido a que, si un atacante logra descubrir que los interpretadores están disponibles, puede utilizarlos para ejecutar comandos arbitrarios en el servidor vía peticiones web que contengan los comandos.

El último componente de los servidores de comercio electrónico son las bases de datos. Las bases de datos son esénciales para todas las aplicaciones de comercio electrónico y autenticación de usuarios. En las bases de datos está la información de mayor importancia para la organización. Por esta razón el acceso a las bases de datos debe estar controlado cuidadosamente. Debido a la importancia de las bases de datos para las aplicaciones de comercio electrónico, la mayoría de los fabricantes de paquetes de bases de datos han desarrollado interfaces entre estas y los servidores web. Estos interfaces han sido probados para asegurar que no contengan vulnerabilidades que puedan ser aprovechadas. Lo que se debe controlar es el acceso que tengan los usuarios a las interfaces de las bases de datos.

Existen dos tipos de interfaces a las bases de datos: a través de los programas o aplicaciones de bases de datos y a través de las interfaces web. El uso de los programas de bases de datos debe estar restringido a los usuarios internos autorizados para operar las bases de datos, esto para evitar el abuso interno de la información contenida en las bases de datos y se deben emplear mecanismos de identificación de usuarios a nivel de las bases de datos. Para los interfaces web se puede restringir el acceso a la base de datos con los mismos mecanismos utilizados por el servidor web para controlar el acceso a las páginas web combinado con los mecanismos de identificación de usuario a nivel de la base de datos. También es posible encriptar la información cuando se transfiere entre la base de datos y el servidor web y entre el servidor web y el cliente o se puede mantener la información encriptada dentro de la base de datos para evitar que los datos sean recuperados aun si la base de datos cae en manos de algún atacante.

La falta de recursos dedicados al desarrollo de mecanismos de seguridad para el server-side se debe en parte a la sobre valuación de los mecanismos de seguridad como la encriptación de datos y los firewalls. La encriptación de datos es buena para proteger los datos en tránsito, pero cuando los datos se almacenan, generalmente se hace en “texto

plano" y es allí donde los atacantes pueden obtenerlos. Por otra parte, los firewalls brindan protección solo contra atacantes "aficionados", un atacante determinado puede violar la protección que brindan los firewalls, aunque estén bien configurados.

2.2.3.4 *Seguridad en el sistema operativo.*

El sistema operativo constituye la base sobre la cual se construyen las aplicaciones de comercio electrónico. Si existen vulnerabilidades en el sistema operativo, entonces los datos almacenados en el servidor están expuestos a un ataque, sin importar los mecanismos de seguridad que presenten las aplicaciones o los protocolos de transporte de datos utilizados en las transacciones de comercio electrónico.

Las fallas en la seguridad de los sistemas operativos generalmente son bien conocidas y se pueden solucionar cambiando parámetros de configuración de los mismos para evitar las opciones por defectos de las que se aprovechan la mayoría de los ataques a los sistemas operativos.

La mayoría de las vulnerabilidades de los sistemas operativos se pueden agrupar en cinco categorías, la idea de agruparlos es tener un marco de referencia para comparar la severidad de las vulnerabilidades. Las categorías son:

- Opciones por defecto:
- Vulnerabilidades en el software de red.
- Ataques de negación de servicio.
- Autenticación débil.
- Hoyos en el sistema operativo.

2.2.3.4.1 Opciones por defecto.

Las opciones por defecto se refieren a las opciones de configuración del software que ha sido recién instalado. La mayoría del software viene configurado para maximizar la facilidad de uso, a veces a costa de la seguridad.

En esta categoría están incluidas las cuentas de usuario que son creadas automáticamente cuando se instala el sistema operativo. El problema con esas cuentas es que muchas veces tienen un identificador bien conocido como "guest" y no requieren contraseña, haciendo fácil la tarea de entrar en el sistema sin autorización. Además, pueden dar acceso a partes vitales del sistema operativo si no se tienen configuradas las restricciones de acceso necesarias.

2.2.3.4.2 Vulnerabilidades en el software de red.

El software de red da soporte a los sistemas de archivos compartidos, login remoto, comunicación entre procesos y toda clase de servicios de Internet. Algunos de estos programas están tan integrados con el sistema operativo que se les conoce como sistema operativo de red (NOS por sus siglas en ingles).

La mayoría de los problemas de seguridad en esta categoría provienen de los mecanismos de autenticación utilizados para iniciar las sesiones de red y compartir recursos entre diferentes equipos conectados a través de la red. Los ataques explotan las vulnerabilidades

de los mecanismos de autenticación para obtener acceso no autorizado a los recursos de un equipo o grupo de equipos.

2.2.3.4.3 Ataques de negación de servicio.

Los ataques de negación de servicio intentan hacer que un servidor web deje de funcionar o pierda acceso a la Internet. Los ataques de negación de servicio pueden variar en su extensión, desde hacer que deje de funcionar una sola computadora hasta un sitio completo. Este tipo de ataque se presenta en dos formas diferentes. La primera evita que los usuarios tengan acceso a los servicios ofrecidos por un servidor. La segunda consume los recursos de un equipo o hace que su sistema colapse.

Las debilidades que este tipo de ataque explota son fallas en las aplicaciones, fallas en el software de red y hasta fallas en los protocolos de red utilizados en la Internet. Las fallas en las aplicaciones y software de red pueden resolverse con facilidad instalando correcciones, pero los ataques que se aprovechan de los protocolos de red son muy difíciles de evitar ya que explotan características propias de esos protocolos que no pueden ser cambiadas o eliminadas. Otra característica que hace a estos ataques peligrosos es que son relativamente fáciles de realizar y las herramientas para llevarlos a cabo están disponibles en Internet.

2.2.3.4.4 Autenticación débil.

La autenticación es utilizada para verificar si un usuario tiene permitido el acceso a los recursos de un sistema. Los sistemas de autenticación no son una medida de seguridad especialmente fuerte debido a que pueden ser engañados con facilidad. El principal problema es la escogencia de las contraseñas por los usuarios, que llevan al problema de autenticación débil.

2.2.3.4.5 Hoyos en el sistema operativo.

Hay un gran número de programas conocidos como software del sistema, que brinda servicios al sistema operativo. Debido a que el software del sistema realiza una serie de funciones para brindar servicios al sistema operativo, este software generalmente necesita privilegios especiales como acceso de súper usuario. Las vulnerabilidades del software de sistema pueden ser aprovechadas por los usuarios no autorizados para escalar privilegios. A diferencia de las otras categorías de vulnerabilidades del sistema operativo, este tipo de software puede protegerse de los usuarios externos mediante el uso de firewalls.

2.2.3.5 ***Mecanismos de seguridad.***

Los mecanismos o requisitos de seguridad pueden variar ligeramente de un sistema de pago a otro dependiendo tanto de las características propias del sistema como por la confianza y seguridad que ofrezca el entorno donde va a interactuar el sistema.

En cualquier caso, podemos decir que los requisitos de seguridad de un sistema de pago electrónico son los siguientes:

2.2.3.5.1 Autentificación de los datos.

En todo método de pago, tanto el comprador como la tienda deben identificarse para comprobar que no existe fraude. En un sistema de pago a través de TPV, existe una entidad certificadora que durante la operación de pago garantiza la autenticidad de la transacción validando la información de tarjeta de crédito y titular de la misma.

La autentificación de otros datos que puedan afectar a la legalidad de la compra realizada se garantiza gracias a protocolos criptográficos de autentificación.

2.2.3.5.2 Disponibilidad y fiabilidad.

Una característica fundamental de los sistemas electrónicos de pago es la alta disponibilidad y fiabilidad de las operaciones. Es un elemento clave en el proceso de pago de una transacción, ya que en ese instante no puede existir una pérdida del servicio.

No obstante, podría producirse algún fallo en el sistema, y una peculiaridad de las transacciones es que o se realizan correctamente o no se realizan. No hay un punto intermedio de recuperación o estado intermedio. De esta forma, la fiabilidad del sistema es total.

Por tanto, un sistema fiable y disponible no solo depende de que sus transacciones lo sean, sino de que toda la arquitectura y elementos del sistema cumplan los mismos requisitos.

2.2.3.5.3 Integridad.

Otro aspecto importante en todo sistema de pago electrónico es la integridad de los datos intercambiados entre los actores. Es decir, no puede haber forma de manipular la información o alterarla mientras se realiza una transacción electrónica.

Para ello existen mecanismos de seguridad como son códigos de autentificación, firma digital, comunicación segura, etc.

2.2.3.5.4 Confidencialidad.

Los datos que se envían en una operación electrónica no pueden ser visibles para terceros, de ahí que se empleen técnicas de encriptado y cifrado de la información por parte de los actores implicados en la transacción.

En este sentido, el comercio se dota de un Certificado de Seguridad emitido por una entidad colaboradora certificadora, que permite el cifrado, encriptado y envío de la información de forma segura, empleando un canal de comunicación seguro (SSL).

Únicamente los extremos de la transacción, comercio y destinatario (entidad bancaria, autentificadora, etc.) son conocedores de la información de forma clara tras un proceso inverso de desencriptado.

Para cumplir con estos requerimientos se han desarrollado mecanismos o combinaciones de mecanismos que permiten asegurar las transacciones. Estos mecanismos se describen a continuación:

2.2.3.5.4.1 Criptografía.

Garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados (privacidad). La encriptación es la mutación de la información a una forma solo entendible con una clave de descripción. Una clave o llave es un número muy grande, en forma de una cadena de unos y ceros.

Ilustración 30: Elementos del sistema de encriptación.

El texto en claro (plaintext) es el mensaje que queremos transmitir de forma confidencial. El cifrado es el proceso de transformar el texto en claro en un texto que nadie pueda interpretar. El descifrado es el proceso de volver a transformar el texto cifrado en el texto en claro original.

Al texto cifrado se le llama también texto encriptado que significa que no se puede acceder a él. Sin embargo, en los libros se usa con más frecuencia el término "cifrado" (ciphertext).

Normalmente al texto en claro se le representa con una M (Mensaje) o una P (Plaintext), y al texto cifrado por una C (Cifrado).

El proceso de la encriptación (cifrado) se representa con una función E () de forma que:

$$C = E(P)$$

Al proceso del descifrado se le representa como una función D () de forma que:

$$P = D(C)$$

Para que un sistema criptográfico sea correcto, tiene que cumplirse la propiedad:

$$P = D(E(P))$$

Existen dos tipos de encriptación, la encriptación de “llave privada” o “llave simétrica” y la encriptación de “llave pública” o “llaves asimétricas”.

2.2.3.5.4.1.1 Criptografía Simétrica o de clave privada.

La criptografía de clave privada (o criptografía simétrica) se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.

Este tipo de criptografía es conocida también como criptografía de clave privada o criptografía de llave privada.

Existe una clasificación de este tipo de criptografía en tres familias: cifrado de bloques (block cipher), cifrado de flujo (stream cipher) y cifrado de funciones resumen (hash functions).

La criptografía simétrica ha sido la más usada en toda la historia, ésta ha podido ser implementada en diferentes dispositivos, manuales, mecánicos, eléctricos, hasta los algoritmos actuales que son programables en cualquier computadora. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar.

Aunque no existe un tipo de diseño estándar, quizá el más popular es el de Fiestel, que consiste esencialmente en aplicar un número finito de interacciones de cierta forma, que finalmente da como resultado el mensaje cifrado. Este es el caso del sistema criptográfico simétrico más conocido, DES.

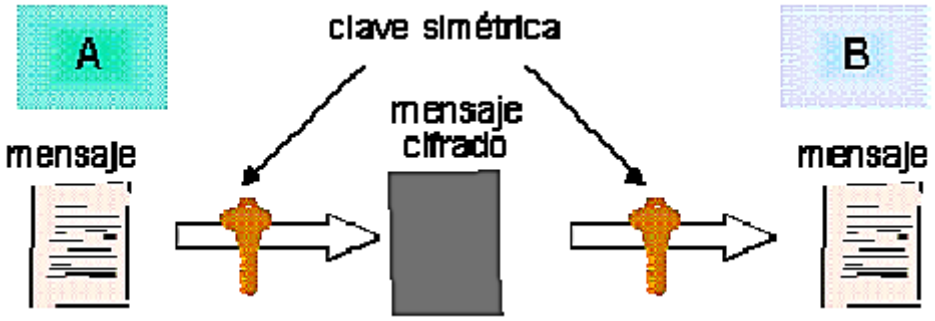


Ilustración 31: Cifrado/descifrado simétrico.

2.2.3.5.4.1.1.1 Algoritmo DES (Data Encryption Standard).

El algoritmo DES toma como entrada un bloque de 64 bits del mensaje y este se somete a 16 interacciones, con una clave de 56 bits. Este sistema fue tomado como estándar y ha sido uno de los más conocidos, usados y estudiados.

DES opera con una llave de longitud de 56 bits, en la práctica el bloque de la clave tiene 64 bits, ya que a cada conjunto de 7 bits se le agrega un bit que puede ser usado como de paridad, pero en sí la clave solo tiene 56 bits de longitud. Dependiendo de la naturaleza de la aplicación, DES tiene 4 modos de operación para poder implementarse: **ECB** (Electronic Codebook Mode) para mensajes cortos, de menos de 64 bits, **CBC** (Cipher Block Chaining Mode) para mensajes largos, **CFB** (Cipher Block Feedback) para cifrar bit por bit o byte por byte y el **OFB** (Output Feedback Mode) el mismo uso, pero evitando propagación de error.

En la actualidad no se ha podido romper el sistema DES desde la perspectiva de poder deducir la clave simétrica a partir de la información interceptada, sin embargo, con un método a fuerza bruta, es decir, probando todas las 2^56 posibles claves se ha podido romper DES a mediados de 1998. Lo cual quiere decir que, es posible verificar todas las claves posibles en el sistema DES en un tiempo corto, lo que lo hace inseguro para propósitos de alta seguridad.

A pesar de su caída, DES sigue siendo ampliamente utilizado en multitud de aplicaciones, como por ejemplo las transacciones de los cajeros automáticos. De todas formas, el problema real de DES no radica en su diseño, sino en que emplea una clave demasiado corta (56 bits), lo cual hace que con el avance actual de las computadoras los ataques por la fuerza bruta comiencen a ser opciones realistas. Mucha gente se resiste a abandonar este algoritmo, precisamente porque ha sido capaz de sobrevivir durante veinte años sin mostrar ninguna debilidad en su diseño, y prefieren proponer variantes que, de un lado evitarían el riesgo de tener que confiar en algoritmos nuevos, y de otro permitirían aprovechar gran parte de las implementaciones por hardware existentes de DES.

La opción que se ha tomado para poder reemplazar a DES ha sido usar lo que se conoce como cifrado múltiple, es decir aplicar varias veces el mismo algoritmo para fortalecer la longitud de la clave, esto ha tomado la forma de un nuevo sistema de cifrado que se conoce actualmente como triple-DES o TDES.

2.2.3.5.4.1.1.2 Algoritmo TDES (Triple DES).

El funcionamiento de TDES consiste en aplicar 3 veces DES de la siguiente manera: la primera vez se usa una clave K1 junto con el bloque B0, de forma ordinaria E (de Encryption), obteniendo el bloque B1. La segunda vez se toma a B1 con la clave K2, diferente a K1 de forma inversa, llamada D (de Desencryption) y la tercera vez a B2 con una clave K3 diferente a K1 y K2, de forma ordinaria E (de Encryption), es decir, aplica de la interacción 1 a la 16 a B0 con la clave K1, después aplica de la 16 a la 1, a B1 con la clave K2, finalmente aplica una vez más de la 1 a la 16 a B3 usando la clave K3, obteniendo finalmente a B3.

Explicado de otra forma podemos decir que TDES responde a la siguiente estructura:

$$C = E_{k1}((E_{k2}{}^{-1}(E_{k1}(M))))$$

Es decir, codificamos con la subclave k1, decodificamos con k2 y volvemos a codificar con k1. La clave resultante es la concatenación de k1 y k2, con una longitud de 112 bits.

Este sistema TDES usa entonces una clave de 168 bits, aunque se ha podido mostrar que los ataques actualmente pueden romper a TDES con una complejidad de 2^112, es decir efectuar al menos 2^112 operaciones para obtener la clave a fuerza bruta, además de la memoria requerida.

En los últimos 30 años se han diseñado una gran cantidad de sistemas criptográficos simétricos, entre algunos de ellos están: RC-5, IDEA, FEAL, LOKI'91, DESX, Blowfish, CAST, GOST, etc. Sin embargo, no han tenido el alcance de DES, a pesar de que algunos de ellos tienen mejores propiedades.

2.2.3.5.4.1.1.3 Algoritmo AES (Advanced Encryption Standard) (Rijndael).

AES es el nuevo estándar de encriptación de datos propuesto por el NIST en octubre de 2000. Es el sustituto de DES.

Este estándar ha sido desarrollado para sustituir a DES, cuya longitud de clave (56 bits), hoy en día resulta ineficiente. Este estándar goza de más confianza que su predecesor, DES, ya que ha sido desarrollado y examinado de forma pública desde el primer momento.

AES es un algoritmo simétrico de encriptación desarrollado para cifrar bloques de longitudes de 128, 192 o 256 bits utilizando claves de longitud de 128, 192 o 256 bits.

Puede ser utilizado en cualquiera de las combinaciones posibles de bloque/longitud.

Es fácilmente extensible a múltiplos de 32 bits tanto para la clave como para la longitud de bloque.

Según sus autores, es altamente improbable que existan claves débiles o semidébiles en AES, debido a la estructura de su diseño, que busca eliminar la simetría en las subclaves. También se ha comprobado que es resistente a criptoanálisis tanto lineal como diferencial. En efecto, el método más eficiente conocido hasta la fecha para recuperar la clave a partir de un par texto cifrado texto claro es la búsqueda exhaustiva, por lo que podemos considerar este algoritmo como uno de los más seguros en la actualidad. Otro hecho que viene a corroborar la fortaleza de AES es que en junio de 2003 fue aprobado por la NSA para cifrar información clasificada como alto secreto.

2.2.3.5.4.1.2 Criptografía Asimétrica o de clave pública.

Los algoritmos asimétricos o de clave pública han demostrado su interés para ser empleados en redes de comunicación inseguras (Internet).

La criptografía asimétrica es aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la criptografía asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas. Diffie y Hellman proponen una forma para hacer esto, sin embargo, no fue hasta que el popular método de Rivest Shamir y Adleman RSA publicado en 1978, cuándo toma forma la criptografía asimétrica; su funcionamiento está basado en la imposibilidad computacional de factorizar números enteros grandes.

Actualmente la Criptografía asimétrica es muy usada, sus dos principales aplicaciones son precisamente el intercambio de claves privadas y la firma digital. Una firma digital se puede definir como una cadena de caracteres que se agrega a un archivo digital que hace el mismo papel que la firma convencional que se escribe en un documento de papel ordinario. Los fundamentos de la criptografía asimétrica se basan en la teoría de números.

En la actualidad la criptografía asimétrica o de clave pública se divide en tres familias, según el problema matemático del cual basan su seguridad. La primera familia la que basa su seguridad en el Problema de Factorización Entera PFE, los sistemas que pertenecen a esta familia son, el sistema RSA y el de Rabin Williams RW. La segunda familia es la que basa su seguridad en el Problema del Logaritmo Discreto PLD, a esta familia pertenece el sistema de Diffie Hellman DH de intercambio de claves y el sistema DSA de firma digital. La tercera familia es la que basa su seguridad en el Problema del Logaritmo Discreto Elíptico PLDE, en este caso hay varios esquemas tanto de intercambio de claves como de

firma digital que existen como el DHE (Diffie Hellman Elíptico), DSAE, (Nyberg-Rueppel) NRE, (Menezes, Qu, Vanstone) MQV, etc.

Aunque a las familias anteriores pertenecen los sistemas asimétricos más conocidos, existen también tipos de sistemas que basan su seguridad en otro tipo de problema como por ejemplo en el Problema del Logaritmo Discreto Hiperelíptico, sobre problemas de retículas y sobre subconjuntos de clases de campos numéricos reales y complejos.

En la práctica muy pocos algoritmos son realmente útiles. El más popular por su sencillez es RSA, que ha sobrevivido a multitud de ataques, aunque necesita una longitud de clave considerable. Otros algoritmos son los de ElGamal y Rabin.

Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos. Por ejemplo, mientras que para algoritmos simétricos se considera segura una clave de 128 bits, para algoritmos asimétricos si exceptuamos aquellos basados en curvas elípticas se recomiendan claves de al menos 2048 bits. Además, la complejidad de cálculo que comportan estos últimos los hace considerablemente más lentos que los algoritmos de cifrado simétrico. En la práctica los métodos asimétricos se emplean únicamente para codificar la clave de sesión (simétrica) de cada mensaje o transacción particular.

2.2.3.5.4.1.2.1 Algoritmo RSA (Algoritmo asimétrico).

El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario. Una clave es un número de gran tamaño, que una persona puede conceptualizar como un mensaje digital, como un archivo binario o como una cadena de bits o bytes.

Cuando se envía un mensaje, el emisor busca la clave pública de cifrado del receptor y una vez que dicho mensaje llega al receptor, éste se ocupa de descifrarlo usando su clave oculta.

Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10100) elegidos al azar para conformar la clave de descifrado.

Emplea expresiones exponenciales en aritmética modular.

La seguridad de este algoritmo radica en que no hay maneras rápidas conocidas de factorizar un número grande en sus factores primos utilizando computadoras tradicionales.

La computación cuántica podría proveer una solución a este problema de factorización.

El algoritmo RSA es un algoritmo de clave pública desarrollado en 1977 en el MIT por Ronald Rivest, Adi Shamir y Leonard Adelman.

Fue registrado el 20 de septiembre de 1983. El 20 de septiembre del 2000, tras 17 años, expiró la patente RSA, pasando a ser un algoritmo de dominio público.

Este popular sistema se basa en el problema matemático de la factorización de números grandes.

El algoritmo RSA funciona de la siguiente manera:

1. Inicialmente es necesario generar aleatoriamente dos números primos grandes, a los que llamaremos p y q.
2. A continuación, calcularemos n como producto de p y q: p*q.
3. Se calcula fi: $fi(n) = (p-1)(q-1)$.
4. Se calcula un número natural e de manera que $MCD(e, fi(n)) = 1$, es decir e debe ser primo relativo de $fi(n)$. Es lo mismo que buscar un número impar por el que dividir $fi(n)$ que de cero como resto.
5. Mediante el algoritmo extendido de Euclides se calcula d: $e.d \ mod \ fi(n) = 1$. Puede calcularse $d = ((Y * fi(n)) + 1)/e$ para Y=1,2,3,… hasta encontrar un d entero.
6. El par de números (e, n) son la clave pública.
7. El par de números (d, n) son la clave privada.
8. Cifrado: La función de cifrado es $C = M^e \ mod \ n$.
9. Descifrado: La función de descifrado es $M = C^d \ mod \ n$.

Ejemplo con números pequeños:

1. Escogemos dos números primos, por ejemplo, p=3 y q=11.
2. $n = 3 * 11 = 33$
3. $fi(n) = (3-1) * (11-1) = 20$
4. Buscamos e: 20/1=0, 20/3=6.67. e=3
5. Calculamos d como el inverso multiplicativo módulo z de e, por ejemplo, sustituyendo Y por 1,2,3,… hasta que se obtenga un valor entero en la expresión: $d = \frac{(Y*fi(n))+1}{e} = \frac{Y*20+1}{3} = \frac{21}{3} = 7$
6. e=3 y n=33 son la clave pública
7. d=7 y n=33 son la clave privada
8. Cifrado: Mensaje = 5, $C = M^e \ mod \ n = \ 5^3 mod \ n = 5^3 \ mod \ 333 = 26$
9. Descifrado: $M = C^d mod \ n = 26^7 \ mod \ n = \ 26^7 \ mod \ 33 = 8031810176 \ mod \ 33 = 5$

Ejemplo visual de RSA.

Un ejemplo pedagógico trivial del algoritmo RSA se muestra en la siguiente animación. Para este ejemplo hemos seleccionado p=3 y q=11, dando n=11 y z=20. Un valor adecuado de d es d=7, puesto que 7 y 20 no tienen factores comunes.

Con estas selecciones, e puede encontrarse resolviendo la ecuación 7e=1(mod 20), que produce e=3. El texto cifrado, C, de un mensaje de texto normal, P, se da por la regla $C = P3(mod \ 33)$. El texto cifrado lo descifra el receptor de acuerdo con la regla $P = C3(mod \ 33)$. Observe la animación tanto en el emisor como en el receptor, donde se muestra el cifrado-descifrado del texto normal “CASA”.

Dado que los números primos escogidos para este ejemplo son tan pequeños, P debe ser menor que 33, por lo que cada bloque de texto normal puede contener sólo un carácter. El resultado es un cifrado por sustitución monoalfabética, no muy impresionante. En cambio

si hubiéramos seleccionado p y q ≃ 10100, podríamos tener n ≃ 10200, para que cada bloque pueda ser de hasta 664 bits (s644 ≃ 10200) u 83 caracteres de 8 bits, contra 8 caracteres para el DES.

2.2.3.5.4.2 Funciones Resumen.

Una función resumen (hash en inglés), proporciona una secuencia de bits de pequeña longitud que va asociada al mensaje, aunque contiene menos información que éste, y que debe resultar muy difícil de falsificar. Existen 2 clases de funciones resumen:

a) Funciones MAC (Message Authentication Code) las mismas que emplean en sus cálculos una clave adicional y,
b) Funciones MDC (Modification Detection Codes) que son aquellas que no usan clave adicional para sus cálculos.

Sabemos que un mensaje m puede ser autentificado codificando con la llave privada Kp el resultado de aplicarle una función resumen, $EKp(r(m))$. Esa información (que denominaremos firma del mensaje m) sólo puede ser generada por el poseedor de la clave privada Kp. Cualquiera que tenga la llave pública correspondiente estará en condiciones de decodificar y verificar la firma. Para que sea segura, la función resume r(x) debe cumplir además ciertas características:

- r(m) es de longitud fija, independientemente de la longitud de m.
- Dado m, es fácil calcular r(m).
- Dado r(m), es computacionalmente intratable recuperar m.
- Dado m, es computacionalmente intratable obtener un m0 tal que $r(m) = r(m0)$.

Estas propiedades son válidas tanto para los MDC como para los MAC, con la dificultad añadida para estos últimos de que el atacante deberá averiguar además la clave correspondiente. De hecho, conocida la clave, un MAC se comporta exactamente igual que un MDC.

2.2.3.5.4.2.1 Estructura de una función MDC.

En general, los MDC se basan en la idea de funciones de compresión, que dan como resultado bloques de longitud fija a, a partir de bloques de longitud fija b, con a < b.

Estas funciones se encadenan de forma iterativa, haciendo que la entrada en el paso i sea función del i-ésimo bloque del mensaje (mi) y de la salida del paso i - 1. En general, se suele incluir en alguno de los bloques del mensaje m al principio o al final, información sobre la longitud total del mensaje. De esta forma se reducen las probabilidades de que dos mensajes con diferentes longitudes den el mismo valor en su resumen.

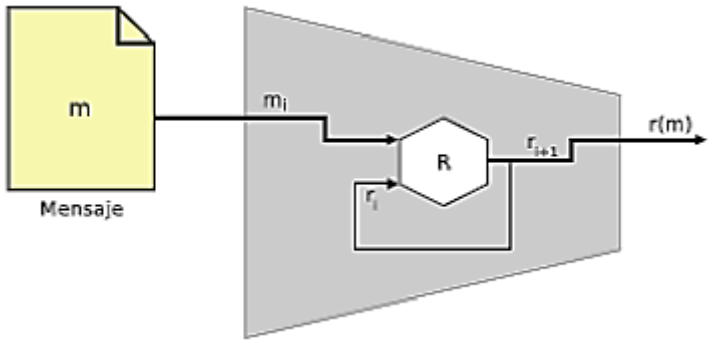


Ilustración 32: Estructura iterativa de una función resumen. R representa la función de compresión, m es el mensaje completo, mi el i-ésimo trozo de m, y ri la salida de la función en el paso i.

2.2.3.5.4.2.2 Algoritmo SHA-1.

La familia SHA (Secure Hash Algorithm, Algoritmo de resumen Seguro) es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST). El primer miembro de la familia fue publicado en 1993 y se lo llamó oficialmente SHA. Sin embargo, ahora se le llama SHA-0 para evitar confusiones con sus sucesores. Dos años más tarde el primer sucesor de SHA fue publicado con el nombre de SHA-1. Existen cuatro variantes más que se han publicado desde entonces cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: SHA-224, SHA-256, SHA-384, y SHA-512 (llamándose SHA-2 a todos ellos).

En 1998 se detectó un ataque a SHA-0, pero no fue reconocido para SHA-1, se desconoce si fue la NSA quien lo descubrió, pero aumentó la seguridad del SHA-1.

SHA-1 ha sido examinado muy de cerca por la comunidad criptográfica pública, y no se ha encontrado ningún ataque efectivo. No obstante, en el año 2004, un número de ataques significativos fueron divulgados sobre funciones criptográficas de hash con una estructura similar a SHA-1; lo que ha planteado dudas sobre la seguridad a largo plazo de SHA-1.

SHA-0 y SHA-1 producen una salida resumen de 160 bits (20 bytes) de un mensaje que puede tener un tamaño máximo de 2^{64}bits, y se basa en principios similares a los usados por el profesor Ronald L. Rivest del MIT en el diseño de los algoritmos de resumen de mensaje MD4 y MD5.

En el 2005, la seguridad del algoritmo SHA-1 se ha visto comprometida por un equipo de investigadores chinos, compuesto por Xiaoyun Wang, Yiqun Lisa Yin y Hongbo Yu (principalmente de la Shandong University en China), quienes han demostrado que son capaces de romper el SHA-1 en al menos 2^{69} operaciones, unas 2000 veces más rápido que un ataque de fuerza bruta (que requeriría 2^{80} operaciones). Los últimos ataques contra SHA-1 han logrado debilitarlo hasta 2^{63}.

A pesar de que 2^{63}, suponen aún un número alto de operaciones, se encuentra dentro de los límites de las capacidades actuales de cálculos, y es previsible que con el paso del

tiempo romper esta función sea trivial, al aumentar las capacidades de cálculo y al ser más serios los ataques contra SHA-1.

La importancia de la rotura de una función hash se debe interpretar en el siguiente sentido: Un hash permite crear una huella digital, teóricamente única, de un archivo. Una colisión entre hashes supondría la posibilidad de la existencia de dos documentos con la misma huella digital.

A pesar de que el NIST contempla funciones de SHA de mayor tamaño (por ejemplo, el SHA-512, de 512 bits de longitud), expertos de la talla de Bruce Schneider abogan por, sin llamar a alarmismos, buscar una nueva función hash estandarizada que permita sustituir a SHA-1. Los nombres que se mencionan al respecto son Tiger, de los creadores de Serpent, y WHIRLPOOL, de los creadores de AES.

2.2.3.5.4.3 Gestión de clave.

La gestión de claves son un conjunto de técnicas destinadas a generar, intercambiar, almacenar y destruir claves.

En el mundo real la gestión de claves es la parte más complicada de la criptografía: diseñar un algoritmo criptográfico seguro es relativamente menos complicado que mantener una clave en secreto; esto es así porque es más fácil encontrar puntos débiles en las personas que en los algoritmos criptográficos.

¿De qué vale montar un sistema criptográfico muy avanzado en una organización, si luego hay empleados fáciles de corromper?
A continuación, vamos a comentar varios aspectos fundamentales relacionados con la gestión de claves.

2.2.3.5.4.3.1 Generación de claves.

La seguridad de todo el sistema depende de la clave, si un espía descubre la clave, de nada sirven todos los demás esfuerzos. Sin embargo, hay una serie de factores que influyen negativamente en la seguridad de la clave:

a) **Pobre elección de la clave:** Para evitar estos ataques, una técnica muy usada es recomendar a los usuarios utilizar passphrases en lugar de passwords, que es una frase a la que se hace un hash para obtener la clave.
b) **Espacios de claves reducidos:** Muchas veces sólo se aceptan subconjuntos del juego de caracteres como claves lo que implica que es fácil de romper la clave por fuerza bruta.
c) **Defectos en la generación de claves aleatorias.** Cuando se usan claves binarias (por ejemplo, clave de sesión, o par de claves pública/privada), hay que tener cuidado de que el algoritmo que usemos realmente genere claves aleatorias.

Muchos sistemas se han atacado aprovechando que la clave que generaba el sistema era predecible. Por ejemplo, las primeras implementaciones de SSL de Netscape generaban una clave de sesión en función de la hora, un espía podía predecir la clave de sesión que

iba a generar el programa si sabía la hora del reloj del host donde se estaba ejecutando Netscape. Esta hora además la mandaba Netscape en sus cabeceras, y aunque no se supiera la hora exacta bastaba con saber la hora aproximada para hacer un ataque por fuerza bruta.

Un estándar para generación de claves muy conocido es ANSI X9.17.

2.2.3.5.4.3.2 Transferencia de claves.

Otro problema es el de cómo se ponen de acuerdo A y B en la clave a usar. Una solución es que A y B se reúnan en un lugar físico y acuerden la clave que van a utilizar, pero esto no siempre es posible.

Otra posible solución es que partan la clave en trozos y envíen cada trozo por un canal distinto (correo, telegrama, teléfono, Internet), así el supuesto espía tendría que espiar todos los canales.

La técnica más usada para el intercambio seguro de claves se basa en la criptografía de clave pública y la veremos a continuación:

Básicamente consiste en que A y B usan criptografía asimétrica para acordar una clave de sesión que luego usan con su algoritmo simétrico para comunicarse; el protocolo es el siguiente:

1) B envía a su clave pública.
2) A genera una clave de sesión aleatoria (binaria), la cifra usando la clave pública de B, y se la envía a B.
3) B descifra el mensaje enviado por A, usando su clave privada, y recupera la clave de sesión.
4) Ambos se comunican cifrando sus mensajes con la clave de sesión.

Pero este protocolo es vulnerable al ataque de “Man in the Middle” por lo que veremos a continuación el intercambio seguro de claves con firmas digitales.

2.2.3.5.4.3.2.1 Intercambio seguro de claves con firmas digitales.

Podemos usar firmas digitales para evitar el man in the middle attack. Para ello necesitamos un árbitro que firme las claves públicas de A y B.

Una vez que A y B tienen sus claves públicas firmadas por el árbitro, el atacante no puede cambiar las claves de A y B, ya que no sabe firmarlas con la firma del árbitro.

Ahora, lo más que puede hacer el atacante activo es impedir que A y B se comuniquen, pero no puede escuchar la comunicación.

2.2.3.5.4.3.3 Almacenamiento de claves.

Las claves binarias (por ejemplo, una clave privada) no las puede memorizar una persona, sino que hay que almacenarlas en disco, pero su almacenamiento en disco es peligroso

porque alguien podría acceder a ellas. Para evitarlo las claves se almacenan cifradas con un password o passphrase.

Ahora la seguridad de la clave depende de dos factores:

1) Las posibilidades que tiene el espía de acceder al fichero (por ejemplo, en una máquina UNIX, si un usuario desactiva el permiso r de un fichero, los demás usuarios no pueden ver sus ficheros, pero el supe usuario de la máquina sí que puede acceder a él).
2) La fuerza del password o passphrase que se usó para cifrar el fichero.

Otra alternativa consiste en almacenar las claves en tarjetas USB destinadas a este fin, de forma que las claves nunca permanecen en disco y si el espía quiere nuestra clave debería quitarnos la tarjeta. Esta solución tiene la ventaja de que podemos estar seguros de si alguien tiene acceso al sistema o no, ya que siempre podemos saber si tenemos la tarjeta en el bolsillo, o no.

Recuérdese que, un posible ataque que puede lanzar el espía para acceder a nuestra clave consiste en estudiar el fichero de memoria virtual del sistema.

Este ataque es posible porque los sistemas operativos modernos paginan los programas de RAM a disco sin avisar, y nosotros nunca sabemos si la clave no se ha paginado a disco en mitad de la ejecución del programa.

2.2.3.5.4.3.4 Previsión de pérdida de claves.

Imaginemos que A trabaja en una empresa que le obliga a cifrar todos sus ficheros. Y supongamos que A muere, entonces todos sus datos se pierden para siempre.

Para evitarlo podemos usar el algoritmo de compartición de secreto: A reparte su clave entre otros empleados de forma que un empleado, por sí solo, no puede acceder a los datos de A, pero si es necesario se pueden reunir todos los empleados y reconstruir la clave de A.

2.2.3.5.4.3.5 El ciclo de vida de una clave.

Normalmente, no se recomienda mantener una clave durante mucho tiempo, ya que esto aumenta la probabilidad de que alguien la descubra, y si la descubre mayor será la cantidad de información a la que podrá acceder. Además, la tentación que tiene el atacante por descubrirla será mayor si la clave no se cambia muy a menudo que si se cambia diariamente.

Por el contrario, los usuarios suelen ser reacios a cambiar regularmente sus claves, con lo que una solución de compromiso podría ser la actualización automática de claves, que consiste en que el sistema cambia periódicamente las claves como un hash de la clave anterior.

2.2.3.5.4.4 Firmas digitales.

La firma digital es una secuencia de datos electrónicos (bits) que se obtienen mediante la aplicación a un mensaje determinado de un algoritmo (fórmula matemática) de cifrado, y que equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje. Desde un punto de vista material, la firma digital es una simple cadena o secuencia de caracteres que se adjunta al final del cuerpo del mensaje firmado digitalmente.

Las firmas digitales, al igual que las firmas normales, se usan para conseguir básicamente cuatro objetivos:

1) **Integridad.** Una vez que el documento se firma, si luego se modifica se detecta el cambio.
2) **Autenticidad.** La firma convence al receptor del documento de que está firmado por quien aparece como firmante.
3) **Irreutilizabilidad.** Nadie puede copiar la firma de un documento a otro documento, y si lo hace la firma se detecta como inválida.
4) **Irrepudiabilidad.** El firmante no puede luego alegar que él no firmó el documento.

2.2.3.5.4.4.1 Firma de documentos con criptografía de clave secreta y árbitro.

Se puede implementar un sistema de firmas digitales usando sólo criptografía de clave secreta y un árbitro.

Supongamos que A quiere firmar un documento y enviárselo a B. También supongamos que el árbitro comparte una clave secreta KA con A y otra clave secreta KB con B.

En este escenario, el protocolo para firmar documentos digitalmente podría ser:

1º) A cifra el mensaje que quiere enviar a B firmado usando KA y se lo envía al árbitro.
2º) El árbitro descifra el mensaje usando KA y lo guarda en su base de datos.
3º) El árbitro cifra el mensaje plano usando KB y se lo envía a B.
4º) B descifra el mensaje con KB.

El árbitro sabe que el mensaje proviene de A porque es el único que comparte la clave secreta KA con él.

B está seguro de que el documento recibido es auténtico ya que se lo ha enviado cifrado el árbitro, que es el único que (además de él mismo) conoce KB.

Este protocolo cumple con los cuatro objetivos que se consiguen con un protocolo de firma digital:

1º) **Integridad.** Si el mensaje se modifica al enviarlo de A al árbitro o del árbitro a B, el proceso de descifrada falla.
2º) **Autenticidad.** Como B confía en el árbitro, y es el único que comparte con el KB, sabe que el mensaje procede de A.
3º) **Irreutilizabilidad.** Si B muestra mensajes firmados que A dice no haber firmado, pueden ir al árbitro que resuelve la disputa consultando su base de datos.
4º) **Irrepudiabilidad.** Si A alega no haber firmado un documento que sí ha firmado, B puede ir al árbitro que determina que el documento sí que está en la base de datos.

Si B quiere demostrar a C la autenticidad de un documento firmado por A pueden seguir el siguiente protocolo:

1º) B cifra el mensaje con KB y se lo envía al árbitro indicándole que quiere demostrar a C que el documento fue firmado por A.
2º) El árbitro descifra el mensaje y comprueba en su base de datos que el documento fue firmado por A.
3º) El árbitro vuelve a encriptar el mensaje con KC y se lo envía a C.
4º) C desencripta el mensaje.

C confía en el árbitro, y sabe que el mensaje es auténtico porque sólo C y el árbitro conocen la clave secreta KC.

Como acabamos de ver, este protocolo funciona, pero presenta dos inconvenientes:

- Debe existir un árbitro en el cual deben confiar todos.
- El árbitro se convierte en un cuello de botella.

Estos problemas los van a resolver los algoritmos criptográficos de firma con clave pública que vamos a ver a continuación.

2.2.3.5.4.4.2 Firma de documentos con criptografía de clave pública.

La criptografía de clave pública es la técnica que se suele usar para generar firmas digitales.

Tiene básicamente dos ventajas respecto a la técnica anterior:

- No necesita un árbitro.
- La clave privada, a diferencia de la clave secreta, no la tenemos que compartir con nadie.

Para firmar digitalmente un documento con técnicas de criptografía asimétrica, tal como se muestra en la siguiente tabla, se utiliza la clave privada para firmar, y la clave pública para comprobar la firma.

	CLAVE PRIVADA	CLAVE PUBLICA
CONFIDENCIALIDAD	Descifrar	Cifrar
FIRMA DIGITAL	Firmar	Verificar

Tabla 1: Uso de las claves públicas/privadas para confidencialidad y firma.

Realmente firmar es equivalente a cifrar con la clave privada, y verificar es equivalente a descifrar con la clave pública, con lo que a veces al proceso de firmar se le llama "cifrar con clave privada", y al de verificar "descifrar con la clave pública".

El protocolo que se sigue para firmar digitalmente un documento es:

1) A cifra el documento con su clave privada, dando lugar al documento firmado.
2) A envía el documento original y su firma a B.
3) B descifra el documento usando la clave pública de A, y verifica el documento, para ello el documento firmado descifrado debe ser igual al documento original. Es decir, si S(KprivadaA, M) es la firma (sign) del mensaje M usando la clave privada de A(KprivadaA), y V(KpúblicaA, M) es la verificación del documento M usando la clave pública de A, se cumple que:

$$V\big(KpúblicaA, S(KprivadaA, M)\big) = M$$
$$D\big(KpúblicaA, E(KprivadaA, M)\big) = M.$$

Siendo E() la función de encriptación (cifrado) y D() la función de desencriptación (descifrado).

Obsérvese que este protocolo, al igual que el anterior, también satisface los cuatro objetivos de las firmas digitales:

1) **Integridad.** Si se modifica el documento, la firma no coincide con la del documento y se detecta el cambio. Es decir, si un atacante modifica el documento tendría que modificar también su firma para evitar que se detecte el cambio, pero el atacante no conoce la clave privada necesaria para recalcular la firma.
2) **Autenticidad.** El receptor sabe que el documento está firmado por quien dice que lo ha firmado porque es el único que conoce la clave privada.
3) **Irreutilizabilidad.** Nadie puede copiar la firma de un documento a otro documento, y si lo hace la firma se detecta como inválida.
4) **Irrepudiabilidad.** El firmante no puede luego alegar que él no firmó el documento, porque él es el único que conoce la clave privada.

Respecto a las principales aplicaciones que tienen hoy en día las firmas digitales, vamos a comentar cuatro de ellas:

1) **Firmar e-mails.** Con S/MIME o PGP podemos firmar e-mails usando una clave privada, y luego el receptor del e-mail puede comprobar su autenticidad usando una clave pública.
2) **Firmar un contrato.** La mayoría de países (incluido Ecuador) ya ha introducido la firma digital como válida para firmar contratos.
3) **Crear servidores seguros.** Podemos diseñar servidores que firmen la información que sirven con el fin de que un atacante no la pueda modificar. Por ejemplo, los servidores DNS seguros firman los nombres DNS que resuelven.
4) **Identificación de usuarios frente al servidor.** Una forma más segura que la identificación por password es que el usuario al mandar una petición al servidor la firme digitalmente.

2.2.3.5.4.4.3 Algoritmos de firmas digitales más usados.

Existen varios algoritmos para firmas digitales, pero los más usados son:

1) RSA, que además de usarse para criptografía de clave pública se puede usar también para firmar digitalmente.
2) DSA (Digital Signature Algorithm), que es un algoritmo propuesto en 1991 por el NIST (National Institute for Standards and Technology). DSA se diseñó con el fin de que sólo se pudiera usar para firmar, pero no para cifrar.

Una diferencia que hay entre RSA y DSA está en lo que respecta a la velocidad: DSA es más rápido para generar la firma que RSA, pero RSA es más rápido validando la firma. Como una firma se valida más veces que lo que se crea, de acuerdo a este criterio sería mejor RSA.

2.2.3.5.4.5 Certificados Digitales X.509.

X.509 define el esquema para proveer servicios de autenticación a los usuarios de servicios de directorios X.500, el cual define una serie de recomendaciones para servicios de directorio. El directorio sirve como un repositorio de llaves públicas (certifican llaves públicas). Un certificado digital es un archivo que identifica inequívocamente a un individuo o un website y permite establecer comunicaciones seguras y confidenciales. Asocia el nombre de una entidad que participa en una transacción segura con la llave pública usada para firmar la comunicación con esa entidad en un sistema criptográfico.

Generalmente los certificados están “firmados” por una Autoridad Certificadora (CA). Los certificados digítales se presentan en tres versiones diferentes, pero la versión 3 es la que se encuentra con más frecuencia en los sistemas hoy en día. Los campos que contiene un certificado digital son los siguientes:

- Versión.
- Número serial.
- Identificador del algoritmo de firma.
- Nombre del emisor.
- Periodo de validez.
- Nombre del usuario.
- Información de la llave pública del usuario.
- Identificador único del emisor (versión 2 y 3).
- Identificador único del usuario (versión 2 y 3).
- Extensiones (versión 3).
- Firma digital de los campos anteriores.

Los certificados tienen las siguientes características:

- Cualquier usuario con acceso a la llave pública de la Autoridad Certificadora puede recuperar la llave pública del usuario que fue certificado.
- Nadie más que la Autoridad Certificadora puede modificar el certificado sin ser detectado.

Como los certificados son inforjables, si un usuario A tiene el certificado de otro usuario B, tiene la seguridad de que los mensajes que encripta con la llave pública de B solo pueden

ser leídos por B, y los mensajes que hayan sido firmados con la clave privada de B son inforjables.

Por la gran cantidad de usuarios, se han creado distintas Autoridades Certificadoras, cada una posee un par de llaves pública y privada, con las cuales emiten sus certificados. Cada Autoridad Certificadora tiene las llaves públicas de las otras Autoridades Certificadoras para así poder verificar la validez de los certificados que no sean emitidos por ella misma.

Las Autoridades Certificadoras pueden también revocar los certificados antes de que estos expiren por alguna de las siguientes razones:

- Cuando se asume que la llave secreta del usuario está comprometida.
- El usuario no seguirá siendo certificado por la Autoridad Certificadora.
- Cuando se asume que el certificado emitido por la Autoridad Certificadora está comprometido.

2.2.3.5.4.6 SSL (Secure Socket Layer).

El Secure Socket Layer o SSL fue desarrollado por Netscape para brindar un canal de comunicación seguro entre los servidores web y los clientes web que decidan utilizarlo. SSL es un protocolo del stack de protocolos TCP/IP. SSL se ubica entre la capa de transporte y la capa de aplicación, debido a que cada capa hace uso de los servicios de las capas inferiores, SSL puede utilizarse para proteger las comunicaciones que se realizaren utilizando cualquiera de los protocolos de la capa de aplicación (Telnet, FTP, SMTP, etc.), sin embargo, actualmente el SSL solo funciona con el HTTP. SSL asegura el canal de comunicación brindando encriptación end-to-end de los datos que se transmiten entre el servidor web y el navegador.

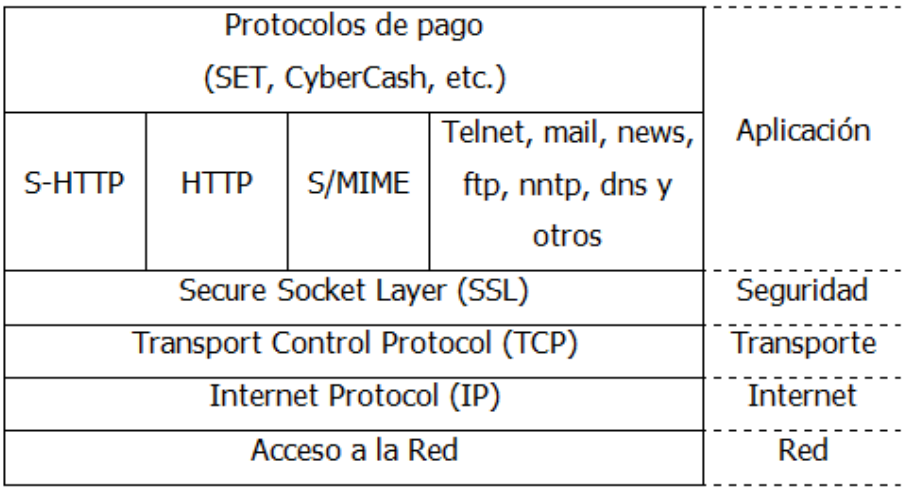


Ilustración 33: Stack de protocolos de comunicaciones.

Además de brindar privacidad a los datos que son transmitidos, SSL provee autenticación de la identidad del servidor web (y opcionalmente del cliente web). Esto significa que, si se logra establecer una comunicación segura, entonces el servidor web está registrado con una Autoridad Certificadora. Las Autoridades Certificadoras se encargan de comprobar que los servidores pertenezcan a compañías legalmente establecidas. En caso de que una

compañía apruebe los requerimientos de una Autoridad Certificadora, esta firmará el certificado de esa compañía.

Para acceder a un recurso utilizando SSL, se coloca “https” en el campo del protocolo del URL, lo cual hace que el navegador haga la conexión con el servidor en el puerto TCP 443, que es el puerto estándar para conexiones seguras en Internet.

Los pasos para establecer una comunicación segura utilizando SSL son los siguientes:

- El browser envía al cliente un mensaje “Client Hello” consistente de la suite de protocolos que maneja el browser y una cadena de “challenge” aleatoria. La suite de protocolos indica los algoritmos que soporta el browser para la generación de llaves, encriptación de datos y cálculo de hash. La cadena “challenge” es única para esa sesión y se utilizará luego para comprobar que se logró establecer una comunicación segura.
- El servidor responde con un mensaje “Server Hello” que consiste de un certificado estándar X.509, una confirmación de que acepta los protocolos del browser y un número identificador de conexión aleatorio. El identificador de conexión también se utilizará para comprobar que se estableció una sesión segura con el cliente.
- El cliente verifica la validez del certificado del servidor web. Para que el certificado del servidor sea aprobado, este debe estar firmado digitalmente por una Autoridad Certificadora que el browser reconozca. Si el certificado es autenticado exitosamente, entonces el browser genera un “master secret” que es un número aleatorio que servirá como semilla para la generación de las llaves para la encriptación simétrica de los datos. El master secret se envía al servidor encriptado con su llave pública.

A partir de este momento no es necesaria la encriptación de llave pública. El master secret se utiliza para generar dos llaves simétricas, una para el envío y otra para la recepción de datos. Debido a que el servidor y el browser utilizan los mismos algoritmos para la generación de llaves y el mismo master secret, las llaves que generan son iguales.

- El browser envía un mensaje de “Client Finish” que contiene el identificador de conexión aleatorio que generó el servidor, encriptado con la llave de envío del browser. Si el servidor generó la misma llave para la recepción de datos, entonces podrá desencriptar el mensaje y comparar el identificador de conexión que recibe con el que generó anteriormente. Si los identificadores coinciden entonces se estableció una comunicación segura.
- Para finalizar la inicialización el servidor envía un mensaje de “Server Finish”. El servidor utiliza su llave de envío para encriptar la cadena de challenge que recibió durante el “Client Hello” y enviársela al browser. Si el browser desencripta la cadena con su llave de recepción y la compara exitosamente con la cadena que generó anteriormente, entonces tiene la seguridad de que se estableció una sesión segura.

La versión más actual de SSL es la v3, existen otro protocolo parecido a SSL que es desarrollado por IETF que se denomina TLS (Transport Layer Security) y difiere en que usa un conjunto más amplio de algoritmos criptográficos. Por otra parte, existe también SSL plus, un protocolo que extiende las capacidades de SSL y tiene por mayor característica que es interoperable con RSA,

DSA/DH y CE (Criptografía Elíptica).

Gráficamente, el procedimiento para establecer una comunicación segura con SSL es el siguiente:

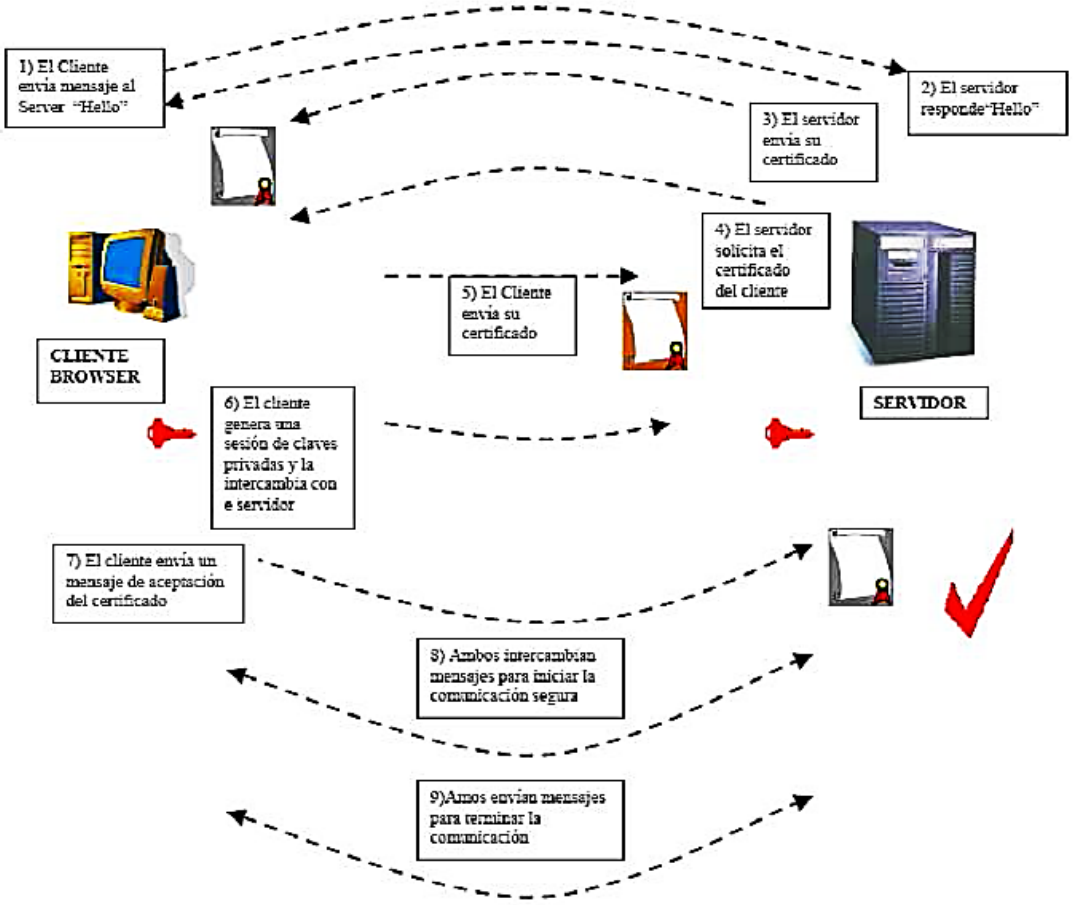


Ilustración 34: Establecimiento de comunicación con el protocolo SSL.

2.2.3.5.4.7 SET (Secure Electronic Transaction).

En 1985 las compañías Visa y MasterCard junto con otras empresas del sector tecnológico como RSA, IBM, Netscape, VeriSign, Microsoft, entre otras, decidieron desarrollar un protocolo respaldado por la industria y estandarizado desde el primer momento. El propósito de este protocolo es favorecer las transacciones electrónicas con tarjetas de crédito a través de redes electrónicas.

SET trata de cubrir los agujeros de seguridad dejados por SSL. Por ejemplo, con SSL solo se protege el número de tarjeta cuando se envía del cliente al comerciante, sin embargo, no hace nada para la validación del número de tarjeta, para chequear sí el cliente está autorizado a usar ese número de tarjeta, para ver la autorización de la transacción del banco del comerciante etc. Todas estas debilidades son cubiertas por SET, éste permite dar seguridad al cliente, al comerciante, al banco emisor de la tarjeta y al banco del comerciante.

El proceso de SET es el siguiente:

1) **El cliente inicializa la compra:** consiste en que el cliente usa el navegador para seleccionar los productos a comprar y llena la forma de orden correspondiente. SET comienza cuando el cliente hace clic en “pagar” y se envía un mensaje de iniciar SET.
2) **El cliente usando SET envía la orden y la información de pago al comerciante:** el software SET del cliente crea dos mensajes uno conteniendo la información de la orden de compra, el total de la compra y el número de orden. El segundo mensaje contiene la información de pago, es decir, el número de la tarjeta de crédito del cliente y la información del banco emisor de la tarjeta. El primer mensaje es cifrado usando un sistema simétrico y es empaquetada en un sobre digital que se cifra usando la clave pública del comerciante. El segundo mensaje también es cifrado, pero usando la clave pública del banco (esto previene que el comerciante tenga acceso a los números de tarjetas de los clientes). Finalmente, el cliente firma ambos mensajes.
3) **El comerciante pasa la información de pago al banco:** el software SET del comerciante genera un requerimiento de autorización, éste es comprimido (con un hash) y firmado por el comerciante para probar su identidad al banco del comerciante, además de ser cifrado con un sistema simétrico y guardado en un sobre digital que es cifrado con la clave pública del banco.
4) **El banco verifica la validez del requerimiento:** el banco descifra el sobre digital y verifica la identidad del comerciante, en el caso de aceptarla descifra la información de pago del cliente y verifica su identidad. En tal caso genera un requerimiento de autorización lo firma y envía al banco que genero la tarjeta del cliente.
5) **El emisor de la tarjeta autoriza la transacción:** el banco del cliente (emisor de la tarjeta) confirma la identidad del cliente, descifra la información recibida y verifica la cuenta del cliente en caso de que no haya problemas, aprueba el requerimiento de autorización, lo firma y lo regresa al banco del comerciante.
6) **El banco del comerciante autoriza la transacción:** una vez recibida la autorización del banco emisor, el banco del comerciante autoriza la transacción la firma y la envía al servidor del comerciante.
7) **El servidor del comerciante complementa la transacción:** el servidor del comerciante da a conocer que la transacción con la tarjeta fue aprobada y muestra al cliente la conformidad de pago, y procesa la orden que pide el cliente terminado la compra cuando se le son enviados los bienes que compró el cliente.
8) **El comerciante captura la transacción:** en la fase final de SET el comerciante envía un mensaje de “captura” a su banco, esto confirma la compra y genera el cargo a la cuenta del cliente, así como acreditar el monto a la cuenta del comerciante.
9) **El generador de la tarjeta envía el aviso de crédito al cliente:** el cargo de SET aparece en el estado de cuenta del cliente que se le envía mensualmente.

2.2.3.5.4.8 S-HTTP (Secure Hyper Text Transfer Protocol).

El Secure Hyper Text Transfer Protocol o S-HTTP es una extensión del protocolo HTTP. S-HTTP fue desarrollado por Enterprise Integration, comercializado por Terisa Systems y

distribuido por el consorcio Commerce Net. S-HTTP trabaja a nivel de la capa de aplicación del stack de protocolos TCP/IP.

S-HTTP fue desarrollado para soportar una gran variedad de mecanismos de seguridad, incluyendo criptografía de llave privada y de llave pública, funciones de hash y firmas digitales. Estos mecanismos pueden ser utilizados por separado o en combinación para brindar diferentes opciones de seguridad. Los mecanismos de seguridad de una sesión pueden ser especificados por cualquiera de las partes. Para cada mecanismo de seguridad se puede especificar que es requerido, opcional o rechazado. Si un mecanismo es requerido, entonces la comunicación se establece solo si el mecanismo especificado está en uso. La especificación opcional indica que el mecanismo será aceptado, pero no es requerido para establecer la comunicación. La opción rechazada indica que la entidad no acepta o no puede implementar determinado mecanismo de seguridad.

A diferencia de SSL que utiliza una serie de mensajes de inicialización S-HTTP envía la información de inicialización encapsulada en los encabezados de los paquetes de información. Esto permite que las opciones de seguridad sean modificadas en cualquier momento después de establecida la comunicación.

Una vez que la comunicación ha sido establecida y se han acordado las opciones de seguridad de la misma, la información se envía en un “sobre digital”. El sobre digital contiene la información encriptada con un algoritmo de llave privada, la firma digital del emisor y la llave privada utilizada para encriptar la información, esta llave está encriptada con la llave pública del receptor. La llave privada utilizada para la encriptación de los datos se envía solo en el primer sobre digital.

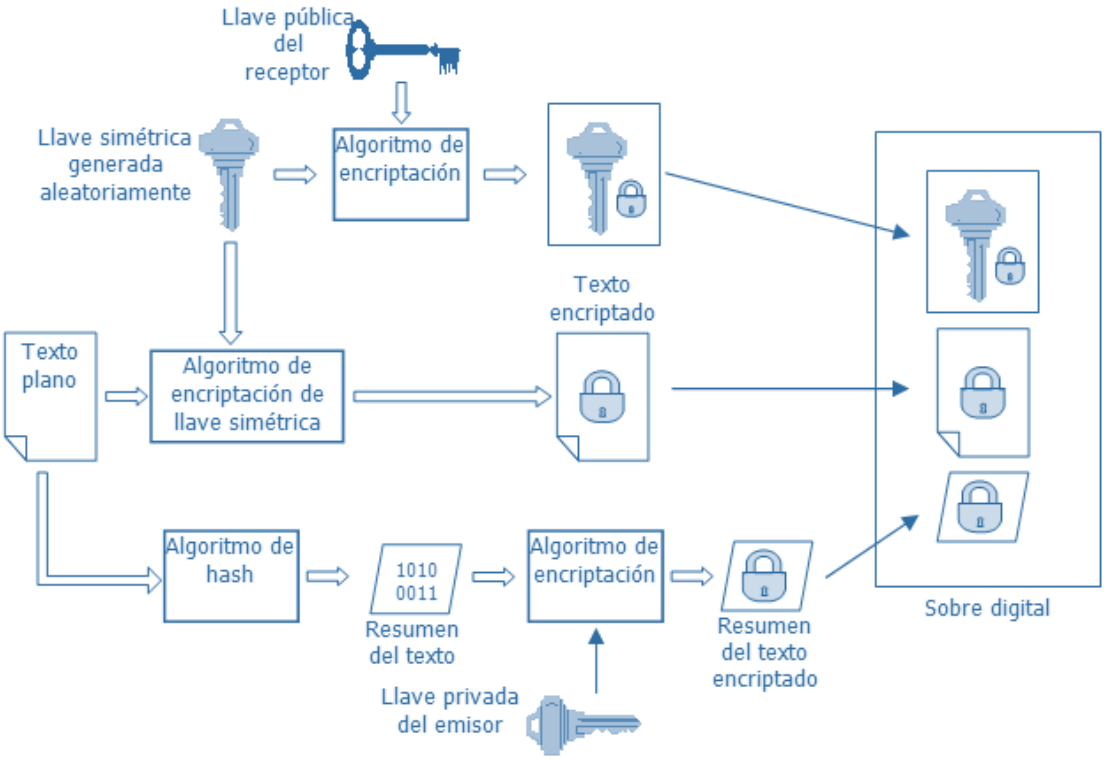


Ilustración 35: Proceso de generación de un sobre digital.

Para abrir el sobre digital, el receptor comprueba la firma digital para verificar la integridad y la autenticidad de la identidad del emisor, luego desencripta la llave contenida en el sobre con su llave privada y por ultimo desencripta el resto de la información con la llave que obtuvo anteriormente.

El S-HTTP no ha tenido tanta aceptación en el mercado como el SSL debido a que este requiere de un proceso de configuración en el servidor y los browsers que es más complicado que el de SSL, el cual viene configurado de fábrica en los navegadores Netscape Navigator y Microsoft Internet Explorer. Debido a que S-HTTP se implanta en la capa de aplicación, solo puede brindar seguridad a las sesiones HTTP, en cambio SSL tiene el potencial de brindar seguridad a las comunicaciones hechas a través de cualquier protocolo de la capa de aplicación. Sin embargo, S-HTTP es más flexible y permite establecer varios niveles diferentes de seguridad en cada sesión.

2.2.3.5.4.9 Firewalls.

Un firewall se define como un software o hardware que permite que solo lo usuarios externos que cumplen con ciertas características accedan a una red privada. Generalmente los firewalls permiten que los usuarios internos tengan acceso total a los servicios externos mientras que restringe el acceso del exterior basándose en una serie de reglas.

En la práctica, los firewalls son una combinación de Routers de monitoreo de paquetes y una computadora que ejecuta una serie de proxis. Los proxis son programas simples que almacenan y envían los paquetes basándose en la evaluación de una serie de reglas.

Para que un firewall cumpla con su función de proteger a la organización, las reglas en las que se basa su operación deben estar configuradas. La incapacidad de definir una política de seguridad que no sea ambigua y los errores en la configuración del firewall para que apoye esa política son las causas de que los firewalls fallen en su función de proteger las redes de los atacantes.

Los firewalls se colocan entre la red corporativa (red segura) y la red externa (Internet). Aunque los firewalls se colocan como barrera entre las redes interna y externa, también pueden ser utilizados para subdividir las redes internas de una organización.

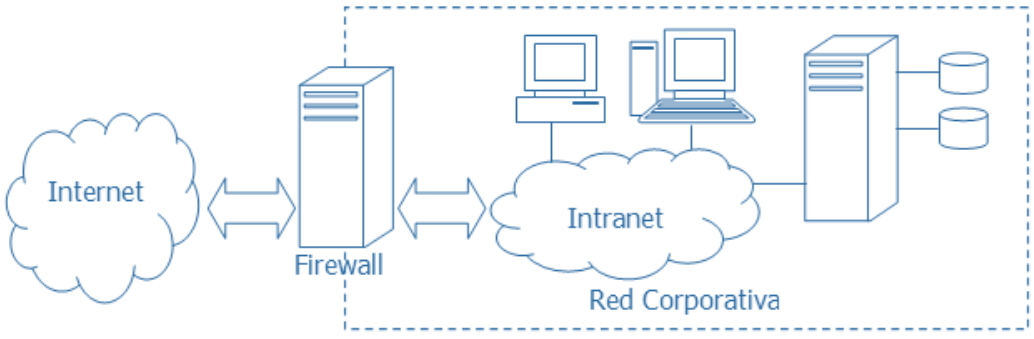


Ilustración 36: Ubicación de los Firewalls en las redes.

Existen diferentes tipos de firewalls, cada uno de ellos ofrece un nivel diferente de seguridad. Los diferentes tipos de firewall son:

- **Sistema de registro de tráfico (traffic logging systems):** Estos sistemas graban toda la información acerca del tráfico de la red que pasa a través del firewall en un archivo o una base de datos para propósitos de auditoria. Estos registros pueden ser generados automáticamente por la mayoría de los servidores web.
- **Routers de monitoreo de paquetes IP:** El router de monitoreo es el firewall más simple, funciona filtrando los paquetes de información que pasan a través de él basándose en un conjunto de reglas que tiene programadas y que se aplican automáticamente.

Las reglas más comunes para el monitoreo de paquetes de información son:

- Protocolo del paquete de información. Controla el tráfico de red basándose en el protocolo del paquete (TCP, UDP, ICMP).
- Aplicación a la cual está dirigido el paquete. Restringe el acceso a ciertas aplicaciones al bloquear el tráfico dirigido al puerto de red que utiliza la aplicación.
- Direcciones IP de origen. Bloquea los paquetes que provengan de ciertas direcciones IP.

- **Firewall endurecido (hardened firewall host):** Un firewall endurecido es un computador dedicado al firewall al que se le han removido todos los recursos innecesarios con el fin de aumentar su seguridad. Un firewall de este tipo obliga a los usuarios externos a conectarse a las aplicaciones que están en el firewall en vez de hacerlo a las aplicaciones que están en un equipo dentro de la red de la organización. La principal función de este tipo de firewall es evitar que usuarios no autorizados ingresen (hagan login) en las computadoras de la red de la organización.
- **Gateway proxy de aplicaciones (proxy application gateway):** Los firewalls también pueden ser creados a través de un software llamado servicio proxy. El computador en el cual se ejecuta el servicio proxy se conoce como gateway de aplicación (application gateway). Si un usuario interno se quiere conectar a un equipo fuera de la red de la organización, primero debe conectarse al proxy y este se conecta al equipo remoto. Igualmente, si un usuario en un equipo remoto quiere conectarse a un equipo en la red interna tiene que hacerlo a través del proxy.

Otra función de este tipo de firewall es mantener un cache de documentos. Un cache es un almacenamiento local de un documento para poder presentarlo más rápidamente que si se descarga del servidor donde se encontraba almacenado originalmente.

Los firewalls son útiles para proteger las brechas de seguridad de los sistemas operativos de los equipos donde se ejecuta el software servidor al restringir los servicios disponibles a los usuarios externos. Esta restricción se logra bloqueando los puertos de red que no deban estar disponibles para los usuarios externos.

Existen 65536 puertos de red, y un servicio puede ofrecerse en cada uno de ellos. Existen programas que revisan los puertos de un equipo para determinar en cuáles de ellos se ofrecen servicios (programas scanner). Luego que un servicio se detecta, se puede iniciar un ataque para tratar de explotar vulnerabilidades en ese servicio. Los firewalls evitan este problema al restringir el acceso a los puertos y permitirlo solo en los puertos en los que se ofrecen servicios al exterior (web, mail, ftp, etc.). El problema es que existe una serie de ataques que se aprovechan de los servicios que si son permitidos por el firewall. Estos ataques explotan las fallas de estos servicios y se conocen como ataques “data driven” (a

través de los datos). Los firewalls no pueden hacer nada para evitar que los errores en los programas servidores sean explotados.

Otro problema de los firewalls es que si existen otros medios para conectar la red interna con el exterior los firewalls se vuelven inútiles. Un ejemplo de esto son los módems instalados en ciertas máquinas para dar acceso remoto a usuarios, estos módems brindan acceso incontrolado a los sistemas en los que están instalados, haciéndolos un problema, ya que si un atacante conoce el número telefónico al que están conectados puede utilizarlos para evadir los firewalls.

2.2.3.6 *Tipos de ataques existentes en el comercio electrónico.*

En la actualidad existen diversos tipos de técnicas para perpetrar fraudes en el comercio electrónico, sobre todo cuando se realizan operaciones de pago mediante el uso del número de la tarjeta en las tiendas virtuales.

Las amenazas concretas hacia el comercio electrónico se dirigen especialmente hacia los datos sensibles del usuario, con el fin de comprometer la seguridad, a nivel económico, técnico y personal. De ellas, el phishing o fraude a través de Internet es la principal amenaza del comercio electrónico.

Entre los tipos de fraudes mencionados nos limitaremos a analizar solamente aquellos que afectan de forma más directa al pago con tarjeta.

2.2.3.6.1 Phishing.

Phishing es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta.

El estafador o phisher suplanta la identidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, SMS o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador.

Ilustración 37: Phishing.

El phishing incluye el envío de correos electrónicos falsos, procedentes, en apariencia, de empresas o entidades legítimas (por ejemplo, entidades bancarias o páginas de compra online o de subastas), y dirigen al destinatario a webs falsas que replican las de la empresa o entidad legítima. La intención de dichos correos cuando se dirigen a clientes de entidades financieras es intentar que estos revelen sus datos personales o bancarios: número de tarjeta de crédito, claves de acceso (PIN), contraseñas para operar, u otro tipo de datos confidenciales y personales.

Objetivos	Ataques de phishing válidos en diciembre 2009.
PayPal.	12663
Tibia.	853
JPMorgan Chase and Co.	727
Sulake Corpotation.	628
Facebook	507
Internal Revenue Service.	424
HSBC Group	144
Bank of America Corporation.	114
Google.	101
NedBank Ltd.	82

Tabla 2: Objetivos más populares de los ataques de phishing.

2.2.3.6.1.1 ¿Cómo funciona?

Los ataques Phishing funcionan de 4 formas.

1) **Recolección de información:** El objetivo del atacante cibernético es engañarte para hacer clic en un enlace que te llevará a una página web que pide tu nombre de usuario y contraseña o, tal vez, tu número de tarjeta de crédito o tu PIN para usar el cajero automático. Estos sitios web tienen el mismo aspecto que los sitios legítimos, poseen las mismas imágenes y dan la sensación de ser páginas de bancos o tiendas, pero son sitios falsos diseñados por el criminal para robar tu información.

2) **Infectar tu computadora con enlaces maliciosos:** Una vez más, el objetivo del atacante es que tú hagas clic en un enlace. Sin embargo, en lugar de recolectar tu información, su objetivo es infectar tu computadora. Si haces clic en el enlace, te redirige a un sitio web que de forma silenciosa lanza un ataque contra tu equipo y, si tiene éxito, infectará tu sistema.

3) **Infectar tu computadora con archivos adjuntos maliciosos:** Estos son correos electrónicos Phishing que contienen archivos adjuntos maliciosos, tales como archivos PDF o documentos de Microsoft Office infectados. Si los abres atacarán tu computadora y si tienen éxito, le darán al atacante control total sobre tu equipo.

4) **Estafas:** Son intentos hechos por delincuentes para estafarte. Ejemplos clásicos incluyen: noticias como que has ganado la lotería, solicitudes de donaciones de caridad después de un desastre reciente o un dignatario que necesita transferir millones de dólares a tu país y está dispuesto a pagarte por ayudarle con la transferencia. No te dejes engañar, estas son estafas creadas por criminales que están detrás de tu dinero.

2.2.3.6.1.2 Protección.

En la mayoría de los casos, solo abrir un correo electrónico es seguro. Para que la mayor parte de los ataques funcionen, tienes que hacer algo después de leer el correo (por ejemplo, abrir el archivo adjunto, dar clic en un enlace o responder la solicitud de información). Aquí te presentamos algunos tips para reconocer un ataque por correo electrónico.

- Sospecha de cualquier correo que requiera de "acción inmediata" o cree un sentido de urgencia. Esta es una técnica común usada por los criminales para apresurar a la gente a cometer un error.
- Sospecha de correos electrónicos dirigidos a "Estimado cliente" o algún otro saludo genérico. Si es tu banco, seguramente sabrá tu nombre.
- Sospecha de errores gramaticales o de ortografía, la mayoría de los negocios corrigen sus mensajes cuidadosamente antes de enviarlos.
- No des clics en los enlaces. En lugar de eso, copia la URL del correo y pégala en tu navegador web. Aún mejor, puedes escribir el nombre del destino en tu navegador.
- Sitúa el ratón sobre el enlace. Esto te mostrará el verdadero destino al que irías si realmente hicieras clic en él. Si la dirección destino del enlace es diferente a la que se muestra en el correo, puede ser un claro indicador de fraude.
- Sospecha de los documentos adjuntos y abre solo aquellos que estés esperando.
- El hecho de recibir un correo electrónico de un amigo no quiere decir que realmente fue él quien lo envió. La computadora de tu amigo podría estar infectada o su cuenta de correo electrónico probablemente comprometida y el malware está enviando ese correo a todos los contactos de tu amigo. Si recibes un correo sospechoso de una fuente confiable o un amigo, háblales para confirmar que efectivamente ellos lo enviaron. Siempre usa un número telefónico que conozcas o puedas verificar de forma independiente, no uno incluido en el cuerpo del correo.

Si después de leer un correo te parece que se trata de un ataque Phishing o una estafa, elimínalo. Realmente, utilizar el correo electrónico de forma segura es solo cuestión de sentido común. Si algo parece sospechoso o demasiado bueno para ser verdad, lo más probable es que se trate de un ataque o de una estafa. Simplemente borra el correo electrónico.

2.2.3.6.2 Pharming.

El Pharming es una modalidad de ataque utilizada por los atacantes, que consiste en suplantar al Sistema de Resolución de Nombres de Dominio (DNS, Domain Name System) con el propósito de conducirte 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 (Acto de explotar una vulnerabilidad en el software de un servidor de DNS, que permite que una

persona se adueñe del dominio de un sitio Web, por ejemplo, y redirija el tráfico hacia otro sitio.)

Ilustración 38: Pharming.

2.2.3.6.2.1 ¿Cómo funciona?

Todos los ordenadores conectados a internet tienen una dirección IP única, que consiste en 4 octetos (4 grupos de 8 dígitos binarios) de 0 a 255 separados por un punto (ej.: 127.0.0.1). Estas direcciones IP son comparables a las direcciones postales de las casas, o al número de los teléfonos.

Debido a la dificultad que supondría para los usuarios tener que recordar esas direcciones IP, surgieron los Nombres de Dominio, que van asociados a las direcciones IP del mismo modo que los nombres de las personas van asociados a sus números de teléfono en una guía telefónica.

Los ataques mediante Pharming pueden realizarse de dos formas: directamente a los servidores DNS, con lo que todos los usuarios se verían afectados, o bien atacando a ordenadores concretos, mediante la modificación del fichero "hosts" presente en cualquier equipo que funcione bajo Microsoft Windows o sistemas Unix.

La técnica de Pharming se utiliza normalmente para realizar ataques de Phishing, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

2.2.3.6.2.2 Protección.

Anti-Pharming es el término usado para referirse a las técnicas utilizadas para combatir el Pharming.

Ilustración 39: Anti-Pharming.

Algunos de los métodos tradicionales para combatir el Pharming son: Utilización de software especializado, protección DNS y addons para los exploradores web, como por ejemplo toolbars.

El Software especializado suele ser utilizado en los servidores de grandes compañías para proteger a sus usuarios y empleados de posibles ataques de Pharming y Phishing, mientras que el uso de addons en los exploradores web permite a los usuarios domésticos protegerse de esta técnica.

La protección DNS permite evitar que los propios servidores DNS sean hackeados para realizar ataques Pharming. Los filtros Anti-Spam normalmente no protegen a los usuarios contra esta técnica.

2.2.3.6.2.2.1 Software especializado.

Aviso de Identidad de doble factor Green Armor® www.greenarmor.com es un sistema único de autenticación donde se verifica en profundidad si el usuario está interactuando con un sistema legal o es un sitio criminal clonado.

Ilustración 40: Greenarmor.

Este proceso no requiere registrarse, no tiene pasos previos durante el acceso a una página con login de usuario. Con ello se obtiene un nivel de seguridad mejorada.

Como funciona: Este producto se fusiona con el sitio web existente y se integra fácilmente, actúa por cierto detrás de la escena, donde verifica si la procedencia de usuario es legítima además de legitimar el negocio.

El usuario ingresa su clave y nombre desde una máquina desconocida en ese período una contraseña es enviada por correo electrónico o SMS como un paquete de información "Token".

Se aplica por cierto una cierta criptografía en los envíos, con el doble control el usuario debe hacer clic en un link provisto para validar su acceso, si el origen es dudoso no se produce la entrada al sistema.

Sólo sitios genuinos pueden generar una marca, que con una serie de cálculos matemáticos aseguran la confiabilidad de la comunicación gemela.

Tampoco ofrece ayuda o preguntas para resolver la contraseña aumentando la seguridad.

2.2.3.6.3 Diferencias entre Phishing y Pharming.

Aunque aparentemente puedan parecer fraudes idénticos, el Pharming va un paso más adelante, creando un grupo de usuarios vulnerables mucho mayor que en el Phishing, ya que mientras en este último se necesita que se realice una acción aislada que el usuario efectúe una operación bancaria accediendo a la página mediante un link que le proporcione el estafador, en el Pharming, sin embargo, el usuario intentará acceder directamente a la web de su banco o tienda on-line para evitar el ya conocido Phishing, convirtiéndose en víctima del Pharming aun adoptando todas las cautelas, ya que el estafador ha introducido un programa que modifica las DNS (Domain Name Server) y el acceso que se produce por el usuario es mediante un re-direccionamiento de la IP, diferente a la que en un principio deseábamos entrar.

Este tipo de estafa es mucho más peligrosa, porque la modificación de las DNS queda archivada en el ordenador, esperando el atacante a que el usuario acceda de nuevo, pudiendo atacar este fraude a un número mayor de usuarios.

2.2.3.6.4 Código Malicioso.

El código malicioso es un código que causa daño a una computadora o sistema incluyendo la web y los correos. Este código no es fácilmente ubicado y se controlada únicamente mediante el uso de herramientas anti-virus. El código malicioso puede o bien activar el mismo o ser como un virus que requiere un usuario para realizar una acción, como hacer clic en algo o abrir un archivo adjunto de correo electrónico.

El código malicioso no sólo afecta a una computadora. También puede entrar en las redes y diseminarse. También puede enviar mensajes a través de correo electrónico, robar información, provocar aún más daño y borrar los archivos. Puede ser en forma de lenguajes de programación, controles ActiveX, complementos del navegador, los applets de Java y más. Es por esto que se recomienda a menudo para desactivar estas opciones en los navegadores Web.

Ilustración 41: Código malicioso.

El código malicioso puede venir en varias otras formas. Un tipo común de código malicioso es el virus, que es un pequeño programa colocarlo en otros programas o archivos y se copia en un ordenador e incluso se extendió a otros ordenadores de la red. Los virus pueden variar desde ser relativamente inofensivos para causar un daño significativo a un sistema.

Los gusanos son piezas de código malicioso que hacen copias de sí mismo. Se crean utilizando principalmente los lenguajes de script.

Los troyanos son formas de códigos maliciosos que parecen como software seguro. Pero así es como entrar en un ordenador. Pueden estar escondidos dentro de otro programa y se instalan con un programa de otra manera segura. A veces le dan a alguien en un lugar remoto de control de la computadora de la víctima.

2.2.3.6.4.1 Análisis de códigos maliciosos.

Cuando se analizan códigos maliciosos, los investigadores sin duda tienen desarrollado el sentido para detectar el riesgo potencial del material con el que trabajan y son adecuadamente precavidos, sin embargo, hay algunas amenazas tan temidas que se revisan tantas veces para asegurarse de no liberarlas por accidente. A pesar de que sin duda existen códigos maliciosos que fueron mucho más costosos para eliminar o que se propagaron más ampliamente, en lo que respecta a los inconvenientes o daños directos ocasionados, los siguientes son los 5 más complejos:

2.2.3.6.4.1.1 CIH (alias Chernobyl):

CIH es el más antiguo de los códigos maliciosos de esta lista; se descubrió por primera vez en 1998. Este virus causó tantos daños entre las víctimas que salieron en las noticias año tras año. Para propagarse, CIH se ocultaba en espacios “vacíos” de archivos no maliciosos, lo que dificultaba mucho su desinfección, ya que el tamaño de dichos espacios varía mucho, por lo que el código del virus se dividía de distintas maneras y se hacía muy difícil asegurarse de que las rutinas de desinfección eliminaban hasta los últimos rastros de los archivos. Esto significaba en muchos casos el reemplazo manual de los archivos ejecutables dañados. Lo que es más grave, si el sistema seguía infectado el día 26 de abril (el aniversario del desastre en Chernobyl, que algunos especulan es la razón por la que se eligió esa fecha) el virus estaba configurado para sobrescribir el primer megabyte del disco

duro, de modo que el equipo se colgaba o mostraba la pantalla azul. En ciertos casos, el virus incluso actualizaba el BIOS, o sea que dejaba el equipo totalmente inutilizable ya que sobrescribía el código que le permite al equipo encender. El virus atacó a más de un millón de equipos en todo el mundo y siguió dando vueltas durante varios años tras el descubrimiento de la última variante.

2.2.3.6.4.1.2 Explore Zip.

Explore Zip también es un virus bastante antiguo; se descubrió por primera vez en 1999. Se remonta a los días en que las personas empezaban a usar el término “amenaza combinada” para describir la táctica cada vez más popular de los gusanos para propagarse mediante una variedad de mecanismos diferentes. Éste código malicioso se propagaba de dos formas: al responder correos electrónicos no leídos con una copia de sí mismo y al buscar archivos compartidos en red donde se pudiera copiar en forma silenciosa. Una vez ejecutado, mostraba un mensaje de error que parecía indicar que se acababa de ejecutar un archivo ZIP defectuoso. En segundo plano, el virus sobrescribía con ceros los archivos .DOC y ciertos archivos fuente de programación, lo que significaba que los archivos quedaban destruidos sin posibilidad de revertirse a menos que se emplearan costosas técnicas de recuperación de datos.

2.2.3.6.4.1.3 CryptoLocker.

CryptoLocker es la amenaza más nueva de la lista; se descubrió por primera vez hace unos meses y también provoca cambios en los archivos de los usuarios afectados. Este malware es del tipo ransomware, es decir que está diseñado para secuestrar la información del usuario y pedir a cambio de la misma una suma de dinero en un período de tiempo antes de destruir la información. A veces, con el ransomware se tiene suerte y se encuentra algún tipo de pista en los archivos o algún defecto en el cifrado que permite descifrar los archivos. Pero en este caso el código malicioso usa cifrado asimétrico (similar a la técnica usada por productos comerciales), sin la clave del atacante es imposible recuperar los archivos.

2.2.3.6.4.1.4 Mebromi

Mebromi fue descubierto en 2011, similar al CIH en que también actualiza el BIOS para almacenar parte de su código. Pone parte de su código disperso en el disco duro, lo que significa que queda fuera del alcance de los mecanismos normales de desinfección. Muchas veces es necesario trabajar sobre la motherboard para lograr la desinfección, lo cual no es una tarea sencilla.

2.2.3.6.4.1.5 ZMist.

Este código malicioso es de la familia de los virus polimórficos: cambian la apariencia de su código entre una infección y otra para mostrarse distintos, y de esa forma tratar de engañar a las soluciones de seguridad. La ventaja es que el código utilizado para cambiar de forma es estático, lo cual puede ser utilizado como forma de identificar el virus. ZMist, descubierto en 2002, se denominó virus “metamórfico” porque llevó esta idea a un nivel incluso más complicado. En lugar de simplemente cambiar su apariencia, incluía código para volver a compilarse entre una infección y otra. Esto lo hacía increíblemente difícil de detectar con la tecnología disponible en ese momento

Estos códigos maliciosos son inquietantes debido a que hacen un gran esfuerzo para evadir su eliminación o para causar un daño permanente en los equipos infectados. Pero ninguno de ellos logró ser imposible de detectar, y la mayoría ni siquiera funciona en las últimas versiones de Windows.

Las primeras dos amenazas lograron tener un gran alcance y realmente provocaron una gran cantidad de daños. Como las amenazas hoy en día tienen una motivación financiera, en general no es una buena idea para ellas anunciar su presencia provocando muchos daños en los sistemas comprometidos, ya que de hecho estarían matando su fuente de ingresos. CryptoLocker vendría a ser una excepción a esta regla, ya que muchas personas pagan para recuperar sus datos. Para el usuario que realizó copias de seguridad de los datos, esto es solo una molestia en lugar de un problema genuino.

Los creadores de malware que buscan el rédito económico nunca van a desperdiciar más tiempo ni dinero en el desarrollo que el necesario para aprovechar el hecho que muchas personas no aplica las buenas prácticas en seguridad. Esto hace que los creadores de malware logren hacer una gran cantidad de dinero con técnicas mucho menos complicadas. Es decir, que si por lo menos se contara con una solución de seguridad y las aplicaciones actualizadas se lograría eludir la mayoría de las amenazas.

2.2.3.6.4.2 Protección.

Para ayudar a proteger el sistema de la infección, el software anti-virus debe ser lo primero que se instala en un ordenador. Los buenos hábitos de computación también son importantes, como no abrir archivos adjuntos de correo electrónico de fuentes desconocidas o la instalación de medios de fuentes desconocidas. Además, la eliminación de software que no ha sido utilizado por largos períodos es una buena idea. Esto elimina aún otra vía para que los códigos maliciosos para entrar en un sistema.

2.2.3.6.5 Ataque Por Inyección.

Los ataques de inyección, más específicamente sqli (Structured Query Language Injection) es una técnica para modificar una cadena de consulta de base de datos mediante la inyección de código en la consulta. El SQLI explota una posible vulnerabilidad donde las consultas se pueden ejecutar con los datos validados.

Ilustración 42: SQLI.

SQLI siguen siendo una de las técnicas de sitios web más usadas y se pueden utilizar para obtener acceso a las tablas de bases de datos, incluyendo información del usuario y la contraseña. Este tipo de ataques son particularmente comunes en los sitios de empresas y de comercio electrónico donde los hackers esperan grandes bases de datos para luego extraer la información sensible. Los ataques sqli también se encuentran entre los ataques más fáciles de ejecutar, que no requiere más que un solo PC y una pequeña cantidad de conocimientos de base de datos.

2.2.3.6.6 DDoS.

La Denegación de Servicio (DoS) o Denegación de Servicio Distribuida (DDoS) son las formas más comunes para congelar el funcionamiento de un sitio web. Estos son los intentos de inundar un sitio con solicitudes externas, por lo que ese sitio no podría estar disponible para los usuarios reales. Los ataques de denegación de servicio por lo general se dirigen a puertos específicos, rangos de IP o redes completas, pero se pueden dirigir a cualquier dispositivo o servicio conectado.

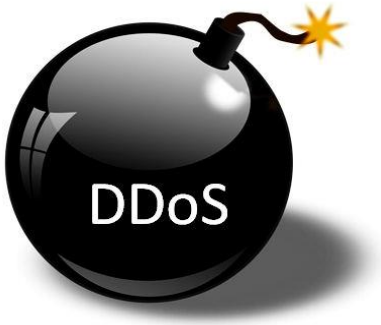


Ilustración 43: DDoS.

Los ataques de denegación de servicio funcionan cuando una computadora con una conexión a Internet intenta inundar un servidor con paquetes. DDoS, por otro lado, son

cuando muchos dispositivos, a menudo ampliamente distribuidos, en un intento de botnet para inundar el objetivo con cientos, a menudo miles de peticiones.

Los ataques DDoS vienen en 3 variedades principales:

- Los ataques de volumen, donde el ataque intenta desbordar el ancho de banda en un sitio específico.
- Los ataques de protocolo, donde los paquetes intentan consumir servicios o recursos de la red.
- Ataques a aplicaciones, donde las peticiones se hacen con la intención de "explotar" el servidor web, mediante la capa de aplicación.

2.2.3.6.7 Ataque de Fuerza Bruta.

Estos son básicamente intenta "romper" todas las combinaciones posibles de nombre de usuario + contraseña en una página web. Los ataques de fuerza bruta buscan contraseñas débiles para ser descifradas y tener acceso de forma fácil. Los atacantes cuentan con buen tiempo, así que el truco es hacer que tus contraseñas sean lo bastante seguras y así el atacante se cansaría antes de descifrar tu contraseña. Mientras que las computadoras se vuelven más y más poderosa la necesidad de contraseñas más fuertes se vuelve cada vez más importante. El caso más reciente de esta vulnerabilidad, se ha visto en cuanto a la vulneración de cuentas de algunos famosos alojados en iCloud.

Ilustración 44: Ataque de Fuerza Bruta.

2.2.3.6.8 Cross Site Scripting (XSS).

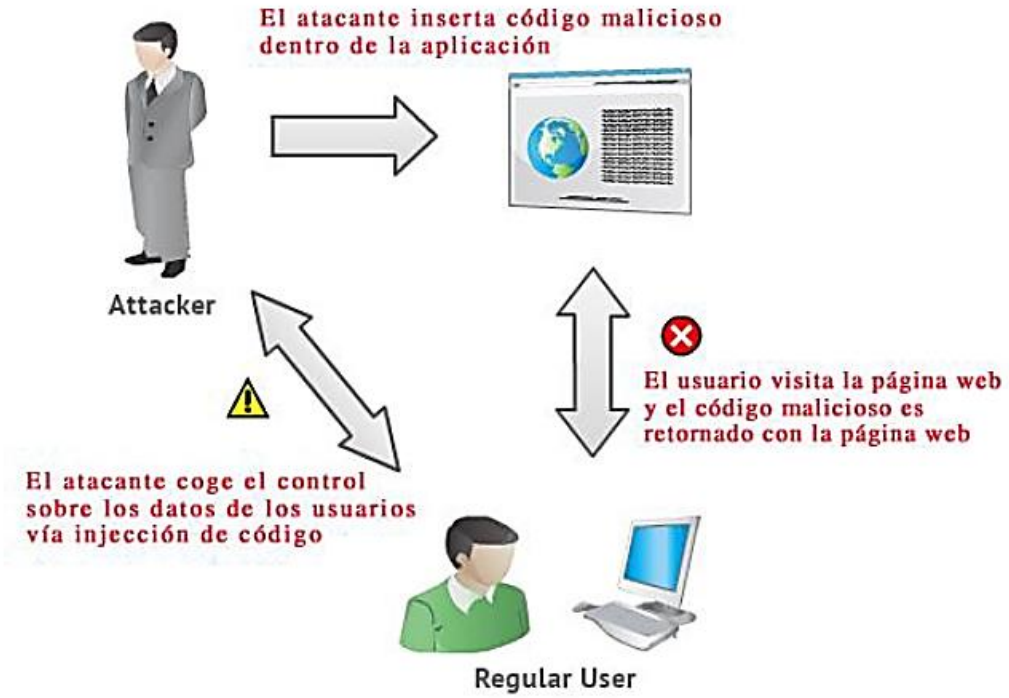


Ilustración 45: Cross Site Scripting.

El XSS se trata de una vulnerabilidad que muchos desarrolladores web dejan pasar, bien por falta de planificación o por desconocimiento. Esta vulnerabilidad suele aparecer por la falta de mecanismos en el filtrado de los campos de entrada que dispone la web, permitiendo el envío de datos e incluso la ejecución de scripts completos.

El código malicioso utilizado en este tipo de ataques está compuesto por cadena de datos: scripts completos contenidos en enlaces o ejecutados desde formularios vulnerables

¿Cómo funciona?
XSS se produce cuando un sitio refleja código que se ha dado, es decir, no se identifican como algo que se puede ejecutar en un navegador y luego se lo devuelve al remitente, en lugar de desinfección correctamente (filtrándola por posibles elementos peligrosos). Por lo que un sitio que es vulnerable a XSS se puede enviar algo como lo siguiente (a menos de etiquetas script) a través de un HTTP GET o POST.

$$alert\ ('Uh\ oh - XSS!')$$

Si a volver una ventana emergente que dice, "Uh oh - XSS" - el sitio es vulnerable. Uno de los lugares más comunes para tener estos problemas es en las formas de búsqueda que la mayoría de los sitios tienen. La clave aquí es que el código es del lado del cliente código que está siendo "recuperó" a usted por el servidor, que a continuación, ejecuta.

El ataque.
Ok, por lo XSS funciona enviando algo a un sitio (a menudo a través de su formulario de búsqueda) con el código de secuencias de comandos en ella y que tiene rebote, ¿verdad?

¿Por qué es un problema? ¿Cómo es que alguien va a hacer una víctima enviar esta potencialmente peligrosa basura a un sitio?

Te envían un enlace.

Los enlaces pueden ser muy largos y complicados - incluyendo el tener una buena cantidad de código en ellos. Así que lo que hacen es escoger un sitio de destino que es vulnerable a XSS, http://www.acmebank.com, decir, y luego construir una consulta en un enlace que incluye el código malicioso. A continuación, enviar estos enlaces por todo el lugar y esperar a que la gente haga clic en ellos.

Las cookies sólo pueden ser leídas por el dominio que las galletas pertenecen. Es por eso que el atacante tiene que conseguir que la víctima para enviar su código malicioso en la web, haciendo clic en los enlaces.

Clasificación de los ataques Cross Site Scripting

Los diversos tipos de ataques que nos podemos encontrar de Cross Site Scripting pueden ser catalogados en dos grandes grupos: XSS persistente o directo, y XSS reflejado o indirecto.

1.- XSS persistente o directo

Este tipo de ataque consiste en embeber código HTML peligroso en sitios que lo permitan por medio de etiquetas <script> o <iframe>. Es la más grave de todas ya que el código se queda implantado en la web de manera interna y es ejecutado al abrir la aplicación web.

Dentro de este tipo nos encontramos el subtipo “Local” que aparece por un mal uso del DOM (Modelo de objetos del documento) con JavaScript, que permite la apertura de nuevas páginas con código malicioso JavaScript incrustado, afectando el código de la primera página en el sistema local. Estos códigos son ejecutados del lado del cliente, por lo que los filtros utilizados en el servidor no funcionan para este tipo de vulnerabilidades.

2.- XSS reflejado o indirecto

Es el tipo de ataque XSS más habitual y consiste en editar los valores que se pasan mediante URL, cambiando el tipo de dato pasado del usuario a la web, haciendo que ese código insertado se ejecute en dicho sitio.

Métodos de inyección de código utilizado en los ataques

A la hora de lanzar un ataque de este tipo, los atacantes pueden utilizar varios tipos de inyección de código distinto. Veamos a continuación cuáles son los más utilizados.

1.- Inyección en un formulario

Se trata del ataque más sencillo. Consiste en inyectar código en un formulario que después al enviarlo al servidor, será incluido en el código fuente de alguna página. Una vez insertado en el código fuente, cada vez que se cargue la página se ejecutará el código insertado en ella.

2.- Inyección por medio de elementos

En este tipo de sistema de inyección de código se utiliza cualquier elemento que viaje entre el navegador y la aplicación, como pueden ser los atributos usados en las etiquetas HTML utilizadas en el diseño de la página.

3.- Inyección por medio de recursos
Aparte de los elementos en la url y los formularios, hay otras formas en la que se puede actuar como son las cabeceras HTTP. Estas cabeceras son mensajes con los que se comunican el navegador y el servidor. Aquí entran en juego las cookies, las sesiones, campo referer…

Consejos para evitar los ataques.
Por suerte, prevenir estos ataques es sencillo, y una vez que aprendamos cómo hacerlo es algo que siempre deberíamos tener presente para evitarlos.

A continuación, veremos algunos consejos prácticos que podemos llevar a cabo para proteger nuestras aplicaciones web mediante la validación de entrada de datos, asegurándonos que cada uno de los campos que utilicemos no contengan código que pueda afectar nuestra aplicación o a nuestros usuarios.

1.- Limitar los caracteres de entrada.
Lo primero que debemos hacer es limitar los caracteres que un usuario puede introducir en los campos de texto. Por ejemplo, si tenemos un campo para introducir el nombre del usuario, no vamos a dejarlo abierto para que se puedan introducir un número indefinido de caracteres, sino que lo vamos a limitar por ejemplo a 20 o 30 caracteres. Para limitar el número de caracteres, podemos utilizar la variable “maxlength” que nos proporciona el estándar HTML.

2.- Sanear los datos.
Cuando hablamos de sanear los datos, nos estamos refiriendo a quedarnos únicamente con la información que nos interesa, eliminando las etiquetas HTML que pueden ser incluidas en una caja de texto. Por ejemplo, si estamos almacenando el nombre de una persona, de poco nos sirve que el usuario lo introduzca en negrita, ya que lo único que nos interesa es su nombre.

Para lograr esta limpieza, podemos utilizar la función “strip_tags”.

3.- Escapar los datos.
Para proteger los datos y mostrarlos tal y como el usuario los introdujo, deberíamos “escapar” los datos al presentarlos al usuario. Es decir, caracteres que deben ser representados por entidades HTML si se desea preservar su significado (por ejemplo, las comillas dobles hay que transformarlas en " que es como se representa en HTML). Con esto evitamos que el navegador lo ejecute y evalúe el código.

Para lograr esto, podemos utilizar la función “htmlspecialchars”. Por ejemplo:

echo "Mostrando resultados de: “. htmlspecialchars($_GET['busqueda']);

Pero aparte de tomar medidas de seguridad para impedir ataques XSS en nuestros sitios, debemos evitar almacenar información relevante de nuestros visitantes en las Cookies, y además encriptar las sesiones de usuario para que en caso de que las capturen no puedan acceder a la información almacenada en ella.

2.2.3.6.9 Otros tipos de ataques.
Existen amenazas con un carácter más técnico distintivas del comercio electrónico:

2.2.3.6.9.1 Carding y Skimming.

Ilustración 46: Carding y Skimming.

Carding: Es el uso ilegitimo de las tarjetas de crédito, o de sus números, pertenecientes a otras personas. Se relaciona con el hacking, porque para conseguir números de tarjetas de créditos, una de las formas es utilizando Ingeniería Social y sobre todo nuestra inteligencia (esto es lo más importante).

El carding consiste en comprar usando la cuenta bancaria o la tarjeta crédito de otro, esto se consigue con un poco de ingeniería social y mucha perseverancia.

Cuando alguna persona utiliza carding para comprar objetos materiales se suele utilizar una dirección falsa con una identificación también falsa, es decir todo el formulario de compra lo llena con datos falsos.

De esta manera el comprador quedara esperando en el lugar indicado la entrega del material como si se tratara de su residencia.

La filosofía de los carders se basa en que existe mucha gente que tiene grandes cantidades de dinero que no cae nada mal utilizar algo de ese dinero para comprar algunas cositas para cada uno de ellos, ya que posiblemente el dueño de la tarjeta ni se dé cuenta de esta compra que él no la hizo.

Skimming: es un método para el robo de datos mediante la clonación de las tarjetas de crédito sin que éstos lo sospechen, y se realiza tanto en cajeros automáticos como en los propios establecimientos.

En los cajeros, los estafadores suelen colocar un lector de tarjetas magnéticas en la ranura donde el cliente inserta la tarjeta. El dispositivo "lee" la información de la banda magnética y la transmite a otro aparato, donde quedan almacenados los datos.

En ocasiones los delincuentes colocan cámaras de vídeo en los cajeros para grabar el código de seguridad (PIN) del usuario mientras éste lo teclea. Por este motivo es muy importante tapar el código en este momento.

El Skimming también se practica en discotecas, restaurantes, tiendas… Para ello, cuando los empleados estafadores solicitan la tarjeta al cliente para cobrar, no sólo utilizan el habitual dispositivo de pago (TPV) sino que, además, pasan la tarjeta por un pequeño lector de bandas magnéticas, que les permite obtener y guardar los datos.

2.2.3.6.9.2 Crimeware.

Ilustración 47: Crimeware.

A las herramientas de software utilizadas en los crímenes cibernéticos en ocasiones se las denomina Crimeware. El Crimeware es el software que:

- se utiliza para cometer un acto criminal.
- por lo general no se considera como una aplicación de software o hardware deseados.
- de forma voluntaria permite que se lleve a cabo el crimen.

Un Crimeware puede robar datos confidenciales, contraseñas, información bancaria, etc. y también puede servir para robar la identidad o espiar a una persona o empresa.

Funcionamiento del Crimeware.

Un programa Crimeware puede actuar solo o teledirigido, pero su principal característica de funcionamiento es que intenta pasar desapercibido. Muchas veces para cumplir su objetivo, el Crimeware debe ir combinado con la técnica de hackeo llamada ingeniería social. La ingeniería social hace referencia a la actividad de manipular o convencer de alguna manera a una persona, para que realice acciones que le servirán al cibercriminal para obtener datos importantes de esa misma persona. La mayoría de las personas suelen ser lo suficientemente ignorantes como para incluso dar sus propias contraseñas.

Los Crimeware están diseñados para robar la identidad de una persona o usuario para acceder a las cuentas online de servicios financieros. En general, el propósito es robar el dinero de esas cuentas.

Un Crimeware puede emplear diversas técnicas para lograr su objetivo criminal, la más común es instalarse ocultamente en una computadora, para capturar información importante del usuario como claves, nombres de usuario y tarjetas de crédito.

Protección contra el Crimeware.

No actuar ingenuamente, nunca dar claves ni datos importantes, utilizar aplicaciones del tipo antivirus, antispyware y cortafuegos.

2.2.3.6.9.3 Clicjacking.

Es una técnica maliciosa que engaña a los usuarios de la web y permite revelar información confidencial de estos o tomar el control de sus computadoras, simplemente haciendo clics en páginas web que parecen inofensivas.

La vulnerabilidad se presenta en casi todos los navegadores y plataformas. La vulnerabilidad fue descubierta por Jeremiah Grossman y Robert Hansen, quienes al principio no dieron detalles para no difundir la técnica, pero sí se comunicaron con empresas importantes como Microsoft, Mozilla, Apple y Adobe para advertirlos.

El problema es tan grave que el atacante podría hasta tomar imágenes de nuestra webcam sin que nosotros nos imaginemos, o hacer que un usuario haga clic sobre un botón, pero en estaríamos haciendo clic en un enlace malicioso. Existen múltiples técnicas de Clicjacking, empleando diferentes tecnologías web como JavaScript, ActiveX, Flash, etc.

Ilustración 48: Clicjacking.

2.3 Sistemas de pago.

En la actualidad podemos decir que Internet es una de las vías más importantes de comunicación, por ello, un sistema de pago electrónico es una pieza fundamental en el proceso de compra-venta dentro del comercio electrónico.

El comercio electrónico por Internet ofrece un nuevo canal de distribución sencillo, económico y con alcance mundiales 24 horas del día todos los días del año, y esto sin los gastos y limitaciones de una tienda clásica: personal, local, horario, infraestructura, etc.

Esto tiene sus ventajas: por un lado, facilita la compra impulsiva, ya quien encontró nuestro producto lo puede adquirir inmediatamente, y por otra parte reduce nuestros costes de facturación y ventas al realizarse la mayor parte del proceso en forma automática.

Aunque es uno de los servicios que cada día cobra más importancia y que promete un cambio radical para las empresas, muchas de ellas sólo han empleado la red para darse a conocer y ofertar sus productos. La razón esencial es la desconfianza que existe sobre la seguridad de las transacciones llevadas a cabo en la red.

2.3.1 Características deben tener los medios de pago en Internet.

- **Facilidad de uso.**
- **Universal.** Aceptado en todas partes, y que sirva para pagar cualquier producto.
- **Liquidez.** Facilidad para utilizar el pago inmediatamente por quien lo recibe para realizar otras compras.
- **Fraccionamiento.** Que pueda realizar pagos exactos.
- Que permita pagar **cantidades grandes o pequeñas.**
- **Intimidad.** Que pueda conservar privadamente la identidad de quien lo usa, para qué lo usa, qué compró, etc.
- **Seguridad.** Que no me lo van a robar, de que, si me lo roban, no les va a servir y de que, si me lo roban y se sirven de él, no voy a tener que pagar lo que compren.
- **Garantía** de que el dinero lo recibe la persona que corresponde y no otra.
- **Acreditación** del pago, un recibo.
- **Coste reducido** de transacción. Buscar la menor comisión del intermediario entre el vendedor y el comprador, donde el este se quede parte de lo pagado. Construir y gestionar la reputación de una marca es sin duda un proceso laborioso que requiere de una importante atención además de un trabajo continuo y constante.

No existe ningún medio de pago perfecto ni a gusto de toda tu clientela. Por tanto, es recomendable que ofrezcas diversas opciones. Incluye diferentes formas de pago en tu negocio.

2.3.2 Métodos de pago utilizados en Internet

Existen numeroso medio de pago en Internet y ninguno de ellos es perfecto. Dependiendo de lo que vayamos a comprar o vender utilizaremos uno u otro. A continuación, enumeraremos los métodos de pago más utilizados:

2.3.2.1 *Métodos off-line.*

Son aquellos métodos en los cuales el pago no se efectúa durante la realización de la compra; se realiza a posteriori o de forma diferida. Dentro de los métodos offline encontramos los siguientes modos de pago:

2.3.2.1.1 Contra reembolso.

El pago contra-reembolso es un medio de pago utilizado en las ventas a distancia (por Internet, teléfono o catálogo) que consiste en abonar el coste del producto comprado, con sus recargos (por entrega y por elegir este medio de pago) directamente a la persona que nos haga la entrega del mismo en nuestro domicilio (el transportista), generalmente en efectivo (moneda y billetes).

Ilustración 49: Contra reembolso.

Para que se pueda hacer un pago contra-reembolso es necesario:

- Que haya algo físico que entregar en el domicilio del cliente. Si no lo hubiera, por ejemplo, un servicio, no podría darse esta forma de pago.
- Que estén presentes en el momento de la entrega del producto el comprador y el representante del vendedor (el transportista).
- Disponer de dinero en efectivo. Si en el momento de la entrega, el consumidor comprador online no dispusiera de monedas o billetes, el transportista no podría entregarle al producto.
- Desembolsar el pedido online completo, que comprenderá el coste del bien comprado IVA incluido, el coste de entrega a domicilio del transportista y el coste de la modalidad de pago contra-reembolso.

Ventajas.

La principal ventaja del pago contra-reembolso en las compras online es que no tiene ningún riesgo para el comprador, ya que puede abrir la mercancía en su hogar, comprobar que corresponde con lo solicitado y, sólo en ese caso, desembolsar su importe en efectivo.

Inconvenientes.

La principal desventaja del pago contra reembolso en las compras online para el comprador es que cuesta dinero en forma de comisión por recurrir a esta forma de pago en vez de a otras (tarjeta bancaria o transferencia bancaria, por ejemplo).

Esta comisión que el comprador soporta cuando elige el pago contra-reembolso se debe al coste que este medio de pago supone para el vendedor:

- Cuando hacemos un pedido contra-reembolso, el comercio online se obliga a entregárnoslo en nuestro domicilio sin haberlo cobrado antes, por lo que existe un alto riesgo de que el comprador (que no tiene nada que perder) no esté en su domicilio en el momento de la entrega, o que simplemente sea un pedido fallido porque el comprador es un "graciosillo".

  Para ello las empresas de comercio electrónico deben asegurarse de que el cliente existe y de que tiene la intención de comprar online, por ejemplo, comprobando que el domicilio de entrega existe y corresponde a un hogar cierto.

- La empresa transportista (MRW, Seur, etc.), tiene que confiar a sus transportistas (muchos son autónomos), "mover" dinero del domicilio del cliente a la empresa vendedora, y le cobran a esta una comisión por ese servicio (seguridad de que el dinero llegue del comprador al vendedor).

2.3.2.1.2 Transferencia bancaria.

Una transferencia bancaria es la operación por la que una persona o entidad (el ordenante) da instrucciones a su entidad bancaria para que envíe, con cargo a una cuenta suya, una determinada cantidad de dinero a la cuenta de otra persona o empresa (el beneficiario). Dicho de otra forma, realizar una transferencia es pasar dinero de una cuenta a otra, bien de la misma entidad o bien en otra entidad.

Las transferencias que tienen lugar dentro de la misma entidad se suelen denominar traspasos.

Ilustración 50: Transferencia bancaria.

Una transferencia bancaria es una operación por la que una persona (el **ordenante**) da instrucciones a su entidad bancaria para que con cargo a una cuenta suya **envíe** una determinada **cantidad de dinero** a la cuenta de otra persona (el **beneficiario** de la transferencia) en la misma o en otra entidad.

La mayoría de las entidades consideran operaciones análogas a las transferencias bancarias, aunque no intervienen **dos cuentas**. Por ejemplo, aquellas en las que la orden de envío especifica que los fondos se entreguen en efectivo al beneficiario. O aquellas en las que el ordenante paga en efectivo en la ventanilla de la entidad para su posterior envío a la cuenta del destinatario en otra entidad de crédito, que se llaman otras órdenes de pago o giros.

Sin embargo, no es análogo ni puede considerarse una transferencia la aceptación de ingresos en efectivo para su abono en una cuenta abierta en la propia entidad receptora.

Cuando la transferencia tiene lugar entre cuentas de la misma entidad de crédito, la operación se suele denominar "**traspaso interno**".

Desde febrero de 2014, se utiliza el IBAN como identificador único de cuenta. Estas siglas corresponden al código internacional estandarizado para la identificación de cuentas bancarias.

Comisiones.
Se trata de un servicio bancario por el que normalmente se cobran comisiones. Casi todas las entidades cobran un porcentaje del importe de la transferencia, pero fijan una cantidad mínima a cobrar.

Si usted utiliza este servicio a menudo merece la pena comparar las tarifas de varias entidades. Las transferencias realizadas a través de Internet suelen salir mucho más económicas, y en ciertos casos son gratuitas.

Recuerde que los costes de las transferencias son los primeros que aparecen en las Tarifas de Comisiones y Gastos que las entidades deben tener a disposición del público, y que se anuncian de forma visible en los tablones de todas sus oficinas.

Las comisiones deben responder a los costes de las transferencias, sin que puedan cargarse diferentes comisiones por conceptos parecidos. Por ejemplo, no cabe cobrar una comisión por el abono en la cuenta y otra por notificar el abono a la persona que ha recibido la transferencia. En todo caso, al ordenar la operación el cliente debe ser informado de los costes, para que pueda aceptarlos de forma expresa.

En España, lo habitual era que la persona que ordenaba la transferencia fuera quien pagara la comisión, salvo instrucciones expresas en contra. Sin embargo, con la entrada en vigor de la nueva Ley de Servicios de Pago, los gastos serán compartidos entre ordenante y beneficiario, salvo que se indique a la entidad que deben repercutirse en su totalidad a uno o a otro.

No se suelen cobrar comisiones en caso de traspasos entre cuentas del mismo titular.

Tipos de transferencias

Las transferencias bancarias se pueden clasificar en función de distintos criterios. Según el área geográfica, las transferencias se clasifican en:

- **Transferencias nacionales (o domésticas):** tanto el envío del ordenante como la recepción de fondos por parte del beneficiario tienen lugar en España. Para realizar una transferencia doméstica, hay que facilitar los 20 dígitos del Código Cuenta Cliente (CCC) del beneficiario. A partir de 2014, el CCC será sustituido por el IBAN, aunque durante un período de transición las entidades podrán facilitar gratuitamente servicios de conversión de CCC para pagos nacionales.
- **Transferencias exteriores o transfronterizas:** el ordenante y el beneficiario se encuentran en países diferentes. Las transferencias exteriores son más fáciles (rápidas y económicas) si se dispone del IBAN (número internacional de cuenta) del beneficiario y el BIC (código de identificación bancaria) del banco del beneficiario. En este caso se consideran transferencias STP (Straight Through Processing) y se realizan de forma totalmente automatizada. Las transferencias exteriores que no son STP tienen comisiones superiores.

Ventajas.

- Sistema seguro ya que la operación es realizada por la entidad bancaria y tras una orden del comprador.

La transacción queda grabada en el banco del usuario y en el banco de la tienda online.

No implica ningún coste al comercio, y al comprador en algunos casos un coste muy bajo.

- Para el comprador, el pago debe realizarlo previamente a la recepción del artículo.

La obligatoria visita al banco del comprador, ya sea físicamente a una oficina o de forma online para poder realizar la transferencia.

No es un sistema automático, y requiere de una comprobación periódica por parte del comercio antes de procesar un pedido.

Es un sistema efectivo pero lento, ya que normalmente el dinero tarda dos días hábiles en llegar a su destino.

El comprador paga la comisión correspondiente asociada a la transacción.

2.3.2.1.3 Domiciliación bancaria.

La domiciliación bancaria es una forma fácil, segura y rápida de pagar sus suscripciones y regular automáticamente las facturas de su cuenta bancaria y es cada vez un método más popular de pago a causa de sus numerosas ventajas.

Pagos mediante domiciliación bancaria son más convenientes. No hay necesidad de hacer viajes a distintos lugares y hacer cola para pagar sus cuentas. Muchas organizaciones ofrecen elección de las fechas de pago, de modo que puede elegir el momento de pagar en función de sus otros compromisos. Si está ocupado, tiene malestar, o está fuera de la ciudad, no necesita preocuparse por las facturas pendientes de pago, lo que se debe se paga automáticamente, incluso sin su presencia física.

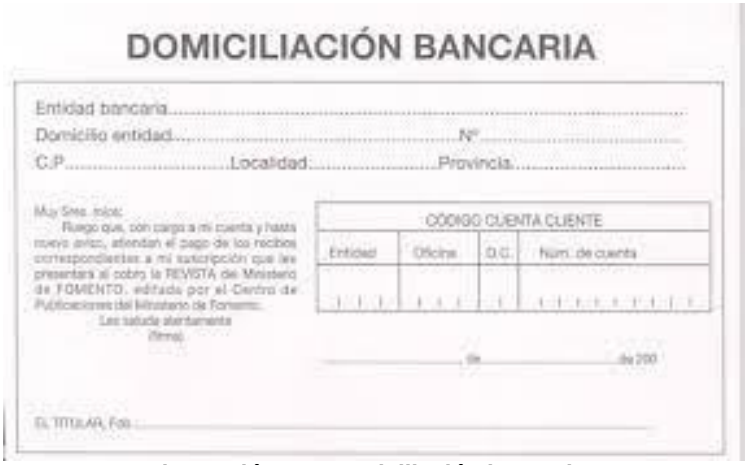


Ilustración 51: Domiciliación bancaria.

La domiciliación bancaria es segura debido a los tres principales aspectos de la garantía de domiciliación bancaria: inmediata garantía de devolución de dinero desde el banco en caso de cualquier error, la notificación previa de la organización en caso de que haya algún cambio en el importe o la fecha, y lo que es más importante, El derecho de cancelar. Es una opción menos costosa. El costo de los viajes se elimina, como es el costo de envío por correo o cheques. Muchas organizaciones también ofrecen descuentos por domiciliación bancaria.

Según los acuerdos entre las empresas de servicios públicos y los bancos, el pago puede realizarse mediante domiciliación bancaria.

Ventajas.

- Sistema seguro.

El comprador se despreocupa de realizar el pago cada vez que adquiera un producto.
El comercio, cobra el artículo antes de servirlo.

- No es un sistema automático, y requiere de una comprobación periódica por parte del comercio antes de procesar un pedido.

Se pierde el control de los pagos realizados dado que no requiere de una intervención por parte del comprador.

Los métodos online, son más rápidos, pero requieren de elementos complementarios que eleven el nivel de seguridad en la transacción.

2.3.2.2 *Métodos on-line.*

Son aquellos métodos en los cuales el pago se realiza en el mismo momento de la realización de la compra mediante conexión directa a través de una pasarela de pago o similar. Dentro de los métodos online encontramos:

2.3.2.2.1 Tarjetas.

Las tarjetas son medios de pago emitidos por una entidad financiera o un comercio. Por su comodidad, facilidad de uso, amplia aceptación y por la seguridad que supone no tener que llevar mucho dinero en efectivo, las tarjetas se han convertido en parte de nuestras vidas.

Son el medio de pago más aceptado para efectuar compras por Internet, en viajes y desplazamientos. Hoy en día, una tarjeta de crédito es casi algo fundamental para alquilar un coche, comprar un billete de avión y reservar una habitación de hotel.

Las **tarjetas bancarias** son las emitidas por una entidad financiera. España es el país europeo con mayor red de cajeros y terminales de puntos de venta, y existen tres redes que gestionan los movimientos generados por las tarjetas bancarias de pago: Euro 6000, Sistema 4B y ServiRed.

También existen **tarjetas no bancarias**, que sirven exclusivamente para comprar en los establecimientos comerciales que las emiten (grandes almacenes, cadenas de tiendas, etc.).

Las **tarjetas de fidelización** pueden ser emitidas por establecimientos comerciales o de servicios (por ejemplo, líneas aéreas) y permiten acumular puntos que dan derecho a descuentos o regalos.

En caso de pérdida o robo, la general aceptación de las tarjetas hace que existan bastantes posibilidades de uso indebido. Consulte cómo proteger la seguridad de sus tarjetas en la correspondiente sección del Kit financiero de supervivencia.

2.3.2.2.1.1 Clases de tarjetas bancarias

Ilustración 52: Tarjeta bancaria.

Pueden ser de débito, de crédito o tarjetas monederos.

2.3.2.2.1.1.1 Tarjetas de débito.

Son las que permiten utilizar los fondos depositados en la cuenta corriente o de ahorro a la que están asociadas. Con ellas se puede sacar dinero en oficinas y cajeros automáticos y también realizar pagos en comercios. En ambos casos la operación se registra de manera inmediata en la cuenta, por lo que es necesario que existan fondos suficientes para hacer frente al pago o a la retirada de efectivo. Esta es la principal diferencia entre las tarjetas de débito y las de crédito.

El banco podría anticiparle la cantidad necesaria si en un momento dado no hubiera suficientes fondos, pero hay que tener en cuenta que los intereses y gastos que se pagan por dejar la cuenta en descubierto pueden llegar a ser muy elevados.

En principio, podría retirarse tanto dinero como hubiera en la cuenta asociada. Sin embargo, por razones de seguridad se puede fijar un límite diario, sobre todo para la retirada de fondos de los cajeros automáticos.

Para realizar la compra, se debe digitar el número de la tarjeta y la fecha de vencimiento de la misma, previa verificación que la tienda acepte este tipo de tarjetas y que sea una zona segura.

2.3.2.2.1.1.2 Tarjetas de crédito.

Permiten realizar pagos u obtener dinero, hasta el límite fijado, sin necesidad de tener fondos en la cuenta bancaria en ese momento (a diferencia de lo que ocurre con las tarjetas de débito).

Recuerde que utilizar una tarjeta de crédito tiene las mismas consecuencias que disponer de cualquier otro crédito o modalidad de financiación: está obligado a devolver el dinero y pagar los intereses establecidos. El límite del crédito disponible debe figurar en el contrato de la tarjeta. Puede variar a lo largo del tiempo, siempre con el conocimiento y el consentimiento previos tanto del titular de la tarjeta como de la entidad financiera. De forma puntual, las entidades pueden autorizar excesos sobre el límite autorizado. Suele existir un límite de crédito máximo para cada categoría de tarjeta ("normal", "plata", "oro"...).

La devolución del dinero que se ha utilizado debe hacerse de la forma y en los plazos previstos, normalmente en los primeros días de cada mes. Se pueden elegir distintas modalidades de pago:

- **Pago mensual por la totalidad**: es la más sencilla y tradicional. El saldo deudor (todos los gastos realizados durante el mes) se paga con cargo a su cuenta el primer día del mes posterior. Cada mes recibirá un extracto con las operaciones realizadas en el periodo anterior y el saldo final que se le cargará en la cuenta asociada. Debe tener dinero suficiente para pagar todo el saldo y liquidar la deuda. Si lo paga de esta forma no se le cargarán intereses.
- **Pago aplazado**: es la modalidad de "cuota flexible" o *revolving*. Permite al titular financiar sus compras según sus necesidades, ya que elige cuánto quiere pagar cada mes. Es decir, con estas tarjetas es posible aplazar el pago mediante una cuota, fija o flexible, como si se tratara de la amortización de un préstamo. Si la

cuota mensual es reducida, puede ocurrir que no sea suficiente para pagar todos los intereses generados hasta ese momento, por lo que la deuda se incrementará en la cantidad necesaria... pasando desde ese momento a generar nuevos intereses. Por eso es muy importante controlar el crecimiento de la deuda que se acumula en cada liquidación, ya que puede crecer de forma exponencial.
Frente a la facilidad y comodidad de utilizar las tarjetas, recuerde que está contratando uno de los créditos más caros que existen. La TAE suele oscilar entre el 11% y el 25%, y en caso de demoras o impago de las cuotas las entidades suelen cargar gastos y comisiones adicionales muy elevados.

Es fundamental tener en cuenta que para que la Tarjeta de Crédito tenga validez, ésta debe contener la denominación de la empresa que emite la tarjeta, así como el sistema de tarjeta de crédito al que pertenece; numeración codificada de la tarjeta; nombre del usuario de la tarjeta y su firma; fecha de vencimiento y la indicación expresa del ámbito geográfico de validez.

2.3.2.2.1.1.3 Tarjetas Monederas.

También llamadas de prepago, permiten hacer desembolsos, en general de pequeño importe, y obtener dinero hasta el límite que su titular haya pactado previamente con la entidad bancaria o de dinero electrónico que la emite, mediante ingreso por caja o cargo en su cuenta.

Los datos con el importe disponible total se almacenan en la tarjeta en un chip, y éste disminuye según efectúa los pagos. Una vez agotado, puede recargarla. Otra modalidad son las tarjetas virtuales. La tarjeta no existe físicamente y sólo es un número, un PIN y una fecha de caducidad, y sirven exclusivamente para realizar pagos por Internet. Las tarjetas virtuales, al ser de prepago, ofrecen mayor seguridad que una tarjeta de crédito o débito normal, ya que en caso de sustracción de los datos de la tarjeta nadie podría sobrepasar el límite. Como no tienen soporte físico, se pueden crear, cargar y descargar en tiempo real.

2.3.2.2.1.2 Características físicas.

Las tarjetas son de plástico y tienen forma rectangular. Pueden ser de colores y diseños muy distintos, pero deben cumplir ciertas normas.

En el **anverso** de la tarjeta debe figurar:

- El nombre de la entidad emisora en la parte superior (una entidad financiera).
- Los logos de marca y aceptación en la parte derecha (4B, Maestro, Euro 6000).
- El chip (si lo hubiese).
- El Personal Account Number (**PAN**), o número de tarjeta.
- La fecha de caducidad de la tarjeta.
- El nombre del titular.

Ilustración 53: Parte frontal de una tarjeta bancaria.

En el **reverso** de la tarjeta figurará:

- La banda magnética: contiene grabados los datos de titular y caracteres alfanuméricos que hacen que los cajeros y terminales actúen de una forma determinada.
- El panel de firmas.
- Contiene además los siguientes elementos de seguridad:
  - El holograma.
  - Carácter especial.
  - Dígitos de impresión.
  - Firma.

Ilustración 54: Parte trasera de una tarjeta bancaria.

2.3.2.2.1.3 Las comisiones.

Existen muchas comisiones asociadas a las tarjetas de débito y crédito, aunque no siempre se cobran todas. Las comisiones que se van a cobrar deben figurar en el contrato y cualquier modificación debe ser comunicada.

Normalmente se cobra una comisión por un importe fijo en concepto de emisión y otro importe cada año (o cada seis meses) para la renovación de las tarjetas.

El importe depende del tipo de tarjeta; a mayor categoría, más alto. Si hay varios beneficiarios, cada tarjeta secundaria suele pagar comisión, aunque a menudo es menor que la de la tarjeta principal.

Se cobran comisiones por la utilización de cajeros que no pertenecen a la entidad emisora de la tarjeta o de su red y por pagos realizados en el extranjero en divisas distintas al euro.

Ventajas e Inconvenientes de las tarjetas de débito.	
Ventajas.	**Inconvenientes.**
Comodidad de hacer pagos y retirar dinero con cargo a su cuenta, consultar saldos y movimientos, realizar transferencias, recargar el teléfono móvil y casi todas las demás operaciones posibles a través de cajeros automáticos.	Normalmente hay que pagar comisiones y gastos de mantenimiento.
Seguridad de no tener que llevar encima dinero en efectivo.	Sólo se puede disponer del importe del saldo en la cuenta en ese momento. Hay que hacer una previsión de fondos.
Facilidad para conseguirlas, casi cualquier persona con una cuenta a la vista puede tener una tarjeta de débito.	Posibilidad de fraude en caso de robo o extravío.
Mejor control de gastos – si no hay dinero no se pueden realizar compras. Esto evita la posibilidad de un exceso de endeudamiento.	

Tabla 3: Ventajas e inconvenientes de las tarjetas de débito.

Ventajas e Inconvenientes de las tarjetas de crédito.	
Ventajas.	**Inconvenientes.**
La misma comodidad y seguridad que las tarjetas de débito.	Normalmente hay que pagar comisiones y gastos de mantenimiento.
Permite comprar ahora y pagar después.	Posibilidad de fraude en caso de robo o extravío.
Protección de emergencias: se podrá contar con dinero en caso de imprevistos.	Si no se paga el saldo total cada mes hay que pagar un interés altísimo.
	Es fácil gastar el dinero que no se tiene y endeudarse en exceso.

Tabla 4: Ventajas e inconvenientes de las tarjetas de crédito.

2.3.2.2.1.4 Obligaciones del titular

Consulte el Kit financiero de supervivencia para saber cómo proteger sus tarjetas y cómo actuar en caso de uso indebido de las mismas.

Como titular de una tarjeta de crédito o débito, usted asume la obligación de responsabilizarse de su conservación y uso correcto, así como del número PIN, si tuviera.

En caso de pérdida o robo, está obligado a avisar de inmediato a la entidad emisora. Desde el momento de la comunicación usted queda, en principio, libre de responsabilidad por el uso indebido de la tarjeta. Es decir, no podrán cobrarle por los pagos que otra persona

realice de forma fraudulenta, después de que usted haya dado el aviso. Por el contrario, hasta el momento del aviso normalmente le corresponde a usted afrontar tales pagos.

Tenga en cuenta que, si alguien conoce el número de su tarjeta, la fecha de caducidad y su nombre, podría incluso realizar compras por Internet, sin necesidad de tener la tarjeta físicamente en su poder.

La mayor parte de las entidades de crédito fijan en 150 € el límite de responsabilidad del cliente si otra persona usa su tarjeta de modo fraudulento antes del aviso de pérdida o robo.

Sin embargo, esa limitación no funciona si usted ha cometido una negligencia grave. Por ejemplo, si no ha tomado medidas razonables para proteger la tarjeta y el número secreto o si avisa con mucho retraso de la pérdida o robo.

Por estas razones es fundamental que conserve y use bien sus tarjetas y los datos confidenciales. A continuación, le ofrecemos algunos consejos básicos para aumentar su seguridad:

- Proteja siempre sus tarjetas como si fueran dinero en metálico.
- Firme la tarjeta en el momento de recibirla, para que nadie más pueda hacerlo.
- Guarde los documentos que acompañan a la tarjeta en un lugar seguro.
- No anote nunca el número secreto junto a la tarjeta, ni lo lleve en el mismo bolso. Memorícelo para no tener que llevarlo escrito.
- No utilice como número secreto datos fáciles de adivinar como el día de su cumpleaños, DNI, etc.
- Sea discreto y proteja su confidencialidad cuando opere con la tarjeta, tanto en establecimientos como en cajeros.
- Si no hace uso habitual de la tarjeta, compruebe periódicamente que sigue en su poder.
- Conserve los justificantes y compruébelos con los cargos cuando reciba su extracto mensual. Si detecta algún cargo dudoso o algún error, informe a su entidad de ello cuanto antes.
- Lleve el número de teléfono que le haya facilitado la entidad para llama en caso de emergencia por si tiene que comunicar la pérdida o robo, pero llévelo siempre en lugar separado de la tarjeta.
- Nunca deje a la vista su número de tarjeta (como en el exterior de un sobre, o en una postal) ni lo facilite a ningún desconocido.
- Guarde bien o destruya toda la documentación que contenga su nombre y número de tarjeta (como los recibos). Es más, no tire los recibos a la basura. Es más seguro cortarlos en pedazos para que nadie pueda obtener la información.
- Lleve sólo las tarjetas de crédito que realmente utiliza, sobre todo en los viajes.
- No utilice nunca una tarjeta de crédito como identificación personal.

2.3.2.2.2 Pago mediante intermediarios.

En la Red existen intermediarios que permiten evitar tener que facilitar los datos bancarios a un vendedor desconocido, que es lo que sucede cuando se paga mediante tarjeta de

crédito a una empresa en la Red que no dispone de una pasarela de pago con una entidad bancaria.

Mediante los intermediarios los datos no se facilitan al proveedor, sino a un tercero de confianza que actúa de intermediario financiero, de manera que es éste el que procede al pago al vendedor. De dicho modo los datos de la tarjeta bancaria se encuentran únicamente en una empresa intermediaria de confianza de forma que el vendedor no conoce nunca los datos reales de la tarjeta o cuenta

El ejemplo más conocido y utilizado de intermediario financiero es PayPal, pero también existen otros intermediarios financieros como puede ser los casos de Google Checkout, Amazon Payments, etc.

Ventajas.

- Sistema rápido al ser online o mediante soporte móvil

  El comprador puede pagar con tarjeta de crédito, tarjeta de débito o por cuenta bancaria.

  Sistema seguro, ya que no se envía en ningún momento al comercio la información financiera o de tarjeta de crédito.

  Sistema global, es aceptado en cualquier transacción nacional e internacional.

- Para el comercio, al igual que si se tratase de una entidad bancaria, hay un coste de comisionado.

2.3.2.2.2.1 PayPal.

Ilustración 55: PayPal.

PayPal es una empresa del sector del comercio electrónico, cuyo sistema permite a sus usuarios realizar pagos y transferencias a través de Internet sin compartir la información financiera con el destinatario, con el único requerimiento de que estos dispongan de correo electrónico. Es un sistema rápido y seguro para enviar y recibir dinero.

PayPal procesa transacciones para particulares, compradores y vendedores online, sitios de subastas y otros usos comerciales. La mayor parte de su clientela proviene del sitio de subastas online eBay, compañía que compró PayPal en octubre de 2002.

¿Para qué sirve PayPal?

- Pagar las compras realizadas por Internet.
- Cobrar las ventas realizadas por Internet.
- Enviar y Recibir dinero entre familiares, amigos o particulares.

¿Cómo funciona PayPal?

El envío de dinero o pagos a través de PayPal es gratuito. El destinatario puede ser cualquier persona o empresa, tenga o no una cuenta PayPal, que disponga de una dirección de correo electrónico.

En el siguiente gráfico, se explica el funcionamiento de PayPal. Esta plataforma actúa como intermediaria en el envío de dinero de un comprador/remitente a un vendedor/destinatario.

En este caso, el comprador puede utilizar PayPal para pagar por medio de tarjeta de débito, tarjeta de crédito, cuenta bancaria o saldo PayPal. En las tres primeras opciones, se deben vincular las cuentas, con la cuenta de PayPal.

El destinatario puede ser cualquier persona o empresa, tenga o no una cuenta PayPal, que disponga de una dirección de correo electrónico. En el caso de que el destinatario no tenga una cuenta de PayPal, se le envía un mail informándole del pago y deberá registrarse para hacerlo efectivo.

Es importante aclarar que el vendedor, siempre recibe saldo PayPal, que luego podrá retirar o transferir a una cuenta bancaria por diferentes medios, dependiendo del país de residencia.

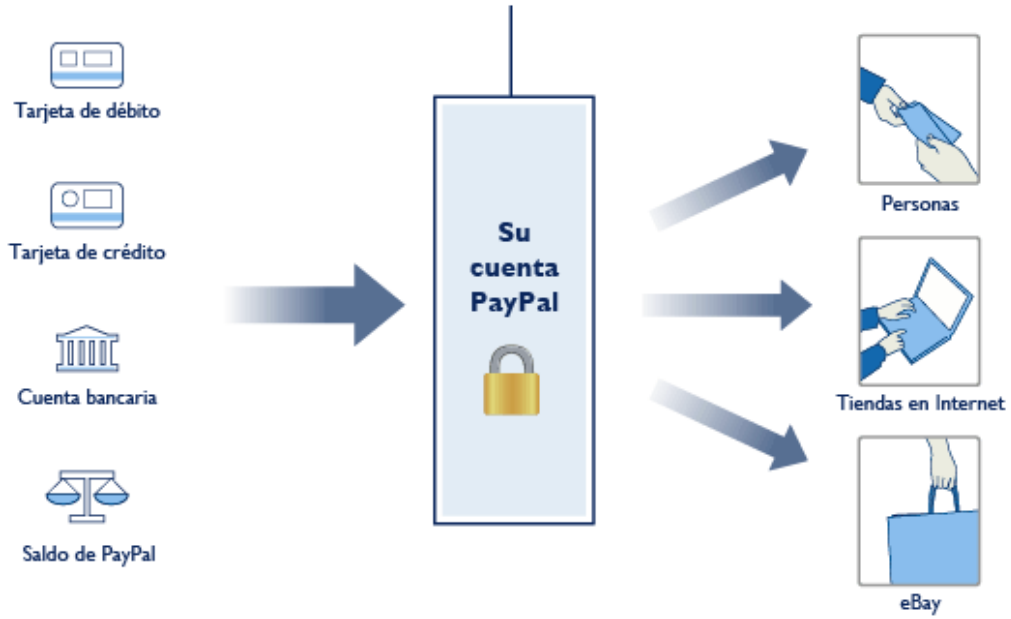


Ilustración 56: Funcionamiento de PayPal.

¿Cuál es su operativa?

No se puede considerar PayPal como un banco, por lo que no se rige por las mismas leyes que las entidades bancarias. A pesar de esto, PayPal tiene que obedecer las reglas del Departamento del Tesoro de los Estados Unidos y de la Autoridad de Servicios

Financieros de la Unión Europea. Algunas de las reglas son para evitar el lavado de dinero y las transacciones no autorizadas.

A diferencia de las entidades bancarias tradicionales, donde el cliente recibe una rentabilidad por tener su dinero depositado en su cuenta, PayPal no ofrece ningún interés por este concepto.

Hay que destacar que PayPal dispone de una política de protección al comprador, de hasta 2.500 USD (o equivalente en otra divisa), donde se cubren problemas de "Artículo no recibido" o de "Artículo muy distinto al descrito", incluyendo no solo el precio del artículo sino también los gastos de envío. Este tipo de protección solo es válida para determinadas compras donde no se incluyan, por ejemplo, artículos intangibles, servicios, vehículos, etc... El punto 13 de las Condiciones de uso del servicio de PayPal informa más detalladamente sobre la protección al comprador.

Por cada transacción, PayPal cobra una comisión variable de entre el 1,9% y el 3,4% + 0,35 EUR al receptor del dinero.

PayPal también percibe dinero por aplicar la conversión de divisa (compuesta por una tarifa variable según "las condiciones del mercado de divisas" que suele ser de entre el 2,5% y el 4%). Aunque a la hora de pagar en una moneda distinta a la principal, PayPal permite que el cambio de divisa lo proporcione la entidad de la tarjeta de crédito.

Como resumen, PayPal cobra por los conceptos de:

- Cargo de una comisión al vendedor por utilizar PayPal como plataforma de cobro.

PayPal no cobra por los conceptos de:

- Realizar un pago a otra persona o empresa (el comprador no paga más que el precio fijado por el vendedor).
- Cargar dinero en la cuenta de PayPal.
- Abrir diferentes cuentas en distintas divisas siempre que sea dentro de PayPal.

¿Por qué es PayPal un método seguro para realizar pagos y transferencias de dinero?
PayPal es un método seguro para realizar pagos y transferencias de dinero porque usa tecnología de encriptación SSL de 128 bits para proteger toda la información confidencial y el destinatario nunca recibe datos financieros como el número de tarjeta o cuenta bancaria ni información personal.

Ventajas de utilizar PayPal para compradores y vendedores.

Ventajas para Compradores.

- Servicio gratuito, sin comisiones ni cuotas.
- Sólo necesitan introducir su dirección de correo electrónico y una contraseña para realizar los pagos.
- No tendrán que introducir los datos de su tarjeta en cada compra.
- Los datos financieros no se comparten con el vendedor.
- Opción de elegir como pagar: Tarjeta, Cuenta Bancaria o Saldo de PayPal.
- Compras protegidas hasta 1000 EUR por la Política de Protección.

Ventajas para Vendedores.

- Sin costes de alta, mantenimiento o cancelación.
- Control de todas sus ventas y acceso a su historial de transacciones desde una sola cuenta.
- Podrá aceptar pagos con Tarjeta, Transferencia Bancaria y Saldo de PayPal con total seguridad.
- Amplio mercado internacional con más de 150 millones de usuarios en 190 países.
- El logotipo de PayPal en los resultados de búsqueda destaca sus artículos sobre los de la competencia.

Tipos de cuenta de PayPal.

- Cuenta Personal (Para particulares que compran).
- Cuenta Premier (Para particulares que compran y venden).
- Cuenta Business (Para empresas que venden en Internet).

2.3.2.2.2.2 Google Wallet.

Ilustración 57: Google Wallet.

Google Wallet es un sistema de pago móvil creado por Google que permite a sus usuarios almacenar tarjetas de débitos, tarjetas de crédito, tarjetas de fidelidad, y tarjetas regalo entre otras cosas, así como una redentora promoción de ventas en su teléfono móvil. Google Wallet utiliza near field communication (NFC) para "hacer pagos rápidos, seguros y convenientes con un simple toque del teléfono en cualquier PayPass terminal habilitado al momento de pagar."

Wallet Digital, Wallet Electrónico o Google Wallet, los derechos de propiedad intelectual pertenecen a Gaston Schwabacher, el número de patente PI 9500345.

Tarifas.
No hay ninguna tarifa por realizar compras en los servicios de Google, tales como Google Play o Google Drive. Solo pagas por las compras que realizas, los impuestos aplicables y los gastos de envío.

Cargos.
El servicio de Google a través del cual realizaste el pedido será el que aparecerá reflejado como un cargo en tu cuenta.

Los cargos se muestran en el resumen como GOOGLE*Nombre del vendedor y, generalmente, aparecen pocos días después de realizar el pedido.

Autorizaciones.

Es posible que veas autorizaciones de pago pendientes cuando verifiques tu cuenta bancaria o tu resumen de la tarjeta. Estas autorizaciones se llevan a cabo para que Google pueda asegurarse de que la tarjeta es válida y también para verificar que cuentas con fondos suficientes en tu cuenta para efectuar la compra.

Estas son solicitudes de autorización y no cargos. No realizas ningún pago por ellas.

Es posible que las autorizaciones permanezcan en tu cuenta entre uno a catorce días hábiles, según el banco. Si todavía ves la autorización pendiente después de catorce días hábiles, comunícate con el banco para obtener más información.

¿Cómo funciona Google Wallet?
De alguna manera el funcionamiento de Wallet es elemental. Basta con introducir los datos sensibles de la tarjeta de crédito o tarjeta de débito e ir a hacer compras. En el caso en el que el punto de venta está equipado con un lector de POS habilitado, sólo tiene que tocar con el teléfono inteligente para cerrar la transacción.

2.3.2.2.2.3 Amazon Payments.

Ilustración 58: Amazon Payments.

Amazon, otra de las grandes empresas de Internet, tiene su propio sistema de pago electrónico, denominado Amazon Payments.

El servicio Amazon Payments te permite usar los métodos de pago que normalmente usas en Amazon.com para pagar bienes y servicios en línea en todos los sitios web que aceptan Amazon Payments. Con una cuenta de Amazon Payments, puedes hacer compras seguras en otros sitios web que aceptan el pago a través de Amazon Payments, sin necesidad de volver a ingresar tu información de pago. Además, el servicio Amazon Payments no tiene ningún costo adicional para ti.

Comenzar a usar Amazon Payments es fácil. Si tienes una cuenta en Amazon.com, la cuenta de Amazon Payments ya ha sido creada automáticamente para ti, y se activará cuando hagas tu primera compra en cualquier sitio web que acepta Amazon Payments. Esta cuenta está ligada a tu cuenta de Amazon.com, y podrás usar las tarjetas de crédito en tu cuenta inmediatamente. Puedes mejorar tu cuenta personal de Amazon Payments para hacer pagos directamente desde tu cuenta bancaria y para recibir pagos de otros usuarios de Amazon Payments.

Amazon Payments almacena tu información financiera de manera confidencial y no deberás compartir la información almacenada por Amazon.com al hacer tus compras. Amazon Payments te proporciona la misma experiencia de compras seguras que ahora disfrutas en

Amazon, haciendo uso de funciones de detección de fraude y administración de riesgo comprobadas.

2.3.2.2.2.4 Dwolla.

Ilustración 59: Dwolla.

Hace poco menos de un año, Iván nos contaba sobre Dwolla, un servicio de pago electrónico con la característica diferencial con otros competidores como PayPal o las tarjetas de crédito tradicionales, de que la operación de pago se realizaba a través de ellos, pero entre emisor y receptor del dinero a cambio de una comisión fija y no un porcentaje del dinero total transferido.

Esto trajo ruido extra porque también se confirmaba que en el futuro se habilitaría la posibilidad de intercambiar dinero, no sólo conociendo el mail del destinatario sino también a través de sus perfiles en las redes sociales.

Pasaron 11 meses y Dwolla nuevamente es noticia, no porque haya incorporado algún tipo de mejora a su servicio sino porque sus usuarios alcanzaron récords de transferencias de entre 30 y 50 millones de dólares al mes, lo que encendió las alarmas en algunos de sus competidores más directos.

Con apenas una comisión de 0,25 centavos de dólar por operación concretada y un promedio de 500 dólares de movimiento por usuario, Dwolla tiene entre ceja y ceja derrotar al maquiavélico sistema de tarjetas de crédito que con sus porcentajes y tasas de interés se convierten en el temor de cualquier usuario.

2.3.2.2.2.5 Autorize.net

Ilustración 60: Autorize.net.

Authorize.Net permite a los comerciantes para autorizar, resolver y administrar tarjetas de crédito y transacciones con cheques electrónicos a través de sitios web, tiendas al por

menor, venta por correo / teléfono para centros (MOTO) de llamada y los dispositivos móviles.

Reputación que puede confiar: Más comerciantes confían Authorize.Net que cualquier otra pasarela de pago para gestionar sus transacciones de pago de forma segura y fiable.

Fácil de integrar: Authorize.Net ofrece varios métodos para vincular los sitios Web de la pasarela de pago. Los comerciantes en línea pueden elegir el método que mejor se adapte a sus necesidades de negocio. Comerciantes minoristas se integran a la pasarela de pago a través de soluciones de punto de venta de terceros.

Gratuito de asistencia al cliente: La satisfacción del cliente es nuestra prioridad número uno. Es por eso que ofrecemos soporte al cliente gratuito a través de teléfono gratuito, correo electrónico y chat en línea. Los representantes están disponibles 24 horas al día, 7 días a la semana por teléfono (vacaciones principales cerrados).

Escalabilidad: Authorize.Net ofrece soluciones valiosas para los comerciantes conscientes de los costos. Si cambian sus necesidades de negocio, puede pasar al servicio de avanzada CyberSource para el procesamiento de la empresa-volumen, los pagos internacionales, servicios avanzados de gestión de riesgos, y más.

Asociaciones Empresariales: Somos una empresa dedicada a proporcionar productos y servicios y herramientas de valor añadido que ayudan a los comerciantes minimizar el riesgo, reducir los costos y aumentar los ingresos.

2.3.3 Pasos para realizar una compra segura.

Para ejecutar una compra segura a través de la Red deben llevarse a cabo los siguientes pasos:

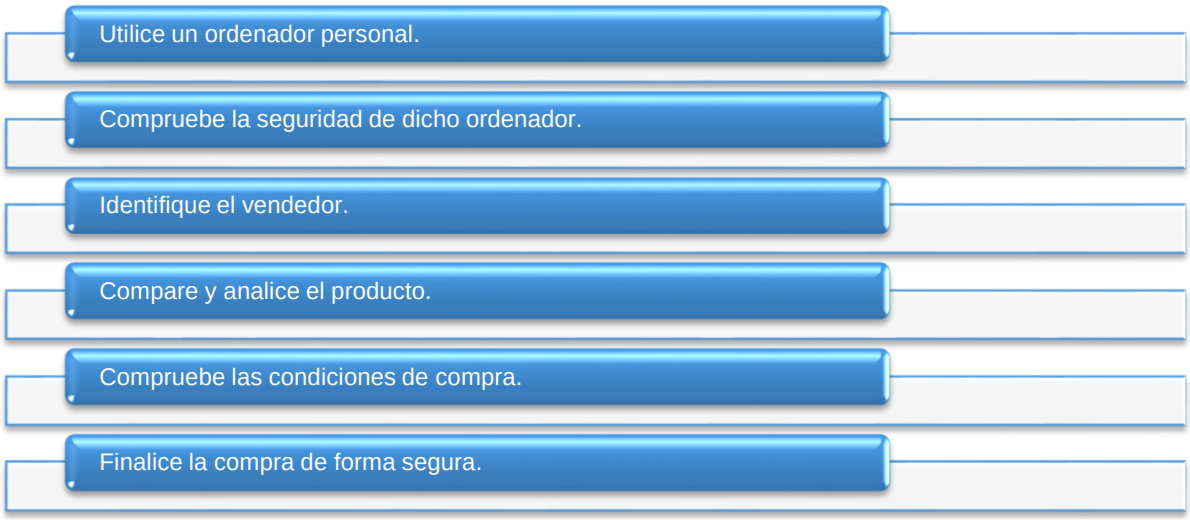


Ilustración 61: Pasos para realizar una compra segura en Internet.

2.3.3.1 *Utilizar un ordenador personal.*

En primer lugar, se debe utilizar un ordenador personal, y no uno de acceso público. Los niveles de seguridad en un ordenador personal bien configurado suelen ser superiores a los que ofrecen los ordenadores de acceso público. Es uno de los motivos por los que la mayoría de compras de productos de comercio electrónico se deben realizan en el hogar.

Ilustración 62: Ordenador personal.

En el caso en que se realice la compra al que posteriormente puedan tener acceso otras personas, al finalizar la compra se debe recordar:

- Eliminar las cookies.
- Eliminar los archivos temporales del navegador web.
- Cerrar la sesión de usuario de los servicios a los que haya tenido acceso en esa sesión o de la oficina virtual de la entidad.

2.3.3.2 *Comprobar que el ordenador es seguro*

El siguiente paso es comprobar que el ordenador desde el que se realiza la compra es seguro. Es recomendable tener un ordenador libre de amenazas a fin de realizar operaciones de comercio electrónico de forma segura. Para ello la Oficina de Seguridad del Internauta (OSI) pone a la disposición del usuario un conjunto de consejos y recomendaciones que se pueden resumir en:

- **Actualizaciones de software:** mantener actualizado el equipo, tanto el sistema operativo como cualquier aplicación que esté instalada, incluido el navegador, para que los códigos maliciosos no puedan encontrar un punto débil en el equipo. Igualmente se deben activar las actualizaciones automáticas.
- **Utilizar software con licencia que ofrezca garantía y soporte.**
- **Cuentas de usuario:** utilizar siempre una cuenta de usuario con privilegios limitados para realizar comercio electrónico.
- **Herramientas:** es imprescindible tener instalado:
  - Un programa antivirus de escritorio y además utilizar ocasionalmente un antivirus en línea.
  - Un programa cortafuegos.
  - Un programa anti-espía de escritorio y utilizar ocasionalmente uno en línea para navegar por Internet.

- **Es recomendable tener instalados otros programas de seguridad como analizadores de URL:** permiten categorizar las páginas a las que se accede a fin de determinar el grado de confianza de las mismas.
- **Utilizar contraseñas robustas y seguras en todos los servicios que se utilicen,** cambiándolas periódicamente y sin revelarlas a nadie, ni anotarlas en lugares visibles o de fácil acceso como pantallas, teclados o crear documentos de texto que contengan dichas claves.
- **Realizar una navegación segura en Internet:**
  - Como se expondrá con más detalle más adelante se debe utilizar una autenticación segura: al introducir el usuario y contraseña la información debe ir cifrada, para cerciorarse de ello es necesario asegurarse que durante el proceso la dirección de la página comience por “https://”, especialmente en ordenadores públicos.
  - Configurar su navegador para que sea seguro.
  - Analizar con un programa antivirus todo archivo que se descargue de Internet.
  - Configurar el correo electrónico de modo seguro: utilizando un filtro anti-spam y no abriendo ficheros sospechosos de fuentes desconocidas.

2.3.3.3 *Verificar la legitimidad de la web*

El siguiente paso para realizar una compra segura consiste en verificar la legitimidad de la web de compra y comprobar que es segura.

El primer paso es identificar al vendedor, para lo que es necesario buscar en la página web la identidad de la empresa.

En particular:

- Se debe verificar la legitimidad del sitio web: los atacantes intentarán engañar mediante correos electrónicos y páginas web que suplantan la identidad del banco o comercio. Es necesario aprender a reconocer páginas web y mensajes fraudulentos, para que esto no ocurra.
- A su vez se puede utilizar como apoyo los filtros antifraude de los navegadores diseñados para alertar al visitar una página fraudulenta y siempre manteniendo el navegador con una configuración segura.
- Si es la primera vez que se utilizan los servicios en línea de una entidad desconocida, se han de tener en cuenta los siguientes consejos para identificar una entidad de garantías:
  - Informarse sobre el sitio antes de comprar: desconfiar de empresas que ofrecen precios demasiado bajos o que no facilitan dirección física y teléfono de contacto. Si estos datos están disponibles, es conveniente comprobar la existencia de la dirección o utilizar el teléfono para comprobar que el establecimiento existe.
  - Leer la Política o Declaración de Privacidad del sitio, ya que todas las empresas que ofrecen sus productos en Internet deben ofrecer información sobre el tratamiento que van a dar a sus datos personales. Ello suele

reflejarse en determinados apartados a pie de página (parte inferior de la web) con el epígrafe de “Aviso Legal”, “Política de privacidad” o similar.

- Informarse de las Condiciones Generales de Contratación de la página web. El vendedor debe poner a disposición del consumidor las condiciones generales de compra a las que deba sujetarse el contrato, de manera que puedan ser guardadas e impresas por parte del destinatario, y si necesitas alguna aclaración, no debe dudar en contactar con la empresa.

2.3.3.3.1 Medidas técnicas para verificar la seguridad de un sitio web.

Se debe comprobar si el sitio posee un certificado de seguridad: un certificado digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Es aconsejable observar en la barra de direcciones del navegador y comprobar que la dirección web comienza por “https://”, normalmente es únicamente “http”. De este modo se indica que la información transcurre cifrada y así se evita que un atacante pueda capturar los datos.

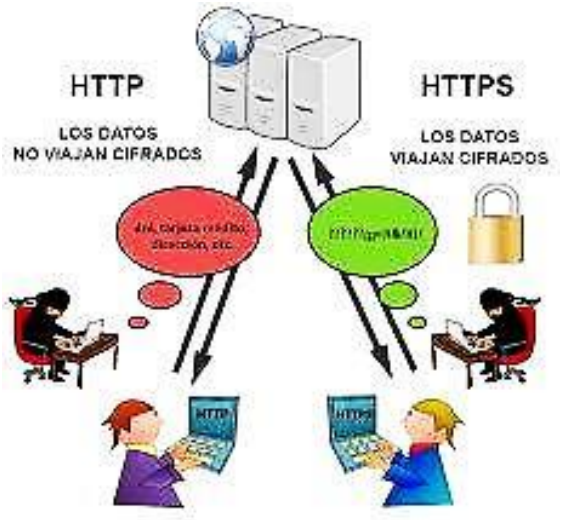


Ilustración 63: Comunicación segura y no segura según el indicativo del protocolo utilizado en la comunicación.

También se debe verificar los indicadores de seguridad del sitio web en el cual se ingresará la información personal: cuando una página web tiene un certificado válido, aparece como indicativo un candado en la parte inferior derecha o en la parte superior que indica que se está usando el protocolo de comunicación seguro HTTPS, que garantiza la comunicación segura entre el servidor y el cliente, evitando de ese modo que personas ajenas capturen los datos intercambiados.

En el portal de compra se muestra el candado de maneras distintas dependiendo del tipo de navegador. Al seleccionar con el ratón dicho candado se abre una ventana que contiene todos los datos del certificado SSL, así como los datos de la entidad de certificación que lo generó.

En función del tipo de certificado SSL que se esté utilizando (SSL o EV-SSL), puede aparecer la barra de dirección o parte de la misma de color verde o azul:

2.3.3.3.2 Certificados seguros para las páginas web.

1) Certificado SSL-EV (extended-validation).

Es el certificado SSL que incorpora más medidas de seguridad. Es el más seguro y confirma la legitimidad de la página.

El certificado aporta información sobre la empresa a la que se compra, asegurando al usuario que dicha información es cierta.

En los distintos navegadores se vería del siguiente modo:

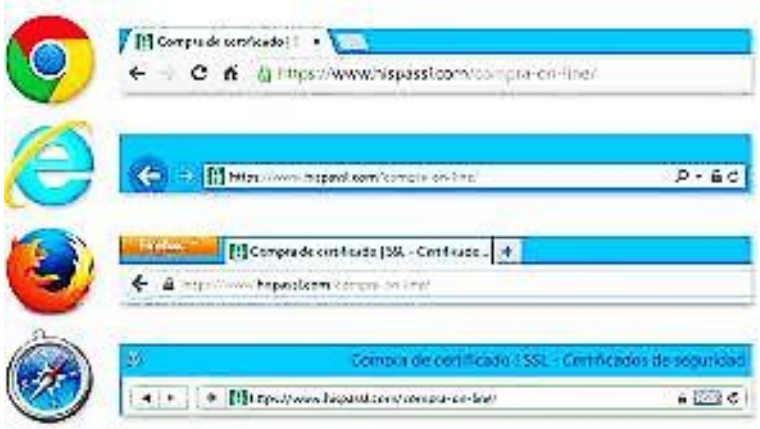


Ilustración 64: Barra de dirección de algunos navegadores cuando accedemos a una página Web que posee un certificado SSL-EV.

2) Certificado SSL.

El certificado SSL que usa la página no proporciona información de identidad, es decir, no se ha llegado a verificar que la dirección pertenece realmente a la entidad.

Por este motivo para poder utilizar la página con unas mínimas garantías el usuario debe estar seguro de que:

- La dirección de la página que va a visitar pertenece a la entidad.
- La dirección en la barra de navegación está bien escrita. En ocasiones los atacantes intentan suplantar las páginas utilizando direcciones similares y creando páginas prácticamente idénticas.

En los distintos navegadores se vería del siguiente modo:

Ilustración 65: Barra de dirección de algunos navegadores cuando accedemos a una página Web que posee un certificado SSL.

Si es posible, y a fin de asegurar el conocimiento mutuo entre las partes, es aconsejable utilizar la firma electrónica con certificado reconocido. En este caso el DNI electrónico incorpora un chip con dicho tipo de firma que facilita la autenticación del usuario.

2.3.3.4 *Comparar y analizar el servicio de la tienda online.*

El siguiente paso antes de realizar la compra es comparar y analizar el servicio de la tienda online.

Es recomendable, una vez se tienen todos los datos, comparar el artículo y el servicio de la web de compra en los diferentes portales especializados que permiten valorar el servicio de las tiendas online. Ejemplos de dichos portales son Ciao (www.ciao.es), Dooyoo (www.doowwyoo.es), Kelkoo (www.kelkoo.es) o Twenga (www.twenga.es).

También es recomendable acceder a comunidades o foros en la Red que reúnan opiniones imparciales de los consumidores, así como información actualizada de los precios y productos ofrecidos por los anunciantes, a la vez que a la web oficial del fabricante donde se puede comprobar que las características técnicas del producto son las mismas que indica el comerciante.

2.3.3.5 *Comprobar las condiciones de compra.*

Antes de realizar la compra el vendedor deberá informar al consumidor de:

- Las características esenciales del producto.
- El precio total (incluidos los impuestos).
- Los gastos de entrega y transporte.

En particular, y haciendo referencia a las condiciones generales de contratación que se vieron en los pasos anteriores, la idea es definir en concreto éstas en la compra que se pretende realizar. Por ello es recomendable comprobar los datos particulares de la compra y que se disponen referenciados en el listado de arriba.

2.3.3.6 *Confirmación de la compra y acuse de recibo de la misma (fase contractual).*

Una vez se han realizado los pasos anteriores de forma correcta, atendiendo a los requisitos de seguridad establecidos, el último paso a la hora de hacer la compra efectiva es aceptar las condiciones de la misma y realizarla.

Con posterioridad al acuerdo de compra, el vendedor está obligado a confirmar al comprador que ha recibido su aceptación a la compra del producto o servicio. Esto puede realizarlo de las siguientes maneras:

1) Mediante una página web resumen de la transacción, siempre que permita almacenar o imprimir una copia como comprobante de compra.

Dicho resumen debe contener cada uno de los conceptos del precio desglosado de forma individual. Así mismo el consumidor ha de tener la opción de modificar dichos datos o anular la compra en el caso de que no le parecieren correctos.

2) Realizando el envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el consumidor haya señalado, en el plazo de las 24 horas siguientes a la recepción de la aceptación. Dicho acuse de recibo incluye generalmente un número de pedido que facilita la identificación y resolución de los problemas por parte del servicio postventa.

Este comprobante tiene los mismos efectos legales que un ticket de compra en un comercio tradicional siendo necesario a la hora de ejercer los derechos del consumidor. Por ello es recomendable imprimir y guardar una copia de dicho recibo junto con una copia de los términos y condiciones de la venta, así como de las características del producto.

2.3.4 Costes en la instalación de las formas de pago.

Dependiendo del carácter de la forma de pago tendremos unos mayores o menores costes que el comercio debe asumir.

Entre estos costes podemos enumerar:

- **Costes por comisionado:** Las entidades bancarias cobran un porcentaje de las transacciones que se realizan a través de su canal de pago.
- **Costes de integración de TPV:** Para poder dotar a un comercio de un pago con tarjeta de crédito, se requiere de una intervención técnica que configure el Terminal de Pago Virtual (TPV) del comercio, con la pasarela de pago de la entidad bancaria.

2.3.5 Principales métricas de los medios de pago.

- **Tasa de Fraude Online:** Porcentaje del total de las transacciones o facturación de la compañía que ha supuesto una pérdida para la compañía debido a operaciones fraudulentas. También se puede medir en porcentaje del beneficio perdido a consecuencia del fraude online.

En el pago con tarjetas de crédito, la mayoría de los fraudes son ocasionados por el uso de tarjetas no autorizadas en operaciones fraudulentas, que ocasionan devoluciones de cargo por parte de los legítimos titulares de la tarjeta.

- **Tasa de Denegación o Rechazo:** Porcentaje del total de transacciones denegadas en el momento de validación de los datos de tarjeta de crédito. La denegación la produce:
  - El procesador de pagos, normalmente por problemas de solvencia/límites/caducidad de la tarjeta o por problemas técnicos.
  - El sistema de gestión de riesgo, al aplicar determinados filtros y restricciones a la aprobación de la transacción analizada.
  - Medición de la "rentabilidad" del sistema de gestión de riesgo: en el corto plazo, la introducción de un sistema de gestión de riesgo aumenta la tasa de denegación, al no procesarse como correctas transacciones que antes se daban por válidas.

- **Tasa de Abandono:** Porcentaje de transacciones abandonadas en el momento de la compra por diferentes motivos, la mayoría de ellos asociados a los procedimientos de autenticación.

- **Tasa de Revisión Manual:** En aquellas empresas que disponen de sistemas de gestión de riesgo, es el porcentaje de operaciones que se revisan manualmente tras su identificación como transacción sospechosa de fraude. Esta cifra suele condicionar en gran medida los presupuestos dedicados a la gestión del fraude, al tratarse de una actividad intensiva en capital humano.

2.4 Principales plataformas.

Las plataformas de Comercio electrónico nos permiten de forma muy sencilla gestionar una tienda on-line con todos los servicios necesarios para publicar nuestros productos, instalar formas de pago y recibir los datos y pedidos de los compradores.

Los productores, proveedores y usuarios logran tener acceso y transmisión mundial de información y su esparcimiento en forma sencilla y económica, sean con fines comerciales o sociales. La apertura de mercados es fundamental para el rápido crecimiento del uso de nuevos servicios y la asimilación de tecnologías nuevas.

Las plataformas más reconocidas en el comercio electrónico tenemos: OpenCart, Magento, OsCommerce, PrestaShop, X-Cart, Zen Cart, VirtueMart, CubeCart, TomatoCart, Shopify, BigCommerce, etc...

Las plataformas más utilizadas se mencionarán a continuación:

2.4.1 OpenCart.

Ilustración 66: OpenCart.

Es un proyecto relativamente joven, pero no por eso deja de ser interesante. Al igual que Magento, OpenCart utiliza la arquitectura Modelo-Vista-Controlador (MVC), en concreto MVC (+L), lo que denominan modelo vista controlador + idioma. Modelo Vista Controlador (MVC) es un patrón de arquitectura de software que separa los datos de una aplicación, la interfaz de usuario, y la lógica de negocio en tres componentes distintos.

El patrón de llamada y retorno MVC (según CMU), se ve frecuentemente en aplicaciones web, donde la vista es la página HTML y el código que provee de datos dinámicos a la página. El modelo es el Sistema de Gestión de Base de Datos y la Lógica de negocio, y el controlador es el responsable de recibir los eventos de entrada desde la vista. Este patrón permite a los desarrolladores mantener y ampliar pequeños segmentos de código específico de una tarea, en vez de tener que hacerlo con una enorme de red de ficheros.

Pero es muchísimo más sencillo y liviano que éste. Fue creado por el inglés Daniel Kerr. Además, que su instalación es muy sencilla, es notable su sencillez y rapidez, combinadas con suficientes funcionalidades como para poder crear una tienda en línea bastante completa.

Al igual que la mayoría de software de tiendas virtuales, se pueden agregar módulos para añadir características adicionales. Cuenta con una aceptable documentación y un foro para aclarar dudas y compartir conocimientos. La comunidad es un tanto pequeña aún (unos 6.000 miembros), pero va en constante aumento. Al igual que en la mayoría de software aquí analizado, se pueden instalar módulos adicionales (gratuitos o comerciales) para ampliar sus funcionalidades.

Respecto a la organización de productos por categorías y la introducción de artículos son sus puntos fuertes, con grandes facilidades, sencillos editores donde podremos añadir

todas las características de nuestro artículo y una buena galería de fotos del producto para ayudar a que el comprador tenga toda la información a su disposición.

Este software se destaca por su sencillez de manejo tanto en la tienda como en el módulo de administración, siendo además su código bastante bien estructurado.

2.4.1.1 *Requisitos*

- Apache 2.0 o superior, o Internet Information Server (IIS)
- PHP 5.0 o superior
- MySql 5.0 o superior
- Sistema Operativo: cualquiera en donde se pueda instalar los requisitos anteriores.

2.4.1.2 *Características.*

- Categorías Ilimitadas.
- Código Abierto Open Source.
- Artículos Ilimitados.
- Documentación Gratis (en inglés).
- Fabricantes Ilimitados.
- Plantillas Intercambiables.
- Monedas Múltiples.
- Redimensionado de Imágenes.
- Lenguajes Múltiples.
- Más de 20 Formas de Pago.
- Comentarios en Artículos.
- Más de 8 Medios de Transporte.
- Valoración Artículos.
- Ampliación de Módulos.

2.4.1.3 *Arquitectura.*

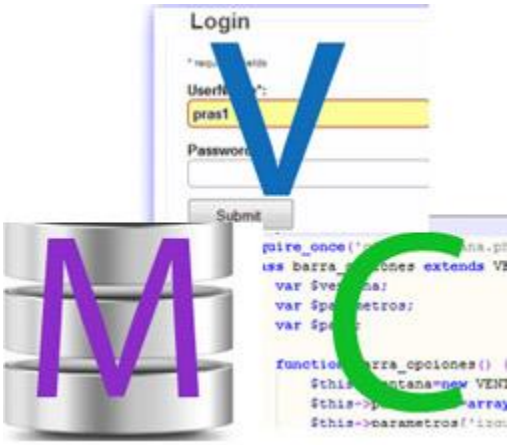


Ilustración 67: Arquitectura OpenCart.

OpenCart utiliza la estructura Modelo-Vista-Controlador (MVC), en concreto MVC(+L), lo que denominan modelo vista controlador + idioma. Modelo Vista Controlador (MVC) es un patrón de arquitectura de software que separa los datos de una aplicación, la interfaz de usuario, y la lógica de negocio en tres componentes distintos.

El patrón de llamada y retorno MVC (según CMU), se ve frecuentemente en aplicaciones web, donde la vista es la página HTML y el código que provee de datos dinámicos a la página. El modelo es el Sistema de Gestión de Base de Datos y la Lógica de negocio, y el controlador es el responsable de recibir los eventos de entrada desde la vista. Este patrón permite a los desarrolladores mantener y ampliar pequeños segmentos de código específico de una tarea, en vez de tener que hacerlo con una enorme de red de ficheros.

2.4.1.4 ***Framework.***

2.4.1.4.1 Bootstrap.

Ilustración 68: Bootstrap.

Es un Framework originalmente creado por Twitter, que permite crear interfaces web con CSS y JavaScript, cuya particularidad es la de adaptar la interfaz del sitio web al tamaño del dispositivo en que se visualice. Es decir, el sitio web se adapta automáticamente al tamaño de una PC, una Tablet u otro dispositivo. Esta técnica de diseño y desarrollo se conoce como “responsive design” o diseño adaptativo.

El beneficio de usar responsive design en un sitio web, es principalmente que el sitio web se adapta automáticamente al dispositivo desde donde se acceda. Lo que se usa con más frecuencia, y que a mi opinión personal me gusta más, es el uso de media queries, que es un módulo de CSS3 que permite la representación de contenido para adaptarse a condiciones como la resolución de la pantalla y si trabajas las dimensiones de tu contenido en porcentajes, puedes tener una web muy fluida capaz de adaptarse a casi cualquier tamaño de forma automática.

Pero si no quieres nada que ver con los media queries, otra muy buena opción es el uso del Framework de Bootstrap.

Aun ofreciendo todas las posibilidades que ofrece Bootstrap a la hora de crear interfaces web, los diseños creados con Bootstrap son simples, limpios e intuitivos, esto le da agilidad a la hora de cargar y al adaptarse a otros dispositivos.

2.4.1.4.2 CodeIgniter.

Ilustración 69: CodeIgniter.

CodeIgniter es un framework de desarrollo de aplicaciones, que puede ser utilizado para desarrollar sitios web, usando PHP. Es un marco de código abierto. Tiene un muy amplio conjunto de funcionalidades, lo que aumentará la velocidad de trabajo de desarrollo de sitios web.

Tiene un muy amplio conjunto de bibliotecas y ayudantes. Mediante el uso de CodeIgniter, se ahorrará mucho tiempo, si está desarrollando un sitio web desde cero. No sólo eso, un sitio web construido en CodeIgniter es seguro también, ya que tiene la capacidad de prevenir diversos ataques que se producen a través de sitios web.

2.4.1.5 ***Vulnerabilidad.***

Vulnerabilidad de falsificación de petición en sitios cruzados (CSRF) en index.php en OpenCart v1.4 permite a atacantes remotos secuestrar la autenticación de un administrador de la aplicación para las peticiones que de creación de una cuenta de administrador a través de una petición POST con el parámetro de ruta establecida a "user/user/insert.".

NOTA: algunos de estos detalles han sido obtenidos de información de terceros.

Impacto

Afecta parcialmente a la integridad del sistema + Afecta parcialmente a la confidencialidad del sistema + Afecta parcialmente a la disponibilidad del sistema.

Productos y versiones vulnerables.

OpenCart 1.4

Mediante la explotación de una vulnerabilidad de cross-site scripting el atacante puede secuestrar el iniciado sesión en la sesión del usuario. Esto significa que el hacker malicioso puede cambiar el iniciado la sesión en la contraseña del usuario e invalidar la sesión de la víctima, mientras que el hacker mantiene el acceso. Como se ve en el ejemplo XSS en este artículo, si una aplicación web es vulnerable a cross-site scripting y la la sesión del administrador es secuestrada, el hacker malicioso explotar el vulnerabilidad tendrá privilegios de administrador completos en que la aplicación web.

La prueba de concepto para las direcciones URL XSS en OpenCart v2.1.0.1:
/opencart/index.php?route=account/address/add (IdDeZona - POST)

Solución.

https://github.com/opencart/opencart/commit/303fa88fe664ded4bf8753b997abd916f0a3c03f

2.4.1.6 *Lugares donde utilizan la plataforma.*

Nombre de la tienda.	Dirección Web
Vanity shop	http://www.diaboliquedesign.com/demo/vanityoc/
Venta de proteínas.	http://www.scicorenutrition.com/
Venta de proteínas.	http://www.blackextremelabs.com/
Sex shop online.	http://www.mysexshop.es/
Viva el musculo	http://www.mysexshop.es/

Tabla 5: Lugares donde utilizan OpenCart.

2.4.2 Magento.

Ilustración 70: Magento.

Aplicación desarrollada por la empresa estadounidense Varien, fue lanzada oficialmente el 31 de marzo de 2008. Su arquitectura se basa en el modelo MVC (Modelo, Vista, Controlador).

Magento está construido sobre el Zend Framework, para asegurar que el código base sea seguro y escalable. Las razones para escoger Zend Framework son muchas, pero a un nivel básico el Zend Framework proporciona una librería de código orientado a objetos con el compromiso de una sólida compañía detrás de él.

Usando este framework, Magento fue construido con tres principios fundamentales en mente:

1. **Flexibilidad:** Creemos que cada solución debería ser tan única como los negocios que están detrás de ella. El código de Magento le permite una personalización perfecta.
2. **Actualizable**: Separando el código del núcleo, del de la comunidad y las personalizaciones; Magento puede ser personalizado fácilmente sin perder la habilidad de actualizarse.
3. **Velocidad y Seguridad**: Los estándares de codificación usados por los desarrolladores, siguen las mejores prácticas para maximizar la eficiencia del software y proporcionan una segura vitrina en línea.

A pesar de que el 15 de abril de 2009 presentaron la versión Enterprise, que tiene un costo bastante elevado, podemos tener acceso totalmente gratuito a la versión Community. La diferencia entre ambas radica en ciertas funcionalidades añadidas a la versión Enterprise, además del soporte y garantía con las que esta última cuenta. Pero el núcleo (core) como tal es el mismo para ambas. Lo que llama la atención de este software de tienda virtual son todas las funcionalidades que tiene. Además, tiene la particularidad de que permite crear diseños innovadores debido a su sistema de layouts, pudiéndose asignar vistas distintas a productos o categorías específicos. En la actualidad cuenta con una comunidad que supera los 180.000 miembros registrados, foros en distintos idiomas y más de 1.700 extensiones (entre gratuitas y comerciales), que pueden ser instaladas de forma muy sencilla, para agregar alguna característica adicional que se necesite. A eso le podemos sumar una gran campaña de marketing desarrollada por Varien, lo cual hace que Magento sea muy dinámico y esté en constante renovación.

Su punto débil es que requiere de un servidor bastante potente, ya que la aplicación consume muchos recursos. Otra desventaja es su extrema complejidad (la última versión 1.4.0.0 pesa casi 55MB, tiene más de 9.000 archivos ubicados en más de 3.000 carpetas y la base de datos tiene 273 tablas), por lo que no es nada sencillo realizar modificaciones al mismo. Claro que esto mejora a medida que uno se familiariza con su estructura.

2.4.2.1 *Requisitos.*

- Apache.
- PHP 5.0 o superior.
- MySql 5.0 o superior.

2.4.2.2 *Características.*

- Posibilidad de personalización del diseño.
- Soporte para multi-idioma.
- Posibilidad de multiplataforma (administrar varias tiendas desde un único panel de administración).
- Gestión total y completa de catálogo y ficha de productos.
- Gestión de clientes.
- Múltiples formas de pago y envío.
- Inventario y control de stock.
- Posibilidad de comentarios y valoraciones
- Web y CMS: 2 en 1.
- Herramientas de marketing:
    - Ventas cruzadas, productos sugeridos, productos relacionados.
    - Configuración de cupones de descuento y promociones.

2.4.2.3 *Arquitectura.*

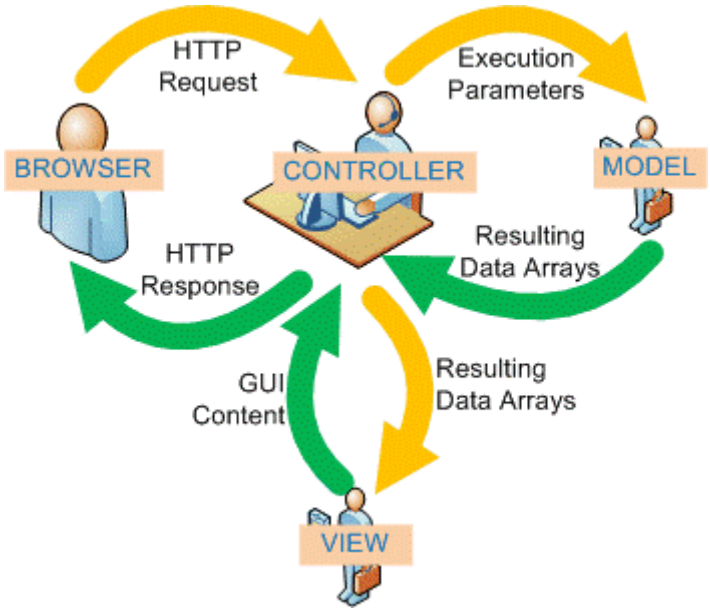


Ilustración 71: Arquitectura Magento.

El Modelo-Vista-Controlador (MVC) es un patrón de arquitectura que separa una aplicación en tres principales componentes lógicos: el modelo, la vista y el controlador. Cada uno de estos componentes se construyen para manejar aspectos específicos de desarrollo de una aplicación. MVC es uno de los marcos de desarrollo web estándar de la industria más frecuentemente utilizado para crear proyectos escalables y extensibles.

Los componentes MVC.
Modelo: El componente de modelo corresponde a todos los datos de la lógica de que el usuario trabaja con relacionados. Esto puede representar los datos que se transfieren entre la Vista y los componentes del controlador o cualquier otra lógica de negocio de datos relacionados. Por ejemplo, un objeto de cliente recuperará la información del cliente de la base de datos, manipular y actualizar datos de vuelta a la base de datos, o utilizarlo para representar datos.

Vista: El componente de vista se utiliza para toda la lógica de la interfaz de usuario de la aplicación. Por ejemplo, la vista del cliente incluiría todos los componentes de interfaz de usuario, tales como cuadros de texto, menús desplegables, etc. que el usuario interactúa con la última.

Controlador: Controladores actúan como una interfaz entre los componentes del modelo y la vista para procesar toda la lógica de negocio y las peticiones entrantes, manipular los datos mediante el componente del modelo y de interactuar con las vistas para hacer que la salida final. Por ejemplo, el controlador de cliente podría manejar todas las interacciones y las aportaciones de la vista del cliente y actualizar la base de datos utilizando el Modelo de Cliente. El mismo controlador se utiliza para ver los datos del cliente.

2.4.2.4 *Framework.*

2.4.2.4.1 Zend.

Ilustración 72: Zend.

Zend Framework (ZF) es un Framework de código abierto para desarrollar aplicaciones web y servicios web con PHP 5. ZF es una implementación que usa código 100% orientado a objetos. En la estructura de los componentes de ZF; cada componente está construido con una baja dependencia de otros componentes. Esta arquitectura débilmente acoplada permite a los desarrolladores utilizar los componentes por separado. A menudo se refiere a este tipo de diseño como "use-at-will" (uso a voluntad).

Aunque se pueden utilizar de forma individual, los componentes de la biblioteca estándar de Zend Framework conforman un Framework de aplicaciones web al combinarse. ZF ofrece una implementación MVC, una abstración de base de datos, y un componente de formularios que implementa la prestación de formularios HTML, validación y filtrado para que los desarrolladores puedan consolidar todas las operaciones usando de una manera sencilla la interfaz orientada a objetos. Otros componentes, como Zend_Auth y Zend_Acl, proveen autentificación de usuarios y autorización diferentes a las tiendas de certificados comunes. También existen componentes que implementan bibliotecas de cliente para acceder de forma sencilla al web services más populares. Cualesquiera que sean las necesidades de su solicitud, usted tiene todas las posibilidades de encontrar un componente de Zend Framework que se pueda utilizar para reducir el tiempo de desarrollo.

2.4.2.5 *Vulnerabilidad.*

Magento es la plataforma de e-commerce y gestor de contenidos web opensource para el comercio electrónico más popular en el mundo actualmente, propiedad de uno de los gigantes de la red: eBay. Hace unos meses la compañía de seguridad Check Point sacó a la luz una vulnerabilidad, que, en el caso de ser explotada, podría comprometer plenamente cualquier tienda online basada en la plataforma Magento.

Pero ahora, su seguridad vuelve a estar en el punto de mira. Esta vez investigadores de la firma de seguridad Sucuri están investigando un nuevo ataque: los ciberdelincuentes están explotando de forma creciente un error hasta ahora desconocido para desviar información de pago de las webs que usan esta plataforma. Los investigadores creen que los cibercriminales están inyectando código malicioso en el fichero core de Magento para robar datos de las tarjetas de crédito.

De ser así, las webs de comercio electrónico que usan este gestor serían vulnerables, es decir, unas 200.000 tiendas online en todo el mundo, que representa cerca del 30% del mercado de e-commerce en todo el mundo.

“La parte mala es que no te darás cuenta de que te está afectando hasta que sea demasiado tarde. En el peor de los casos, no será evidente hasta que no aparezca en tu cuenta bancaria “, asegura el investigador de Sucuri en su blog.

En su blog, como recoge The Hacker News, los investigadores de Sucuri han encontrado el script del ataque que roba el contenido de las peticiones POST e identifica los pagos de las tarjetas antes de almacenarlos en un formulario encriptado que sólo el atacante puede descifrar.

La petición POST es uno de los tipos de petición HTTP más utilizados para enviar los datos a los servidores. POST se usa mayormente para enviar formularios web (como los de las tiendas online) donde los datos son cifrados para enviarlos de forma segura al servidor.

Es más, para evadir la detección, las herramientas de los atacantes incluyen una función que limpia los agentes de usuario. Es decir, que no dejarán rastro, y los afectados no se darán cuenta hasta que sea demasiado tarde. Se trata, por tanto, de un ataque muy sofisticado.

Como explican en el blog los investigadores, y como muestran todos los datos y estudios recientes, el robo de tarjetas de crédito en Internet está al alza. Explican las posibles soluciones y precauciones que pueden llevar a cabo las tiendas online para protegerse, aunque es Magento el que tendrá que solucionarlo mediante los parches adecuados.

Fallos de seguridad EN Magento.

Magento, una de las plataformas más extendidas a nivel mundial para tiendas Online, cuenta entre sus nuevas actualizaciones, con una nuevo parche de seguridad considerado como crítico, ya que soluciona más de 9 fallos que podrían en riesgo la seguridad de la tienda online.

El número de ataques debido a estos fallos de seguridad han crecido exponencialmente según podemos ver en la gráfica cedida por Gata Security Labs.

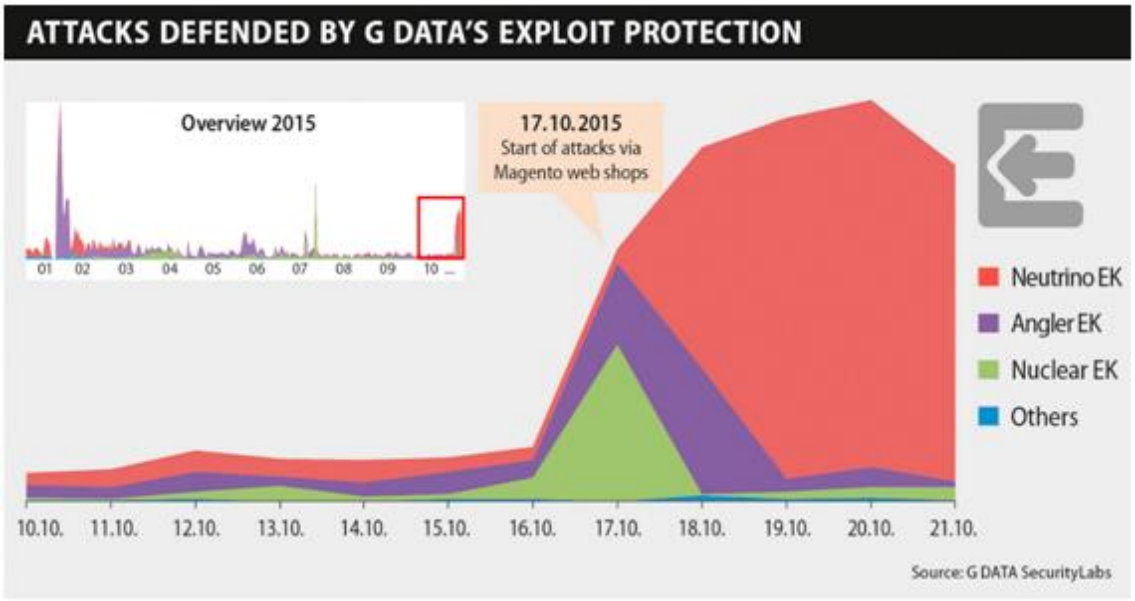


Ilustración 73: Defensa de ataques por G DATA Security Labs.

El parche conocido con la nomenclatura SUPEE-6788 soluciona los siguientes riesgos:

1) Vulnerabilidad grave, los mensajes de logs del sistema de Magento durante el proceso de instalación pueden volcar información de la cadena de conexión con la base de datos, dejando contraseñas de MySQ Len texto claro usable por nuestros atacantes.
2) Vulnerabilidad grave, la funcionalidad de filtro de plantillas de correo electrónico permitiría que, mediante un ataque, podrían acceder a los emails de cambio de usuarios o notificaciones de contraseñas.
3) Vulnerabilidad grave, un fallo en el framework de Magento "Zend Framework" podría permitir el acceso a los archivos "xml" de configuración.
4) Vulnerabilidad grave, ataque por infección de SQL que podría permitir que extensiones externas al núcleo puedan realizar consultas directas a la base de datos extrayendo información de ventas o clientes.
5) Vulnerabilidad grave, error en la ejecución de tareas programadas mediante "cron.php", un atacante que podría ejecutar un exploits colocado en el directorio de la tienda.
6) Vulnerabilidad media, posibilidad de inyección de código malicioso en los campos personalizados, están en riegos aquellas tiendas online con uso de este tipo de campos. El fallo permitiría el acceso a ficheros de instalación del sistema.
7) Vulnerabilidad media, Cross Site Scripting, error en el frontend de la tienda que permitiría la ejecución de código XSS.
8) Vulnerabilidad media, ejecución de código usando informes de error y productos descargados de la tienda.
9) Vulnerabilidad baja, es posible detectar la url de administración que, posteriormente, un atacante podría usar para realizar un ataque de fuerza bruta mediante intentos de usuarios y contraseñas.

10) Protección insuficiente en el restablecimiento de contraseñas. El token de generación de contraseñas no es deshabilitado, lo que podría permitir el robo de credenciales.
11) Fallo en la carpeta "dev" de Magento, carece de un archivo htaccess que impida el acceso desde el navegador, es un directorio que debe ser protegido de exploración y buscadores.
12) Cross Scripting, envenenamiento de caché. La información de pasarelas de pago y páginas de la tienda online eran almacenadas en cache, esto supone un riesgo ya que un ataque podría permitir el acceso a estos archivos que almacenan información de tarjetas de crédito y datos de usuario. Sin duda, esta es una de las vulnerabilidades más críticas y que deben solventarse de inmediato.

Magento propone una serie de prácticas de seguridad para mantener nuestra tienda online a salvo. Si se precisa de mantenimiento o de una actuación de expertos en Magento, puede contactar con digital Dotpara planificar su proceso de actualización, así como un plan de contingencias para mantener a salvo tanto la tienda como los clientes que la usan.

Como pueden comprobar, los parches de esta actualización solo llegan hasta la versión de Magento 1.7, por lo que se recomienda si tiene una versión inferior, realizar un Upgrade completo de la versión hasta la 1.9.2.

Si lo desea, puede buscar todas las últimas versiones, así como parches de seguridad para su tienda onlineen: https://www.magentocommerce.com/download

Este fallo no dicta que Magento se haya convertido en una plataforma Ecommerce no apta para tiendas Online, todo lo contrario, sigue siendo una gran apuesta. Las tendencias de esta Ecommerce van en aumento fuera de España, lo cual lo hace un gran competidor frente a Prestashop o Woocomerce.

Entre algunas de las ventajas que ofrece esta plataforma, se encuentran su experiencia en el sector, la cantidad de extensiones y de los que podremos dotar a nuestra tienda, su sistema de WebService para integrarlo con programas de facturación, ERP o sistemas de Logística de Almacén.

Otra gran ventaja, es su facilidad de desarrollo y su integración con su versión para la comunidad Multitienda.

Actualmente, se cifra que en todo el mundo se cuenta con unas 200.000 tiendas de las cuales un 30% se cifra en esta E-Commerce.

Volviendo al fallo de seguridad descubierto, recomendamos su actualización de inmediato, ya que existen kits de exploits como Nuclear, Angler y Neutrino, que están difundiéndose desde el 17 de octubre.

2.4.2.6 *Lugares donde utilizan la plataforma.*

Nombre de la tienda.	Dirección Web
Toms	http://www.toms.com/

Nike	http://store.nike.com/es/es_es/
My own bike	http://www.myownbike.de/
Ghirardelli	http://www.ghirardelli.com/
Ebay	http://www.ebay.com/

Tabla 6: Lugares donde utilizan Magento.

2.4.3 OsCommerce.

Ilustración 74: OsCommerce.

Este es sin duda el más conocido de todos los programas para tiendas en línea y ha servido de inspiración a una gran cantidad de sucesores.

Está dando vueltas en el mundo de la Internet desde el año 2000. Su creador es Harold Ponce de León. La comunidad que lo respalda es bastante numerosa, superando los 200.000 miembros. Debido al tiempo que tiene en el mercado, cuenta con mucha documentación, módulos (más de 5.000), ayuda y tutoriales en numerosos foros y páginas Web que se dedican al tema. Tiene una gran madurez lo que hace que sea muy robusto y confiable. El punto débil es que se ha rezagado con respecto a los estándares actuales. El diseño está basado en tablas, lo cual está en des uso y hace que cambiar la apariencia de la tienda sea un tanto difícil.

Historia.
La primera modificación, la versión 1.1, se anunció el 17 de mayo de 2000 con actualizaciones, correcciones e introducción de nuevas funciones, en cuanto a la herramienta de administración se actualizó en junio del mismo año.

En noviembre de 2010 se lanzó la versión 2.2 para hacerlo más estable. La versión 2.3 fue realizada teniendo en cuenta la inclusión de herramientas de las redes sociales.

La versión 3.0 fue lanzada el 31 de marzo de 2011 y es la mayor reescritura del programa incorporando objetos en el panel de control y plantillas para el cambio visual, incluye además la petición de nombre de usuario y contraseña durante la instalación.

La última versión es la 3.0.2 lanzada el 06 de agosto de 2011, en la que se le realizó algunas mejoras y se le introdujeron nuevas aplicaciones.

2.4.3.1 *Requisitos.*

- Apache.
- PHP 3.0 o superior.

- MySql 4.0 o superior.

2.4.3.2 *Características.*

- Los pedidos, clientes y productos se almacenan en una base de datos de fácil consulta vía administración-web.
- Los clientes podrán comprobar el histórico y el estado de sus pedidos una vez registrados.
- Los clientes pueden cambiar sus datos de perfil de usuario desde su apartado cliente.
- Múltiples direcciones de envío por usuario, para regalos, por ejemplo.
- Búsqueda de productos.
- Posibilidad de permitir a los usuarios valorar los productos comprados, además de comentarlos.
- Posibilidad de implementar un servidor seguro (SSL).
- Puede mostrar el número de productos en cada una de las categorías.
- Lista global o por categoría de los productos más vendidos y más vistos.
- Fácil e intuitiva navegación por categorías.
- Plataforma multi-idiomas, por defecto estarán disponibles el español, inglés y alemán.

2.4.3.3 *Arquitectura.*

Al igual que Magento, OsCommerce presenta una arquitectura basado en el modelo de tres capas o MVC.

2.4.3.4 *Framework.*

2.4.3.4.1 960 gs.

Ilustración 75: 960 GS.

960 Grid System es un framework CSS, es una declaración de estilos que dispone las clases necesarias para implementar columnas en una página web, de diversos tamaños, con las que maquetar contenidos de una forma fácil y ordenada.

La mayoría de las actuales resoluciones de pantalla que utilizan los usuarios es de 1024 x 768, por este motivo se basa en un diseño de 960px de ancho, con configuraciones de 12 y 16 columnas que vamos combinando según las necesidades pudiendo montar de una forma sencilla webs con múltiples secciones diferentes en tamaño, zonas para cajas, etc.

Estas divisiones se configuran de forma natural, donde simplemente tendremos que ir sumando los tamaños que vamos concatenando para llegar a esas columnas que estamos usando como guía.

2.4.3.5 *Vulnerabilidad.*

Las dos vulnerabilidades que afectan a osCommerce y podrían permitir llevar a cabo ataques de cross-site scripting (XSS) y cross-siterequest forgery (XSRF) para obtener un usuario administrador del sitio.

Recursos afectados:

- Las vulnerabilidades han sido confirmadas en osCommerce 2.3.3 aunque versiones anteriores también podrían estar afectadas.
- A partir de la versión 2.3.3.1 se encuentran solventadas.

Detalles de las dos vulnerabilidades descubiertas por Chris Wood:

1) La primera vulnerabilidad tiene su origen en un error de falta de comprobación del parámetro de entrada “products_id” en la página “product_info.php” antes de ser devuelto al usuario podría permitir a un atacante remoto llevar a cabo ataques XSS (cross-site scripting) y ejecutar código HTML y javascript arbitrario en el navegador de un usuario en el contexto de un sitio afectado.

http://<URL_DEL_SITIO>/product_info.php?products_id=4<script>alert('Vulnerabilidad XSS');</script>

2) La segunda vulnerabilidad de debe a un error de falta de validación del origen de las peticiones HTTP en la página “administrators.php” del módulo de administración podría permitir a un atacante remoto realizar ataques CSRF (cross-site request forgery) y realizar acciones como crear o eliminar usuarios.

Más información.

osCommerce v2.3.3 Admin Takeover Exploit
http://www.invivid.com/files/2013/oscomm_233_exploit.pdf

Otra vulnerabilidad en la plataforma de comercio electrónico OsCommerce v2.3.3.4 que permite es la inyección de SQL.

Recursos afectados.

OsCommerce v2x.

Detalle e Impacto de la vulnerabilidad

Se ha publicado una vulnerabilidad en el foro oficial de OsCommerce que permite la inyección de SQL. El uso de un saneamiento inadecuado de un parámetro en un comando select en la base de datos permitiría a un atacante acceder a los datos de la misma, pudiéndose llegar a insertar un nuevo usuario y contraseña que de acceso total a la aplicación de comercio.

Recomendación

OsCommerce ha publicado la modificación necesaria para solucionar esta vulnerabilidad en su repositorio de código.
https://github.com/gburton/oscommerce2/commit/e4d90eccd7d9072ebe78da4c38fb048bfe31c902

Más información.
Oscommerce Sql Injection Vulnerability
http://forums.oscommerce.com/topic/396035-oscommerce-0day-sql-injection-vulnerability/
https://github.com/gburton/oscommerce2/commit/e4d90eccd7d9072ebe78da4c38fb048bfe31c902
http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_tecnicos/vulnerabiliad_inyeccion_sql_oscommerce_20140210

2.4.3.6 *Lugares donde utilizan la plataforma.*

Tipo de tienda.	Dirección Web
FNAC	http://www.fnac.es/
Pixamania	http://www.pixmania.es/index.html
Redcoon	http://www.redcoon.es/

Tabla 7: Lugares donde utilizan OsCommerce.

2.4.4 PrestaShop.

Ilustración 76: PrestaShop.

Fue creado por un grupo de estudiantes de informática franceses en 2005. Más adelante, el proyecto toma mayor seriedad cuando en agosto de 2007 lanzan la primera versión estable. Está basado en el motor de plantillas Smarty, y también se hace uso de AJAX. Es un script muy liviano, por lo que no exige demasiado en cuanto a servidor se refiere. Cuenta con un buen número de funcionalidades, que lo convierte en una opción muy completa para hacer una tienda en línea. Modificar su código fuente es relativamente sencillo, y además se pueden instalar módulos adicionales (gratuitos o comerciales) para ampliar sus funcionalidades. Su comunidad va en constante ascenso, contando actualmente con más de 50.000 miembros. Igualmente tiene un foro con distintos idiomas, en los que sus lectores pueden aclarar dudas y compartir experiencias

2.4.4.1 *Requisitos.*

- Apache.
- PHP 5.0 o superior.

- MySql 5.0 o superior.

2.4.4.2 *Características.*

- Posibilidad de agregar un número ilimitado de artículos a la tienda.
- Posibilidad de creación de un número ilimitado de categorías, que permite una estructura de árbol (categorías, subcategorías, etc.).
- Potente interfaz de administración web, que le permitirá poder realizar una gestión completa de su tienda online: configuración, alta de productos y categorías, control de pedidos, métodos de pago y envío, etc.
- Código 100% abierto Open Source que le permite tener control total sobre la programación de la tienda y poder realizar cambios.
- Modelos flexibles de impuestos: posibilidad de configurar distintos impuestos en función de país o el código postal de envío.
- Opción de asignar distintos tipos de impuestos en función del producto y crear impuestos combinados.
- Posibilidad de aplicar descuentos a los productos de forma individual con la opción adicional de programar un intervalo de fechas en el que se aplicará el descuento.
- Cupones de descuento: se podrán generar cupones de descuento por porcentaje o importe fijo, de un único uso o varios. También se podrá definir los productos o las categorías para las que el cupón tendrá efecto.
- Opción de seleccionar la moneda con la que se trabajará en la tienda.
- Opción de venta de productos descargables tales como software, mp3, ebooks, etc. Proceso automático de descarga. Se puede fijar un número máximo de descargas. También el número de días que se podrá descargar el fichero.

2.4.4.3 *Arquitectura.*

PrestaShop se basa en una arquitectura de 3 capas:

- **Objeto/Datos.** Acceso a la base de datos es controlado mediante archivos en la carpeta “classes”.
- **Control de Datos.** El contenido proporcionado por el usuario es controlado por los archivos en la carpeta raíz.
- **Diseño.** Todos los archivos del tema en la carpeta "themes".

Este es el mismo principio que en la arquitectura MVC (Modelo-Vista-Controlador), sólo que de una manera más simple y accesible.

El equipo de desarrollo de PrestaShop escogió no utilizar un marco de PHP, como Zend Framework, Symfony o CakePHP, con el fin de permitir una mejor legibilidad y por lo tanto edición más veloz.

Esto también logra un mayor rendimiento, ya que el software sólo se realiza de las líneas de código que necesita y no contiene un montón de bibliotecas genéricas suplementarias.

- Una arquitectura de 3 capas tiene muchas ventajas:

- Facilidad para leer el código del software.
- Los desarrolladores pueden agregar y editar códigos más rápido.
- Diseñadores gráficos e integradores de HTML pueden trabajar dentro de los confines de la carpeta /themes sin necesidad de entender o leer una sola línea del código PHP.
- Los desarrolladores pueden trabajar en datos y módulos adicionales que los integradores de HTML pueden utilizar.

2.4.4.4 *Framework.*

2.4.4.4.1 Smarty.

Ilustración 77: Smarty.

Smarty es un motor de plantillas para PHP. Más específicamente, esta herramienta facilita la manera de separar la aplicación lógica y el contenido en la presentación. La mejor descripción está en una situación donde la aplicación del programador y la plantilla del diseñador juegan diferentes roles, o en la mayoría de los casos no la misma persona.

Por ejemplo: Digamos que usted crea una página web, es decir, despliega el artículo de un diario. El encabezado del artículo, el rotulo, el autor y el cuerpo son elementos del contenido, estos no contiene información de cómo quieren ser presentados. Estos son pasados por la aplicación Smarty, donde el diseñador edita la plantilla, y usa una combinación de etiquetas HTML y etiquetas de plantilla para formatear la presentación de estos elementos (HTML, tablas, color de fondo, tamaño de letras, hojas de estilo, etc...). Un día el programador necesita cambiar la manera de recuperar el contenido del artículo (un cambio en la aplicación lógica.). Este cambio no afectara al diseñador de la plantilla, el contenido llegara a la plantilla exactamente igual. De la misma manera, si el diseñador de la plantilla quiere rediseñarla en su totalidad, estos cambios no afectaran la aplicación lógica. Por lo tanto, el programador puede hacer cambios en la aplicación lógica sin que sea necesario reestructurar la plantilla. Y el diseñador de la plantilla puede hacer cambios sin que haya rompimiento con la aplicación lógica.

2.4.4.5 *Vulnerabilidad.*

La vulnerabilidad tiene que ver con la forma en que el hash de la contraseña se maneja con ambas las contraseñas de administrador y las cuentas de los clientes. Lo que puede ocurrir es que un atacante podría ser capaz de adivinar la siguiente contraseña en la generación de contraseñas al azar.

PrestaShop ha ofrecido tanto a los archivos de origen y un módulo que puede arreglar las últimas ramas de cada versión de PrestaShop. Si está utilizando una versión que no es la última rama es posible que tenga problemas con la corrección.

PrestaShop, en general, es muy seguro, incluso con esta vulnerabilidad es todavía difícil de obtener acceso a su sitio. Haría falta de planificación y el conocimiento interno de su empresa. PrestaShop sólo ha tenido otras 2 vulnerabilidades reportadas bajo nivel en los últimos 3 años, así, que es muy excepcional para el software de comercio electrónico.

Seguridad en su tienda.

Usted puede tomar medidas activas para asegurar su tienda para asegurarse de que no ha sido hackeado o cualquiera de sus datos de cliente se vea comprometida. Uso de una buena política de seguridad es una columna vertebral del comercio electrónico, los clientes que están confiando con sus datos, tiene que ser un buen administrador con los datos que les confían. A continuación, se presentan algunos de los pasos que le recomendamos tomar para proteger su tienda.

- Cambie su contraseña de back office con frecuencia.
- Cambiar la ubicación de su oficina cada dos meses.
- Utilizar un archivo de htpassword añadir una capa adicional de seguridad.
- El uso de un .htaccess para permitir o denegar direcciones IP.
- En lugar de utilizar un disco de recordar contraseña, utilice una frase de ver este cómic para más detalles.
- Mantenga actualizado el software del servidor al día.
- Utilice sólo los plugins de fuentes de confianza.

A la luz de un problema de seguridad que hemos tenido conocimiento de, hoy estamos lanzando varias opciones para garantizar una tienda para nuestros usuarios y colaboradores:

- Las nuevas versiones de PrestaShop 1.4.x y 1.5.x. Versión 1.6.1.0 es seguro.
- Los archivos de revisión de las últimas versiones de cada rama - 1.4.11.0, 1.5.6.2 y 1.6.0.14.
- El módulo de revisión de seguridad, que se aplica por encima de los archivos de revisión de una manera mucho más fácil de usar.
- archivos Zip de los archivos modificados para los 1.4, 1.5, 1.6 y ramas.

¿Qué versiones están afectadas?

El problema de seguridad que se ha descubierto afecta a todas las versiones de PrestaShop, excepto la versión 1.6.1.0 y Cloud PrestaShop.

Por lo tanto, afecta a las ramas 1.4.x, 1.5.x, 1.6.x y hasta 1.6.0.14.

En resumen, si aún no ha actualizado a PrestaShop 1.6.1.0, lo más probable es que su tienda es vulnerable a este problema.

Temas y módulos no se ven afectados, ya que funciona tal cual una vez que haya instalado la revisión.

¿Cómo puedo arreglar mis tiendas de almacén / mis clientes?
Para aquellos que todavía no han actualizado a PrestaShop 1.6.1.0, estamos proporcionando varias maneras de solucionar el problema:

- Para las personas no técnicas, hemos creado el módulo de revisión de seguridad, que se aplicará la corrección para las últimas versiones de los 1.4, 1.5 y 1.6 ramas. Esto significa que se garantiza que funcione para PrestaShop 1.4.11.0, 1.5.6.2 y 1.6.0.14. El módulo funciona para las tres ramas: simplemente instalarlo y activarlo, y va a aplicar el parche.
- Para los técnicos, o aquellos para los que el módulo no puede aplicar el parche, se puede obtener un parche para las versiones más recientes de cada rama (1.4, 1.5, 1.6) en GitHub.

Al igual que el módulo, estos parches sólo funcionan con la última versión de cada rama, a saber 1.4.11.0, 1.5.6.2 y 1.6.0.14, y ningún otro - no sin cambios por su parte, de todos modos.

Si su tienda no está al tanto de la última rama (1.6), es altamente recomendable para actualizar a la última versión de la rama antes de aplicar el parche

Si no se puede actualizar, es a usted para adaptar el archivo de revisión de su situación específica.

- Además, puede descargar los archivos de ficheros actualizados para las ramas 1.4, 1.5 y 1.6. Contienen sólo los archivos que han sido modificados desde la última versión de cada rama. Haga clic aquí para ver los enlaces.

Si no ha realizado cambios en estos ficheros allí, que sólo puede reemplazar los archivos antiguos con los nuevos.

Desde la versión 1.6.1.0 contiene la corrección para la rama 1.6, no estamos lanzando una versión 1.6.0.15.

En efecto, el módulo se aplica a los parches para cada rama, que eran de diseño para trabajar en las versiones más recientes: 1.6.0.14, 1.5.6.2, 1.4.11.0. Por lo tanto, podría no funcionar para las versiones más antiguas. Si se encuentra en esta situación, hemos escrito una guía rápida sobre cómo aplicar el parche manualmente.

En cualquier caso, le sugerimos que siempre mantenga su tienda actualizado con la versión más reciente y segura de PrestaShop: a lo sumo, 1.6.1.0; en el peor, la última versión de 1.5 o 1.4 rama.

Para aquellos de ustedes que han muy personalizada los archivos principales, por favor, tomar todas las precauciones antes de instalar el módulo, antes de combinar los parches,

o antes de cargar los archivos modificados. Puede que tenga que adaptar el parche para su instalación específica.

Tenga en cuenta que el módulo no funcionará en todas las configuraciones de servidor de Windows, y algunos limitan configuraciones de Linux. En esos casos, es a usted para adaptar el parche en su configuración específica.

Yo uso una versión antigua de PrestaShop, ¿qué puedo hacer?
El módulo funciona para las versiones recientes de los 1.4, 1.5 y 1.6.0 ramas. Las versiones anteriores de estas ramas deben trabajar también, aunque los más antiguos podrían tener problemas.

El módulo no funcionará para PrestaShop 1.0, 1.1, 1.2 ni 1.3.

Si tiene una versión anterior de PrestaShop, nuestro mejor y más frecuente es el asesoramiento para modificar sus tiendas. Al menos debe estar en la versión 1.4 de PrestaShop, ya que las versiones anteriores no verán más actualizaciones - la rama 1.3, por ejemplo, no ha recibido ninguna actualización desde marzo de 2011, hace más de cuatro años.

Entendemos que algunos de ustedes podrían ser bloqueados en una versión tan antigua. A tal fin, hemos publicado recientemente un artículo listado de 4 maneras fáciles que cualquiera podría asegurar su tienda.

En resumen, las 4 formas de asegurar su tienda son:

- Manteniendo su tienda al día con la última versión, así como todos sus módulos.
- La protección de su carpeta de la oficina de vuelta con una contraseña de .htaccess.
- El uso de un nombre no regular para su carpeta de back office (es decir., Algo más único que / admin1234).
- El uso de contraseñas más complejas, o incluso frases de paso que son únicos para su tienda.

¿Cómo se descubrió el problema y se resolvió?
El problema fue descubierto por el consultor de seguridad Vicente Herbulot (@ us3r777), que en contacto con nosotros directamente en security@prestashop.com bajo el modelo de "una fuente responsable". Gracias Vicente!

El problema se solucionó por el equipo de seguridad de PrestaShop, con la ayuda de Vicente. El módulo fue creado por los desarrolladores del núcleo.

¿Qué es una fuente responsable?
Una fuente responsable (y privada) es una práctica habitual cuando alguien se encuentra con un problema de seguridad: antes de hacerlo público, el descubridor informa al equipo central al respecto, de modo que una solución puede ser preparado, y por lo tanto minimizar el daño potencial.

2.4.4.6 *Lugares donde utilizan la plataforma.*

Tipo de tienda.	Dirección Web
Headict	http://www.headict.com/
E-Golf Ball	http://www.egolf-balls.com/fr/
Zaabar	http://www.zaabar.com/fr/
Museo del Prado	http://www.tiendaprado.com/
Stickaz	http://www.stickaz.com/en/

Tabla 8: Lugares donde utilizan PrestaShop.

2.4.5 Tecnologías.

2.4.5.1 *MySql.*

Ilustración 78: MySql.

MySql es un sistema de gestión de bases de datos relacional (inglés RDBMS - Relational DataBase Management System) multi-hilo (multithread) y multiusuario, que usa el lenguaje SQL (Structured Query Language).

MySql se ha convertido muy popular gracias a su velocidad al ejecutar consultas y su apoyo de forma nativa por parte del lenguaje PHP (hasta la versión 4.X de este lengua-je ya que a partir de la versión 5 deja de estar lo), en la elaboración de aplicaciones web, en el entorno del software libre.

Se puede hacer uso de MySql en aplicaciones de todo tipo (web, de escritorio u otros) de forma libre y gratuita bajo las condiciones de la licencia GPL. Si se quiere integrar MySql como parte de un producto privativo es necesario adquirir una licencia de uso específica para este propósito.

2.4.5.2 *PHP.*

Ilustración 79: PHP.

(PHP Hypertext Pre-processor). Lenguaje de programación usado generalmente en la creación de contenidos para sitios web. Es un lenguaje interpretado especialmente usado para crear contenido dinámico web y aplicaciones para servidores, aunque también es posible crear aplicaciones gráficas utilizando la biblioteca GTK+.

Generalmente los scripts en PHP se embeben en otros códigos como HTML, ampliando las posibilidades del diseñador de páginas web enormemente.

La interpretación y ejecución de los scripts PHP se hacen en el servidor, el cliente (un navegador que pide una página web) sólo recibe el resultado de la ejecución y jamás ve el código PHP.

Permite la conexión a todo tipo de servidores de base de datos como MySql, Postgres, Oracle, ODBC, DB2, Microsoft SQL Server, Firebird y SQLite.

PHP es una alternativa a otros sistemas como el ASP.NET/C#/VB.NET de Microsoft o a ColdFusion de Macromedia, a JSP/Java de Sun Microsystems, y a CGI/Perl.

2.4.5.3 *HTML.*

Ilustración 80: HTML.

HTML, siglas de HyperText Markup Language («lenguaje de marcas de hipertexto»), hace referencia al lenguaje de marcado para la elaboración de páginas web. Es un estándar que sirve de referencia del software que conecta con la elaboración de páginas web en sus diferentes versiones, define una estructura básica y un código (denominado código HTML)

para la definición de contenido de una página web, como texto, imágenes, videos, juegos entre otros. Es un estándar a cargo de la W3C, organización dedicada a la estandarización de casi todas las tecnologías ligadas a la web, sobre todo en lo referente a su escritura e interpretación. Se considera el lenguaje web más importante siendo su invención crucial en la aparición, desarrollo y expansión de la World Wide Web. Es el estándar que se ha impuesto en la visualización de páginas web y es el que todos los navegadores actuales han adoptado.

El lenguaje HTML basa su filosofía de desarrollo en la diferenciación. Para añadir un elemento externo a la página (imagen, vídeo, script, entre otros.), este no se incrusta directamente en el código de la página, sino que se hace una referencia a la ubicación de dicho elemento mediante texto. De este modo, la página web contiene sólo texto mientras que recae en el navegador web (interpretador del código) la tarea de unir todos los elementos y visualizar la página final. Al ser un estándar, HTML busca ser un lenguaje que permita que cualquier página web escrita en una determinada versión, pueda ser interpretada de la misma forma (estándar) por cualquier navegador web actualizado.

Sin embargo, a lo largo de sus diferentes versiones, se han incorporado y suprimido diversas características, con el fin de hacerlo más eficiente y facilitar el desarrollo de páginas web compatibles con distintos navegadores y plataformas (PC de escritorio, portátiles, teléfonos inteligentes, tabletas, vipers etc. No obstante, para interpretar correctamente una nueva versión de HTML, los desarrolladores de navegadores web deben incorporar estos cambios y el usuario debe ser capaz de usar la nueva versión del navegador con los cambios incorporados. Normalmente los cambios son aplicados mediante parches de actualización automática (Firefox, Chrome) u ofreciendo una nueva versión del navegador con todos los cambios incorporados, en un sitio web de descarga oficial (Internet Explorer). Por lo que un navegador desactualizado no será capaz de interpretar correctamente una página web escrita en una versión de HTML superior a la que pueda interpretar, lo que obliga muchas veces a los desarrolladores a aplicar técnicas y cambios que permitan corregir problemas de visualización e incluso de interpretación de código HTML. Así mismo, las páginas escritas en una versión anterior de HTML deberían ser actualizadas o reescritas, lo que no siempre se cumple. Es por ello que ciertos navegadores aún mantienen la capacidad de interpretar páginas web de versiones HTML anteriores. Por estas razones, aún existen diferencias entre distintos navegadores y versiones al interpretar una misma página web.

2.4.5.4 *CSS.*

Ilustración 81: CSS.

Hoja de estilo en cascada o CSS (siglas en inglés de cascading style sheets) es un lenguaje usado para definir y crear la presentación de un documento estructurado escrito en HTML o XML2 (y por extensión en XHTML). El World Wide Web Consortium (W3C) es el encargado de formular la especificación de las hojas de estilo que servirán de estándar para los agentes de usuario o navegadores.

La idea que se encuentra detrás del desarrollo de CSS es separar la estructura de un documento de su presentación.

La información de estilo puede ser definida en un documento separado o en el mismo documento HTML. En este último caso podrían definirse estilos generales con el elemento «style» o en cada etiqueta particular mediante el atributo «style».

2.4.5.5 *Java Script.*

Ilustración 82: JavaScript.

Java Script nos permite realizar multitud de efectos sobre una página web, es un lenguaje de programación que se ejecuta en el cliente, y entre otras cosas es el encargado de validar en el cliente los datos, realizar efectos visuales en las páginas web, realizar cambios en la página web a través del DOM, o iteraciones con el servidor utilizando AJAX, por ejemplo.

Java Script posee innumerables Framework para facilitarnos el desarrollo de aplicaciones. Estas librerías nos facilitan enormemente el uso de efectos visuales, validación de formularios, etc.

2.4.5.6 *JQuery.*

Ilustración 83: JQuery.

JQuery es una biblioteca basada en Java Script, que fue realizada por John Resiga, nos permite simplificar la manera de interactuar con los documentos HTML, simplificando al máximo los cambios que podemos realizar en el DOM a través de Java Script.

Este Framework nos facilita enormemente el desarrollo de efectos visuales en las páginas web, es de los más utilizados y muchas páginas que visitamos actualmente utilizan este Framework.

2.4.5.7 *Crossdomain.xml.*

Ilustración 84: Crossdomain.xml.

Flash Player entre sus políticas de seguridad no permite acceder a datos de cualquier dominio que no sea en donde está alojado el archivo flash. Es decir, si tengo mi archivo flash en el dominio dominio1.com y está tratando de cargar un archivo del dominio2.com, Flash player no permitirá cargar este archivo a no ser que se tenga permisos sobre este archivo.

Crossdomain.xml permite definir qué dominios o Ip pueden acceder al contenido que tenemos alojados. Cuando Flash player va a cargar un archivo que pertenece a otro dominio lo primero que hace es intentar cargar crossdomain.xml para verificar si se tiene permiso para acceder a esta información.

2.4.5.8 *JSON.*

Ilustración 85: JSON.

JSON, acrónimo de JavaScript Object Notation, es un formato ligero para el intercambio de datos. JSON es un subconjunto de la notación literal de objetos de JavaScript que no requiere el uso de XML.

La simplicidad de JSON ha dado lugar a la generalización de su uso, especialmente como alternativa a XML en AJAX. Una de las supuestas ventajas de JSON sobre XML como formato de intercambio de datos en este contexto es que es mucho más sencillo escribir un analizador sintáctico (parser) de JSON. En JavaScript, un texto JSON se puede analizar fácilmente usando la función eval (), lo cual ha sido fundamental para que JSON haya sido aceptado por parte de la comunidad de desarrolladores AJAX, debido a la ubicuidad de JavaScript en casi cualquier navegador web.

En la práctica, los argumentos a favor de la facilidad de desarrollo de analizadores o del rendimiento de los mismos son poco relevantes, debido a las cuestiones de seguridad que plantea el uso de eval () y el auge del procesamiento nativo de XML incorporado en los navegadores modernos. Por esa razón, JSON se emplea habitualmente en entornos donde el tamaño del flujo de datos entre cliente y servidor es de vital importancia (de aquí su uso por Yahoo!, Google, etc., que atienden a millones de usuarios) cuando la fuente de datos es explícitamente de fiar y donde no es importante el no disponer de procesamiento XSLT para manipular los datos en el cliente.

2.4.5.9 *.htcaccess.*

Ilustración 86: .htcaccess.

Un archivo .htaccess (hypertext access) o archivo de configuración distribuida es un archivo en formato ASCII cómo el que cualquiera puede crear con el bloc de notas, popularizado por el Servidor HTTP Apache, que es el más usado en el mundo cuando hablamos de servidores Web. Permite definir diferentes directivas de configuración para cada directorio (con sus respectivos subdirectorios) sin necesidad de editar el archivo de configuración principal de Apache.

Cuando hablamos de “directivas” nos referimos a la terminología que usa Apache para los comandos que se usan para los archivos de configuración.

Los archivos .htaccess son usados frecuentemente para especificar restricciones de seguridad para un directorio en particular, de aquí el sufijo “access “. Los servidores suelen usar el .htaccess para reescribir Url largas y complejas, en otras más simples y fácilmente recordables, permiten bloquear a usuarios por su dirección IP y/o dominio, bloquear bots y arañas web. También permite controlar las páginas de errores cuando estos ocurren del lado del servidor.

Gracias al .htaccess podemos controlar el comportamiento de nuestro sitios y aplicaciones Web para que estos sean un poco más seguros, hacer redirecciones, crear mensajes de error más personalizados, restringir el acceso a determinadas carpetas, evitar que se listen directorios específicos, etc.

El archivo .htaccess tiene muchas posibilidades, pero visto desde el punto de vista de la seguridad, mencionemos algunas opciones a la hora de configurarlo:

- Evitar que se liste el contenido de un directorio.
- Evitar el acceso de archivos y carpetas.
- Páginas de errores personalizadas.
- Evitar el hotlink.
- Bloquear a usuarios o a sitios.
- Obligar a que se use una conexión segura.

2.4.5.10 ***Ajax.***

Ilustración 87: Ajax.

AJAX, acrónimo de Asynchronous JavaScript And XML (JavaScript asíncrono y XML), es una técnica de desarrollo web para crear aplicaciones interactivas o RIA (Rich Internet Applications). Estas aplicaciones se ejecutan en el cliente, es decir, en el navegador de los usuarios mientras se mantiene la comunicación asíncrona con el servidor en segundo plano. De esta forma es posible realizar cambios sobre las páginas sin necesidad de recargarlas, mejorando la interactividad, velocidad y usabilidad en las aplicaciones.

Ajax es una tecnología asíncrona, en el sentido de que los datos adicionales se solicitan al servidor y se cargan en segundo plano sin interferir con la visualización ni el comportamiento de la página, aunque existe la posibilidad de configurar las peticiones como

síncronas de tal forma que la interactividad de la página se detiene hasta la espera de la respuesta por parte del servidor.

JavaScript es el lenguaje interpretado (scripting language) en el que normalmente se efectúan las funciones de llamada de Ajax mientras que el acceso a los datos se realiza mediante XMLHttpRequest, objeto disponible en los navegadores actuales. En cualquier caso, no es necesario que el contenido asíncrono esté formateado en XML.

Ajax es una técnica válida para múltiples plataformas y utilizable en muchos sistemas operativos y navegadores dados que está basado en estándares abiertos como JavaScript y Document Object Model (DOM).

2.4.6 Herramientas.

2.4.6.1 *Apache.*

Ilustración 88: Apache.

El servidor Apache es un servidor HTTP de código abierto para plataformas Unix, Windows, Macintosh, etc. que implementa el protocolo HTTP/1.1 y la noción de sitio virtual. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular NCSA HTTPD 1.3, pero más tarde fue reescrito por completo. El servidor Apa-che se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation. Ahora Apache presenta entre otras características mensajes de error altamente configurables, bases de datos de autenticación y negociado de contenido.

Apache tiene amplia aceptación en la red: desde 1996, Apache, es el servidor HTTP más usado. Alcanzó su máxima cuota de mercado en 2005 siendo el servidor emplea-do en el 70% de los sitios Web en el mundo, sin embargo, ha sufrido un descenso en su cuota de mercado en los últimos años.

2.4.7 Errores más comunes de las plataformas del comercio electrónico.

2.4.7.1 *Personalización gráfica.*

Una característica tan importante para una tienda como es su diseño gráfico no es algo que sea igual de fácil de personalizar en todas las tiendas. Si quieres una tienda que se pueda diseñar con rapidez, a un precio razonable y que no esto no produzca problemas técnicos, descarta Magento y escoge una tienda que cuente con un motor de plantillas como el que tiene PrestaShop u OpenCart, que se llama Smarty.

Smarty separa el diseño de los demás aspectos de la tienda, lo que hace que apenas existan restricciones técnicas a la hora de conseguir el diseño más atractivo y persuasivo.

2.4.7.2 *Posible crecimiento futuro de la tienda.*

O necesitas una tienda muy grande y compleja o no la necesitas, pero no lo hagas “por si acaso”.

Tu tienda tiene el tamaño que tiene, acéptalo y no le des vueltas a lo que pasará dentro de un año. Para entonces te habrán surgido 1000 problemas que ni te imaginabas y ya existirán nuevas soluciones de comercio electrónico y marketing online que ni siquiera se te han pasado por la cabeza todavía.

Haz lo que sea más económico ahora e invierte el resto en publicidad. Ojalá el problema sea que dentro de un año has crecido tanto que tienes que cambiar de tienda.

Además, con el coste adicional en tiempo y dinero que supone tener una tienda sobredimensionada, podrás contratar la última tecnología que exista entonces.

OpenCart es una solución excelente para tiendas con pocos productos y que requieren pocos cambios.

2.4.7.3 *Facilidad de gestión.*

Curiosamente nadie repara en valorar el tiempo necesario para aprender a gestionar y gestionar cada plataforma y sin embargo es uno de los mayores gastos, ya sea en tiempo o en dinero, en los que se tendrá que incurrir una vez que la tienda esté en funcionamiento.

De los ejemplos que nombro al inicio del artículo, OpenCart es el más fácil y rápido de aprender y de gestionar, seguido de PrestaShop y X-Cart, y Magento es el más difícil.

Si no se tienen conocimientos de bases de datos (MYSQL) es muy importante valorar las facilidades que las distintas plataformas ofrecen en cuanto a la importación y exportación masiva de productos.

En este caso X-Cart es el mejor, seguido de Magento, que es algo problemático. PrestaShop es muy bueno con la importación y regular con la exportación y OpenCart es el más limitado en ambos aspectos.

2.4.7.4 *Velocidad de funcionamiento y coste de alojamiento.*

No todas las plataformas de comercio electrónico son igual de eficientes en su funcionamiento. Para funcionar a una velocidad aceptable algunas plataformas necesitan un servidor de unas características técnicas superiores, y por tanto más caras.

OpenCart, por su sencillez, es el más ligero de todos y funciona bien incluso con el plan de alojamiento compartido más barato del mercado.

PrestaShop es algo más pesado, pero también funciona de manera muy aceptable en un servidor compartido, aunque conviene que sea algo mejor. En este aspecto X-Cart es similar a PrestaShop.

Y lo de Magento es un auténtico despropósito. La baja calidad del código con el que está programado y la pésima gestión de su base de datos hace necesaria la contratación de un servidor dedicado. Y aunque así vaya a funcionar rápido, hay que tener en cuenta que desde el punto de vista técnico Magento es una auténtica chapuza.

2.4.7.5 *Dependencia de tu agencia de desarrollo web.*

Existen empresas de desarrollo web que ofrecen su propia plataforma de comercio electrónico. Esto es lo que nunca jamás debes escoger.

Las plataformas que menciono en este artículo, y otras muchas, son software libre. Lo que significa que cualquiera puede utilizarlas, y por tanto tienen millones de usuarios en todo el mundo. Además, están soportadas por una gran comunidad de programadores en internet que las mejoran a diario.

Las soluciones propias de una agencia de desarrollo web, software propietario, son sólo utilizadas por sus clientes y no son universalmente conocidas. Esto significa que, si por cualquier motivo quieres cambiar de proveedor, lo más seguro es que no puedas hacerlo y tengas que rehacer la tienda desde cero.

Además, la contratación de estas plataformas suele ser en modo “de alquiler”, por lo que además de pagar una cuota mensual ni siquiera tienes derecho a utilizar la plataforma con otra empresa diferente.

Algo completamente diferente es el “desarrollo a medida”, es decir, cuando un equipo de programadores desarrolla una solución que se ajusta con exactitud a los requisitos del cliente. Esta es la solución ideal para tiendas grandes, para integración con CRMs o ERPs y en los casos en los que se desean muchas funcionalidades distintas de las habituales de una tienda online típica.

2.4.7.6 *Configuración regional.*

Gastos de envío, idiomas, métodos de pago e impuestos, pese a que pueda parecer básico, no es algo a lo que todas las plataformas de comercio electrónico den una buena solución. Además, en España tenemos una peculiaridad no prevista por muchas tiendas online, y es que tenemos dos tipos de IVA en un mismo país.

PrestaShop es el que ofrece la configuración regional más flexible y completa, X-Cart y Magento dan una respuesta aceptable y OpenCart se queda algo corto en la gestión de distintos IVA dentro de un mismo país.

2.4.8 Tabla comparativa.

	OpenCart	Magento	OsCommerce	PrestaShop
Complejidad de instalación.	✓	✓	×	✓
Problemas de actualización.	✓	✓	✓	×
Requerimientos del sistema.	✓	×	✓	✓
Simplicidad.	✓	×	✓	×
Módulos preinstalados.	✓	×	×	×
Interfaz gráfica.	✓	✓	×	✓
Popularidad de uso.	✓	✓	×	✓
Velocidad en el acceso.	✓	×	✓	✓
Open Source (Código Abierto).	✓	✓	✓	✓
Documentación.	✓	✓	✓	×
Categorías Ilimitadas.	✓	✓	✓	✓
Productos Ilimitados.	✓	✓	✓	✓
Fabricantes Ilimitados.	✓	✓	✓	✓
Templates Intercambiables.	✓	✓	×	✓
Multi Lenguaje.	✓	✓	✓	✓
Multi Monedas.	✓	✓	✓	✓
Comentarios en Productos.	✓	✓	✓	×
Valoración de Productos.	✓	✓	✓	×
Descarga de Productos.	✓	✓	✓	×
Auto Redimensionado de Imágenes.	✓	✓	×	✓
Múltiples Tipos de Impuestos.	✓	✓	✓	✓
Productos Relacionados.	✓	✓	×	×
Páginas de Información Ilimitadas.	✓	✓	✓	✓
Cálculo de Peso de Envío.	✓	✓	✓	✓
Sistema de Cupones de Descuento.	✓	✓	×	✓

Optimización Motores de Búsqueda.	✓	✓	✗	✓
Sistema de Módulos.	✓	✓	✓	✓
Copia/Restauración Base de Datos.	✓	✓	✓	✓
Impresión de Facturas.	✓	✓	✓	✓
Reportes de Ventas.	✓	✓	✓	✓

Tabla 9: Tabla comparativa.

2.5 Aspectos legales.

El comercio electrónico es un ámbito con muchas implicaciones jurídicas que conviene conocer y aplicar. Pero, además, es un ámbito en el que el Derecho siempre va por detrás, ante los continuos cambios en los modelos de negocio.

El crecimiento de un mercado electrónico global ha afectado a numerosos aspectos legales, incluyendo: seguridad en la red y las transacciones, protección de los derechos de propiedad intelectual y material con copyright en el entorno digital, la gestión de los sistemas de pago, la legalidad de los contratos electrónicos y diferentes aspectos de la jurisdicción en el ciberespacio.

1) Ley de Servicios de la Sociedad de la Información.

La norma de referencia es la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE).

Generación de Condiciones de Contratación y Condiciones de Uso. recomendación de inscripción en Registro de bienes muebles.

Ya no necesidad de Inscripción del nombre del dominio, art. 9 LSSI suprimido por Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

2) Contratación Electrónica.

Presenta varías particularidades por su propia naturaleza respecto a otros tipos de formalización de acuerdos. A continuación, se detallan los principales aspectos que regula la LSSI. La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetará a las reglas generales del ordenamiento jurídico.

Cuando los contratos celebrados por vía electrónica estén firmados electrónicamente se estará a lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Los terceros de confianza: Las partes podrán pactar que un tercero archive los contratos electrónicos y que consigne la fecha y la hora en que dichas comunicaciones han tenido lugar. La intervención de dichos terceros no podrá alterar ni sustituir las funciones que corresponde realizar a las personas facultadas con arreglo a Derecho para dar fe pública.

a. Obligaciones.

- **Obligaciones previas a la contratación:** el prestador de servicios de la sociedad de la información que realice actividades de contratación electrónica tendrá la obligación de poner a disposición del destinatario, antes de iniciar el procedimiento de contratación:
  - Los trámites que deben seguirse para celebrar el contrato.
  - Si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible.
  - Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos.
  - La lengua o lenguas en que podrá formalizarse el contrato.
- **Obligaciones posteriores a la contratación:** el oferente está obligado a confirmar la recepción de la aceptación al que la hizo por alguno de los siguientes medios:

- El envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la aceptación.
- La confirmación, por un medio equivalente al utilizado en el procedimiento de contratación, de la aceptación recibida, tan pronto como el aceptante haya completado dicho procedimiento, siempre que la confirmación pueda ser archivada por su destinatario.

3) Protección de Datos.

- **Dato personal:** Cualquier información que permita identificar o hacer identificable a una persona. Por ejemplo: la imagen de una persona, una huella dactilar, el número de cuenta corriente…
- **Normativa de referencia:**
  - Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.
  - Real Decreto de 19 de enero de 2008 por el que se aprueba el Reglamento de Desarrollo de la LOPD.
  - Nuevo régimen de sanciones en la Ley de Economía Sostenible.
- **Organismo supervisor:** AGPD.
  - Es importante destacar el papel de la Agencia Española de Protección de Datos como centro de consulta de la legislación actual vigente, posibles sanciones a las que nos podemos encontrar, guías de ayuda, etc.

a. Implicaciones prácticas Protección de Datos: Pasos a seguir:

- **Obtención del consentimiento.**
  - LOPD art. 5 reconoce a toda persona el derecho a saber por qué, para qué y cómo van a ser tratados sus datos personales y decidir acerca de su uso. Quien recoge datos personales debe informar de modo muy claro y comprensible sobre:
    - Su identidad y dirección.
    - La existencia de un fichero o tratamiento en el que incluirán los datos.
    - La finalidad para la cual los necesita o requiere.
    - Si los van a facilitar con posterioridad a un tercero.
    - Cómo ejercitar los derechos de acceso y rectificación, cancelación y oposición (ARCO).
- **Inscripción del Fichero en AGPD:**
  - Procedimiento de inscripción y notificación de ficheros en la Agencia Española de Protección de Datos. Formulario NOTA.
  - **Modalidades de presentación:** presencial, envío por Internet mediante firma física, envío por Internet mediante certificado digital.
  - Descripción de los ficheros, tipo de tratamiento realizado, datos recabados, etcétera. Importancia de su cumplimiento: riesgo de sanciones.

- **Establecimiento de Medidas de Seguridad:**
  - Implementación de medidas de seguridad establecidas en LOP D y Reglamento.
  - Importante: generación del Documento de Seguridad. Existen tres niveles de seguridad, en función de los tipos de datos tratados:
    - Nivel Básico.
    - Nivel Medio.
    - Nivel Alto.
  - Son tres niveles acumulativos.
- **Acceso a datos por cuenta de terceros. Habrá que diferenciar:**
  - Cesión de datos a terceros: identificación / consentimiento.
  - Encargo de tratamiento de datos, art. 12.
    - Celebración de contrato de encargo de tratamiento.

Ejemplo de Cláusulas tipo Protección de Datos.

Le informamos que los datos personales que voluntariamente nos facilite, serán incorporados a un fichero titularidad de XXX, con CIF XXX, y domicilio en XXX. La finalidad del fichero es gestionar adecuadamente su relación comercial con XXX. Puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición por carta, adjuntando fotocopia de su DNI, dirigida a:

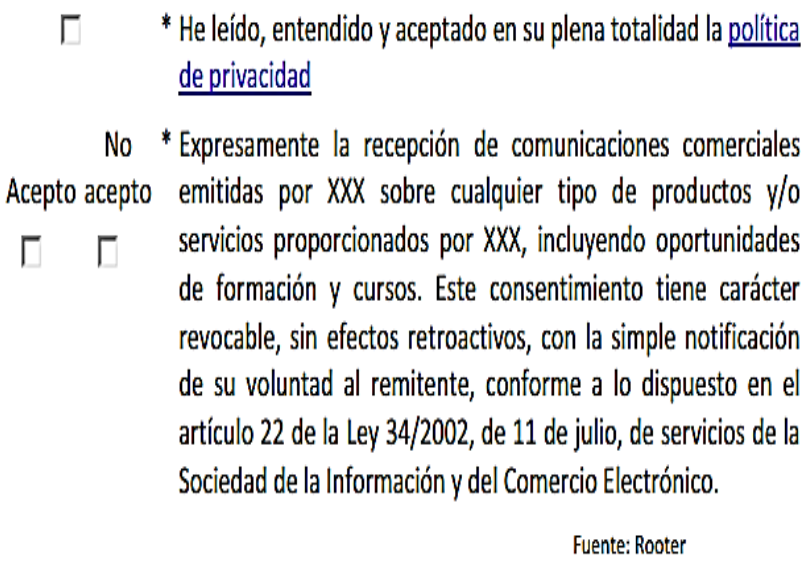
A. CONTENIDO DEL AVISO EN MATERIA DE PROTECCIÓN DE DATOS

7º. Protección de Datos de Carácter Personal

Esta cláusula será aplicable a todos los tratamientos de datos realizados a través de la web www.dia.es, excepto a aquellos producidos en la parte relativa al Club Dia, que se inicia en http://www.dia.es/webdia/login.html, que se regirán por la Política de privacidad definida específicamente para esa área de la web.

En cumplimiento de lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, DIA% le informa de que, los datos facilitados por el Usuario, a través de los distintos formularios incorporados en el portal dia.es, serán tratados en los ficheros propiedad de DIA%, que, a los efectos legales oportunos, se identifica como responsable de los mismos.

Ilustración 89: Ejemplo de clausula tipo de protección de datos.



☐ * He leído, entendido y aceptado en su plena totalidad la política de privacidad

No Acepto ☐ | acepto ☐ * Expresamente la recepción de comunicaciones comerciales emitidas por XXX sobre cualquier tipo de productos y/o servicios proporcionados por XXX, incluyendo oportunidades de formación y cursos. Este consentimiento tiene carácter revocable, sin efectos retroactivos, con la simple notificación de su voluntad al remitente, conforme a lo dispuesto en el artículo 22 de la Ley 34/2002, de 11 de julio, de servicios de la Sociedad de la Información y del Comercio Electrónico.

Fuente: Rooter

Ilustración 90: Ejemplo de modelo de aceptación.

4) Defensa de los consumidores.

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

Los consumidores tienen derecho a recibir información correcta, objetiva, cierta, eficaz, comprensible y suficiente de los productos, bienes y servicios puestos a su disposición.

Antes de la compra de un producto o de la contratación de un servicio, el consumidor tiene:

- Derecho a un presupuesto previo.
- Derecho a que se utilicen métodos de venta autorizados.
- Derecho a que se prohíba edición y difusión de publicidad ilícita.
- Derecho a que se prohíba la fabricación y venta de productos inseguros.

En el momento en que se compra un producto o se contrata un servicio, el consumidor tiene:

- Derecho a recibir copia del contrato.
- Derecho a recibir factura de la compra.
- Derecho a que se expongan o queden claros los precios y tarifas.
- Derecho a que se midan y comprueben con exactitud las cantidades compradas.

Después de comprar un producto o de contratar un servicio, el consumidor tiene:

- Derecho a recibir los documentos de garantía y los manuales de instrucciones en los bienes de naturaleza duradera.
- Derecho a disponer de servicios técnicos para los supuestos de avería.
- Derecho a disponer de hojas de reclamaciones.

En relación a la publicidad, habrá que tener en consideración lo dispuesto en la Ley 34/1988, de 11 de noviembre, General de Publicidad, aplicable a cualquier producto o servicio puesto a disposición de los consumidores. Además, sectores como la alimentación deben cumplir con una normativa propia. Por ejemplo:

- Real Decreto 1334/1999, de 31 de julio, por el que se aprueba la norma general de etiquetado, presentación y publicidad de los productos alimenticios.
- Real Decreto 1414/2005, de 25 de noviembre, por el que se regula el procedimiento para la tramitación de las solicitudes de inscripción en el Registro comunitario de las denominaciones de origen protegidas y de las indicaciones geográficas protegidas, y la oposición a ellas.
- Real Decreto 1801/2003, de 26 de diciembre, sobre seguridad general de los productos.

a. Defensa de los consumidores y envío de comunicaciones comerciales.

Ley 44/2006, de 29 de diciembre, de Mejora de la protección de los consumidores y usuarios.

- **Art. 94 regula las comunicaciones comerciales y la contratación electrónica.** En las comunicaciones comerciales por correo electrónico u otros medios de comunicación electrónica y en la contratación a distancia de bienes o servicios por medios electrónicos, se aplicará además de lo dispuesto en este título, la normativa específica sobre servicios de la sociedad de la información y comercio electrónico. Cuando lo dispuesto en este título entre en contradicción con el contenido de la normativa específica sobre servicios de la sociedad de la información y comercio electrónico, ésta será de aplicación preferente.

- **Artículo 96 regula las comunicaciones comerciales:**
  - En todas las comunicaciones comerciales deberá constar inequívocamente su carácter comercial.
  - En el caso de comunicaciones telefónicas, deberá precisarse explícita y claramente, al principio de cualquier conversación con el consumidor y usuario, la identidad del empresario y la finalidad comercial de la llamada.
  - La utilización por parte del empresario de las técnicas de comunicación que consistan en un sistema automatizado de llamada sin intervención humana o el telefax necesitará el consentimiento expreso previo del consumidor y usuario.
  - En todo caso, deberán cumplirse las disposiciones vigentes sobre protección de los menores y respeto a la intimidad. Cuando se utilicen datos personales procedentes de fuentes accesibles al público para la realización de comunicaciones comerciales, se proporcionará al destinatario la información que señala la Ley Orgánica de Protección de Datos de Carácter Personal, y se ofrecerá al destinatario la oportunidad de oponerse a la recepción de las mismas.

5) **Envío de Comunicaciones Comerciales.**
   - **Art. 20 LSSI establece requisitos:**
     - Comunicaciones comerciales y remitente claramente identificables.
     - Si se realiza por correo electrónico incluirá la palabra “Publicidad” o “Publi”.
     - En caso de ofertas promocionales que incluyan descuentos o premios deberá: solicitar autorización organismo competente, identificación de la normativa de aplicación, condiciones de acceso y participación fácilmente accesibles y expresadas de forma clara e inequívoca.
   - **Art. 21 regula las condiciones de envío:**
     - Prohibido el envío que previamente no hubiera sido solicitado o autorizado expresamente por los usuarios. Es necesario contar con el consentimiento informado, concretando; responsable del fichero, finalidades concretas del tratamiento, posibilidad de ejercicio ARCO, etc.
     - Otro de los aspectos a tener en cuenta es la inclusión de las direcciones en el campo de copia oculta. Deber de secreto establecido en el art. 10 de la LOPD. Obligación de no poner a disposición de terceros los datos de los destinatarios de las comunicaciones, bien con la utilización de listas, o bien incluyendo dichos datos en el campo “Copia Oculta” (CCO o BBC) disponible en todos los gestores de correo electrónico. Consecuencia del incumplimiento, posibles sanciones de la AGPD (2000 €).

6) **Propiedad Intelectual.**

La Propiedad Intelectual en nuestro ordenamiento hace referencia al derecho de autor.

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

Implica:

- Cómo gestionar mis propios contenidos.
- Cómo gestionar contenidos titularidad de terceros.

Importante: no se protegen las ideas, sino la plasmación de esas ideas.

Protección por la mera creación, no requiere registro.

a. Gestión de Contenidos Propios.

Las empresas deberán velar por el cumplimiento de lo dispuesto en la Ley de Propiedad Intelectual.

Deberán formalizar contratos de cesión de derechos con los trabajadores.

Si bien es cierto que, en el ámbito laboral, se presumen la cesión de derechos al empleador.

b. Gestión de contenidos de terceros.

Páginas web incorporan contenidos tales como:

- obras literarias.
- obras musicales
- obras fotográficas
- etcétera.

Para poder utilizar todos estos contenidos, se deberá recabar la autorización de todos de los titulares de derechos. Por ejemplo: bancos de imágenes…O vía entidades de gestión - SGAE, CEDRO, VEGAP…

Así mismo, se deberá realizar una adecuada gestión de todos estos contenidos, procurando una rápida retirada de todos aquellos contenidos que estén infringiendo derechos de autor.

7) Propiedad Industrial.

Varios tipos de derechos, cada uno con una legislación aplicable:

- Diseños industriales: protegen la apariencia externa de los productos
- Marcas y Nombres Comerciales (Signos Distintivos): protegen combinaciones gráficas y/o denominativas que ayudan a distinguir en el mercado unos productos o servicios de otros similares ofertados por otros agentes económicos.
- Patentes y modelos de utilidad: protegen invenciones consistentes en productos y procedimientos susceptibles de reproducción y reiteración con fines industriales.

Se otorgan mediante un procedimiento por el organismo competente (OEPM; OAMI).

Además, conviene realizar un adecuado registro del “NOMBRE DE DOMINIO”, para evitar posibles usurpaciones de terceros.

8) Términos y Condiciones.

Los “Términos y Condiciones” recogen las cuestiones básicas que las diferentes normas vistas (LSSI, LOPD, etc.) obligan a incluir en toda web.

Estructura propuesta:

- Aviso Legal o Condiciones Generales de Uso.
- Eventualmente, Condiciones Particulares (asociadas al registro de usuarios).
- Política de Privacidad y Protección de Datos Personales.
- Política de Copyright (en casos de especial relevancia, se sugiere desligarlo del Aviso Legal).

2.6 Extensiones del comercio electrónico.

2.6.1 M-Commerce o comercio móvil.

Ilustración 91: M-Commerce.

El término E-Commerce denota los procesos de negocio sobre la Internet, tal como la compra y venta de bienes que pueden ser B2B (negocio a negocio) o B2C (negocio a consumidor**)**.

En esta definición no se determina el tipo de dispositivo: móvil o fijo, o el medio de acceso a Internet: alámbrico o inalámbrico. M-Commerce por su parte es todo acerca del comercio electrónico inalámbrico, esto es, donde los dispositivos móviles son usados para hacer negocios por internet. Como tal M-Commerce es un subconjunto de E-Commerce.

Varias definiciones de M-Commerce son presentadas**,** entre ellas tenemos:

- Aplicación de las redes y dispositivos de comunicaciones inalámbricas a la ejecución de transacciones con valores monetarios de forma directa o indirecta.
- La eficiente entrega de las capacidades del comercio electrónico en las manos del consumidor en cualquier lugar y en cualquier tiempo, vía tecnología inalámbrica.
- Uso de los dispositivos móviles para transacciones de negocios realizadas sobre una red de telecomunicaciones móviles, posiblemente envolviendo la transferencia de valores monetarios.
- Transacción electrónica o interacción de información, llevada a cabo en dispositivos móviles y redes móviles, lo que conduce a la transferencia de valores reales o percibidos a cambio de información, bienes o servicios.
- Alguna transacción con un valor monetario que es conducido vía una red de telecomunicaciones móvil.

En todas ellas se puede establecer como elemento común el empleo de un terminal o dispositivo móvil para comunicarse a través de una red de comunicaciones móvil; y cuyo objetivo de esta comunicación se define en algunos casos como el desarrollo de transacciones que envuelven valores monetarios de manera directa o indirecta, y en otras generaliza el término a servicios que conllevan comunicación, información, transacción y entretenimiento.

El uso de estos dispositivos móviles hace que el usuario pueda acceder a las aplicaciones de M-Commerce en cualquier lugar y tiempo, dándole una accesibilidad total al usuario, esto se presenta como una de las mayores ventajas de M-Commerce con respecto a aplicaciones que envuelven un dispositivo de acceso cableado.

Sin embargo, aún se presentan algunas limitaciones por superar como las capacidades que ofrecen los dispositivos móviles; la heterogeneidad tanto en equipos como en sistemas

operativos y tecnologías de red utilizadas; la necesidad de una mayor seguridad en la transmisión de los datos debido a la característica misma del acceso inalámbrico, entre otras.

A pesar de estas limitaciones, la rápida proliferación de dispositivos como: teléfonos móviles, asistentes digitales personales (PDA), entre otros dispositivos, ha permitido que el comercio móvil sea considerado como la nueva forma de comercio electrónico.

Existe una gran cantidad de aplicaciones desarrolladas y potenciales aplicaciones del comercio móvil, lo que dificulta en gran medida la clasificación de las mismas, una de esas clasificaciones es enfocada en los servicios a prestar, es la que se nos presenta y que divide a estas aplicaciones en cuatro categorías principales: servicios de comunicación móvil, servicios de información móvil, servicios de transacciones móvil y servicios de interacción móvil.

En cambio, se clasifica las aplicaciones en: manejo de inventarios móviles, localización de productos, manejo de servicios proactivos, acción móvil, entretenimiento y otros.

Se presentan las siguientes categorías de aplicaciones: comercio, educación, planificación de los recursos de la empresa, entretenimiento, manejo y despacho de inventarios, tráfico, manejo de viajes.

Esto nos muestra el potencial que tienen el comercio móvil y las múltiples aplicaciones que se han desarrollado o se pueden desarrollar en una sociedad en donde la movilidad es una característica propia, y las redes y dispositivos móviles tienen un crecimiento acelerado tanto en tamaño como en capacidades de transferencia de datos y calidad de servicio.

2.6.1.1 *Ventajas y desventajas del M-Commerce.*

Ventajas:

- Acceso más sencillo a la gama de productos.
- Más rapidez en la compra.
- Acceso a productos específicos si accedes desde tu móvil.
- Acceso a ofertas especiales si accedes desde tu móvil.
- Posibilidad de introducir códigos BIDI en las campañas publicitarias.
- Podemos acceder a nuestras tiendas favoritas en cualquier momento y lugar.
- Aumentaremos la productividad y competitividad de nuestra empresa.
- No requiere un gran desarrollo, por lo que no necesitamos ser una gran empresa ya consolidada para lanzarlos a ello.
- Todo el proceso de compra se hace más sencillo.
- Mejorará nuestro posicionamiento en el mercado, tenemos un nuevo lugar para vender y mostrar nuestros productos literalmente a la mano de nuestro público.
- Se reducen costes.
- Conseguiremos más información de nuestros compradores gracias a diversas aplicaciones de recogida de datos como la geo localización.

Desventajas:

- No es aconsejable para productos que requieren una compra muy meditada o análisis conciso.
- Nuestro consumo de datos puede verse altamente disminuido y también puede que necesitamos una conexión excelente para poder realizar nuestras compras con éxito.
- Todavía hay cierta desconfianza incluso entre la gente joven para comprar desde nuestro móvil.
- La marca debe crear una versión web móvil amigable, sencilla, segura que haga la compra atractiva y genere confianza. Además, tendremos que tener en cuenta los sistemas operativos mayoritarios que se usan para ver cómo adaptamos nuestra versión móvil a cada uno de ellos de manera eficaz y exitosa.
- Los productos no podrán tener mucha explicación en cuanto a características, composición, etc., debido a que la carga de página sería muy lenta.
- Los días de entrega del producto todavía varían en muchas ocasiones dependiendo desde qué dispositivo se haga la compra.

2.6.1.2 *Retos para el desarrollo de M-Commerce*

Mientras los dispositivos móviles han sido adoptados ampliamente, el crecimiento del comercio móvil ha sido limitado debido a diferentes factores, muchos de ellos centrados alrededor de la tecnología y la seguridad de las transacciones.

Nos presenta las siguientes limitaciones:

- **Limitaciones de los dispositivos.** En comparación con las computadoras de escritorio, los dispositivos inalámbricos como los PDAs y teléfonos móviles tienen generalmente características limitadas de potencia de procesamiento, memoria y tiempo de vida de las baterías, lo cual, junto con características de diseño como pequeñas pantallas de visualización y mecanismos simples de entrada, garantizan que los diseñadores de aplicaciones se enfrenten a enormes retos en el diseño alrededor de esas limitaciones.
- **Tecnología.** Las cuestiones tecnológicas que enfrenta la industria inalámbrica se refieren a los dispositivos móviles (requisitos de los protocolos) y la infraestructura de comunicación (optimización y eficiencia del ancho de banda, interfaces de comunicación, interferencia de las tecnologías de comunicación actuales y las futuras y costo de la infraestructura).
- **Seguridad.** Las limitaciones de los dispositivos, junto con las diferentes configuraciones de red significan que las tecnologías inalámbricas presentan un mayor riesgo de escuchas ilegales y piratas informáticos. Uno de los mayores problemas por resolver por la industria es los temas de seguridad.

- **Fiabilidad y utilidad de las aplicaciones.** Cuestiones sociales como la aceptación de los dispositivos móviles y culturales ajustadas a las aplicaciones inalámbricas son consideraciones primordiales para los mercados inalámbricos. De particular interés es la compatibilidad de las aplicaciones con el estilo de vida del usuario, puesto que tiene un significativo efecto sobre la intención de uso más que el costo.

Superar estas limitaciones es un reto importante para lograr el éxito del comercio móvil. La característica inalámbrica del medio de acceso del usuario plantea una serie de retos adicionales al comercio móvil con respecto al tradicional comercio electrónico, entre estos podemos establecer los de: estandarización, regulación, seguridad y autentificación y los sistemas de pago móvil.

La seguridad en el comercio móvil es definida como los procedimientos tecnológicos y de gestión aplicados al comercio móvil para proveer las siguientes propiedades a la información y sistemas del comercio móvil: confidencialidad, autentificación, integridad, autorización, disponibilidad y no repudiación.

2.6.1.3 *Formas de M-Commerce.*

Es este un campo de muy reciente nacimiento en lo que a explotación comercial ser refiere, que está en constante cambio y actualización. Esto, que puede parecer una desventaja, nos ofrece por el contrario una oportunidad, ya que no existen parámetros prefijados sobre lo que se puede o no se puede hacer en la explotación comercial de esta funcionalidad, permitiéndonos ser mucho más creativos a la hora de aportar nuevas ideas.

Hasta la fecha, existen diversas formas de explotación y uso del M-Commerce, algunas más conocidas que otras, que, de forma resumida, son las siguientes:

- **Comercio electrónico:** Entradas de espectáculos, venta de productos, reservas de hoteles y restaurantes, etc.
- **Códigos QR:** Son imágenes bidimensionales que componen un código de almacenamiento de información de respuesta rápida (las siglas QR corresponden al término anglosajón Quick Response, o respuesta rápida). Originados en 1994 por la compañía Denso Wave (parte de Toyota) como una forma de almacenamiento de información en una matriz de puntos, se comenzaron a usar para ubicar referencias en almacenes logísticos, pasando con el tiempo a usos comerciales. Su principal característica es que son de código abierto, es decir, de uso libre tanto en su creación como en su lectura por parte de empresas y usuarios.
- **Códigos BiDi:** Un tipo de código QR, cuya principal diferencia, más allá de la técnica, es que son de código propietario, es decir, cerrado. Su uso, promovido en España por los principales operadores de telefonía móvil, supone un pago por parte de las empresas anunciantes a dicho operador, y, en caso de remitir a un enlace de una información en la red, el correspondiente coste de tarifa de datos del dispositivo móvil que realice la lectura del mismo.
- **Geolocalización:** Localización de personas en tiempo real, callejeros interactivos y guías de ciudades, localización de tiendas cercanas, localizar las flotas, distribuir operarios en un área y conocer en todo momento su lugar exacto, enviar un mensaje

a los amigos que estén en una zona concreta, estado del tráfico en tiempo real, etc., aprovechando el posicionamiento por GPS del terminal móvil del usuario.

- **Realidad aumentada:** en gran medida ligada con la geolocalización y con el uso de códigos QR (aunque no necesariamente), nos permite mostrar objetos virtuales, tales como representaciones 360º de un producto, carteles publicitarios de una marca, objetos 3D, etc., en la visualización de un entorno real a través de la cámara de nuestro dispositivo móvil.
- **Juegos.**
- **Etc.**

2.6.1.4 *Principales Dispositivos para el M-Commerce.*

En la actualidad el mercado de dispositivos móviles está copado por dos grandes sistemas operativos, que se incluyen, en diferentes versiones, en la mayor parte de los Smartphone y dispositivos móviles. No son los únicos, pero la tendencia del mercado, o al menos su aceptación es clara.

Esto, para el desarrollo de aplicaciones y soluciones de M-Commerce, es una ventaja, ya que nos permite centrarnos, si así lo decidimos, en las principales plataformas a la hora de invertir recursos de desarrollo en las mismas. Ambos Sistemas Operativos (OS) requieren al desarrollador el envío de sus Apps para previa aprobación e integración en los llamados Marketplace o Repositorios de Aplicaciones. A continuación, analizaremos brevemente los mencionados sistemas:

A) Android: Sistema operativo para dispositivos móviles propiedad de Google, basado en código abierto (Linux), y, por tanto, modificable por las comunidades de desarrolladores de forma sencilla. Su repositorio es “Google Play”. Este sistema está presente tanto en los dispositivos móviles de fabricación propia de Google (HTC), como en dispositivos de terceras marcas, lo cual ha favorecido su penetración en el mercado. Si bien, las diferentes versiones que coexisten, así como las políticas de actualización de los operadores, han hecho en ocasiones poco controlable la calidad del sistema por parte de Google.

B) iOS: Sistema operativo de Apple, de estructura cerrada (sistema propietario), y que únicamente está presente en los dispositivos móviles de la propia compañía (iPhone, iPad, etc.). Líder indiscutible hasta la llegada de Android, mantiene claras diferencias de valoración por parte de los compradores a iguales características técnicas, ya que su éxito radica en la calidad exigida para las Apps a incluir en su Marketplace, así como en la claridad y facilidad de su uso por parte de los usuarios. Los requisitos de entrada de una APP para su tienda de Apps (App Store) son muy estrictos y con duras condiciones económicas.

C) Otros:
   a. Windows Mobile. Sistema de la compañía líder en sistemas operativos para PC, sus versiones anteriores han tenido problemas de estabilidad y usabilidad que aparentemente se han solucionado con su último reléase.

b. BlackBerry: Propiedad de la compañía del mismo nombre, que basa su éxito en la especialización de uso profesional de sus dispositivos. Su repositorio es el BlackBerry App World.
c. Symbian: Sistema operativo de Nokia (con aportaciones de otros fabricantes en el pasado), en claro desuso por haberse superado por la competencia, llegando incluso Nokia a aliarse con Windows para la implantación del OS de éste en sus Smartphone. Tiene recorrido en mercados emergentes por la facilidad de distribución de dispositivos de bajo coste en los mismos.

2.6.1.5 *Aplicaciones M-Commerce.*

Para las empresas grandes y pequeñas que desean no solo mantenerse a flote, sino también prosperar en el segmento del comercio electrónico, las aplicaciones móviles M-Commerce son sin duda la clave para alcanzar el éxito. Hay muchos ejemplos que podemos mencionar, sin embargo, a continuación, les hablamos de las más exitosas.

Red box: La aplicación móvil E-Commerce de Red box está disponible tanto para Android como para iPhone; se trata de una aplicación que le permite al usuario navegar a través de una base de datos de películas antes de realizar su compra en la tienda física. De esta manera los clientes reducen el tiempo de espera y eso se traduce en una mayor satisfacción.

Best Buy: La App de Best Buy también es un gran ejemplo de aplicaciones móviles E-Commerce exitosas que ofrece grandes beneficios a los clientes. De entrada, la aplicación integra una función para el escaneo de códigos QR de los productos, acceso a los comentarios de los clientes, además de investigar, seleccionar y comprar desde la propia tienda online.

Amazon Student: Los estudiantes universitarios representan un grupo demográfico considerable de personas que usan Smartphone que con esta aplicación ellos pueden explorar libros de texto para comparar precios antes de comprarlos. Incluso les permite cambiar una tarjeta de regalo en Amazon.

Zong: Esta aplicación E-Commerce está disponible para móviles Android y básicamente se trata de una plataforma de compras destinada a las redes sociales. Los usuarios pueden comprar créditos de los más recientes juegos móviles simplemente con introducir su número de teléfono, incluso se pueden realizar transacciones a la factura mensual del móvil.

Yelp: Otro claro ejemplo de cómo usar la plataforma móvil para E-Commerce que en este caso permite a los usuarios investigar y seleccionas las empresas locales basadas en comentarios de los clientes, incluso los comerciantes online que tienen anuncios en el sitio también se ven beneficiados de la aplicación.

2.6.1.6 *Beneficios para los usuarios.*

- Movilidad (permanente para el usuario)

- Posicionamiento (en función de donde se está el usuario)
- Personalización (una herramienta personal)
- Seguridad (en la realización de transacciones)
- Comunicaciones personales sencillas para llamadas de voz, mensajes por correo electrónico e intercambiar información rápidamente con sus colegas y amigos.
- Facilita el acceso a numerosos servicios, en todo momento y lugar, con capacidad de interactuar con el sistema y personalizar sus características.
- El M-Commerce es un nuevo canal de venta que puede ser utilizado por todas las compañías, con independencia de su tamaño.

2.6.1.7 *Del E-Commerce al M-Commerce.*

Durante los años 90 la introducción de Internet y el comercio electrónico redibujaron tanto la forma en que se realizaban los negocios, como la manera en que los consumidores interactuaban con las empresas. Gracias a esto las compañías tuvieron la oportunidad de automatizar muchos procesos que anteriormente eran manejados manualmente.

El Mobile Commerce (M-Commerce), construye sus beneficios sobre los avances realizados por el E-Commerce, pero haciendo posible la interacción para una audiencia más grande y de una forma más personalizada.

Una diferencia importante entre E-Commerce y M-Commerce es la oportunidad de conectar los objetos con su información relacionada de una forma más directa. Sin embargo, en la base de esta visión se hace indispensable mantener la identificación única de los objetos a nivel mundial.

2.6.2 S-Commerce o comercio por redes sociales.

Ilustración 92: S-Commerce.

El S-Commerce, que en español puede ser traducido como comercio social, es una ramificación del comercio electrónico que usa las redes sociales virtuales para promover y/o facilitar la compra/venta de productos y servicios on-line.

El CRM (Customer Relationship Management), es un modelo de gestión de la empresa que enfatiza la orientación al cliente mediante una relación más directa y cercana a él.

Una de las evoluciones experimentadas por el CRM ha sido el S-Commerce. El término “Social Commerce” fue creado en 2005 por Yahoo! y consiste en una ramificación del comercio electrónico que supone el uso de las redes sociales para la compra y venta en

línea de productos y servicios. Desde el año 2009 este término ha empezado a ser más utilizado con el incremento del uso de las redes sociales.

Ilustración 93: Redes sociales del S-Commerce.

El significado que aporta la palabra “social” cuando se asocia a la de comercio, es que existe una conexión, un vínculo, que motiva a los clientes a participar, contribuir y crear experiencias. El resultado esperado de estas interacciones es la relevancia, credibilidad y reputación que el cliente siente o piensa de la marca o producto. Es decir, que se producen relaciones marca-cliente a través de emociones. También se habla de mercadeo social, comercio social y ventas sociales, haciendo referencia que se desarrollan con la ayuda de las redes sociales y sus aplicaciones.

Craig Donato (CEO de Oodle, el Marketplace de Facebook) distinguió entre el comercio electrónico tradicional y el “Social Commerce". Para él, el E-Commerce es algo automático, no humano. Sin embargo, el S-Commerce se basa en conversaciones, relaciones, sobre re-humanizar el comercio online. En lugar de simplemente buscar información, los consumidores descubren productos a través de referencias y recomendaciones de gente en la que confían.

En las redes sociales, las personas vuelcan una gran cantidad de información sobre sus gustos y personalidad y además tienen acceso a los gustos y preferencias de personas cercanas a ellos. Mediante “Listas compartidas”, valoraciones de otros usuarios, consejos, etc., el acceso de los usuarios de las redes sociales a nuevos productos aumenta exponencialmente. Además, esto supone un feedback barato y muy amplio para las empresas. Recopilan datos sobre costumbres y gustos de consumo de grupos e individuos concretos y obtienen decenas de comentarios con información sobre la experiencia vivida del usuario que a su vez son leídos por otros posibles compradores. Esto es un arma de doble filo ya que también proporciona al cliente la posibilidad de expresar sus quejas, por lo que la empresa tiene que hacer un gran esfuerzo para obtener la satisfacción del cliente en este tipo de comercio.

Las empresas introducen enlaces y ofertas en la interfaz habitual de cada una de las redes sociales de forma que solo son utilizados por aquellos usuarios interesados en el producto o servicio desde el inicio. A través de bonos y descuentos en futuras compras, las empresas fidelizan el cliente y lo incorporan como público objetivo en servicios de la misma categoría.

Por lo tanto, podemos resumir que el objetivo del "S-Commerce" es convertir los “Me Gusta” tan conocidos del Facebook en compras.

2.6.2.1 *Tipos de Social Commerce.*

Comercio social, a veces es abreviado como "S-Commerce," es un término comúnmente utilizado para describir nuevos modelos de venta al por menor o las estrategias de marketing que incorporan establecieron redes sociales y / o comunicación peer-to-peer para impulsar las ventas en línea. O, como consultor de marketing Heidi Cohen más sucintamente lo define, es "medios de comunicación social se reúne compras."

Sin embargo, varios sitios de comercio sociales conocidas son anteriores al levantamiento popular de las redes sociales por más de media década. EBay, una plataforma peer-to-peer de venta fundada en 1995, es uno de ellos. Epílogo, un sitio de 13 años de edad, que permite a los usuarios publicar, discutir y venden su propia fantasía y ciencia ficción arte, es otra.

Hoy en día, el comercio social denota una amplia gama de tiendas, recomendar y vender comportamientos. Hemos hecho nuestro mejor esfuerzo para agruparlos en siete categorías, pero me encantaría llegar tus comentarios para mejorarlas en la sección de comentarios.

2.6.2.2 *Siete tipos de Social Commerce.*

1) **Plataformas peer-to-peer de ventas (eBay, Etsy, Amazon Marketplace):** Marketplace basados en la comunidad, o bazares, donde las personas se comunican y venden directamente a otros individuos.
2) **Las ventas impulsadas por las redes sociales (Facebook, Pinterest, Twitter):** Ventas impulsadas por referencias de redes sociales establecidas, o llevarán a cabo en las propias redes (es decir, a través de una pestaña de "tienda" en Facebook).
3) **Grupo de compra (Groupon, LivingSocial).** Productos y servicios que se ofrecen a un precio reducido si suficientes compradores se comprometen a hacer la compra.
4) **Recomendaciones Peer (Amazon, Yelp, JustBoughtIt):** Webs que los exámenes de productos o servicios agregados, recomiendan productos basados en la historia de compra de los demás (es decir, "Los usuarios que compraron este artículo también compraron x Se elemento y," como se ve en Amazon), y / o premiar a los individuos para compartir productos y compras con amigos a través de redes sociales.
5) **Comercial User-comisariada (La Fantasía, Lyst, Svpply):** Centros comerciales centradas en los sitios donde los usuarios crear y compartir listas de productos y servicios para otros a comprar desde.

6) **Comercio Participativa (Threadless, Kickstarter, CutOnYourBias):** Los consumidores involucrarse directamente en el proceso de producción a través del voto, la financiación y el diseño de productos de manera colaborativa.
7) **Comercial Social (Motilo, Fashism, GoTryItOn).** Los sitios que intentan replicar las compras en línea con tus amigos mediante la inclusión de las funciones de chat y foro para el intercambio de consejos y opiniones.

2.6.2.3 *Diferencias en E-Commerce y S-Commerce.*

La naturaleza del medio: Una de las diferencias más perceptibles entre el comercio electrónico y el social commerce es el lugar donde se desarrolla el proceso de compra-venta. Mientras que el E-Commerce ubica el proceso de compra en la web, el social commerce genera una interacción fluida entre el entorno web y las redes sociales. De esta forma, el social commerce se presenta como un paso al frente en la evolución de la compra online, trasladando parte o la totalidad del proceso en el lugar en el que los consumidores pasan gran parte de su tiempo.

Usuario, epicentro del proceso de compra Actualmente, muchas marcas hablan de la importancia del consumidor y su importancia en la toma de decisiones corporativas. No obstante, pocos aplican este criterio en sus plataformas de venta online. Las soluciones de social commerce ponen énfasis en el consumidor, y lo sitúan en el epicentro del acto de compra. De esta manera, la tienda no se convierte en un escaparate estanco, sino que ofrece una experiencia única y personalizada en función del usuario que lo visite.

Componente social Una de las máximas del Social Commerce es dotar al proceso de compra de un componente más social. De esta manera, los consumidores pueden llevar a cabo el proceso de compra online al mismo tiempo que comentan sus adquisiciones, reciben recomendaciones de sus amigos, comparten información… En definitiva, el Social Commerce abre la puerta a la interacción y al intercambio de información durante el proceso de compra.

Relación marca-consumidor Otro de los aspectos claves que diferencia ambas modalidades es la capacidad de interacción con el público potencial. El E-Commerce ha sido tradicionalmente un canal estático e unidireccional, en el que el consumidor decidía comprar o no partiendo de la información dispuesta. Con la integración de las redes sociales en el punto de venta, abrimos la puerta a un canal de comunicación mucho más fluido que facilita la interlocución entre los comerciantes y consumidores, y entre usuarios. De esta forma, se puede afirmar que el Social Commerce contribuye de manera efectiva al fortalecimiento del vínculo entre marcas y consumidores.

Conocimiento del consumidor A diferencia del E-Commerce, el social commerce facilita a las marcas un conocimiento más exhaustivo de sus clientes 2.0. En esta tipología de comercio, los compradores dejan de ser números para convertirse en personas cuyo perfil las empresas conocen gracias al grafo social. Asimismo, la información que estos usuarios comparten a través de las redes también puede ayudar a los vendedores a generarse una idea sobre el entorno en el que se mueve el cliente, sus aficiones, etc.

Adecuación de la oferta Esta diferencia emerge como consecuencia de la anterior. Un mayor conocimiento del consumidor permite ofrecer productos que se adapten a los gustos y necesidades de los consumidores. Hasta el momento las recomendaciones de la e-tienda se basaban en criterios de navegación o complementariedad entre los productos visitados. En cambio, las nuevas aplicaciones de social commerce (como es el caso de Social-Buy.com) ofrecen a las marcas un completo motor de recomendaciones mediante el cual son capaces de ofrecer una selección de productos adaptados a los gustos y preferencias de cada usuario. De este modo, el social commerce, a diferencia del E-Commerce, facilita que la oferta adecuada llegue al consumidor adecuado.

Compra en exclusiva Si bien 2011 fue el año de los "groupones", este año muchas marcas van a apostar por ofrecer directamente condiciones de compra especiales a su cliente con el objetivo de premiar la fidelidad a la marca. En este sentido, el social commerce se presenta como el escenario ideal para llevar a cabo este tipo de acciones a través de los llamados "descuentos sociales". Este tipo de promociones permite a los usuarios conseguir rebajas por el simple hecho de publicar un producto en las redes sociales o recomendarlo a sus amigos.

2.6.2.4 *El futuro de Social Commerce.*

Comercio social está todavía en su infancia. Ninguna de las principales redes sociales: Facebook, Twitter, Pinterest. Sin embargo, han descubierto la manera de llevar las transacciones directamente a sus plataformas, en lugar dirigir los minoristas a utilizar devengados y pagados los medios para atraer clientes a sus tiendas en línea.

Los minoristas en línea, también, están experimentando continuamente con nuevos modelos y métodos de comercialización para permitir una mayor peer-to-peer y las interacciones grupales, consciente de que las recomendaciones de amigos (y en menor grado, los extranjeros) pueden jugar un papel importante en las compras. Según Gartner, el 74% de los consumidores confían en las redes sociales para orientar sus compras.

Como son probados y probados para aumentar las ventas y la satisfacción del cliente de estos modelos, más serán incorporados. Basta con mirar el número de sitios, desde Anthropologie.com de Zappos.com, que ahora incluye comentario de los compradores. Botones de "Me gusta" y "Pin It" están apareciendo cada vez más hasta sitios para animar a los compradores a compartir sus hallazgos con sus redes en línea, también. Y minoristas establecidos incluyendo Nike y ModCloth están permitiendo a los compradores a tomar un gran papel en el proceso de producción, invitándolos a diseñar sus propios zapatos (Nike) y voto en lo que los diseños se almacenan en el almacén (ModCloth).

2.6.3 F-Commerce o comercio por Facebook.

Ilustración 94: F-Commerce.

Facebook Commerce también llamado F-Commerce se refiere a la realización de ventas de productos o servicios a través de las páginas de Facebook, es decir Comercio Electrónico en Facebook. Las ventas pueden realizarse completamente en Facebook o iniciarse en Facebook y completarse en el sitio Web.

Aunque F-Commerce inició con grandes empresas, puede ser una excelente alternativa para las pequeñas y medianas empresas que no tengan el conocimiento o el dinero para crear una tienda electrónica en el sitio Web.

Un aspecto importante de este tipo de comercio es que hay previsiones que apuntan a que en 2016 el mercado global del social commerce alcanzará los 30.000 millones de dólares.

2.6.3.1 *Ventajas y Desventajas del Facebook Commerce.*

Ventajas:

- **Más de 750 millones de clientes potenciales.** Como mencionamos antes, Facebook es una herramienta cada vez más utilizada en los países de habla hispana y las personas que la visitan gastan mucho tiempo allí.
- **Relacionamiento**. En Facebook se tienen muchos mecanismos para generar confianza al usuario. Si un usuario ha hecho clic en “Me gusta” o ha comprado con anterioridad se convierte en fan, lo que permite que las noticias que publiquemos con descuentos, promociones y nuevos productos aparezcan en su página de inicio en Facebook.
- **Propagación.** Gracias al botón “Me gusta” nuestra tienda electrónica y sus contenidos tienen mayores probabilidades de convertirse en “virales”.
- **Menores costos.** Los costos respectos a una tienda electrónica en un sitio Web son más bajos debido a que no hay que comprar nombre de dominio ni contratar hosting. Esta característica la hace ideal para pequeñas y medianas empresas.
- **Facilidad de uso.** La actualización de la tienda electrónica en Facebook la podrá realizar una persona que no sea técnica por su facilidad de uso.

Desventajas:

- **Dependencia Facebook.** Si Facebook decide en un futuro cambiar sus políticas y, por ejemplo, no permitiera la presencia de tiendas online, se perderá todo lo logrado con la página.

- **Derecho sobre los contenidos.** Las políticas de Facebook no son de todo claras en este sentido y puede originar que con un cambio de políticas perdamos el derecho sobre las imágenes y contenido de nuestra tienda electrónica.

2.6.3.2 *Tipos de Facebook Commerce*

1) Iniciar la venta en Facebook:

La gran mayoría de las empresas que utilizan Facebook para vender inician el proceso de ventas en Facebook y lo terminan en su tienda electrónica en el sitio Web. Las empresas pueden llevar la experiencia de Facebook a sus sitios web.

Esta es una excelente y fácil solución para aquellas empresas que tienen tienda electrónica en su sitio Web y quieren generar ventas desde Facebook.

Un ejemplo muy exitoso en este tipo de F-Commerce es la tienda en Facebook de Lady Gaga. Los visitantes pueden ver los productos en la página de Facebook, pero a la hora de comprar se direccionan a la tienda electrónica en su sitio Web.

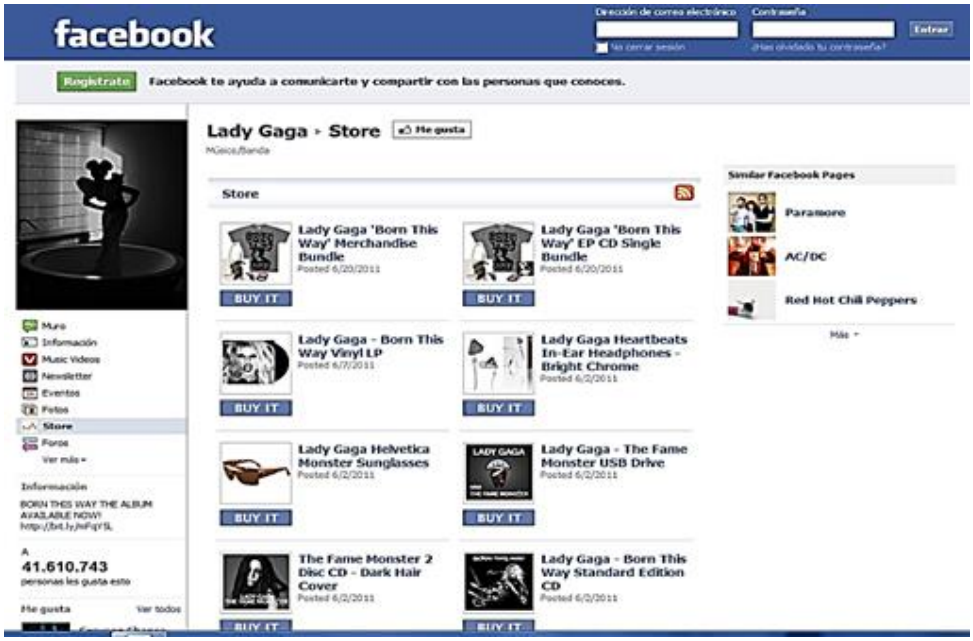


Ilustración 95: Primer ejemplo del F-Commerce.

2) Iniciar y terminar la venta en Facebook:

Esta alternativa está siendo más usada cada día y permiten realizar todo el proceso de venta directamente en Facebook, incluido el pago. Significa una presencia comercial completamente transaccional en Facebook.

1-800-Flowers es la empresa pionera de este tipo de F-Commerce ya que inicio las ventas en Facebook en julio de 2009.

La segunda empresa que incursionó en este tipo de F-Commerce con mucho éxito fue Delta Airlines. Delta desarrollo en agosto de 2010 una completa aplicación en su página de Facebook que le permite a los usuarios reservar vuelos y compartir la información de destinos con sus amigos de Facebook.

Ilustración 96: Segundo ejemplo de F-Commerce.

2.6.3.3 *¿Cómo crear una tienda en Facebook?*

Existe una gran cantidad de herramientas que hacen del F-Commerce una opción útil para las pequeñas y medianas empresas.

1) Payvment.

Payvment es otra aplicación gratuita, muy sencilla de montar y con gran variedad de opciones para poder montar una tienda online a tu medida.

Para ponerlo a funcionar se requiere instalar la aplicación y luego configurarla. Sus visitantes verán la tienda como una pestaña más dentro de la página, podrán navegar por los productos, agregarlos en un carrito y realizar los pagos de forma segura con PayPal. Por el momento sólo acepta pago vía PayPal.

Para ver una tienda virtual en Facebook utilizando Payvment, puede visitar la página de Facebook de DealExtreme.

2) SocialMediaShops.

SocialMediaShops es una herramienta gratuita que permite crear una tienda electrónica en Facebook. Esta aplicación es completamente en español y muy fácil de manejar para personas que no tengan conocimientos técnicos. SocialMediaShops permite personalizar la tienda con la imagen de la empresa, cargar información de productos, cargar imágenes e implementar una pasarela de pago.

Ilustración 97: Socialmediashops.

SocialMediaShops, además de tener el potencial de E-Commerce sobre Facebook tiene poderosas herramientas de viralidad para potencializar el comercio social (Social Commerce), de tal forma que cada venta pueda generar ventas adicionales.

Adicionalmente, la aplicación tiene una poderosa herramienta de estadísticas para hacer seguimiento de las visitas y compras dividido por sexo, edad, país de procedencia, entre otros.

2.6.3.4 ***Otras herramientas gratuitas.***

1) **Carttini:** es una aplicación gratuita de venta por Facebook y que le permite además vender productos que tenga en su catálogo.

Basta crear una cuenta e informar los productos que quieres poner a la venta, con precio, gastos de envío, fotos, comentarios y formato de exhibición. Es posible elegir productos de su base de datos, con lo que no es necesario tener un negocio ya establecido.

2) **VendingBox:** le ayuda a montar su tienda en Facebook de manera gratuita y sólo pagarás una comisión por venta. Si tiene una tienda electrónica en su sitio Web en: OsCommerce, Magento o ZenCart, permite una integración automática con tu tienda en Facebook.

Un sistema de creación de tiendas virtuales que puede integrarse en una página de Facebook, ofreciendo personalización estética, varios idiomas e integración con otras plataformas de comercio electrónico.

3) **Infusedcommerce:** Se trata de una opción no gratuita que permite configurar una tienda añadiendo elementos, incluyendo formas de pago (tarjetas de crédito), informando sobre servicios de entrega y ofreciendo un carrito de la compra extremadamente intuitivo para cualquier posible cliente.

3 DISEÑO METODOLOGICO.

3.1 Descripción general del proyecto.

En este proyecto se pretende la instalación e implementación de diferentes plataformas web (OpenCart, Magento, OsCommerce) para la simulación de un sitio de comercio electrónico.

3.2 Etapas del trabajo

Para abordar todo lo planteado en el trabajo se dividió la realización del proyecto en las siguientes etapas:

3.2.1 Recolección de datos.

Esta etapa analizamos y seleccionamos contenidos teóricos y prácticos que nos permitió obtener mayores conocimientos sobre el componente curricular del comercio electrónico, así como la obtención de información relacionada con las tecnologías más reciente que se están utilizando de manera masiva y que son tendencia en la red. Se realizó dicha investigación a través de la lectura de libros, sitios web e información facilitada por fuentes externas.

3.2.2 Creación del documento teórico.

En esta etapa seleccionamos toda la información teórica que puede ser de utilidad para la creación y enriquecimiento del documento. En este documento consta de conceptos básicos, tecnologías empleadas, clasificación, seguridad, sistemas de pago, practicas desarrolladas etc.

3.2.3 Creación del documento practico.

En esta etapa se investigó acercas de tecnologías usadas actualmente el comercio electrónico, y los aspectos más importantes que se podrían configurar en las diferentes plataformas luego se hizo una clasificación del orden en cómo se realizarán dividendo dichos aspectos en diferentes prácticas de laboratorio.

3.2.4 Redacción del documento final.

Esta etapa se hace una redacción y organización del documento final, el cual contiene la explicación de cada una de las etapas de este proyecto.

3.3 Materiales utilizados.

En esta sección se enumeran diferentes materiales empleados en este trabajo tanto hardware como software.

Hardware	
Componente	**Características**
Disco duro	8 Gb (por cada nada máquina virtual)
Memoria RAM	126 Mb (servidor dhcp), 126 Mb (servidor dns), 512 Mb (servidor web), Mb 512 (cliente).

Tabla 10: Hardware utilizado.

Software		
Componente	**Funcionamiento**	**Servidor instalado**
Oracle virtual box 5.0	Es un programa de virtualización donde podremos instalar en nuestro ordenador cualquier sistema operativo de forma “virtual”.	
Dhcp	Asigna direcciones IP a otras máquinas de la red.	Servidor Dhcp
Dns	Permitirán saber la localización del sitio Web que pediste y dirigir tu petición por la red hasta el ordenador en cuestión.	Servidor Dns
Apache2	es el encargado de aceptar las peticiones de páginas (o recursos en general) que provienen de los visitantes que acceden a nuestro sitio web y gestionar su entrega o denegación, de acuerdo a las políticas de seguridad establecidas.	Servidor web
Php5	es un lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico.	Servidor web
MySql	es un sistema de gestión de bases de datos relacional, multihilo y multiusuario.	Servidor web
Ubuntu server 15.04	es un sistema operativo basado en GNU/Linux y que se distribuye como software libre. Tiene un entorno de texto.	Servidor dhcp y dns
LUbuntu 15.04	es una distribución oficial del proyecto Ubuntu que tiene por lema "menos recursos y más eficiencia energética", usando el gestor de escritorio LXDE	Servidor web
Windows XP	Es una distribución de Windows, se caracteriza por el uso de ventanas, y es multiusuario y multitarea.	Cliente

Tabla 11: Software utilizado.

Plataformas web		
Plataforma	**Concepto**	**Versión**
OpenCart	Este software se destaca por su sencillez de manejo tanto en la tienda como en el módulo de administración.	2.0.3.1
Magento	Permite crear diseños innovadores debido a su sistema de layouts, pudiéndose asignar vistas distintos a productos o categorías específicos.	1.9.1.0
OsCommerce	Es un programa de comercio electrónico y administración online que se ofrece para una licencia GNU General Public License (GPL). Permite montar muy fácilmente una tienda online.	2.3.3.4

Tabla 12: Plataformas utilizadas.

4 DESARROLLO PRÁCTICO.

4.1 Organización de las practicas.

Introducción.

La asignatura “Comercio Electrónico” correspondiente a la Electiva VI que pertenece al plan académico 2011 de la carrera de Ingeniería en Telemática del Departamento, de Computación de la UNAN-León y se imparte en el segundo semestre del IV año de la carrera e incluye en su currículo, 2 horas semanales de teoría y 2 horas semanales de laboratorio.

El contenido de este documento podrá ser revisado (de forma no significativa) para adaptar los trabajos y tareas del laboratorio a la evolución de la asignatura en su conjunto.

Programación.

Practica 1: Elección de plataforma.

Practica 2: Configuración de una red para el comercio electrónico.

Practica 3: Manejo de productos y categorías.

Practica 4: Instalación y configuración de métodos de pago.

Practica 5: Configurar elementos como lo costes de envío, monedas, impuestos.

Practica 6: Creación de cuentas a clientes.

Practica 7: SSL.

Practica 8: Descuentos, fichas especiales, puntos de recompensa.

Practica 9: Realizar compras.

Practica 10: Devolución de producto, dinero, contactar comprado – vendedor.

Practica 11: Instalación aplicaciones M-Commerce.

Evaluación.

Los contenidos del laboratorio tendrán un valor del 40% en la calificación global de la asignatura.

Organización de las practicas.

Practicas	Horas presenciales.	Horas no presenciales.	Total.
Practica 1: Elección de plataforma.	2	4	6
Practica 2: Configuración de una red para el comercio electrónico.	4	6	10
Practica 3: Manejo de productos y categorías.	4	4	8
Practica 4: Instalación y configuración de métodos de pago.	4	6	10
Practica 5: Configurar elementos como lo costes de envío, monedas, impuestos.	4	4	8
Practica 6: Creación de cuentas a clientes.	4	6	10
Practica 7: SSL.	2	2	4
Practica 8: Descuentos, fichas especiales, puntos de recompensa.	2	2	4
Practica 9: Realizar compras.	2	2	4
Practica 10: Devolución de producto, dinero, contactar comprado – vendedor.	2	4	6
Practica 11: Instalación aplicaciones M-Commerce.	2	4	6
Total horas	32	44	76

Tabla 13: Organización de las practicas.

Practica 1: Elección de plataforma.

Objetivo:

- Instalación y elección de múltiples plataformas del comercio electrónico.
- Realización de una comparativa entre las plataformas instaladas.

Duración:

- 1 sesiones de laboratorio.

Introducción.

Las plataformas de Comercio electrónico nos permiten de forma muy sencilla gestionar una tienda on-line con todos los servicios necesarios para publicar nuestros productos, instalar formas de pago y recibir los datos y pedidos de los compradores.

Para una mejor comprensión de las bondades que dicho servicio ofrece para los comerciantes on-line, instalaremos múltiples plataformas con el fin de ver cuál es la más eficiente en funcionamiento, no produzca problemas técnicos, facilidad de gestión de la plataforma, etc.

Sugerencias en el desarrollo de las prácticas.

Para el desarrollo de esta práctica se recomienda instalar máquinas virtuales haciendo uso del sistema operativo Ubuntu.

Las plataformas vienen predefinidas en el lenguaje en inglés y se recomienda no cambiarlo.

Desarrollo del Laboratorio.

En la presente práctica se instalará un total de 4 plataformas, entre ellas se encuentran: OpenCart, Magento, OsCommerce, PrestaShop, X-Cart, Zen Cart, VirtueMart, CubeCart, TomatoCart, Shopify, BigCommerce, etc... En cada una de ellas se instalará los paquetes requeridos a cada plataforma.

Practica 2: Configuración de una red para el comercio electrónico.

Objetivo:

- Creación de una red con el fin de realizar una simulación de una tienda virtual.

Duración:

- 2 sesiones de laboratorio.

Introducción.

1. **DHCP:**

El servicio DHCP es uno de los más empleados dentro de cualquier infraestructura de red por facilitar la configuración de los equipos y lograr la conectividad deseada dentro de la red a costa de un pequeño esfuerzo por parte de los administradores de la red.

2. **Domain Name Service (DNS):**

El DNS es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP.

Sugerencias en el desarrollo de las prácticas.

Para el desarrollo de esta práctica se recomienda eliminar el modo gráfico en cada una de las máquinas que funcionarán tanto como router como servidores y únicamente mantenerlo en aquellas que serán utilizadas en modo cliente. Se debe tener en cuenta que como servidor DNS deberá ser asignado por el servidor DHCP a las máquinas clientes debe utilizarse el que la red local asigne a la máquina real.

Desarrollo del Laboratorio.

1. **Configuración de una máquina como Router + Servidor DHCP + PortFordwarding + NAT.**

Para este primer apartado, se han seleccionado cuatro funcionalidades básicas que este tipo de sistemas implementan y que se explican a continuación:

- **Router:** Permite que el equipo encamine paquetes entre redes distintas. Esta funcionalidad la hemos trabajo en la práctica.
- **Servidor DHCP:** Asigna IP's a las máquinas que se lo solicitan.
- **NAT:** Es un mecanismo utilizado por router IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Su uso más común es

permitir utilizar direcciones privadas (definidas en el RFC 1918) para acceder a Internet.

- **Port Forwarding:** La redirección de puertos es la acción de redirigir un puerto de red de un nodo de red a otro. Esta técnica puede permitir que un usuario externo tenga acceso a un puerto en una dirección IP privada (dentro de una LAN) desde el exterior vía un router con NAT activado.

2. Configuración de una maquina como DNS.

Se deberá de configurar un servidor DNS primario para la zona "practia.net". Dentro de esta zona se deberá configurar que el servidor DNS resuelva las siguientes traducciones:

Nombre	Dirección IP
ns1.practica.net	192.168.0.2
www.practica.net	192.168.2.2

El esquema que se debe montar para esta práctica es el siguiente:

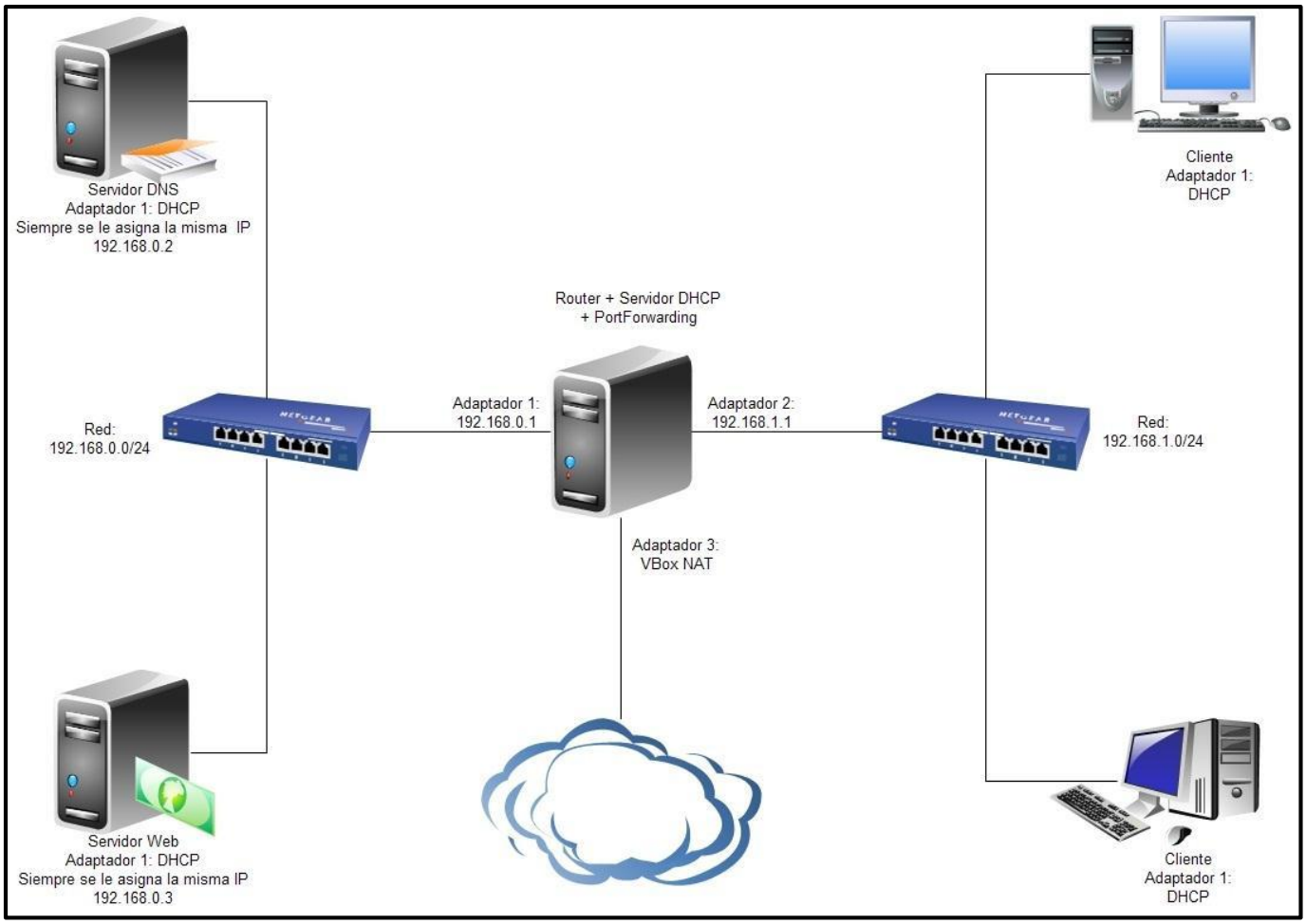


Ilustración 98: Esquema de red.

Practica 3: Manejo de productos y categorías.

Objetivo:

- Creación de categorías y productos.
- Inserción de nuevos fabricantes.
- Modificación de banners.
- Cambiar los productos en destacados.

Duración:

- 2 sesiones de laboratorio.

Introducción.

El manejo de productos y categorías de los productos es lo que define que el comercio electrónico tenga resultado.

Sugerencias en el desarrollo de las prácticas.

Para el desarrollo de esta práctica se sugiere eliminar los productos y categoría que tengan la plataforma, todo esto dependerá de qué tipo de productos ofrecerá su tienda on-line.

Desarrollo del Laboratorio.

En esta práctica agregaremos un total de 30 productos en 5 categorías diferentes. Estas categorías y productos deben de ser diferentes a las que trae la plataforma que han elegido.

Practica 4: Instalación y configuración de métodos de pago.

Objetivo:

- Instalación de módulo de pago de PayPal.
- Configuración del módulo instalado.

Duración:

- 2 sesiones de laboratorio.

Introducción.

El sistema de pago electrónico es fundamental en el proceso de compra-venta dentro del comercio electrónico.

PayPal es un sistema de intermediación financiera que le permite realizar compras y ventas online en forma segura.

Sugerencias en el desarrollo de las prácticas.

Para la realización de esta práctica se usará cuentas en PayPal, se hará uso de tarjeta de débito o crédito.

Se recomienda tener la cuenta de PayPal de modo Empresarial o Premium y no personal.

Desarrollo del Laboratorio.

Se procederá a instalar el módulo de PayPal, luego de haber instalados se procederá a configurarlo de manera que se creará una cuenta de dicho medio de pago como vendedor.

Practica 5: Configurar elementos como lo costes de envío, monedas, impuestos.

Objetivo:

- Instalación y configuración de diferentes tipos de costo de envió.
- Creación de moneda local.
- Inserción de un impuesto.

Duración:

- 2 sesiones de laboratorio.

Introducción.

Los gastos de transporte son los costos incurridos por el envío de productos desde el productor o el distribuidor hasta un cliente o consumidor. En algunos casos, el cliente paga por los gastos de transporte como parte de su factura. Algunos proveedores ofrecen un envío gratis como parte de la promoción de bienes.

La moneda hace referencia a cualquier forma de dinero que se encuentra en circulación utilizado por todo el público.

El impuesto es el tributo, exacción o la cantidad de dinero que se paga al Estado, a la comunidad autónoma o al ayuntamiento obligatoriamente, y está establecida sobre las personas, físicas o jurídicas, para contribuir con la hacienda pública, financiar los gastos del Estado y otros entes y servicios públicos.

Desarrollo del Laboratorio.

1) Se instalar y configurara 3 tipos de costo de envió como se muestra a continuación.
   - Importes de “envío gratuito”.
   - Importes “basado en peso”.
   - Importes de “tarifa plana”.
2) Se creará un tipo de moneda local.
3) Se creará impuestos el impuesto del I.V.A.

Practica 6: Creación de cuentas a clientes.

Objetivo:

- Creación de cuentas a clientes.
- Visualizar información de los clientes.
- Búsqueda de clientes registrados.
- Creación de grupos de clientes.
- Habilitación de servicio de atención al cliente

Duración:

- 2 sesiones de laboratorio.

Introducción.

Un cliente es tanto para los negocios y el marketing como para la informática un individuo, sujeto o entidad que accede a recursos, productos o servicios brindados por otra.

Para los negocios, el cliente es aquel individuo que, mediando una transacción financiera o un trueque, adquiere un producto y/o servicio de cualquier tipo (tecnológico, gastronómico, decorativo, mueble o inmueble, etcétera). Un cliente es sinónimo de comprador o de consumidor.

Desarrollo del Laboratorio.

- Se creará un total de 6 usuarios de los cuales se crearán 3 usuarios de forma manual haciendo uso del modo administrador y 3 usuarios desde la página principal.
- Se creará 2 grupos de usuarios que contendrán a 3 usuarios cada uno.
- Se visualizará la información de un determinado cliente.
- Demostrar las diferentes maneras de buscar un determinado cliente desde el administrador.
- Acceder al servicio al cliente y configurarlo.

Practica 7: SSL.

Objetivo:

- Instalación del protocolo de seguridad SSL.
- Configuración del protocolo instalado.

Duración:

- 1 sesiones de laboratorio.

Introducción.

SSL: permitir el tráfico que se enviará de forma segura entre las partes remotas sin la posibilidad de que el tráfico sea interceptado y leída por alguien en el medio. También juegan un papel decisivo en la validación de la identidad de los dominios y servidores a través de Internet mediante el establecimiento de un servidor como de confianza y genuina por una autoridad certificadora.

Desarrollo del Laboratorio.

- Instalar SSL en el Servidor Web.
- Habilitar el modulo SSL.
- Crear un subdirectorio para colocar los archivos de certificado.
- Crear llave y certificado.
- Configurar el archivo de SSL.
- Activación del host virtual SSL.
- Habilitar SSL en la plataforma web.

Practica 8: Descuentos, fichas especiales, puntos de recompensa.

Objetivo:

- Aplicación de descuentos a productos.
- Creación de fichas especiales.
- Utilización de puntos de recompensa.

Duración:

- 1 sesiones de laboratorio.

Introducción.

Descuento: son cupones tienen un código que se puede aplicar al momento de pagar, pueden ser por precio fijo o por porcentaje de la compra, etc., estos cupones no se aplican directamente al producto por lo tanto todos los productos mantienen su precio.

Fichas especiales: son precios especiales que cambia el valor del precio del producto al precio especial de nuevo. Precios especiales para un grupo de clientes se mostrará el precio especial sólo si el cliente está conectado como ese grupo.

Puntos de recompensa: Los clientes pueden ganar puntos de fidelidad para la compra de productos de su tienda, y luego canjearlos después de que se han acumulado suficientes puntos.

Desarrollo del Laboratorio.

- Se creará 6 productos nuevos.
- Se aplicará descuentos a los productos.
- Se creará fichas especiales.
- Utilizar puntos de recompensa.

Practica 9: Realizar compras.

Objetivo:

- Realizar el proceso de compra- venta en la tienda virtual.
- Mostrar la ejecución correctamente el proceso.
- Verificar la transacción del proceso en la parte del vendedor como del comprador.

Duración:

- 1 sesiones de laboratorio.

Introducción.

Compra-venta: Se conoce popularmente como compraventa a aquel comercio en el cual se compran y venden cosas, especialmente aquellas usadas o antiguas y por supuesto con un valor mucho más accesible que en cualquier otro comercio en el cual se ofrecen piezas similares pero nuevas y sin uso.

Desarrollo del Laboratorio.

- Elegir un productor para realizar la compra.
- Realizar la compra con la cuenta de un cliente.
- Revisar en la cuenta del vendedor la transacción realizada por el cliente.

Practica 10: Devolución de producto, dinero, contactar comprado – vendedor.

Objetivo:

- Realizar la devolución de un producto.
- Devolver el dinero como muestra de transacciones.
- Enviar un mensaje entre comprador y vendedor

Duración:

- 2 sesiones de laboratorio.

Introducción.

Devolución de un producto: es el acto por el cual devolvemos a un comerciante el producto previamente comprado.

Devolución de dinero: es la acción de devolver dinero a un cliente sobre el producto devuelto.

Contactar comprador-vendedor: esta acción se debe cuando existe algún tipo de desacuerdo entre alguno de ellos.

Desarrollo del Laboratorio.

- Realizaremos la devolución del producto comprado en la práctica anterior.
- Comprobar cada paso del proceso de la devolución de un producto tanto como vendedor como comprador.
- Realizar la devolución del dinero obtenido en la compra de la práctica anterior, esto con el fin de verificar como se realiza una transacción en PayPal.
- Enviar un mensaje al vendedor.

Practica 11: Instalación aplicaciones M-Commerce.

Objetivo:

- Instalación de un emulador de Android en Windows.
- Instalación de aplicaciones M-Commerce.
- Obtener conocimientos sobre el funcionamiento de dichas aplicaciones.

Duración:

- 2 sesiones de laboratorio.

Introducción.

Una aplicación móvil es un programa que usted puede descargar y al que puede acceder directamente desde su teléfono o desde algún otro aparato móvil como por ejemplo una Tablet o un reproductor MP3.

Los sistemas operativos móviles Android, Apple, Microsoft y BlackBerry tienen tiendas de aplicaciones que operan en línea en las cuales usted puede buscar, descargar e instalar las aplicaciones. Algunos comerciantes minoristas también operan tiendas de aplicaciones en internet.

Sugerencias en el desarrollo de las prácticas.

Como emulador de Android en Windows se sugiere instalar el software con nombre de BlueStacks.

Alguna aplicación de m-commerce no está disponible en algunos países como es el caso de “YELP”.

Desarrollo del Laboratorio.

Previamente instalaremos nuestro emulador en este caso BlueStacks. Una vez instalado el emulador procederemos a instalar 2 de las aplicaciones que utilizaremos, entre ellas tenemos (Red Box, Yelp, Amazon Student, Zong, Best Buy, Wallapop).

Una vez instalados las aplicaciones procederemos a estudiar sus funcionamientos.

5 CONCLUSIONES Y RECOMENDACIONES.

5.1 Conclusiones.

Con la finalización de este trabajo monográfico, consideramos que hemos logrado cumplir con los objetivos propuestos, llegando a las siguientes conclusiones:

1) La facilitación de información teórica, les proporciona a los estudiantes transmitir y procesar información acerca de lo que es el comercio electrónico, que luego será utilizada en las practicas con el fin de que dichos estudiantes puedan realizar las prácticas con los conocimientos previos adquiridos en la clase teórica.

1) El diseño de un adecuado formato de prácticas facilitará a los estudiantes una correcta comprensión de la práctica a realizar.

2) La secuencia en que se han organizado las prácticas propuestas, permitirá a los estudiantes más facilidad para la solución de estas.

3) Con el fin de determinar cuál de estas plataformas utilizadas (OpenCart, Magento, OsCommerce), era la más viable a utilizar obtuvimos como resultado que ha sido la plataforma OpenCart, siendo que esta es una plataforma muy sencilla, completa y fusil de adaptar, con posibilidades de adaptarle más módulos para brindar nuevas funcionalidades o mejorar las existentes.

4) Con la implementación del servicio de pago de PayPal logramos hacer una simulación donde se hizo posible la realización de una compra y venta de un producto determinado, y así logramos comprender el uso de este medio de pago, luego hicimos unos de sus servicios como entidad del comercio electrónico, ya que es uno del pago más utilizados hoy en día.

5) Se han abordado temas nuevos relacionados con el comercio electrónico para el aprendizaje de los estudiantes, lo cual resulta necesarios para estar al día con las nuevas tendencias tecnológicas, ya que el comercio electrónico es un área de crecimiento en nuestro país.

Con las conclusiones antes mencionadas, podemos afirmar que hemos logrado desarrollar un documento más actualizado en el área teórica y práctica, con el cual los estudiantes y docentes podrán uso. Gracias a este documento lograran obtener conocimientos básicos sobre el manejo de una tienda virtual haciendo uso de plataformas web con el seguimiento ordenado de las propuestas de prácticas de laboratorios que hemos desarrollado.

5.2 Recomendaciones.

Las recomendaciones que se describen a continuación son a base de una futura actualización del documento.

1. Se ha intentado que los temas presentados aquí, estén lo más actualizados hasta la fecha de presentación de este trabajo. Sin embargo, dado que el Comercio electrónico está en constante crecimiento, es necesario que en el futuro se realice una actualización de este trabajo con respecto a las futuras tecnologías o métodos que se hacen uso en el desarrollo del comercio electrónico.

2. Se tiene que hacer necesario trabajar con las versiones actualizadas de las plataformas de comercio electrónico debido a que estas son susceptibles a la corrección y mejoramientos de los errores que presentan las versiones anteriores, además brindan nuevas funcionalidades más sencillas y completas con las cuales se hace uso en el desarrollo de las prácticas de laboratorio.

3. Se aconseja profundizar en las diferentes funcionalidades y/o módulos(gratuitos), que ofrecen cada una de las plataformas de comercio, para obtener una mejor utilización.

4. Incorporar una pasarela de pago alternativo, para luego implementarlo en las practicas con los que se puede realizar transacciones de compra/ventas simuladas.

5. Incursionar en la planificación e implementación de prácticas orientada al uso de las ramificaciones del comercio electrónico como son M-Commerce, S-Commerce y F-Commerce.

6 BIBLIOGRAFÍA

Aplicadas, O. T. (s.f.). *Modelos de negocios en el ecommerce.* Obtenido de http://www.todoecommerce.com/modelos-de-negocios-en-el-e-commerce.html

Campano, J. F. (s.f.). *8 modelos de negocio en dispositivos moviles*. Obtenido de http://www.jaimefernandez.com/8-modelos-de-negocio-en-dispositivos-moviles/

Consuvec. (s.f.). *Comercio electronico*. Obtenido de http://www.eurosur.org/CONSUVEC/contenidos/Consejos/comercio/comercio_e/comercio_e.htm

Diaz, A. H. (s.f.). *Cual es la forma de pago online mas segura en internet.* Obtenido de http://alfredohernandezdiaz.com/2013/05/15/forma-pago-online-mas-segura-internet/

Digital, A. E. (2011). *Libro blanco del comercio electronico.* Obtenido de http://documentos.camarazaragoza.com/comercio-electronico/destacados/Libro%20Blanco%20Comercio%20Electr%C3%B3nico%202a%20Edicion%202012.pdf

ecommerce, A. (s.f.). *5 aplicaciones moviles ecommerce*. Obtenido de http://www.actualidadecommerce.com/5-aplicaciones-moviles-ecommerce/

eCommerce, A. (s.f.). *las 5 plataformas de pago online mas populares*. Obtenido de http://www.actualidadecommerce.com/las-5-plataformas-de-pago-online-mas-populares/

Freire, A., Moreia, C., Navas, S., & Pilco, M. (2013). *Tipos de comercio electronico.* Obtenido de https://cmelendez.wikispaces.com/file/view/TIPOS+DE+COMCERCIO+ELECTR%C3%93NICO+BIEN.pdf

Google. (s.f.). *Clases de comercio electronico.* Obtenido de http://suite101.net/article/clases-de-comercio-electronico-b2b-b2c-b2a-b2e-c2c-c2g-b2g-a26589#.VPjsmHyG-gY

Google. (s.f.). *Claves de evolucion del ecommerce.* Obtenido de https://sites.google.com/site/webcelectronico/evolucion-del-comercio-electronico/claves-de-evolucion-del-e-commerce

Google. (s.f.). *Factores que influyen en la evolucion.* Obtenido de https://sites.google.com/site/webcelectronico/evolucion-del-comercio-electronico/factores-que-influyen-en-la-evolucion

Google. (s.f.). *Historia y origen del comercio electronico*. Obtenido de https://sites.google.com/site/webcelectronico/evolucion-del-comercio-electronico/historia-y-origen

Google. (s.f.). *Manual practico del comercio electronico.* Obtenido de https://books.google.com.ni/books?id=AUKnBlV6cAMC&pg=PA44&lpg=PA44&dq=Sujetos+intervinientes+en+el+comercio+electr%C3%B3nico+administracion&sourc

e=bl&ots=Bnr-jNyRpO&sig=9fTd_Ux5YtiV-zmO7r4Vme9ji_M&hl=es&sa=X&ei=mMT9VKfeNveTsQSUoIDwDw&ved=0CCwQ6AEwAw#v=one

hoy, I. (s.f.). *Tipos de comercio electronico*. Obtenido de http://www.informatica-hoy.com.ar/aprender-informatica/Tipos-de-Comercio-Electronico.php

hoy, I. (s.f.). *Tipos de comercio electronico*. Obtenido de http://www.informatica-hoy.com.ar/aprender-informatica/Tipos-de-Comercio-Electronico.php

Karen, A. V., Valeria, B., Jéssica, B., & Rumiguano. (s.f.). *Aplicaciones del comercio electronico.* Obtenido de Comercio electonico: https://cmelendez.wikispaces.com/file/view/APLICACIONES.pdf

Magento. (s.f.). *Magento Sitio Oficial*. Obtenido de https://magento.com/

Manzevitsch, D. A. (20 de 8 de 2003). *Introduccion a la seguridad en entornos de comercio electronico*. Obtenido de http://www.maestrosdelweb.com/segecom/

Manzevitsch, D. A. (20 de 08 de 2003). *Introducción a la Seguridad en Entornos de Comercio Electrónico*. Obtenido de http://www.maestrosdelweb.com/segecom/

marketing, P. d. (s.f.). *Ventajas y desventajas del mcommerce*. Obtenido de http://principiosdemarketing.com/blog/2014/11/17/ventajas-y-desventajas-del-m-commerce/

Martínez López, L., Mata Mata, F., & Rodríguez Domínguez, R. M. (2009). Sistemas de pagos seguros. Seguridad en el comercio eletronico. *Revista de Estudios Empresariales.*, 63 - 76. Obtenido de http://revistaselectronicas.ujaen.es/index.php/REE/article/viewFile/359/322&force=1

Miessler, D. (s.f.). *Cross-site Scripting Explicación*. Obtenido de https://danielmiessler.com/study/xss/

Mireyalex. (s.f.). *Internet como herramienta vital.* Obtenido de http://mireyalex.tripod.com/id16.html

Monografias.com. (27 de 7 de 2009). *Comercio electronico*. Obtenido de http://www.monografias.com/trabajos15/comercio-electronico/comercio-electronico.shtml

OpenCart. (s.f.). *OpenCart Sitio Oficial*. Obtenido de http://www.opencart.com/

Ordóñez, J. (18 de 06 de 2015). *5 plataformas para crear tu tienda online con exito*. Obtenido de Marketing 4 commerce: http://marketing4ecommerce.net/5-plataformas-para-crear-tu-tienda-online-con-exito/

OsCommerce. (s.f.). *OsCommerce Sitio Oficial*. Obtenido de https://www.oscommerce.com/

Pacheco, L. J. (s.f.). *Comercio electronico*. Obtenido de Seguridad en el comercio electronico: http://www.geocities.ws/leandrojpachec/hwct/T4/comercio_electronico.html

Piatic. (2010). *Sistemas de pago en el comercio electrónico*. Obtenido de http://www.piatic.net/piatic/contenidos/actuaciones/fichas-divulgativas/Sistemas-de-pago-en-el-comercio-electronico

Portaley. (15 de 0 de 2013). *Seguridad en comercio electronico, metodos de pago seguros*. Obtenido de http://portaley.com/2013/10/seguridad-en-comercio-electronico-metodos-de-pago-seguros/

PrestaShop. (s.f.). *PrestaShop Sitio Oficial*. Obtenido de https://www.prestashop.com/es/

Raspaloks. (24 de 5 de 2012). *Comercio electronico.* Obtenido de http://comercio-mahra.blogspot.com/

Rodriguez, E. M. (9 de 12 de 2013). *Ventajas y desventajas del comercio electronico: El punto del vista del cliente*. Obtenido de http://www.actualidadecommerce.com/ventajas-y-desventajas-del-ecommerce-el-punto-del-vista-del-cliente/

Santiago, H. J. (3 de 2004). *Seguridad en el comercio electronico.* Obtenido de http://www.javeriana.edu.co/biblos/tesis/derecho/dere6/DEFINITIVA/TESIS24.pdf

SkynetCusco. (s.f.). *Ventajas y desventajas del comercio electronico*. Obtenido de http://www.portal.skynetcusco.com/index.php/comercio-electronico/comercio-electronico8/534-ventajas-y-desventajas-del-comercio-electronico-

Slideshare. (22 de 04 de 2012). *Problemas de seguridad al realizar comercio electronico*. Obtenido de http://es.slideshare.net/Ditsy/problemas-de-seguridad-al-realizar-comercio-electrnico-12637637?qid=47df6834-ae78-42b0-ba43-4de1d333e1b8&v=default&b=&from_search=2

Slideshare. (s.f.). *Seguridad en el comercio electronico.* Obtenido de http://es.slideshare.net/ramso24/seguridad-en-el-comercio-electrnico-14661044

7 ANEXOS.

7.1 Cuestionario de unidades teóricas.

Apartado 1: Comercio Electrónico.

1. ¿Qué es comercio electrónico?
2. ¿Cuáles son las Características del comercio electrónico?
3. ¿En qué consiste el comercio electrónico?
4. Mencione las ventajas del comercio electrónico.
5. Mencione las desventajas del comercio electrónico.
6. Mencione las subcategorías del comercio electrónico.
7. ¿Qué sujetos intervienen en el comercio electrónico?
8. Mencione los tipos de comercio electrónico según los participantes o sujetos que intervienen.
9. ¿Cuál es el impacto económico del comercio electrónico?
10. Mencione las arquitecturas del comercio electrónico.
11. Explique la arquitectura Open Trading Protocolo (OTP).

Apartado 2: Seguridad

1. ¿Para qué sirve la autenticación?
2. ¿Qué es Criptografía?
3. Mencione las características de la Criptografía.
4. Mencione los algoritmos criptográficos.
5. Expliqué en que consiste el protocolo SSL.
6. Explique en qué consiste el protocolo SET.
7. ¿Qué son los certificados digitales?
8. ¿Qué es la firma digital?
9. Menciona las características de la firma digital.

10. Es el proceso de transformar texto simple o datos en texto encriptado que no puede ser leído por nadie más que el receptor. ¿A qué termino se refiere?

11. Mencione 5 tipos de ataque en el comercio electrónico y explique uno de ellos.
12. Menciona las partes de una firma digital.

Apartado 3: Sistemas de pago.

1. Menciones y explique los tipos de tarjetas.

2. ¿Qué formas de pago Off line se utilizan?

3. ¿Qué características deben de tener los medios de pago?

4. Definir y distinguir los distintos medios de pago que se puede realizar en una transacción electrónica.

5. Defina ejemplos donde se utilizan los medios de pago.

6. ¿Qué es un sistema de pago?

7. ¿Qué es una transferencia bancaria?

8. Mencionar la métrica que deben de tener los medios de pago.

9. ¿Cómo funciona PayPal?

10. Mencione los pasos para realizar una compra segura.

Apartado 4: Plataformas del comercio electrónico.

1. Menciones algunas de las plataformas más reconocidas en el comercio electrónico.

2. ¿Qué es una plataforma web?

3. ¿Qué tecnologías son implementadas en las plataformas web?

4. ¿Qué es Bootstrap y que plataformas utilizan este framework?

5. Explique en qué consiste Crossdomain.xml.

6. ¿Cuál es la función del archivo htcaccess?

7. ¿Cuáles son las características que presenta Magento?

8. ¿Cuál es el punto débil de OsCommerce?

9. ¿Qué requisitos del sistema son necesarios para la instalación de las plataformas?

10. Mencione los errores más comunes de las plataformas del comercio electrónico.

Apartado 5: Aspectos legales.

1. ¿En qué consiste la contratación electrónica?
2. ¿Cuáles son las obligaciones de la contratación electrónica?
3. ¿En qué consiste la protección de datos?
4. ¿Qué es la defensa de los consumidores?
5. ¿Qué son los términos y condiciones?
6. ¿Qué es la propiedad intelectual?
7. Mencione y explique las leyes del Envío de Comunicaciones Comerciales.
8. ¿En qué consiste la propiedad intelectual?

Apartado 6: Extensiones.

1. Menciones las principales extensiones del comercio electrónico.
2. ¿Cuáles son las diferencias entre S-Commerce y F-Commerce?
3. ¿A qué se refiere el termino M-Commerce?
4. Menciones tres ventajas y tres desventajas del M-Commerce.
5. Menciones las principales limitaciones del M-Commerce.
6. ¿Qué es geolocalización?
7. Analizar brevemente los principales dispositivos del M-Commerce.
8. Mencionar y explicar los tipos de S-Commerce.
9. Mencionar las herramientas del F-Commerce.
10. ¿En qué consiste las listas compartidas de S-Commerce?

7.2 Glosario.

Addons: es una aplicación (o programa informático) que se relaciona con otra para agregarle una función nueva y generalmente muy específica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de la interfaz de programación de aplicaciones.

Applet Java: es un programa que puede incrustarse en un documento HTML, es decir en una página web. Cuando un navegador carga una página web que contiene un applet, este se descarga en el navegador web y comienza a ejecutarse. Esto permite crear programas que cualquier usuario puede ejecutar con tan solo cargar la página web en su navegador.

Arpanet: las siglas de Advanced Research Projects Agency Network, es decir, la Red de la Agencia de Proyectos de Investigación Avanzada, organismo conocido ahora como Agencia de Proyectos de Investigación Avanzados de Defensa.

Bancarrota: Cese de una actividad comercial al no poder hacer frente a las obligaciones de pago y no alcanzar el activo a cubrir el pasivo.

Campañas adhoc: trabaja desde el prisma de las Clínicas jurídicas, aunando el conocimiento científico de los profesionales docentes vinculados con la Asociación (Doctores y Profesores universitarios), junto con el saber y dinamismo propio de los estudiantes que colaboran con nosotros.

Código QR: Un código QR (quick response code, «código de respuesta rápida») es un módulo útil para almacenar información en una matriz de puntos o un código de barras bidimensional creado en 1994 por la compañía japonesa Denso Wave, subsidiaria de Toyota. Se caracteriza por los tres cuadrados que se encuentran en las esquinas y que permiten detectar la posición del código al lector. La sigla «QR» viene de la frase inglesa «Quick Response» («Respuesta Rápida» en español), pues los creadores (un equipo de dos personas en Denso Wave, dirigido por Masahiro Hara) tenían como objetivo que el código permitiera que su contenido se leyera a alta velocidad.

Core Competencies: es un concepto en la teoría de gestión presentado por, CK Prahalad y Gary Hamel. Se puede definir como "una combinación armonizada de múltiples recursos y habilidades que distinguen a una empresa en el mercado".

Cgi: Interfaz de entrada común (en inglés Common Gateway Interface, abreviado CGI) es una importante tecnología de la World Wide Web que permite a un cliente (navegador web) solicitar datos de un programa ejecutado en un servidor web. CGI especifica un estándar para transferir datos entre el cliente y el programa. Es un mecanismo de comunicación entre el servidor web y una aplicación externa cuyo resultado final de la ejecución son objetos MIME. Las aplicaciones que se ejecutan en el servidor reciben el nombre de CGIs.

client_side: hace referencia a las operaciones que son realizadas por el cliente en una relación cliente/servidor. Su recíproco es server-side. Generalmente un cliente es una aplicación de computadora (ej.: un navegador web), que se ejecuta en la computadora local del usuario o estación de trabajo, y se conecta a un servidor.

Criptodivisas: Una criptodivisas es un medio digital de intercambio que nació en 2009 de la mano del creador o creadores de la criptodivisas más empleada, el bitcoin, que emplearon el pseudónimo Satoshi Nakamoto.

cXML: cXML (comercio eXtensible Markup Language) es un protocolo, creado por Ariba en 1999, destinado a la comunicación de los documentos de negocio entre adquisiciones, aplicaciones de comercio electrónico concentradores y proveedores. cXML se basa en XML y proporciona formales esquemas XML para las transacciones comerciales estándar, lo que permite a los programas modificar y validar documentos sin previo conocimiento de su forma. El protocolo no incluye toda la amplitud de las interacciones algunas partes deseen comunicarse. Sin embargo, se puede ampliar a través del uso de elementos extrínsecos y dominios recién definidos para diversos identificadores. Esta expansión es el límite de configuraciones de punto a punto necesarias para la comunicación.

DAKOSY: Como uno de los líderes de TI y servicios de software para proveedores de la industria del transporte, DAKOSY AG, con sede en Hamburgo, ha estado proporcionando servicios de comunicación del puerto, así como soluciones para el transporte de carga internacional y despacho de aduanas desde 1982. DAKOSY se estableció como el Sistema de Comunidad Portuaria para el Puerto de Hamburgo por miembros de la industria de Seaport. DAKOSY es a día de hoy una empresa privada 100%, cada uno un tercio propiedad de Transitarios, agentes de revestimiento / líneas navieras y operadores de terminales. Como centro proveedor del sistema y la limpieza DAKOSY ofrece una amplia gama de información y de datos de servicios de centro para sus clientes. Más de 2.000 empresas de toda Europa utilizan los centros de datos del estado de la técnica DAKOSY AG's para su comunicación empresarial electrónica. Estas empresas incluyen casas de fama mundial de comercio, empresas de marca, las empresas industriales, transitarios, empresas navieras, agentes de revestimiento, transportistas (mar y aire), compañías de transporte y diversas autoridades (aduanas, policía portuaria y así sucesivamente).

Desgeografización: no existen las fronteras entre los países, todos podemos contratar, lo cual genera una mayor demanda de los bienes o servicios y la reducción de los precios, de los mismos.

Distribución de copias en celuloide: Los distribuidores, generalmente empresas independientes de las productoras, compran los derechos de exhibición en salas de cine, o para su emisión por televisión, y venden los derechos de la película a los exhibidores (individuales o cadenas de exhibidores), cadenas de televisión, videoclubes u otros establecimientos donde se vendan las cintas de vídeo. Son también encargados de la publicidad y de la promoción de las películas, de hacer las copias necesarias para la exhibición y de controlar las cifras de ingresos y gastos. El productor cede al distribuidor un porcentaje de los ingresos de la película que por lo común alcanza el 50%. Además, el distribuidor deduce de los beneficios del productor el importe de las copias de la película Internetting Project. En 1973 la agencia de proyectos de investigación (DARPA) inicio el programa de investigación para investigar las técnicas y tecnologías de interconexión de redes de paquetes de varios tipos. El objetivo era desarrollar protocolos de comunicación que permitan a los equipos en red comunicarse de forma transparente a través de múltiples redes de paquetes, vinculados. Esto se llama internetting Project y el sistema de redes que surgieron de la investigación que se conocía como internet. El sistema de protocolos que

se desarrolló en el trascurso de este esfuerzo de investigación se hizo conocido como el TCP-IP protocol suite, después de los dos protocolos iniciales desarrollados: transmisión control protocolo (TCP) y el protocolo de internet (ip).

dot-com boom y dot-com bust: se refiere a la burbuja de inversión especulativa que se formó en torno a las empresas de Internet entre 1995 y 2000. Los altos precios de Internet de nueva creación animan a los inversores a verter más dinero en cualquier empresa con un ".com" o una "e-algo "en su plan de negocios. Este exceso de capital animó a las empresas de Internet a formar, a menudo con muy poco de planificación, con el fin de entrar en una parte del dinero fácil que estaba disponible en el momento.

Enforcement: Organismo de seguridad del estado.

eMule: es un programa para intercambio de archivos con sistema P2P utilizando el protocolo eDonkey 2000 y la red Kad, publicado como software libre para sistemas Microsoft Windows. Está escrito en C++. Creado en un principio como alternativa al programa eDonkey.

Gnutella: es un proyecto de software distribuido para crear un protocolo de red de distribución de archivos entre pares, sin un servidor central.

Hash: Se llaman funciones hash criptográficas a aquellas funciones hash que se utilizan en el área de la criptografía. Este tipo de funciones se caracterizan por cumplir propiedades que las hacen idóneas para su uso en sistemas que confían en la criptografía para dotarse de seguridad. Estas propiedades las hacen resistentes frente ataques maliciosos que intentan romper esa seguridad.

Hotlink: Indica que alguien está usando un enlace a una imagen que está archivada en otro sitio web en lugar de guardar una copia de la imagen en el sitio web en el que se mostrará la imagen. Por ejemplo, en lugar de guardar una imagen .gif y cargarla en su propio sitio web, la persona usa un enlace de tipo absoluto hacia la imagen, semejante a http://sitioweb.com/imagen.gif, en lugar de un enlace de tipo relativo.

Intellectual_capital: es el conocimiento intelectual de esa organización, la información intangible (que no es visible, y, por tanto, no está recogida en ninguna parte) que posee y que puede producir valor.

Internetting Project: es un esfuerzo intelectual de colaboración entre varias instituciones académicas para estudiar el impacto social, económico y político de la Internet.

Kazaa: fue una aplicación para el intercambio de archivos entre pares que utiliza el protocolo FastTrack. Kazaa fue comúnmente utilizado para intercambiar música (principalmente en formato mp3) y películas (en formato DivX). Su popularidad declinó conforme Sharman Networks y sus socios fueron objeto de demandas relacionadas con derechos de autor. Después Atrinsic, Inc compró la marca Kazaa para relanzarlo como un servicio de suscripción legal, eliminando el Software Kazaa manejando todo vía web. Desde agosto de 2012, el sitio web de Kazaa fue desactivado definitivamente.

LSSICE y la LOPD: Con la entrada en vigor de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE, Ley 34/2002 de 11 de julio en vigor desde

octubre de 2003) y la Ley Orgánica de Protección de Datos (LOPD, Ley 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal), es que los propietarios de páginas Web o portales comerciales deben cumplir con una serie de requisitos específicos para no ser sancionados por el organismo regulador: la Agencia Española de Protección de Datos (AEPD). Las consecuencias de su incumplimiento conllevan a sanciones ya no sólo son administrativas, sino que además de ellas se pueden derivar responsabilidades civiles, penales y laborales.

Metcalfe: el valor de una red de comunicaciones aumenta proporcionalmente al cuadrado del número de usuarios del sistema (n2). Formulada por primera vez en 1976 por Robert Metcalfe en relación con Ethernet, la ley de Metcalfe explica muchos de los efectos de red de las tecnologías y redes de comunicación, como Internet o la World Wide Web.

Monedas fiduciarias: sistema monetario en el cual el valor de la moneda está establecido por declaración y no está respaldado por un activo fijo, como por ejemplo el Oro. Actualmente, la mayoría de las monedas mundiales son monedas fiduciarias. Comparar con Estándar de Oro.

Paradigm_change: Los cambios de paradigma tienden a aparecer en respuesta a la acumulación de anomalías críticos, así como la propuesta de una nueva teoría con el poder de abarcar tanto los datos más antiguos pertinentes y explicar las anomalías relevantes. Nuevos paradigmas tienden a ser más dramático en las ciencias que parecen ser estable y maduro, como en la física a finales del siglo 19. En ese momento, una declaración atribuye generalmente al físico Lord Kelvin famoso afirmó, "No hay nada nuevo por descubrir en la física ahora. Todo lo que queda es más y más preciso de medición."

Pymes: La sigla "PYME" corresponde a "pequeñas y medianas empresas" tal como se definen en la legislación de la UE.

Retail: es un término de la lengua inglesa que se emplea para nombrar a la venta minorista. La comercialización de productos al por menor:

RosettaNet: es una organización sin fines de lucro consorcio destinado a establecer estándares procesos para la puesta en común de los negocios de información (B2B). RosettaNet es un consorcio de las principales de informática y electrónica de consumo, componentes electrónicos, fabricación de semiconductores, telecomunicaciones y logística empresas que trabajan para crear e implementar, normas de proceso abierto e-business de toda la industria. Estas normas forman un lenguaje de e-business común, alinear los procesos entre los socios de cadena de suministro a nivel mundial.

Server Side: es un conjunto de directivas que se escriben en las páginas HTML y que se evalúan en el servidor web cuando se solicita la página HTML. SSI permite añadir contenido generado de forma dinámica a las páginas web, sin tener que programar toda la página mediante CGI, ASP, PHP o alguna tecnología similar.

Sistema de clearing bancario: Tanto para la banca como para las finanzas, el Clearing denota todas las actividades desde el momento en que se haga el compromiso de una transacción hasta que sea establecida. El Clearing es necesario debido a que la velocidad

de las operaciones es mucho más rápida que el tiempo para completar la transacción objetivamente hablando.

Supermercado mayorista Amigazo: A mediados de los años 1980 esta empresa desarrolló un sistema para procesar órdenes de pedido electrónicas, por el cual los clientes de esta empresa emitían ordenes de pedido desde sus empresas y esta era enviada en forma electrónica. Esta implementación trajo importantes beneficios a Amigazo, ya que se eliminaron gran parte de errores de entregas y se redujeron los tiempos de procesamiento de dichas órdenes. El beneficio fue suficiente como para que la empresa Amigazo, instale un equipo a sus clientes habituales.

SWIFT: Swift es un lenguaje de programación multiparadigma creado por Apple enfocado en el desarrollo de aplicaciones para iOS y Mac OS X. Fue presentado en WWDC 20142 y está diseñado para integrarse con los Frameworks Cocoa y Cocoa Touch, puede usar cualquier biblioteca programada en Objective-C y llamar a funciones de C. También es posible desarrollar código en Swift compatible con Objective-C bajo ciertas condiciones. Swift tiene la intención ser un lenguaje seguro, de desarrollo rápido y conciso.

Toolbar: es un componente de la interfaz gráfica de usuario, mostrada usualmente en pantalla a modo de fila, columna, o bloque, que contiene iconos o botones, que, al ser presionados, activan ciertas funciones de una aplicación. Muchas de las aplicaciones y sistemas operativos desarrollados permiten a los usuarios personalizar las barras de herramientas y ajustarlas a sus necesidades.

Token: Un token de seguridad (también token de autenticación o token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación. Los tokens electrónicos tienen un tamaño pequeño que permiten ser llevados cómodamente en el bolsillo o la cartera y su diseño permite llevarlos en un llavero. Los tokens electrónicos se usan para almacenar claves criptográficas como firmas digitales o datos biométricos, como las huellas digitales.

Value_chain: es un modelo teórico que permite describir el desarrollo de las actividades de una organización empresarial generando valor al cliente final, descrito y popularizado por Michael Porter en su obra Competitive Advantage: Creating and Sustaining Superior Performance (1985).

Webcast: Un webcast es un diseño de transmisión a Internet donde transmite un medio en vivo similar a un programa de televisión o una emisora de radio. Las aplicaciones clientes de Webcast permiten que un usuario conecte con un servidor, que está distribuyendo (lo cual se diría "which is webcasting (...)" en inglés) el webcast.

xCBL: xCBL es una colección de XML especificaciones (tanto DTD y XML Schema) para su uso en el comercio electrónico. Fue creado por Commerce One Inc. y se mantiene por Perfect Comercio. xCBL se llamaba originalmente Biblioteca Common Business (CBL). La estandarización xCBL comenzó en 1997. Esto llevó a la creación de xCBL 2.0 que cubrió 12 especificaciones de los documentos de negocio diferente, destinado principalmente para la comunicación electrónica de documentos en -business-to-business (B2B) la contratación a través de Internet. xCBL 2.0 se basó principalmente en la existente Intercambio

Electrónico de Datos (EDI) normas e introdujeron el esquema de XML orientada a objetos (SOX) biblioteca de esquemas para la validación XML.