

Sistema de información para empresas (2019-2020)
GRADO EN INGENIERÍA INFORMÁTICA
UNIVERSIDAD DE GRANADA

Tema 4

Comercio electrónico



**UNIVERSIDAD
DE GRANADA**

Antonio Jesús Heredia Castillo

26 de mayo de 2020

Índice

1. Tienda virtual	3
1.1. Comercio electrónico	3
1.2. Tienda virtual	4
2. Firma digital y e-factura	4
2.1. ¿En que se basa la firma digital?	5
2.2. ¿Qué son los certificados digitales?	6
2.3. Factura electrónica	6
3. Seguridad técnica de e-pagos	7
3.1. Transacciones electrónicas seguras	8
4. Internacionalización (soporte de múltiples lenguajes)	9
5. Herramientas para la creación de tiendas virtuales	10
6. Marco legal del comercio electrónico	11
6.1. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico	11
6.2. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal	13

1. Tienda virtual

1.1. Comercio electronico

El **comercio electrónico** (e-commerce) consiste en la **compra y venta de productos** o servicios a través de **medios electrónicos**, tales como internet. En un **inicio solo** se aplicaba a la realización de transacciones **mediante medios electrónicos** aunque al final se ha popularizando como forma de pago por medios electrónicos.

Entre empresas se denomina **B2B** (business-to-business) que puede estar **abierto a cualquiera** que esté interesado, **o estar limitado a participantes** específicos pre-calificados.

Las características únicas son:

- ▶ **Ubicuidad** Debe ser independiente de su ubicación temporal y geográfica.
- ▶ **Alcance global:** Se habilita el comercio a través de los límites culturales y nacionales sin problemas ni modificaciones.
- ▶ **Estándares universales:** Hay un conjunto de estándares de medios técnicos en todo el mundo.
- ▶ **Riqueza:** es posible transmitir mensajes de video, audio y texto.
- ▶ **Interactividad:** funciona a través de la interacción con el usuario
- ▶ **Densidad de la información:** reduce los costos de la información y eleva la calidad.
- ▶ **Adecuación:** permite entregar mensajes personalizados a individuos y grupos.
- ▶ **Tecnología social:** generación de contenido por parte del usuario y redes sociales.

Todas las aplicaciones se basan en una **infraestructura**. Esta puede ser **de servicios comerciales comunes, de red, de los mensajes y de distribución de información, de interfaces o de plataformas y lenguajes multimedia para la infraestructura pública de red.**

Las empresas **participan** en cuatro categorías básicas, entre **organizaciones y clientes** (B2C), entre **organizaciones y organizaciones** (B2B), dentro de una **misma organización** (B2E) y entre **organizaciones y administración** (B2A o B2G).

Existen compañías que utilizan el comercio electrónico para **muchos aspectos**. Alguno de estos pueden ser la creación de nuevas formas de **marketing**, acceso **interactivo con los catálogos**, **venta** directa o **soporte técnico** ininterrumpido.

También tiene diferentes **beneficios** como la **reducción de trabajo administrativo**, **transacciones** mas **rápidas**, **acceso** más **fácil** a la **información** y **reducción** de la necesidad de **rescribir** la **información** en los sistemas de información.

El **libro blanco del comercio electrónico** es una publicación coordinada por la Asociación Española de la Economía Digital. En esta publicación se intenta plasmar un **manual práctico para vender productos o servicios** en internet. **Reúne datos cuantitativos**, así como **ejemplos**, **referencias** y **herramientas de utilidad** para cualquier empresa que esté o quiera estar presente en el comercio electrónico.

1.2. Tienda virtual

Es un espacio para vender producto o servicios a terceros en internet. Es como el convencional pero como medio para realizar las transacciones la web. Se consideran **legalmente** como **ventas a distancia**, **disponiendo** el comprador de una serie de **derechos** en la **contratación** de estos servicios o productos a distancia. Ofrece al cliente **rapidez** en la compra y posibilidad de hacerlo desde cualquier lugar.

Se suele **pagar** mediante **tarjeta de crédito** y se **envían** los productos por **agencia de transporte** (aunque existen variaciones). La mayoría de tiendas **requieren** la **creación de un usuario**. Es muy **importante** hacer compras en línea solo en **sitios reconocidos y con buena reputación**, debido a las amenazas existentes, además de usar una **conexión segura**.

Hay cinco aspectos a considerar para tener éxito con una tienda online:

- ▶ **Diseño web**: hay que tener una web bien construida, respete los estándares y sea cómoda para el cliente.
- ▶ **Política de devolución de productos**: Hay que articular como podrán los usuarios devolver artículos que no estén satisfechos.
- ▶ **Generar confianza en el usuario**
- ▶ **Canal de distribución**: Cuanto más consigamos automatizar las tareas más peticiones podremos atender.
- ▶ **Política de precios**: conseguir automatizar lo máximo posible el proceso logístico nos permite ofrecer precios que no están al alcance del comercio tradicional.

2. Firma digital y e-factura

Se entiende como firma digital una **secuencia de datos electrónicos** que se obtiene aplicando a un mensaje determinado un algoritmo de cifrado asimétrico y que **equivale** funcionalmente a la **firma autógrafa** en orden a la

identificación del autor.

Para que dos personas puedan intercambiar entre ellos mensajes electrónicos fiables se debe cumplir los siguiente requisitos.

Identidad, que se pueda atribuir de forma indubitada a una determinada persona.

Integridad, que el mensaje recibido sea igual que al emitido.

No repudiación, que el emisor no pueda negar que no ha enviado el mensaje. **Confidencialidad**: implica que el mensaje no haya podido ser leído por terceros.

2.1. ¿En que se basa la firma digital?

La **criptografía** es la **base** de la firma digital. Se suelen combinar **dos técnicas** distintas, que son la **criptografía asimétrica** (de clave publica) y las **funciones hash**. Entendemos criptografía como las **técnicas** o algoritmos que nos permite **cifrar y descifrar mensajes**. Podemos entender dos tipos de sistemas criptográficos, simétricos o asimétricos.

En los **simétricos** las dos personas que van intercambiar mensajes utilizan la **misma clave para cifrar y descifrar** el mensaje. Tienen el **inconveniente** de que hay que **intercambiar previamente la clave** por un medio seguro, además existe la necesidad de que exista **una clave para cada dos personas**. Esto hace que el cifrado simétrico **no sean aptos para redes abiertas** como internet. Los sistemas **asimétricos** se basan en el cifrado mediante la utilización de **un par de claves diferentes** (privada y pública). Una de sus características es que la **clave privada es secreta** y solo lo conoce el que cifra el mensaje, **la clave pública** puede ser conocida por **cualquiera**. Un dato importante es que **a partir de la clave publica no se puede deducir** la clave **privada**. El sistema asimétrico mas conocido es **RSA**.

Los mensajes que se intercambian pueden tener un **gran tamaño**, hecho que **dificulta** el proceso de **cifrado**. Por ello **no se cifra** el mensaje **entero**, sino un **resumen** del mismo obtenido **aplicando** al mensaje una **función hash**. Generalmente tienen un tamaño de **160 bits**. **Este resumen** de dimensión fija es el que **se cifrará** utilizando la clave privada del emisor del mensaje. Finalmente el proceso es **importante que se pueda saber** y establecer la **fecha exacta** en la que se ha enviado. Para ello se usan **sellos temporales** que es una función que se atribuye generalmente a los **prestadores de servicios de certificación** mediante la cual se fija la fecha de los mensajes.

Cambien es necesario en ocasiones **garantizar la confidencialidad**, para ello se usa también el cifrado asimétrico, pero en este caso se **cifra** con la clave **publica** y se **descifra** usando la clave **privada**.

Estas claves **no pueden ser creadas por cualquier individuo**. Pero si cualquier persona puede acudir a un **“Prestador de servicios de Certificación”** para obtener el certificado digital.

2.2. ¿Qué son los certificados digitales?

Un certificado digital es un archivo electrónico que tiene un tamaño máximo de 2 Kbytes y que contiene los datos de identificación personal de A (emisor de los mensajes), la clave pública de A y la firma privada del propio Prestador de Servicios de Certificación. Ese archivo electrónico es cifrado por la entidad Prestadora de Servicios de Certificación con la clave privada de ésta.

Estos certificados digitales tienen una duración determinada, pero pueden ser renovados. Gracias al certificado digital, el par de claves obtenido por una persona estará siempre vinculado a una determinada identidad personal.

Para obtener una firma digital lo primero que hay que hacer es dirigirse a una empresa que tenga carácter de prestador de servicios de certificación y solicitar a ellos el par de claves y el certificado digital. Ellos comprobarán nuestra identidad y el prestador de servicios crea el par de claves y genera el certificado digital. Nos entregaran una tarjeta donde esta grabado tanto el par de claves como el certificado digital. Con esa tarjeta y un lector, podré utilizar la información grabada en ella.

2.3. Factura electrónica

La facturación electrónica es un equivalente funcional de la factura en papel y consiste en la transmisión de las facturas o documentos análogos entre emisor y receptor por medios electrónicos (ficheros informáticos) y telemáticos (de un ordenador a otro), firmados digitalmente con certificados reconocidos.

Los campos obligatorios de una factura según el artículo 6 del RD 1496/2003 son:

- Núm. Factura
- Fecha expedición
- Razón Social emisor y receptor
- NIF emisor y receptor
- Domicilio emisor y receptor
- Descripción de las operaciones (base imponible)
- Tipo impositivo
- Cuota tributaria
- Fecha prestación del servicio (si distinta a expedición)

3. Seguridad técnica de e-pagos

Un sistema de pago electrónico (EPS) es un sistema de pago que facilita la aceptación de pagos electrónicos para las transacciones en línea a través de internet. Los EPS realizan la transferencia del dinero entre compradores y vendedores en una acción de compra-venta electrónica a través de una entidad financiera autorizada por ambos. Como ejemplos de sistemas de pago electrónico nos encontramos las pasarelas de pago o TPV (terminal de punto de venta) virtual para el pago con tarjeta, los sistemas de monedero electrónico y los sistemas que se conectan directamente con la banca electrónica del usuario.

En el pago con tarjeta, la pasarela de pago valida la tarjeta y organiza la transferencia de dinero.

En el monedero electrónico, se almacena el dinero del comprador en formato electrónico y se transfiere al sistema durante el pago.

El pago a través de banca electrónica enlaza un número de operación o venta del comercio a la cuenta del cliente. Esto reduce el riesgo de fraude.

Entre los inconvenientes es que a la gente le incomoda comprar a través de Internet ya que no están seguros de que se garantice la seguridad. Además de que la gente quiere garantizar su anonimato.

Podemos encontrar diversos sistemas de pago electrónicos:

- ▶ **Cajeros electrónicos:** se trata de sistemas en los que los clientes abren cuentas en unas entidades de Internet.
- ▶ **Dinero electrónico:** Es difícil de definir en un medio tan extenso. Pero a todos los efectos se define como aquel dinero creado, cambiado y gastado de forma electrónica.
- ▶ **Cheques electrónicos:** Un sistema de cheques puede ser considerado como un compromiso entre un sistema de tarjetas de crédito y uno de micro-pagos o dinero electrónico (anónimo).
- ▶ **Tarjetas de Crédito**

Una pasarela de pago es un proveedor de servicios de aplicación de comercio electrónico que autoriza pagos a negocios electrónicos. Equivalente a un TPV pero online. Estas pasarelas cifran información sensible y facilitan la transferencia de información. Además realiza una serie de tareas para procesar una transacción, de manera transparente para el comprador. El funcionamiento es el siguiente. Cuando el cliente realiza el pedido ingresa los detalles de su tarjeta de crédito, si es a través de un sitio web se cifra mediante SSL. El vendedor entonces reenvía los detalles de la transacción a su pasarela de pago. Esta recibe la información y la reenvía al banco, el banco a su vez reenvía la información al banco emisor de la tarjeta de crédito y este recibe el pedido de autorización y ya aprueba o rechaza la transacción.

Un **TPV** (terminal punto de venta) hace referencia al dispositivo y tecnologías que ayudan en la tarea de gestión de un establecimiento de venta al público para que pueda contar con sistemas informáticos especializados mediante una interfaz accesible para los vendedores. El nombre **datáfono**, erróneamente llamado TPV, se da al equipo que se instala en los establecimientos comerciales.

La **tarjeta monedero**, o monedero electrónico, es el sistema de micropagos multipropósito más eficiente. Sirve para aquellas transacciones de bajo monto y alto volumen. La tarjeta monedero contiene un **chip** electrónico que se recarga con dinero y permite pagar productos y servicios deslizando la tarjeta en el lector cuyo importe exacto se descargará o acreditará del chip.

3.1. Transacciones electrónicas seguras

Transacciones Electrónicas Seguras (SET) es un protocolo estandarizado, diseñado para salvaguardar las compras pagadas con tarjeta a través de redes abiertas. SET nos ofrece:

- ▶ **Autenticación**: todas las partes pueden autenticarse mutuamente mediante certificados digitales.
- ▶ **Confidencialidad**: la información de pago se cifra para que no pueda ser espiada.
- ▶ **Integridad**: garantiza que la información intercambiada, como número de tarjeta, no podrá ser alterada.
- ▶ **Gestión del pago**: SET gestiona tareas asociadas a la actividad comercial de gran importancia.

En SET hay implicadas varias entidades, tales como el **banco emisor** que emite la tarjeta del cliente, el **banco adquirente** que establece una relación con el comerciante, **el titular de la tarjeta y el comerciante**. Además también no encontramos a la **pasarela de pagos** que es el mecanismo por el cual se procesan y autorizan las transacciones, **el procesador** que nos proporciona servicios adicionales y la **autoridad de certificación**.

Podemos explicar el funcionamiento de SET en diez pasos:

1. **Decisión de compra del cliente**. El cliente está navegando por el sitio web del comerciante y decide comprar un artículo
2. **Arranque del monedero**. El servidor del comerciante despierta a la aplicación monedero del cliente.
3. **El cliente comprueba el pedido** y transmite una orden de pago de vuelta al comerciante.
4. **El comerciante envía la petición de pago a su banco** todo ello convenientemente **cifrado y firmado**.

5. El banco adquiriente valida al cliente y al comerciante y obtiene una autorización del banco emisor del cliente
6. El emisor autoriza el pago.
7. El adquiriente envía al comerciante un testigo de transferencia de fondos.
8. El comerciante envía un recibo al monedero del cliente
9. El comerciante usa el testigo de transferencia de fondos para cobrar el importe de la transacción.
10. El dinero se descuenta de la cuenta del cliente

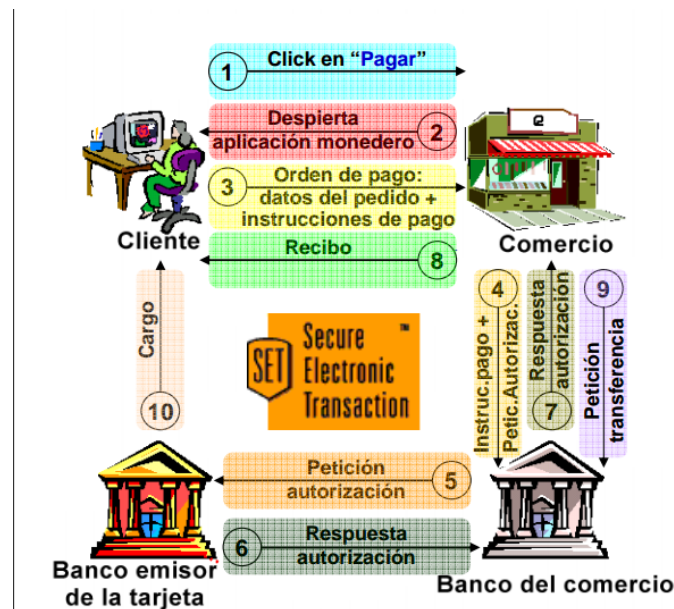


Figura 1: Los diez pasos de SET

4. Internacionalización (soporte de múltiples lenguajes)

Hay varios puntos que debe plantearse toda empresa (de internet o no) antes de lanzarse a conquistar el mundo:

- ▶ **Analizar el potencial:** exportador de tu empresa: Identificar los puntos fuertes y débiles de nuestro producto en los nuevos mercados.
- ▶ **Conocer el mercado:** Hemos de analizar los gustos y necesidades de cada país, sus canales de comercialización, datos históricos y las tendencias de futuro.

- **Analizar a la competencia:** Saber con quién tendrá que competir nuestro producto
- **Adaptar el producto o servicio a la demanda de cada mercado:** Debemos centrar los esfuerzos en aquellos productos o servicios que creamos que pueden tener mayor acogida e ir ampliando poco a poco.
- **Definir una estrategia de entrada en el país:** Buscar un socio local y crear una joint venture, buscar uno o varios distribuidores de tu sector, aliarse con prescriptores
- **Planificar tus recursos humanos:** A medio plazo siempre es necesario buscar socios o desarrollar talento en el país de destino.

Además tenemos que tener algunos detalles como tener una traducción impecable, comprar dominios locales, crear contenidos específicos para cada país, adaptarnos a la moneda y forma de pago, crear un plan de marketing online, medir y adaptarse a los resultados y hacer test.

5. Herramientas para la creación de tiendas virtuales

Para programas de comercio electrónico **B2C** tenemos dos grandes opciones. O se instala una aplicación desarrollada por terceros en servidor propio o se contrata una aplicación a modo de tienda llave en mano en alquiler, outsourcing, transfiriendo a empresas especializadas toda la gestión técnica de la tienda online. Actualmente hay aplicaciones de comercio electrónico B2C muy buenas tanto gratis como de pago que han permitido la creación de tiendas virtuales que están en producción desde hace muchos años. Aunque hay mucho software gratuito para tiendas online, vamos a ver los más conocidos.

Magento uno de los sistemas más utilizados. Tiene capacidades limitadas, pero aun así está muy por encima de sus competidores. Es un software que requiere conocimientos avanzados de informática y tiene un sistema de administración muy complejo. A favor tiene que es muy potente, es atractivo visualmente, implementación de módulos sencilla, funciones de SEO y URL amigables, entre otros. En contra es que tiene costes altos, personalización complicada, panel de control complicado y consume muchos recursos.

Opencart es de código abierto y basado en PHP. Solución muy buena si quieres tener un coste mínimo. A favor tenemos que tiene un diseño muy atractivo, implementar módulos es sencillo, puedes organizar productos por categorías, la curva de aprendizaje es muy baja, entre otros. En contra que la comunidad es pequeña y los temas son escasos.

OScommerce posiblemente ha sido el mejor gestor para tiendas online, pero ya se ha quedado atrasado. A favor tenemos que es multilingüaje, tiene una gran comunidad, muchos módulos, gestión avanzada de envíos e instalación

sencilla. En contra es que es un proyecto estancado y cualquier modificación necesita grandes conocimientos de PHP, muchos bugs e inseguridad.

Prestashop es de los mas nuevos y el favorito de muchos. Tiene una buena indexación y AJAX completamente integrado le da un aspecto muy actual. A favor tiene que es fácil y rapido de usar, coste económico multitud de módulos, optimización SEO, bajo consumo, permite códigos de barras, panel de control muy intuitivo, entre otros. En contra que el soporte es francés o inglés y como siempre esta en evolución no hay una versión estable.

En conclusión la hora de elegir un CMS o otro, debéis tener en cuenta lo amplio que va a ser el proyecto:

- ▶ Magento te aportará diseño y escalabilidad
- ▶ Opencart funcionalidad y sensatez
- ▶ Oscommerce te dará robustez y experiencia
- ▶ Prestashop facilidad y colaboración

6. Marco legal del comercio electrónico

Existen diferentes directivas relacionadas con el comercio electrónico. Las que marca el Parlamento Europeo son:

- ▶ Directiva 2002/65/CE del Parlamento Europeo y del Consejo, de 23 de septiembre relativa a la comercialización a distancia de servicios financieros destinados a los consumidores
- ▶ Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).
- ▶ Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).
- ▶ Directiva 98/84/CE del Parlamento Europeo y del Consejo de 20 de noviembre, relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso

6.1. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

Esta ley regula el régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica. Estos servicios serán

Todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

No tendrán la consideración de servicios de la sociedad de la información los servicios prestados por medio de telefonía vocal, fax o télex. Tampoco el intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan. Ni los servicios de radiodifusión televisiva o el teletexto televisivo y otros servicios equivalentes.

Las sanciones por el incumplimiento de la ley pueden ser: leves hasta 30.000€. Las graves desde 30.001€ hasta 150.000 € y las muy graves desde 150.0001€.

Los prestadores de servicios deben indicar en su página web el nombre o denominación social y datos de contacto, el número de inscripción que le corresponda en el registro mercantil, su NIF y el precio de los productos, indicando si incluye o no los impuestos aplicables, gastos de envío y cualquier otro dato que deba incluirse en cumplimiento de normas autonómicas aplicables.

Si se necesita una autorización administrativa, los datos de la misma, los identificativos del órgano encargado de su supervisión. Si es una profesión regulada los datos del colegio profesional y los datos del colegiado. Los códigos de conducta a los que este adherido.

Los prestadores de servicios informarán a los destinatarios de manera clara y completa la utilización y finalidad de sus datos que han sido recogidos. Además podrán rechazar el tratamiento de sus datos de forma sencilla y gratuita. Cuando exista tarificación adicional se deberá realizar el consentimiento previo, informando y expreso del usuario.

No tienen la obligación de supervisar los contenidos que alojan, transmiten o clasifican en un directorio de enlaces, pero deben colaborar con las autoridades públicas cuando se les requiera para interrumpir la prestación de un servicio o retirar un contenido, en cambio si pueden incurrir en responsabilidad si toman una participación activa en su elaboración o si conociendo la ilegalidad de un material, no actúan con rapidez para retirarlo.

Los proveedores de acceso a Internet están obligados a informar a sus usuarios sobre los medios técnicos que permiten la protección frente a las amenazas de seguridad en Internet y sobre las herramientas para el filtrado de contenidos no deseados. También deben informar sobre las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos.

6.2. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

Tiene por objeto **garantizar y proteger**, en lo que concierne al **tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas**, y especialmente de su honor, intimidad y privacidad personal y familiar.

Las sanciones tienen una **elevada cuantía**. Dichas sanciones van desde **900€ a 40.000€** las leves, las graves **40.0001€ a 300.000€** y las muy graves van desde **300.001€ a 600.000€**.

Los datos personales se **clasifican según su sensibilidad**, siendo obligatorio en todo caso la **declaración de los ficheros de datos protegidos** a la Agencia Española de Protección de Datos.

Hay que informar siempre de:

1. De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
2. Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
3. De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
4. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
5. De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante

Excepción: No será necesaria la comunicación en tres meses de dicha información si los datos han sido recogidos de “fuentes accesibles al público”

Existe consentimiento **inequívoco**, **tácito**, **expreso** (si hacen referencia a origen racial, salud y vida sexual) y el **expreso y por escrito** (relativos a ideología, afiliación sindical, religión y creencias).

Sólo podrán ser **comunicados** a un **tercero** **con** el previo **consentimiento del interesado**.

No será preciso si esta autorizado **por una ley**, son recogidos de **fuentes públicas**, por desarrollo, cumplimiento y **control jurídico** o cuando sea destinatario **el defensor del pueblo, ministerio fiscal o jueces**. Además de cuando sea cesiones entre administraciones públicas o sean datos **relativos a la salud y sea necesarios por urgencia**.

Sera **nulo** el consentimiento cuando la información que se facilite al interesado **no le permita conocer la finalidad a que destinarán los datos** se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar. El consentimiento **tiene un carácter de revocable**