Aspectos Legales del Comercio Electrónico

cecarm
negocio electrónico en la Región de Murcia

www.cecarm.com

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
Crecemos con Europa
GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
plan avanza
Región de Murcia
regiónde murcia SI
fundación integra

CECARM

- El proyecto Cecarm pretende impulsar y potenciar el desarrollo del Negocio Electrónico (Comercio Electrónico y Factura Electrónica) en la Región de Murcia
- Se crea al amparo del I Plan para el Desarrollo de la Sociedad de la Información (PDSI) en la Región de Murcia 2002 - 2004), "regióndemurciaSI"
  - Acción 3.8: Creación Servidor regional de Comercio Electrónico
- II PDSI 2005-2007
  - Acción 3.4: Servicios para la potenciación del Comercio Electrónico

CECARM

- Actualmente es una de las acciones enmarcadas en el III Plan para el Desarrollo de la Sociedad de la Información en la Región de Murcia (regióndemurciaSI 2008-2010), que impulsa la Dirección General de Telecomunicaciones y Sociedad de la Información y se engloba dentro del desarrollo del programa Pyme Digital del Plan Avanza en la Región de Murcia.

CECARM

- Financiación:
  - Consejería de Economía y Hacienda
  - Ministerio de Industria, Turismo y Comercio
  - Fondos Europeos para el Desarrollo Regional (FEDER)
- Coordinación:
  - Fundación Integra

CECARM: objetivos

- Ofrecer todo tipo de información de y para la comunidad de usuarios del Comercio Electrónico de la Región, tanto consumidores como empresarios.
- Facilitar la visibilidad de las empresas de la Región de Murcia en Internet e incentivar la incorporación de dichas empresas al negocio online.
- Sensibilizar y formar a empresarios, emprendedores, universitarios y formación profesional.
- Favorecer y potenciar el Comercio Electrónico en hogares y empresas.

CECARM: servicios y contenidos

Servicios

- Consultoría online
- Diagnóstico web
- Directorio Murcia Comercial
- Sello Cecarm
- Formación

Contenidos:

- Guías
- Artículos y monografías
- Entrevistas
- Casos de éxito
- Simuladores
- Normativa
- Compras seguras y derechos del consumidor
- Noticias y agenda

Medios:

- Consultores especialistas que asesoran a los usuarios
- Talleres formativos
- Portal www.cecarm.com

Aspectos legales del Comercio Electrónico

Comercio Electrónico. Luces y Sombras.

- **Inmenso potencial. Luz.**
  - España. Nueve (9) millones de internautas compradores. ONTSI 2007.
  - Crecimientos espectaculares de volumen de negocio.
  - Infraestructuras de Comunicaciones capaces de soportar grandes volúmenes de transacciones.
  - Soporte de las Administraciones Públicas.
  - Ámbito de actuación universal.
  - Marcos Normativos específicos.

Comercio Electrónico. Luces y Sombras.

- **Inmenso potencial. Luz.**
  - Mil trescientos millones (1.300.000.000) de personas conectadas a Internet a nivel universal.
  - Ciento noventa millones (190.000.000) de servidores web.
  - Doce mil millones (12.000.000.000) de páginas web publicadas .
  - Incorporación permanente.

Comercio Electrónico. Luces y Sombras.

- **Inmenso potencial. Luz.**
  - Sistema bancario implicado en el desarrollo a través de productos específicos (pasarelas de pago).
  - Administraciones Públicas liderando la Sociedad de la Información (Ley 11/2007, Ley 56/2007, etc.).
  - Fomento de la confianza en el medio.
  - Protección del consumidor.
  - Protección del establecimiento.

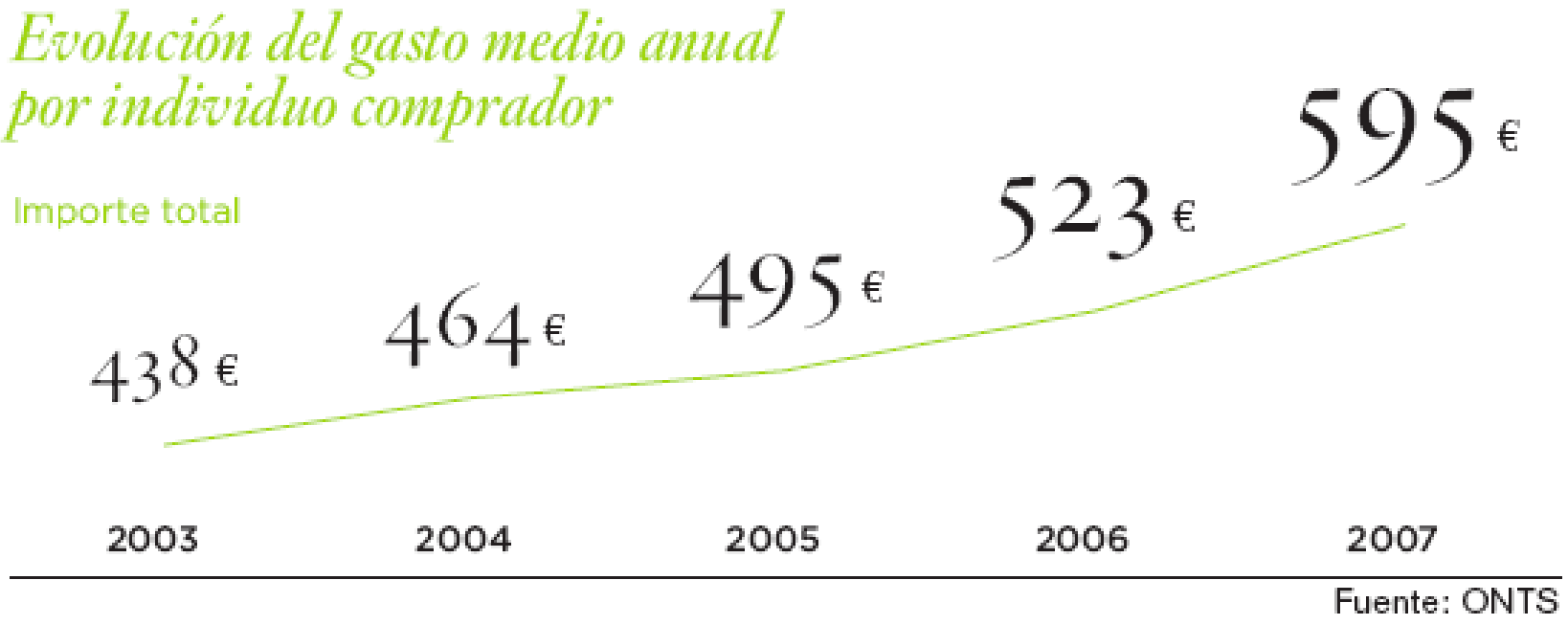
Comercio Electrónico. Luces y Sombras.

- **Lento desarrollo. Sombra.**
  - Escasos Portales Transaccionales.
  - Desconfianza.
  - Inercia.
  - Influencia de la "burbuja tecnológica".
  - ONTSI 2007 → 88% de las Empresas españolas no tienen presencia activa en Internet.
  - Relación desfavorable entre **Fomento** y Resultado.

Comercio Electrónico. Luces y Sombras.

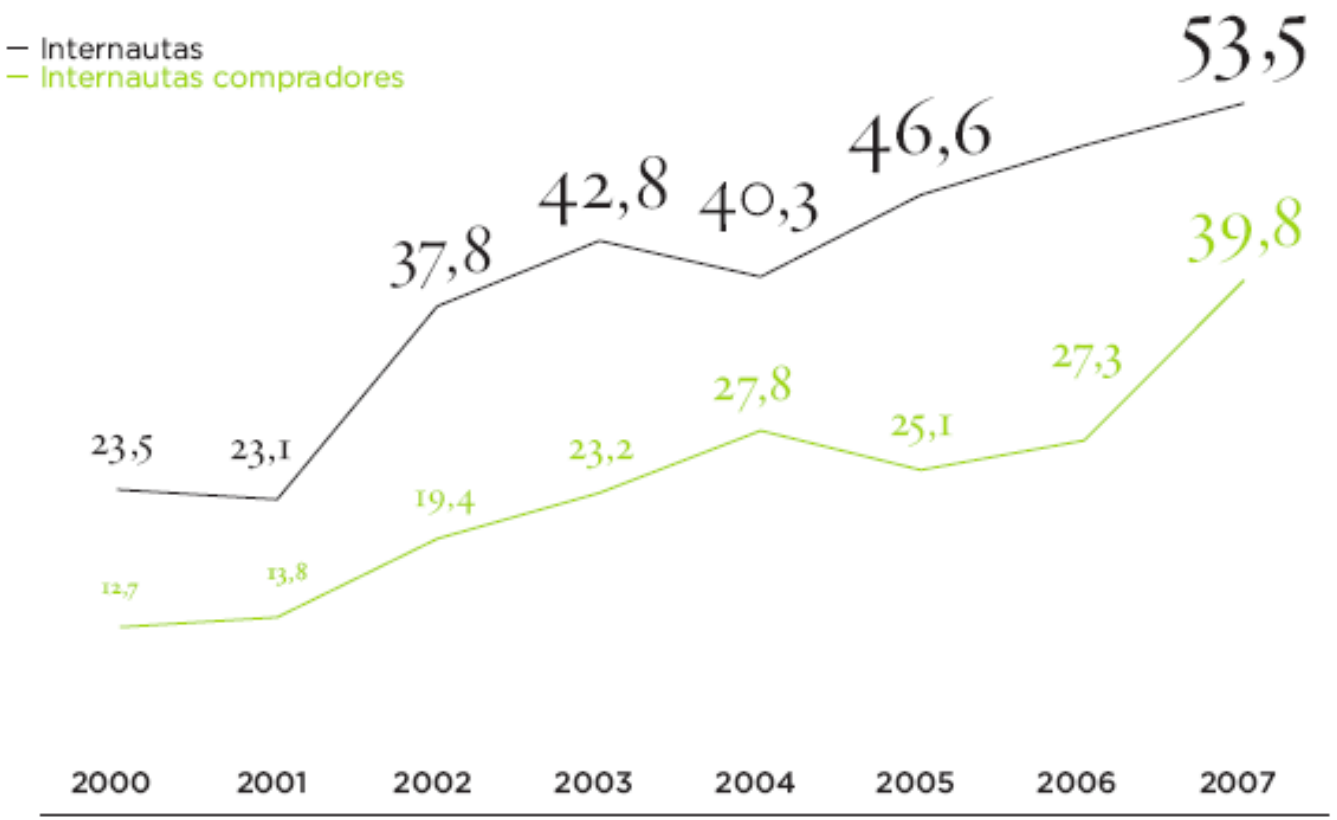
- **Lento desarrollo. Sombra.**
  - Pérdida de Mercados potenciales.
  - Fuga de negocio.
  - Obsolescencia del modelo.
  - Infrautilización de capacidades.
    - Técnicas.
    - Organizativas → Reingeniería de Procesos de Negocio.
  - Presencia en Planes Estratégicos.

Comercio Electrónico. Números. ONTSI.



Comercio Electrónico. Números. ONTSI.

Evolución en el porcentaje de internautas e internautas compradores

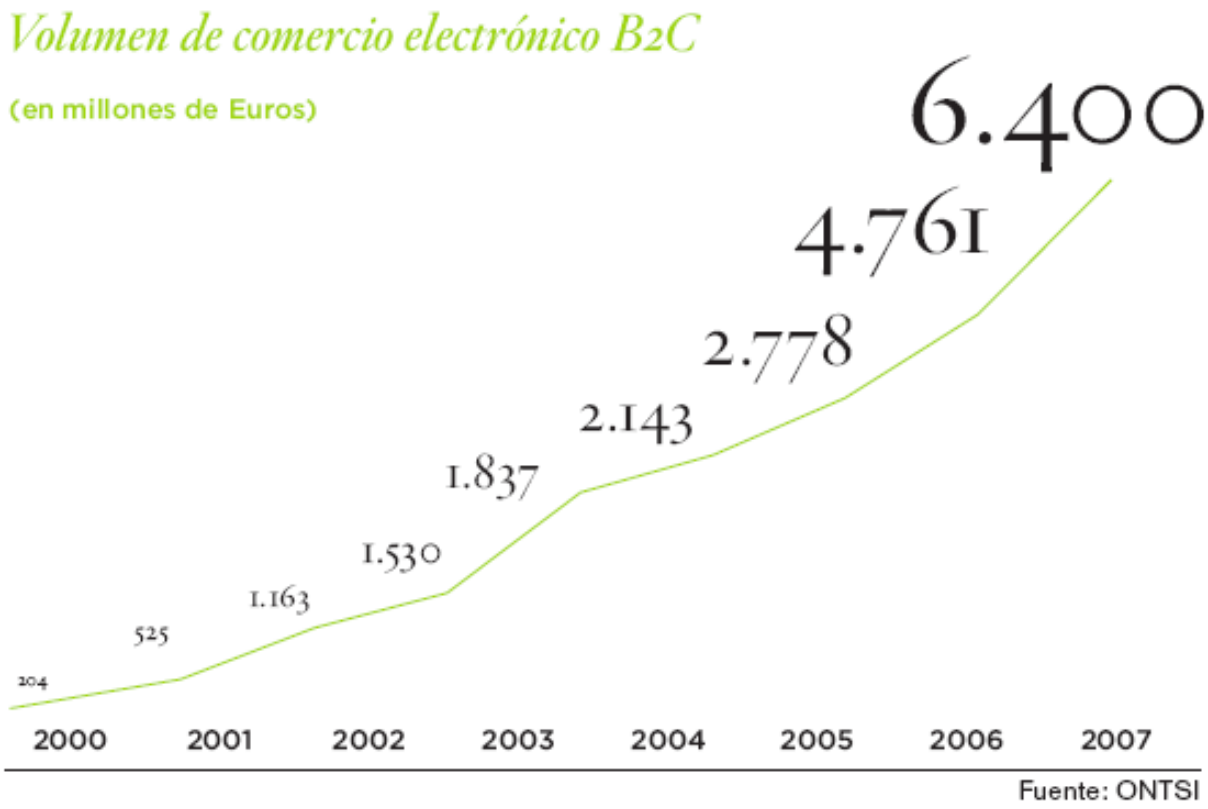


Base I: Total de la Poblacion de 15 y más años / Base II: Total de internautas (%) Fuente: ONTSI

Comercio Electrónico. Números. ONTSI.

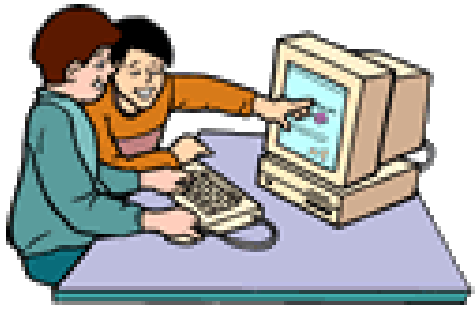
- Crecimiento por debajo de la media europea y, sobre todo, de USA.

- USA. 2007. Forrester y Jupiter Research). 175 billones de dólares (billion = 1.000.000.000) .



Comercio Electrónico. Números.

- Previsiones 2008-2012. Mercado Europeo.
  - De 100 a 174 millones de compradores en Internet.
  - De 1.000€ a 1.500€ anules de consumo / persona.
  - De 103 a 263 millones de euros en volumen de negocio.
  - Influencia directa sobre el 50% del comercio minorista.
  - **Español → Tercer idioma en Internet.**



¿ Crisis ?

Nuevos Modelos

Impuestos y Normativas Legales

- Fiscalidad Directa de Comercio Electrónico
  - Concepto de Comercio Electrónico
  - Imposición directa sobre Comercio Electrónico
  - Problemática asociada a los conceptos de establecimiento permanente y cánones
  - Normativa sobre Comercio Electrónico
  - Tributación del Comercio Electrónico en el IVA
  - Régimen Especial de Tributación del Comercio Electrónico

Agencia Tributaria

Impuestos y Normativas Legales

- Fiscalidad Directa del Comercio Electrónico
  - Concepto de Comercio Electrónico
    - Servicios prestados a título oneroso, a distancia, por vía electrónica y a petición del destinatario.
    - Servicios no remunerados por sus destinatarios, cuando se trate de una actividad económica para el prestador de servicios

Impuestos y Normativas Legales

- NO son Servicios:
  - Servicios prestados por medio de telefonía vocal, fax o télex.
  - Intercambio por correo electrónico.
  - Servicios de radiodifusión televisiva
  - Servicios de radiodifusión sonora
  - Teletexto televisivo

- Característica fundamental del comercio electrónico:
  - La oferta y la aceptación de la misma se realizan ON-LINE, pudiendo o no efectuarse el pago también on-line.

Impuestos y Normativas Legales

- Imposición directa sobre comercio electrónico
  - Son los mismos impuestos directos que se aplican al comercio tradicional y demás actividades económicas: IRPF, sociedades, impuesto sobre renta de no residentes

Impuestos y Normativas Legales

- Concepto de establecimiento permanente según Modelo de Convenio OCDE
  - **Lugar fijo de negocios mediante el que una empresa realiza toda o parte de su actividad (Instalación, centro, emplazamiento)**
  - Las instalaciones están fijadas o vinculadas a un lugar físico y permanecen fijas durante un periodo de tiempo.
  - La actividad es productiva y contribuye al beneficio global de la empresa.
- Aplicación del EP al Comercio Electrónico:
  - A) Lugar Fijo de Negocios: Una página web no tiene una localización física. El servidor en el que la página está almacenada y a través del que se accede, es un equipo con localización física. Una página web no puede considerarse un EP, sin embargo si la empresa que tiene la página tiene a su disposición el servidor, el lugar en el que esté localizado puede considerarse un EP.

Impuestos y Normativas Legales

- Aplicación del EP al Comercio Electrónico:
  - B) Lugar Fijo de Negocios: Un servidor puede ser un EP si permanece localizado en un lugar durante un periodo suficiente para ser considerado fijo.
  - C) Lugar Fijo de Negocios: Un servidor y una página web podría considerarse EP si dicho equipo proporciona utilidades que le permiten realizar toda o parte de su actividad principal. No es necesario presencia del personal en la empresa.
  - D) Actividades auxiliares o preparatorias: si las actividades realizadas sobre el servidor son exclusivamente de preparación no se podría considerar EP:
    - Enlaces de comunicación
    - Publicidad de bienes o servicios
    - Uso del servidor como espejo (seguridad)
    - Recogida de información de mercado para la empresa
    - Suministro de la información.

Impuestos y Normativas Legales

- Aplicación del EP al Comercio Electrónico:
  - E) La figura del ISP como agente: presta los servicios de hosting y otros conexos para alojar las páginas web de Comercio Electrónico. El ISP no constituye un EP de la empresa que realiza Comercio Electrónico.
  - F) La figura de la página web como agente: la página web no es una persona, por lo tampoco puede ser considerada un EP.

Impuestos y Normativas Legales

- Normativa sobre Comercio Electrónico
  - A) Normativa general
    - Regulación básica de la UE contenida en la directiva 2000/31/CE sobre aspectos jurídicos de los servicios de la sociedad de la información (Directiva de Comercio Electrónico)
    - Internamente se refleja en la Ley 34/2002 de Servicios de la sociedad de la información y comercio electrónico.
  - B) Normativa sobre obligaciones contractuales y protección de consumidores
    - Normativa internacional sobre obligaciones contractuales del Convenio de Roma reflejado en la ley de 19/07/08 en la que el derecho aplicable es el del lugar donde resida el consumidor.

Impuestos y Normativas Legales

- Normativa sobre Comercio Electrónico
  - B) Normativa sobre obligaciones contractuales y protección de consumidores
    - Reglamento CE 44/2001 sobre la competencia judicial en materia civil y mercantil, en el que se permite interponer acciones judiciales bien en los tribunales de su lugar de residencia o bien en el estado miembro del domicilio del suministrador.
    - Ley 26/1984 para la defensa de consumidores y usuarios.
    - Ley 7/1996 de ordenación del comercio minorista.
    - Ley 7/1998 sobre condiciones de contratación y el RD 1906/1999 sobre la contratación telefónica o electrónica con condiciones generales.

Impuestos y Normativas Legales

- Normativa sobre Comercio Electrónico
  - C) Normativa de seguridad en el comercio electrónico
    - Ley 59/2003 sobre Firma Electrónica para dar seguridad a las transacciones electrónicas, garantizando la confidencialidad, integridad del mensaje y pagos on-line, identificación y no repudio del mensaje por su autor y destinatario.
  - D) Normativa sobre protección de datos y de la intimidad de las personas.
    - Ley 15/1999 de protección de datos de carácter personal.

Impuestos y Normativas Legales

- Normativa sobre Comercio Electrónico
  - E) Normativa sobre propiedad intelectual e industrial.
    - Directiva 29/2001/CE sobre derechos de autor y derechos afines en la sociedad de la información.
    - RD 1/1996 sobre Ley de Propiedad Intelectual
    - Ley 11/1986 de patentes de invención y modelos de utilidad.
    - Ley 17/2001 de marcas
  - F) Normativa sobre responsabilidad civil de los intermediarios
    - En la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE, Ley 34/2002), se regula la responsabilidad civil de los intermediarios, incluida la que deriva en delito (virus, acceso a ordenadores sin consentimiento, sitios de acceso no autorizado, etc.)
  - G) Normativa sobre fiscalidad directa
    - Convenios para evitar la doble imposición
    - RE 5/2004 sobre la Ley del Impuesto sobre la renta de no residentes.

Impuestos y Normativas Legales

- ¿Cómo tributan los servicios prestados por vía electrónica?
  - ¿El prestador del servicio está establecido en España o en algún país de la Unión Europea?
    - A) En España (Península y Baleares)
      - Se aplicará el régimen general de tributación del IVA
      - Si el destinatario (Empresario o Profesional) del servicio tiene su sede o EP en España (Península y Baleares):
        - Lugar de prestación → Territorio Español
        - IVA 16 %
      - Si el destinatario o consumidor reside en un país de la UE:
        - Lugar de prestación → País donde reside el consumidor
        - No repercutir IVA
      - Si el destinatario o consumidor está establecido fuera de la UE:
        - Lugar de prestación → Estado del destinatario
        - IVA no repercutible excepto si la explotación de los servicios es en España (16%)

Impuestos y Normativas Legales

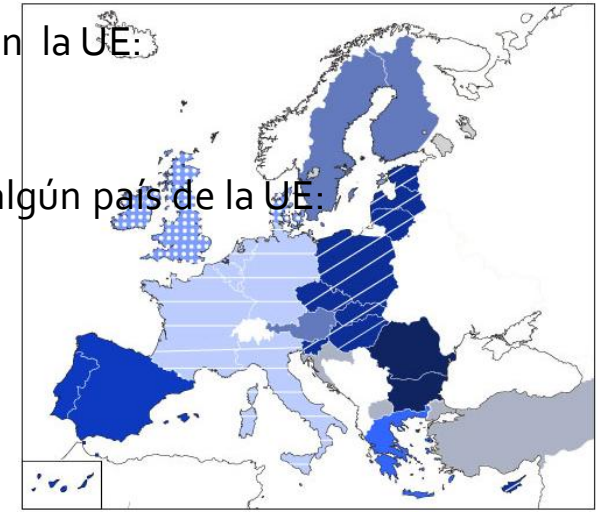
- ¿Cómo tributan los servicios prestados por vía electrónica?
  - ¿El prestador del servicio está establecido en España o en algún país de la Unión Europea?
    - A) En España (Península y Baleares)
      - Si el destinatario (Empresario o Profesional) esta establecido en Canarias, Ceuta o Melilla:
        - Lugar de realización NO es el territorio español → Territorio del destinatario
        - No repercutir IVA
      - Si el destinatario (Particular) reside en España (Península y Baleares) o en algún país de la UE:
        - Lugar de realización → España
        - IVA repercutible 16%
      - Particular establecido fuera de la Comunidad:
        - Lugar de realización → Estado del destinatario
        - No repercutir IVA

Impuestos y Normativas Legales

- ¿Cómo tributan los servicios prestados por vía electrónica?
  - ¿El prestador del servicio está establecido en España o en algún país de la Unión Europea?
    - B) Prestador de servicio está establecido en un país de la UE (no España).
      - Aplicación del régimen general del IVA
      - Destinatario (empresario o profesional) establecido en el mismo estado:
        - Lugar → el mismo Estado miembro
        - IVA → el general vigente en dicho país
      - Destinatario (empresario o profesional) establecido en otro país miembro distinto:
        - Lugar → estado del destinatario
        - IVA → no repercutir salvo que los servicios se exploten en otro país miembro
      - Destinatario (Particular) establecido en la UE:
        - Lugar → el país del destinatario
        - IVA → del estado del particular.
      - Destinatario (Particular) fuera de la UE:
        - Lugar → el estado del destinatario
        - IVA → No repercutir

Impuestos y Normativas Legales

- ¿Cómo tributan los servicios prestados por vía electrónica?
  - ¿El prestador del servicio está FUERA de la Unión Europea pero dispone de un EP en España o en la UE?
    - A) Si es afirmativa, aplicar el régimen de tributación del IVA (apartado anterior)
    - B) En caso contrario:
      - Destinatario (empresario o profesional) establecido en España:
        - Lugar → España
        - No repercutir IVA
      - Destinatario (empresario o profesional) establecido en la UE:
        - Lugar → país del destinatario
        - No repercutir IVA
      - Destinatario (particular) establecido en España o en algún país de la UE:
        - Lugar → Territorio español o estado miembro
        - Aplicar IVA general del país del destinatario



Impuestos y Normativas Legales

- Régimen especial de tributación del Comercio Electrónico
  - El suministrador deberá identificarse en un solo estado miembro, pero debe declarar todos los servicios prestados por vía electrónica a particulares en todos los estados de la UE.
  - Si está identificado en España, está obligado:
    - Declaración electrónica de inicio, modificación y cese de operaciones.
    - Presentación electrónica de declaración trimestral del IVA
    - Ingreso del IVA en el momento de presentación de la declaración.
    - Registro de las operaciones incluidas en este régimen especial
    - Expedición y entrega de factura de las operaciones acogidas a este régimen.

Marcos Normativos

- LOPD (Ley 15/1999).
- RDLOPD (RD 1720/2007).
- LSSI-CE (Ley 34/2002).
- LISI (Ley 56/2007).
- Ley de Firma Electrónica (Ley 59/2003).
- Marcos Complementarios.
- Adaptaciones al nuevo medio.

LOPD / RDLOPD

Normativa

- UE:
  - Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.
- ESPAÑA:
  - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD): Transposición al ordenamiento jurídico español de la Directiva 95/46/CE.
  - Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD.
  - Instrucciones dictadas por la Agencia de Protección de Datos, que tienen por objeto aclarar y apoyar la interpretación de la ley con el fin de adecuar los tratamientos a los principios establecidos en la misma.
  - Reglamentación Autonómica (Madrid, País Vasco, Cataluña)

¿En qué consiste la protección de datos?

- Derecho fundamental que garantiza a toda persona un **poder de control** sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.
- La propiedad del dato NO es de quien lo posee sino de su titular: derecho a decidir cuándo, cómo, dónde y por quién es tratado.
- Afecta a los ficheros en soporte papel y automatizados.

LOPD / RDLOPD

- **¿En qué consiste un Proyecto de adaptación?**
  - **Obligaciones Formales**: Registro de Ficheros, elaboración del Documento de Seguridad, atención de derechos.
  - **Obligaciones Organizativas**: Cumplimiento de la Normativa interna reflejada en el Documento de Seguridad, definición de las funciones y obligaciones del personal, formar e informar...
  - **Obligaciones Técnicas/Recursos**: Contraseñas, copias de seguridad, control de accesos...
- **Ventajas:**
  - Cumplimiento de la normativa vigente.
  - Evitar la comisión de infracciones que impliquen sanciones económicas de la AEPD.
  - Gestión eficaz de la Seguridad de la Información: Bases de datos de nóminas, CV's, clientes ...
  - Confianza de los titulares de los datos en la imagen pública de la empresa.
  - Gestión de la Calidad.

LOPD / RDLOPD

- Nivel BÁSICO.
  - Nombre y apellidos, DNI, dirección, mail, teléfono, estado civil,...
- Nivel MEDIO.
  - Hacienda Pública, servicios financieros, solvencia, infracciones penales y administrativas así como los que permitan valorar el perfil de la persona.
- Nivel ALTO.
  - Ideología, Religión, Creencias, Origen racial, Afiliación sindical, Salud, Vida sexual y datos derivados de actos de violencia de género.
    - Los datos referidos al origen racial, salud y vida sexual sólo podrán ser recabados, tratados y cedidos con consentimiento expreso del afectado.
    - Los datos referidos a la ideología, religión, creencias y afiliación sindical sólo podrán ser recabados, tratados y cedidos con consentimiento expreso y por escrito del afectado.

Niveles de seguridad de los datos

LOPD / RDLOPD

Principios: Calidad de los datos

- Deben ser los necesarios, o sea, adecuados, pertinentes y no excesivos conforme a la finalidad para la que se hayan recabado.
- No podrán usarse para finalidades incompatibles (=distintas) a las que consintió el afectado, y se cancelarán cuando dejen de ser necesarios para las mismas.
- Los datos deben ser exactos y actuales.
- Serán eliminados cuando dejen de ser necesarios.
- Nunca serán recogidos o conseguidos por medios fraudulentos: forma legal.

LOPD / RDLOPD

Principios: Información

- Cuando se recogen datos, hay que informar de:
  - La existencia de un fichero con sus datos.
  - La finalidad del fichero y del recabo.
  - Los posibles destinatarios de la información.
  - Si es obligatorio o no responder y las consecuencias de en caso de no responder.
  - La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
  - La identidad y dirección del responsable del fichero y el modo de ejercicio de los derechos.
- Esta información debe aparecer claramente en todos los cuestionarios e impresos.

LOPD / RDLOPD

Principios: Consentimiento.

El **afectado** es el **VERDADERO PROPIETARIO** de los datos personales y se **NECESITARÁ SIEMPRE** el consentimiento **INEQUÍVOCO** de éste para el tratamiento de los mismos.

- El consentimiento se recabará siempre de forma legal.
- El consentimiento, dependiendo del tipo de datos, será inequívoco, expreso o escrito. Recomendación: por escrito por que la carga de la prueba recae en la empresa.
- El afectado puede revocar su consentimiento en cualquier momento.

LOPD / RDLOPD

Principios: Consentimiento

- **Regla general:** necesario el consentimiento del titular o afectado para poder efectuar una cesión de sus datos.
- **Excepciones**:
  - Cuando una ley así lo disponga.
  - Necesarios para el mantenimiento o cumplimiento de un contrato o precontrato de una relación de negocio.
  - Proteger un interés vital del interesado.
  - Datos que figuren en fuentes accesibles al público.

LOPD / RDLOPD

Principios: Cesión o Comunicación.

- **Toda revelación de datos realizada a una persona distinta del interesado** -la simple consulta que un tercero realice, aunque sea a distancia y sin creación de un nuevo fichero o tratamiento nuevo-.

- **Será necesario**:
  - Que la cesión se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.
  - Consentimiento del afectado.

- **Excepciones al consentimiento** (autorización por Ley, datos de fuentes accesibles al público, el tratamiento responda a la libre y legítima aceptación de una relación jurídica y sea necesario para para el desarrollo, cumplimiento y control, en caso de urgencia, los destinatarios sean: Defensor del Pueblo, Ministerio Fiscal, Jueces, Tribunales y el Tribunal de cuentas).

- **Cesiones entre empresas del grupo**:
  - Especificar cada una de ellas o su actividad y finalidad (exigido por la AEPD)

LOPD / RDLOPD

Principios: Acceso por cuenta de 3º

- **Figuras**: Responsable fichero y encargado del tratamiento.
- **En caso de prestación de servicios, no se trataría de una cesión** si:
  - Existe un contrato escrito.
  - Se establece expresamente que el encargado del tratamiento sólo tratará esos datos conforme a las instrucciones del responsable del fichero.
  - No los aplicará o utilizará para un fin distinto al que figure en el contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
  - Una vez finalizada la prestación contractual, los datos deberán ser destruidos o devueltos al responsable del fichero.
  - El encargado del tratamiento implementa las medidas de seguridad correspondientes al nivel de los datos tratados.

LOPD / RDLOPD

Derechos ARCO (I)

- **Derecho de Acceso:**
  - Derecho a solicitar y obtener información de los propios datos de carácter personal incluidos en ficheros.
  - El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, su origen,
  - Plazo de contestación: 30 días.
- **Derecho de Rectificación y Cancelación:**
  - Derecho a la rectificación y cancelación de los datos, en particular, si son inexactos o incompletos, inadecuados o excesivos
  - Plazo de contestación: 10 días.
  - Si la cancelación es denegada, se notificará al interesado la negativa y el motivo, por un medio que permita acreditar el envío y la recepción.
  - La solicitud sólo podrá ser denegada cuando la haga una persona distinta del titular de los datos, por lo que es necesario aportar fotocopia del D.N.I.

LOPD / RDLOPD

Derechos ARCO (II)

Derecho de Oposición:

- Cuando el consentimiento no sea necesario para el tratamiento, el titular de los datos puede oponerse al mismo (Ej. datos recabados fuentes accesibles al público).
- La solicitud sólo podrá ser denegada cuando la haga una persona distinta del titular de los datos, por lo que es necesario aportar fotocopia del D.N.I.
- Plazo de 30 días desde la recepción de la solicitud, se activará el derecho de oposición, pudiendo conservar una referencia, con el objetivo de evitar posibles usos futuros para acciones no autorizadas por el interesado.
- Se remitirá por un medio que nos permita acreditar el envío y la recepción, la información a la dirección indicada por el interesado en el plazo de diez días.
- Si la oposición es denegada, también se notificará al interesado la negativa y el motivo.

LOPD / RDLOPD

Documento de Seguridad

- Recoge el conjunto de medidas, tanto técnicas como organizativas, implantadas para garantizar la seguridad de la información y, en especial, de los datos de carácter personal.
- Está formado por una Parte General y unos Anexos.
- Recoge Funciones y Obligaciones para TODOS los usuarios que manejan información (automatizado + papel).

Funciones y Obligaciones del Personal

- Clasificación de Usuarios.
- Claves de Acceso.
- Confidencialidad de la información.
- Gestión de Soportes.
- Incidencias.
- Telecomunicaciones.
- Soporte papel.
- Acceso a Internet.
- Uso del correo electrónico.
- Propiedad intelectual.

LOPD / RDLOPD

Clasificación de Usuarios

- Usuario: Se identifica a la persona autorizada para acceder a datos o recursos.
- No todos los usuarios necesitan acceder a la misma información para hacer su trabajo. Por eso, la definición de perfiles debe realizarse en atención a las necesidades del puesto y sus funciones.
- Responsable de Seguridad: persona encargada de coordinar y controlar las medidas definidas en el Documento de Seguridad.

LOPD / RDLOPD

Claves de Acceso

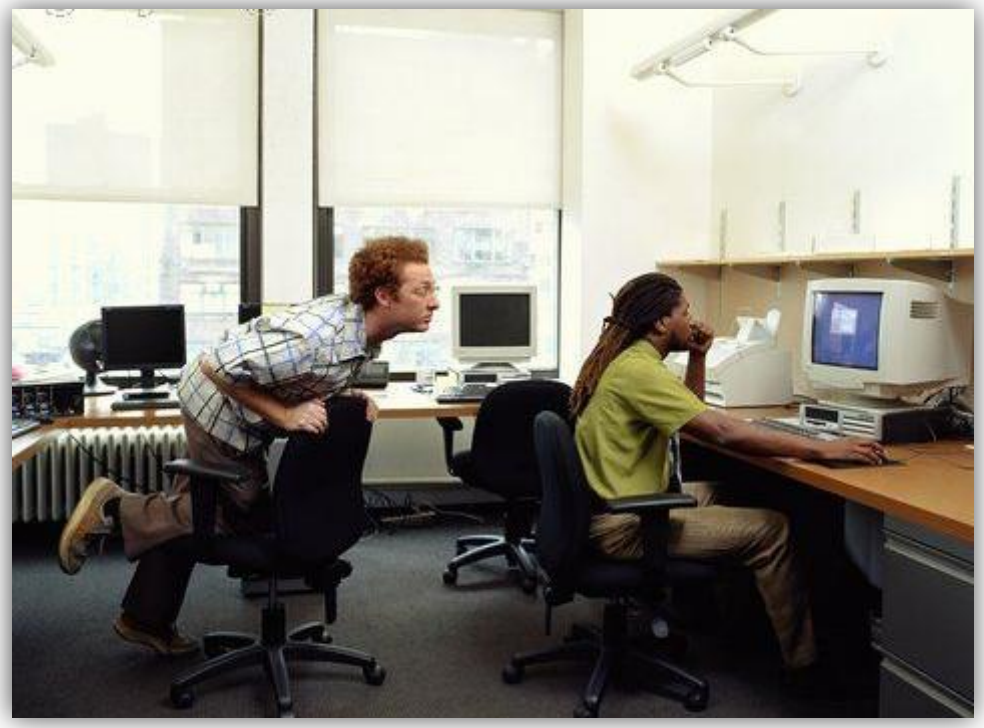
- Son individuales, personales e intransferibles y no deberán ser comunicados a otras personas. Si sospecha que otra persona las conoce deberá solicitar al Responsable de sistemas para que le asigne una nueva clave.
- El usuario es responsable de las consecuencias que puedan derivarse de su mal uso, divulgación o pérdida.
- El uso de la clave asignada a cada usuario implicará la aceptación, como documento probatorio, de la operación efectuada. Salvo prueba en contrario, se presumirá que los actos que se lleven a cabo con el identificador y la clave asignados han sido realizados por el usuario titular de los mismos.

LOPD / RDLOPD

Confidencialidad de la Información

- No podrá enviarse información confidencial de la Compañía al exterior sin autorización.

- No se podrá utilizar para fines personales información propiedad de la Compañía.



- En caso de que por motivos directamente de trabajo se tenga información confidencial bajo cualquier tipo de soporte se debe entender dicha posesión como temporal, con obligación de secreto y a devolver.

LOPD / RDLOPD

Secreto Profesional

- Todo el personal tiene el deber de guardar secreto profesional de todos los hechos y noticias que conozca por razón de su actuación profesional, que subsistirá incluso después de haber cesado en su puesto.
- El secreto profesional exige la no revelación de hechos, datos o informaciones de carácter reservado o confidencial.

Gestión de soportes

- Hay que pedir autorización para poder sacar de la oficina equipos, disquetes u otros soportes con información para evitar que personas no autorizadas accedan a ella.

LOPD / RDLOPD

Soporte papel

- **Política de Mesas limpias:** A la finalización de la jornada o de la utilización de un documento debe guardarse en su archivo para evitar que cualquier persona acceda a la información. Dichos archivos deben permanecer cerrados con llave.
- No se deben dejar documentos en impresoras o fotocopiadoras compartidas.
- Está prohibido tirar directamente a las papeleras o bolsas de basura cualquier documentación impresa que contenga datos de carácter personal. Aunque únicamente aparezca el nombre de empleados o clientes habrá que utilizar una destructora de papel o depositarla en los contenedores que se habiliten para su destrucción.

Incidencias

- Es obligación de todo el personal comunicar al Responsable de Seguridad cualquier incidencia que se produzca en los sistemas de información a que tengan acceso.
- Se entiende por incidencia cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.
- Dicha comunicación deberá realizarse en un plazo de tiempo no superior a UNA HORA desde el momento en que se produzca dicha incidencia o desde el momento en que se tenga conocimiento de la misma.

LOPD / RDLOPD

Procedimiento de RRHH

- Firmar compromisos de confidencialidad y del conocimiento y aceptación de la normativa interna sobre protección de datos.
- Informar a los empleados de la existencia de un fichero, de la finalidad de la recogida de sus datos, de los destinatarios de la información, de la posibilidad de ejercitar los derechos que le asisten, y de la identidad y dirección del responsable de los ficheros.
- Responder las solicitudes de empleo recibidas.

Procedimiento de contratación

- Para la contratación de servicios que impliquen o puedan implicar un acceso a datos de carácter personal habrá que seguir el procedimiento establecido por la Compañía.

LOPD / RDLOPD

Ámbito de aplicación y tratamientos excluidos

Ámbito de aplicación

- Datos de carácter personal registrados en soporte físico (informatizado o no), que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Tratamientos excluidos

- Tratamientos de datos referidos a personas jurídicas.
- Ficheros que se limiten a incorporar datos de personas físicas que presten sus servicios en aquéllas (nombre y apellidos, las funciones o puestos desempeñados, dirección postal o electrónica, teléfono y número de fax profesionales).
- Datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros.
- Datos referidos a personas fallecidas.

LOPD / RDLOPD

Deber de informar: Acreditación

- La información tiene que facilitarse a través de un medio que permita acreditar su cumplimiento.
- El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar.
- Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos.
- Se podrá proceder al escaneado de la documentación en soporte papel, siempre que se garantice que en la automatización no se ha producido ninguna alteración de los soportes originales.

LOPD / RDLOPD

Encargado de tratamiento: Subcontratación

Norma general.
El encargado del tratamiento no podrá subcontratar, salvo con autorización del responsable y realizando la contratación en nombre y por cuenta del mismo.

Posibilidad de subcontratar sin autorización del responsable.
Cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

Necesidad de subcontratar durante la prestación del servicio.
Si esta circunstancia no está prevista en el contrato, deberán someterse al responsable del tratamiento los extremos indicados anteriormente.

LOPD / RDLOPD

Prestaciones de servicios sin acceso a datos personales

- **Personal propio:**

  El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso a:

  - los datos personales,
  - los soportes que los contengan,
  - los recursos del sistema de información,

  para la realización de trabajos que no impliquen el tratamiento de datos personales.

- **Personal ajeno:**

  El contrato de prestación de servicios recogerá expresamente:

  - La prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer .

Ejemplos. – Servicios de:

- Limpieza.
- Mantenimiento.
- Destrucción de papel.

LOPD / RDLOPD

Ejercicio de los derechos ARCO

1. Obligación de informar al afectado de su derecho a recabar la tutela de derechos de la AEPD.

2. Corresponde al responsable de los ficheros la prueba del cumplimiento del deber de respuesta, debiendo conservar la acreditación de su cumplimiento.

3. Posibilidad de las personas vinculadas a un fallecido a ejercitar el derecho de cancelación de sus datos .

4. Se regula por primera vez el derecho de oposición. Ej. oponerse a que se traten los datos para fines de publicidad y prospección comercial.

LOPD / RDLOPD

Titulo VIII: Medidas de Seguridad (I)

<u>Art. 82 Encargado del Tratamiento</u>: distinción según el lugar donde el encargado trate los datos:

- <u>En los locales del responsable</u>:

  - Constancia en el DS.

  - Compromiso del personal del encargado al cumplimiento de las medidas de seguridad previstas en el DS.

- <u>Acceso remoto:</u>

  - Si se prohíbe al encargado incorporar los datos a sistemas o soportes distintos de los del responsable, este último deberá hacerlo constar en su DS.

  - Compromiso del personal del encargado al cumplimiento de las medidas de seguridad previstas en el DS.

- <u>En los locales del encargado</u>:

  El Encargado elaborará su propio DS identificando:

  - El fichero o tratamiento.

  - El responsable del mismo.

  - Las medidas de seguridad a implantar en relación con dicho tratamiento.

LOPD / RDLOPD

Titulo VIII: Medidas de Seguridad (II)

- **Art. 86. Régimen de trabajo fuera de los locales:**
  - Cuando los **datos personales**:
    - se **almacenen en dispositivos portátiles** o
    - se **traten fuera de los locales** del responsable de fichero o tratamiento o del encargado del tratamiento,
  - **será preciso**:
    - **una autorización previa** del responsable del fichero o tratamiento que conste en el DS (para un usuario/ perfil de usuarios y determinando un periodo de validez).
    - **garantizar el nivel de seguridad** correspondiente al tipo de fichero tratado.

LOPD / RDLOPD

Historial sanciones impuestas por la AEPD

AÑO	SANCIONES PRESUPUESTADAS	SANCIONES IMPUESTAS	% INCREMENTO ANUAL	PROCEDIMIEN-TOS Y ACTUACION.	% INCREMENTO ANUAL
2002	1.299.130	7.989.166,22		723	
2003	1.502.520	8.372.379,74	5%	1.393	92,7%
2004	1.858.120	16.439.801,58	96%	1.788	28,4%
2005	2.000.000	21.105.083,99	28%	2.190	22,5%
2006	2.200.000	24.422.292,48	16%	2.530	15,5%
2007	4.600.000	19.674.480,03	-19,44	3.136	23,9%

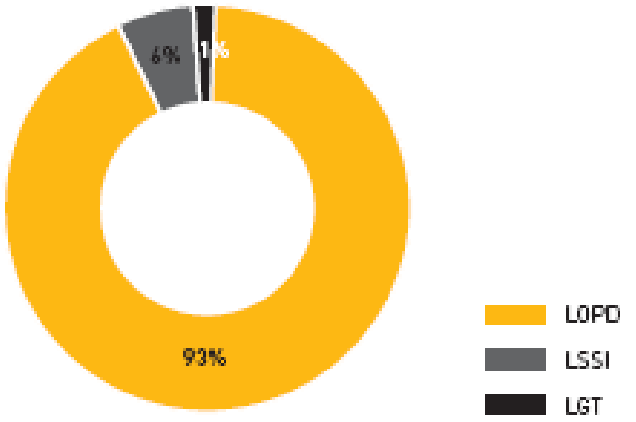
2006	2007	2008	% VAR. 2007/2008
24.422.292,48 €	19.674.480,03 €	22.625.839,38 €	+15

cecarm
negocio electrónico en la Región de Murcia

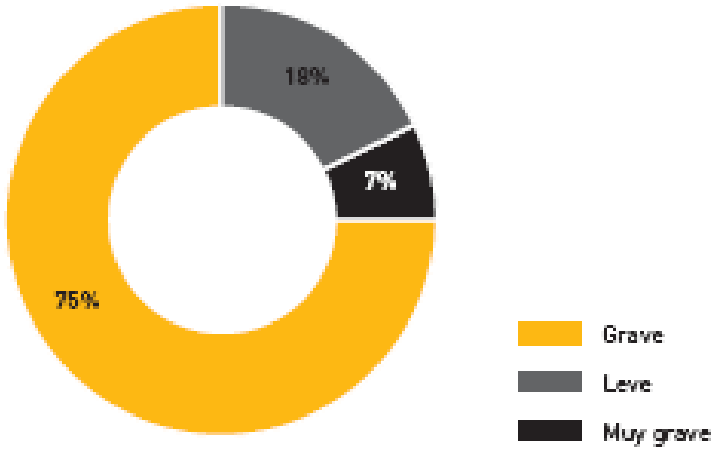
LOPD / RDLOPD

Sanciones impuestas por la AEPD. Mem. 2008

Sanciones impuestas según ley infringida 2008



Sanciones impuestas según gravedad 2008



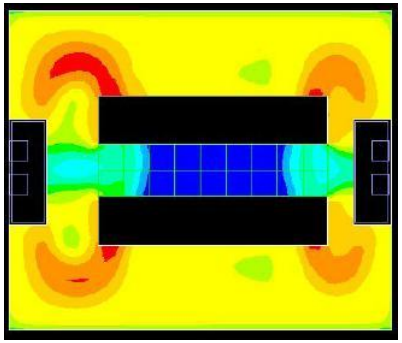
INFRACCIÓN	MULTA
Leve	De 600 a 60.000 €
Grave	De 60.001 a 300.000 €
Muy grave	De 300.001 a 600.000 €

LOPD / RDLOPD

Calificación de Infracciones.

- **Infracciones leves:**

  - No atender la solicitud por parte del interesado de rectificación o cancelación de sus datos.
  - No proporcionar información que solicite la AEPD.
  - No solicitar la inscripción del fichero en el Registro General de Protección de Datos, cuando no constituya infracción grave.
  - Recoger datos personales de afectados sin proporcionarles información sobre su tratamiento y derechos, de modo expreso y preciso.
  - Incumplimiento del deber de secreto profesional (en nivel básico).
  - .....

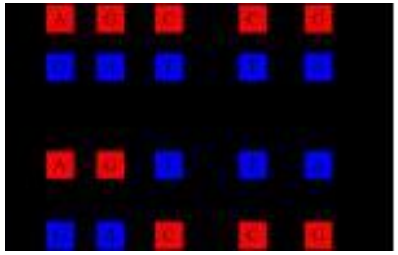


LOPD / RDLOPD

Calificación de Infracciones.

- **Infracciones graves:**

  - Crear ficheros de titularidad pública sin autorización.
  - Crear ficheros de titularidad privada o iniciar recogida de datos con finalidades ilegítimas.
  - Tratar los datos con violación de los principios establecidos en la Ley, o con incumplimiento de las reglas de protección.
  - Impedimento al afectado del ejercicio de sus derechos.
  - Mantener los SI sin las debidas condiciones de seguridad.
  - Incumplimiento del deber de información al interesado, cuando los datos hayan sido recabados por una persona distinta al afectado.
  - Vulneración del deber de guardar secreto sobre datos de nivel de seguridad medio.
  - Obstrucción a la inspección que necesite realizar la AEPD.
  - ...



LOPD / RDLOPD

Calificación de Infracciones.

- **Infracciones muy graves:**

  - Recogida de datos de forma engañosa y/o fraudulenta.
  - **Comunicación o cesión de datos no permitida por la Ley**.
  - Recabar y tratar datos de nivel de alto sin consentimiento.
  - Quebrantar la prohibición de crear un fichero con la finalidad exclusiva de almacenar datos de nivel alto.
  - No cesar en el uso ilegítimo de tratamiento de datos cuando sea requerido por el Director de la AEPD o las personas titulares.
  - Tratar los datos de forma ilegítima y atentar contra el ejercicio de los derechos fundamentales.
  - Obstaculizar de forma sistemática el ejercicio de los derechos.
  - Vulneración del deber de guardar secreto sobre los datos de nivel alto.
  - …

LOPD / RDLOPD

Notificación de ficheros.

- Notificación previa de los ficheros a la Agencia Española de Protección de Datos.
  - Cuando en nuestra página web recojamos datos personales, ya sea de clientes, usuarios, potenciales clientes, etc., se debe proceder a notificar todos estos ficheros que contienen datos personales a la Agencia Española de Protección de Datos (AEPD), obligación que debe realizarse previamente al inicio de las tareas de tratamiento de los datos.
  - Dicha notificación es gratuita. Para realizar la notificación utilizaremos el Sistema de Notificaciones Telemáticas de la AEPD denominado Programa NOTA, al que puede accederse desde la página Web *www.agpd.es. En esta página también podremos encontrar una guía rápida* sobre como cumplimentar el formulario y una serie de preguntas frecuentes que nos ayudarán a realizar este trámite.
  - Realizaremos una notificación diferente para cada uno de los ficheros que queramos inscribir. Algunos ejemplos de ficheros de datos de carácter personal que normalmente se tratan en una empresa con página web de comercio electrónico son: Clientes, Potenciales clientes, Suscriptores y Usuarios.

LOPD / RDLOPD

Notificación de ficheros.

- Notificación previa de los ficheros a la Agencia Española de Protección de Datos.
  - Una vez que se descargue el programa NOTA encontraremos que recoge varias notificaciones tipo entre las que se encuentra la notificación "ficheros de clientes", que nos facilitará cumplimentar el formulario de notificación. Aparte de los ficheros que hemos mencionado, la empresa normalmente también tendrá otros ficheros a declarar (P.ej. Empleados, entre otros).
  - La forma de envío del formulario de notificación de creación del fichero dependerá de la opción que hayamos seleccionado por correo postal o por Internet con o sin firma electrónica.
  - Una vez inscrito el fichero, la AEPD nos enviará por correo postal una resolución con el código de inscripción otorgado a cada fichero.
  - No obstante, si transcurrido un mes no hemos recibido ninguna noticia, se produce silencio administrativo positivo, es decir podemos dar por inscrito correctamente el fichero.

LOPD / RDLOPD

Formularios.

- **Formularios de recogida de datos:**
  - Obligación de información.
  - Cuando en la página web se utiliza un formulario para recabar datos personales de los usuarios o clientes, o bien para permitir la suscripción a un boletín o comunidad, es obligatorio incluir un aviso legal en materia de protección de datos, cuyo contenido debe informar de lo siguiente (Artículo 5 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal):

    1. de la existencia de un fichero o tratamiento de datos;
    2. de la finalidad de su recogida y de los destinatarios de la información;
    3. del carácter obligatorio o facultativo de la respuesta a las preguntas que se plantean;
    4. de las consecuencias de la obtención de los datos o de la negativa a suministrarlos;
    5. de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición;
    6. de la identidad y dirección del responsable del tratamiento de los datos.

LOPD / RDLOPD

Formularios.

- Formularios de recogida de datos:
- Para cumplir con esta obligación, es necesario situar un aviso legal específico bien visible justo debajo del formulario, o bien insertar un enlace permanentemente visible en la Web a nuestra política de privacidad.

LOPD / RDLOPD

Modelo de Aviso Legal.

- Ejemplo de aviso legal
  - En virtud de lo dispuesto en la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que mediante la cumplimentación del presente formulario sus datos personales quedarán incorporados y serán tratados en los ficheros titularidad de *(nombre de la Compañía), con el fin de (indicar la finalidad de la recogida de datos), así como para mantenerle informado, incluso* por medios electrónicos, sobre cuestiones relativas a la actividad de la Compañía y sus servicios.

    Usted puede ejercer, en cualquier momento, los derechos de acceso, rectificación, cancelación y oposición de sus datos de carácter personal mediante correo electrónico dirigido a *(indicar e-mail) o bien mediante* un escrito dirigido a *(indicar dirección postal), acompañando siempre* una fotocopia de su D.N.I. o documento de identidad suficiente.

LOPD / RDLOPD

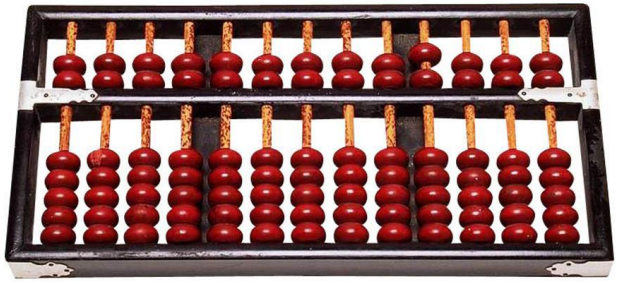
Contrato de Tratamiento de Datos

- **Contrato de tratamiento de datos**.
  - Cuando la página web en la que se recojan datos personales esté alojada en los servidores de otra empresa, un informático que no es de nuestra empresa haga el mantenimiento de la página web o una empresa vaya a prestarnos un servicio de tratamiento de datos y en consecuencia va ya a tener acceso a la información que hay en nuestra base de datos, por ejemplo, para normalizar la base de datos, será necesario firmar un contrato de tratamiento de datos.
  - Dicho contrato está regulado en el **artículo 12** de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal y en los artículos 20, 21 y 22 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Ley 34/2002 + Ley 56/2007

Correo electrónico comercial.

- **¿Cuándo pueden enviarse e-mails o sms publicitarios?**
  - Como norma general, está prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico o SMS, si previamente el destinatario no las ha solicitado o, en su caso, no nos ha autorizado de forma previa y expresa para poder enviárselas.
  - No obstante, si mantenemos con el destinatario una relación contractual previa, es decir, si ya es nuestro cliente, podremos enviarle comunicaciones comerciales referentes a productos o servicios de nuestra empresa, siempre que éstos sean similares a los que inicialmente fueron objeto de contratación por éste.



Ley 34/2002 + Ley 56/2007

Correo electrónico comercial.

- **¿Cuándo pueden enviarse e-mails o sms publicitarios?**
  - En cualquier caso, tanto en el momento de recoger los datos del destinatario, como dentro de cada comunicación comercial que le enviemos, debemos además de informarle sobre las cuestiones de protección de datos antes referenciadas, ofrecerle la posibilidad de dejar de recibir este tipo de comunicaciones, poniendo para ello a su disposición un medio sencillo y gratuito como, por ejemplo, el envío de un correo electrónico a una dirección determinada o mediante un formulario en nuestra página Web.

Ley 34/2002 + Ley 56/2007

Información al destinatario.

- Cuando mandamos una comunicación electrónica de carácter comercial o publicitario, es imprescindible que el destinatario pueda identificarla como tal. Por ello, es obligatorio incluir al comienzo del mensaje la palabra *publicidad o la abreviatura publi. Además, **la empresa** que realiza* la promoción debe identificarse claramente.
- Si el contenido del mensaje versa sobre ofertas o concursos promocionales, como descuentos, premios y regalos, deberán incluirse de forma clara las condiciones de acceso o participación, o bien indicar donde éstas pueden consultarse.

Ley 34/2002 + Ley 56/2007

Información sobre las cookies.

- Cuando en la página web utilicemos cookies u otros dispositivos de almacenamiento y recuperación de datos, que se instalen en el ordenador del usuario, para guardar información necesaria para la navegación del usuario por nuestra web o cualquier otra causa, se debe informar de manera clara y completa sobre su utilización y finalidad, así como ofrecerles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.

- Se puede cumplir con esta obligación, por ejemplo, informando de ello en el aviso legal o en las condiciones de contratación de la página web, así como informando sobre cómo pueden rechazar la instalación de estos archivos a través de los programas de navegación que el usuario utilice..

Ley 34/2002 + Ley 56/2007
Información obligatoria en la página web.

- En un lugar permanentemente accesible de la página Web, debe aparecer la información relativa al **titular** de la misma. Esta obligación consta en el artículo 10 de la LSSICE (Ley 34/2002).

- Modelo genérico de texto para cumplir con esta obligación:
  - Información general
  - En cumplimiento de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, se indican los datos de información general de *(indicar página Web):*
    - Titular: *(nombre y apellidos o denominación social)*
    - C.I.F.: *(número)*
    - Dirección: *(indicar dirección postal)*
    - Contacto: *(indicar e-mail)*
    - Tel.: *(número)*
    - Fax.: *(número)*
    - Datos registrales: *(en su caso, indicar)*

Ley 34/2002 + Ley 56/2007

Información obligatoria en la página web.

Código Tipo o Sello de Calidad.

- Cuando se trate de una página web de una Empresa o profesional que, parea realizar su actividad, requiera de autorización administrativa o inscripción en cualquier Registro, deberán constar los datos de dicha autorización o Registro.

- Asimismo, en caso de que la Empresa se haya adherido a algún código tipo o Sello de Calidad, como el de CECARM, así deberá constar en el Aviso Legal.

Ley 34/2002 + Ley 56/2007

Información obligatoria en la página web.

Código Tipo o Sello de Calidad.

La página web debe cumplir las siguientes condiciones:

✓Informa de la realización de la actividad de la empresa desde la Región de Murcia, ofreciendo información detallada de sus datos registrales, de contacto y localización.

✓Tiene actualizada la tienda, el catálogo y los formularios web.

✓Posibilita transacciones comerciales para la venta de productos o servicios, ofreciendo información detallada de los mecanismos de pedido, garantía, plazos de entrega y devolución, reclamaciones, así como del precio final (producto/servicio, impuestos, gastos de manipulación, portes, etc.)

✓Dispone de un servicio de atención al cliente en funcionamiento, ofertando, además del correo electrónico, al menos otro canal de contacto, y respondiendo en un breve periodo de tiempo.

✓Informa claramente y en un lugar visible del cumplimiento de cuantas leyes le sean aplicables (Ley de Protección de Datos, LSSICE, propiedad intelectual, Ley de Ordenación del Comercio Minorista, etc.)

✓La empresa deberá estar adherida al Sistema Arbitral de Consumo de la Comunidad Autónoma de la Región de Murcia

Ley 34/2002 + Ley 56/2007
Información obligatoria en la página web.

- Según el tipo de página web o servicio que ofrezcamos, también es necesario informar en las condiciones generales de contratación de:
  - Las características esenciales del bien o servicio.
  - Los gastos de entrega y transporte, en su caso.
  - El plazo de vigencia de la oferta y del precio y, en su caso, la ausencia del derecho de desistimiento en los supuestos previstos.
  - La duración mínima del contrato, si procede, cuando se trate de contratos de suministro de bienes o servicios destinados a su ejecución permanente o repetida.
  - Las circunstancias y condiciones en que el empresario puede suministrar un bien o servicio de calidad y precio equivalentes, en sustitución del solicitado por el consumidor y usuario, cuando se quiera prever esta posibilidad.
  - La forma de pago y modalidades de entrega o de ejecución.
  - En su caso, indicación de si el empresario dispone o está adherido a algún procedimiento extrajudicial de solución de conflictos.

Ley 34/2002 + Ley 56/2007
Información obligatoria en la página web.

- Según el tipo de página web o servicio que ofrezcamos, también es necesario informar en las condiciones generales de contratación de:
  - La dirección del establecimiento del empresario donde el consumidor
  - y usuario pueda presentar sus reclamaciones.
  - La información relativa a los servicios de asistencia técnica u otros servicios postventa y a las garantías existentes.
  - Las condiciones para la denuncia del contrato, en caso de celebración
  - de un contrato de duración indeterminada o de duración superior a un año.
  - Cuando se utilicen técnicas de comunicación con sobrecostes:
    - El coste de la utilización de la técnica de comunicación a distancia cuando se calcule sobre una base distinta de la tarifa básica.

Ley 34/2002 + Ley 56/2007

Contratación OnLine.

- Cuando en una página Web se ofrece la posibilidad de contratar un servicio o adquirir un producto, **antes de iniciar el proceso**, el interesado debe poder acceder fácilmente a la siguiente información:
  - Los distintos 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.
  - Condiciones generales a que, en su caso, deba sujetarse el contrato, posibilitando que éstas puedan ser almacenadas y reproducidas por el destinatario.
- Toda esta información es la que suele configurar las denominadas "Condiciones Generales de la Contratación" que aparecen accesibles en los sitios Web.

Normas de Comercio

Contratación OnLine.

- Por otra parte, una vez finalizado el proceso de contratación, tenemos la obligación de confirmar al usuario la recepción de su aceptación, lo que haremos por alguno de los siguientes medios:

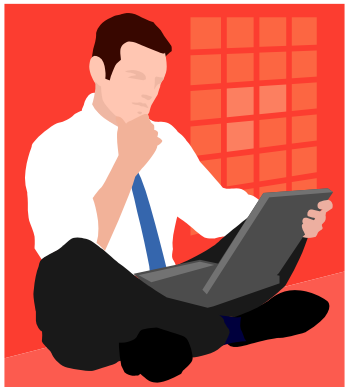
    1. Enviando un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el usuario haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la aceptación.
    2. Generando una confirmación de la aceptación recibida, tan pronto como el aceptante haya completado el procedimiento, siempre que éste pueda archivar la confirmación.

- En el caso de que la recepción de la aceptación se confirme mediante acuse de recibo, se presumirá que su destinatario puede tener constancia de ello desde que el acuse haya sido almacenado en el servidor en que esté dada de alta la cuenta de correo electrónico de éste.

Normas de Comercio

Contratación OnLine.

- Esta obligación de confirmar la recepción de la aceptación, no será
- necesaria si las dos partes así lo han acordado y ninguna de ellas tiene la consideración de consumidor.
- Tampoco será necesaria si el contrato se ha celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, siempre que no se hayan utilizado estos medios exclusivamente para eludir el cumplimiento de dicha obligación.



Normas de Comercio

Contratación OnLine.

- Cuando la parte que realiza la oferta y el que la acepta se encuentran en lugares distintos, como ocurre en la contratación online, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela enviado el aceptante, no puede ignorarla sin faltar a la buena fe.

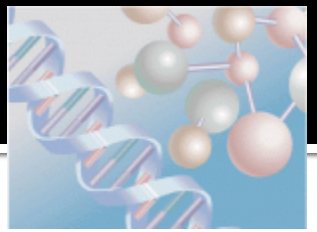
- Por lo tanto, para que el contrato surta efectos entre las partes es necesario que el comprador responda expresamente aceptando la oferta y que dicha aceptación llegue a ser conocida por el vendedor. En este sentido, nunca podremos articular mecanismos en los que el hecho de no responder a la oferta pueda entenderse como una aceptación de la misma.

- En cuanto al lugar de los contratos celebrados por vía electrónica, debe tenerse en cuenta que si se realizan entre empresa y consumidor, el lugar de celebración será donde éste tenga su residencia habitual.

- Si el contrato se formaliza entre empresarios o profesionales y éstos no han pactado nada al respecto, se presumirá celebrado en el lugar en que esté establecido el prestador de servicios, pero las partes pueden pactar cualquier otro sitio.

Normas de Comercio

Contratación OnLine. La entrega.



- **Plazo de entrega.**
- A menos que las partes hayan acordado otra cosa, el vendedor debe ejecutar el pedido en un plazo máximo de treinta días a partir del día siguiente a aquel en que ha recibido la comunicación de pedido del comprador.

- Al cliente, en principio ,se le ha de entregar lo que éste ha comprado.

- Ahora bien, es posible que no se pueda cumplir el plazo de entrega porque el producto solicitado no está disponible, en cuyo caso debe informarse rápidamente de ello al consumidor y ofrecerle la posibilidad de recuperar cuanto antes, en un plazo de treinta días como máximo, las sumas que haya abonado hasta ese momento.

- Debe tenerse en cuenta que si no se respeta este plazo de abono, el consumidor **puede exigir que se le devuelva el doble de la cantidad adeudada**, pudiendo solicitar, además, una indemnización por daños y perjuicios si éstos se producen.
- En caso de no tener disponible el producto solicitado, también se puede informar al consumidor de la posibilidad de enviarle otro de características similares y de igual o superior calidad.

Normas de Comercio

Contratación OnLine. Las devoluciones.

- Desde el día en que el comprador recibe el producto, éste tiene un plazo de siete días hábiles para poder devolver el producto. Debe tenerse en cuenta que no se puede penalizar al comprador en caso de que decida hacer uso de este derecho de desistimiento.

- El comprador no está obligado a indicar ningún motivo para ello. No podrán devolverse todos los productos ya que existen limitaciones, entre otras, por ejemplo, productos perecederos, archivos de canciones, etc.

- Ejercitado este derecho, el vendedor debe devolver al comprador todas las cantidades íntegras, exceptuando los gastos de envío del producto, en un plazo máximo de treinta días. Si no se respeta este plazo, el consumidor puede exigir que se le devuelva el doble de la cantidad adeudada, pudiendo solicitar, además, una indemnización por daños y perjuicios si éstos se producen.

Normas de Comercio

Contratación OnLine. Las devoluciones.

- El comprador no puede ejercitar su derecho de desistimiento, entre otros, en los siguientes casos:
  - Contratos de suministro de bienes cuyo precio esté sujeto a fluctuaciones de coeficientes del mercado financiero que el vendedor no pueda controlar.
  - Contratos de suministro de bienes confeccionados conforme a las especificaciones del consumidor o claramente personalizados, o que, por su naturaleza, no puedan ser devueltos o puedan deteriorarse o caducar con rapidez.
  - Contratos de suministro de grabaciones sonoras o de vídeo, de discos y de programas informáticos que hubiesen sido desprecintados por el consumidor, así como de ficheros informáticos, suministrados por vía electrónica, susceptibles de ser descargados o reproducidos con carácter inmediato para su uso permanente.
  - Contratos de suministro de prensa diaria, publicaciones periódicas y revistas.
  - Contratos de prestación de servicios cuya ejecución haya comenzado, con el acuerdo del consumidor y usuario.
  - Contratos de servicios de apuestas y loterías.

Normas de Comercio

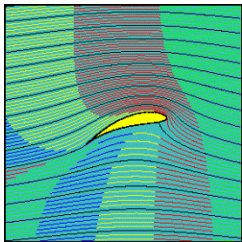
Contratación OnLine. Productos deteriorados.

- Cuando se deba reparar o sustituir el producto que hayamos enviado por que este no funciona hay que tener en cuenta que tanto la reparación como sustitución deben ser gratuitas para el consumidor y usuario, es decir, no se lo puede cobrar los gastos que haya que realizar para reparar o sustituir el producto, especialmente los gastos de envío, así como los costes relacionados con la mano de obra y los materiales.

- Deberán llevarse a cabo en un plazo de tiempo razonable y sin mayores inconvenientes para el consumidor y usuario de acuerdo con la naturaleza de los productos y de la finalidad que tuvieran para el consumidor y usuario.

- La reparación y la sustitución suspenden el cómputo de los plazos durante los cuales el consumidor puede reclamar por el mal funcionamiento del producto, por no servir para los usos para los cuales se compró o por no ajustarse a las características ofrecidas.

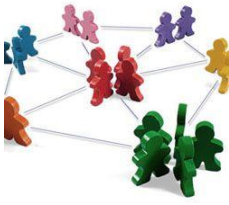
- Durante los seis meses posteriores a la entrega del producto reparado, el vendedor responderá de las faltas de conformidad que motivaron la reparación, presumiéndose que se trata de la misma falta de conformidad cuando se reproduzcan en el producto defectos del mismo origen que los inicialmente manifestados.



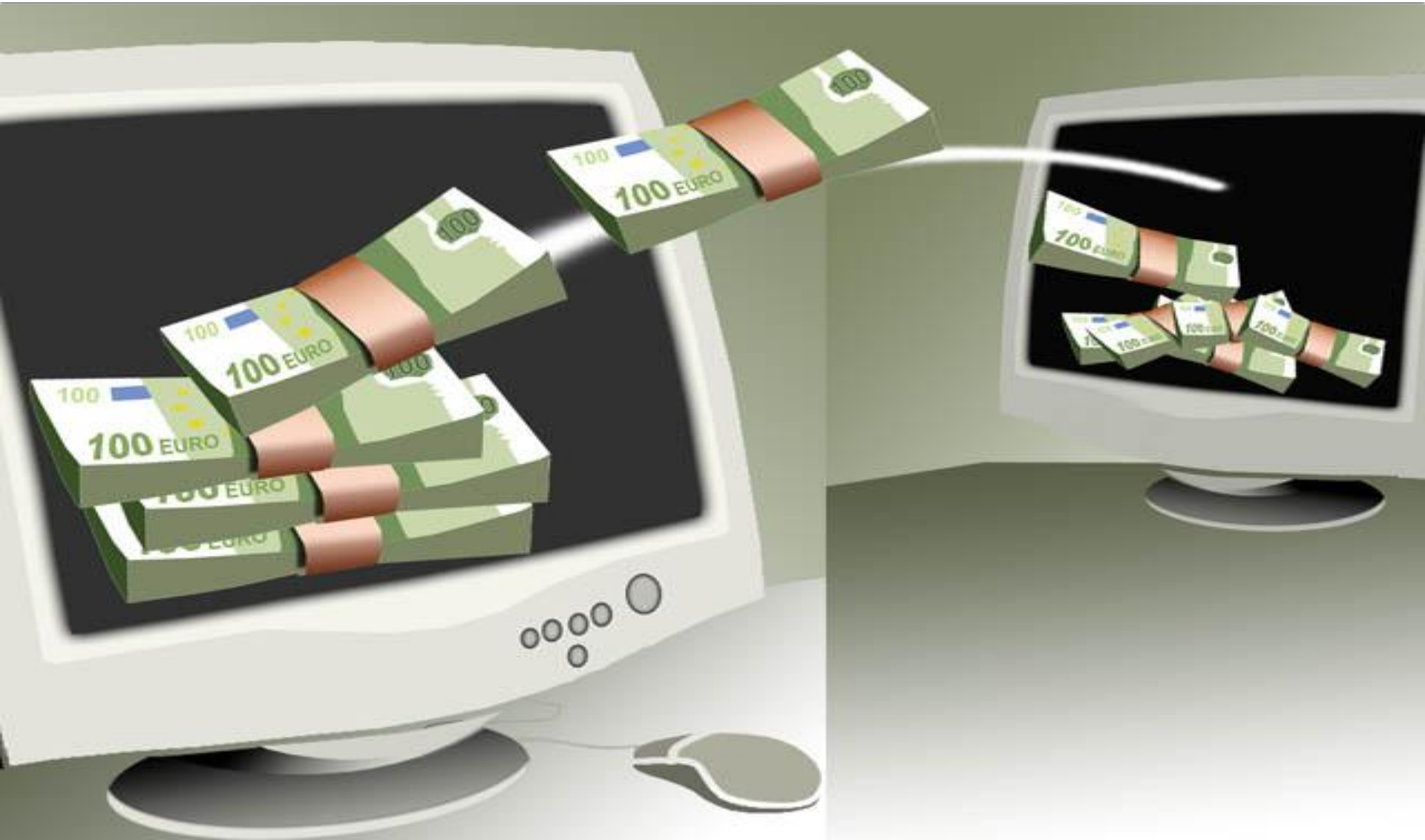
Normas de Comercio

Contratación OnLine. Productos deteriorados.

- Si concluida la reparación y entregado el producto, éste sigue siendo no conforme con el contrato, el consumidor y usuario podrá exigir la sustitución del producto, salvo que esta opción resulte desproporcionada, la rebaja del precio o la resolución del contrato.
- Si la sustitución no lograra poner el producto en conformidad con el contrato, el consumidor y usuario podrá exigir la reparación del producto, salvo que esta opción resulte desproporcionada, la rebaja del precio o la resolución del contrato.
- El consumidor y usuario no podrá exigir la sustitución en el caso de productos no fungibles, ni tampoco cuando se trate de productos de segunda mano.
- El plazo de tiempo durante el cual el vendedor responde de las faltas de conformidad que se manifiesten es de dos años desde la entrega, aunque en los productos de segunda mano, el vendedor y el consumidor podrán pactar un plazo menor, que no podrá ser inferior a un año desde la entrega.
- Salvo prueba en contrario, se presumirá que las faltas de conformidad que se manifiesten en los seis meses posteriores a la entrega del producto, sea éste nuevo o de segunda mano, ya existían cuando la cosa se entregó, excepto cuando esta presunción sea incompatible con la naturaleza del producto o la índole de la falta de conformidad.



Situaciones de Fraude en el Comercio Electrónico



Situaciones de Fraude en el Comercio Electrónico

- Introducción a los fraudes en la red
- Consejos básicos de Seguridad contra el fraude On-line
- Legislación Española relacionada con los Delitos Informáticos
- Consejos Grupo de Delitos Telemáticos – Guardia Civil
- Tipos de Fraude en la Red

Situaciones de Fraude en el Comercio Electrónico

- Introducción a los fraudes en la red
  - Estafas y fraudes son prácticas habituales de personas sin escrúpulos para aprovecharse de los usuarios y/o de los comerciantes.
  - Ejemplo típico:
    - Usuarios contactando con un tercero a través de un portal de subastas que una vez realizado el pago desaparecen sin entregar los productos.
  - Figura clave: un Tercero de Confianza que es el intermediario entre dos partes que realizan el acuerdo por medios electrónicos.

Situaciones de Fraude en el Comercio Electrónico

- Introducción a los fraudes en la red
  - Similar a un Notario para dar fe en el contrato de forma que ninguna de las partes pueda repudiar el contrato previamente firmado.
  - Existen diferentes métodos para garantizar la autenticidad y aceptación de estos acuerdos y contratos. Es labor del usuario elegir el método de mayor **confianza**.
  - Cada vez es mayor la alarma social ante estas estafas, lo que provoca que los estafadores maquillan cada vez mas el campo de actuación para que el usuario acepte.

Situaciones de Fraude en el Comercio Electrónico

- Introducción a los fraudes en la red
  - Ciertos usuarios/vendedores engañan a sus compradores haciéndoles ver que deben acudir a una Tercera parte neutral para que el comprador se sienta tranquilo ante la transacción.
  - La página web a través de la que se realiza la transacción es una estratagema para dar mayor confianza al cliente, y así recibir la transferencia.
  - Una vez la transferencia llega, el vendedor desaparece, la página de terceros de confianza queda desactivada y el comprador se queda sin dinero y sin producto.

cecarm
negocio electrónico en la Región de Murcia

VeriSign Secured ™

Situaciones de Fraude en el Comercio Electrónico

- Introducción a los fraudes en la red
  - No todas las compras y servicios ofrecidos en la Red son para timar a los cliente.
  - Hay que saber con quién se trata y para ello en España existe la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI), que intenta evitar este tipo de acciones, abogando por una Internet segura para poder acceder a multitud de servicios.

Situaciones de Fraude en el Comercio Electrónico

- Consejos básicos de seguridad contra el Fraude On-Line
  - La **Seguridad Total no Existe**. La única herramienta eficaz es la información y prevención.
  - Primero y Fundamental:
    - Mantener nuestro ordenador actualizado (instaladas las últimas versiones del sistema operativo y navegador web, utilizar un programa antivirus junto con un cortafuegos actualizarlos frecuentemente).

Situaciones de Fraude en el Comercio Electrónico

- Consejos básicos de seguridad contra el Fraude On-Line
  - Comercio Electrónico y Compras en línea.
    - Asegurarse de que la empresa vendedora dispone en su página de una pasarela de pagos segura
    - Las direcciones web donde se introduzcan datos personales y de pago, deben comen comenzar por https:// y debe aparecer un dibujo de candado en el navegador
    - No aceptar el pago por ningún tipo de servicio de envío de dinero.
    - Comprobar que en la website de la tienda on-line aparecen los datos fiscales de la misma, sede social y formas de contrato. Leer y verificar el "Aviso Legal".

Situaciones de Fraude en el Comercio Electrónico

- Consejos básicos de seguridad contra el Fraude On-Line
  - Comercio Electrónico y Compras en línea.
    - **Consejo**: Realice una búsqueda en internet con el nombre de la tienda y encontrará muchos resultados, si son negativos → Desconfíe.
    - Para la compra a un particular (subastas on-line o páginas de compra-venta) hay que tener en cuenta:
      - Saber con quién se trata. Si se paga por transferencia, hay que solicitar un recibo y poner el concepto exacto y el destinatario.
    - Desconfiar de los anuncios de venta donde se ofrecen productos de alto valor a un precio muy por debajo del mercado, sobre todo si se requiere una señal.

Situaciones de Fraude en el Comercio Electrónico

- Consejos básicos de seguridad contra el Fraude On-Line
  - Comercio Electrónico y Compras en línea.
    - Para pagos **contra reembolso**, algunas agencias de mensajería permiten la **apertura del paquete antes del pago**. Este servicio debe pactarse entre comprador y vendedor ya que supone un coste extra y hay que solicitarlo.
    - Guardar copias de todo: anuncio de venta, mensajes privados, mensajes de correo, direcciones de correo v de la web donde se anunciaba.

Situaciones de Fraude en el Comercio Electrónico

- Consejos básicos de seguridad contra el Fraude On-Line
  - Muy recomendable
    - Disponer de una cuenta bancaria y una tarjeta de débito asociada a esta que utilizaremos exclusivamente para nuestras transacciones en internet.
    - Sólo se dispondrá del efectivo suficiente para estas operaciones y aunque nuestros datos caigan en malas manos, no podrán obtener ningún beneficio.

Situaciones de Fraude en el Comercio Electrónico

- Consejos básicos de seguridad contra el Fraude On-Line
  - Phishing y derivados
    - Nunca nuestro banco, ni nuestro ISP o cualquier otro servicio nos pedirán por mail que "*por motivos de seguridad, administración u otro"* introduzcamos nuestros datos personales.
    - Para acceder a servicios bancarios on-line, abrir una ventana nueva en el navegador y teclear la dirección del mismo. Nunca a través de enlaces o hipervínculos por mail u otra web.
    - Hay que asegurarse de estar en un servidor seguro (https://) y que aparece un dibujo de candado en el navegador.

Situaciones de Fraude en el Comercio Electrónico

- Consejos básicos de seguridad contra el Fraude On-Line
  - E-mail, Scam y Hoaxes
    - Desconfiar de cualquier mensaje de un remitente desconocido por muy sugerente que resulte el asunto. Lo ideal es borrarlo directamente.
    - Cuidado con las ofertas de trabajo recibidas por email. Habitualmente se pide gestionar cantidades de dinero con un porcentaje de retribución. Es una versión moderna del timo "Las Cartas Nigerianas" → blanqueo de dinero procedente de actividades ilícitas, por lo tanto es delito.
    - No reenviar mensajes en cadena conocidos como HOAX, perjudicando y congestionando los servidores de correo, facilitando una base de datos de cuentas al autor para ser vendidas y usadas para publicidad (SPAM).

Situaciones de Fraude en el Comercio Electrónico

- Consejos del Grupo de Delitos Telemáticos de la Guardia Civil
  - Consejos para el comercio electrónico.
    - Comuníquese con el vendedor o comprador para informarse del producto o su cliente. Guarde todas las conversaciones por si se produce el fraude. El contacto telefónico es más fiable que los correos y amplían el campo de la investigación.
    - Aunque no es fiable al 100% la valoración del vendedor o comprador que hacen algunos portales de subastas, pueden ayudarle a decidirse. Informe Ud. de la transacción.

Situaciones de Fraude en el Comercio Electrónico

- Consejos del Grupo de Delitos Telemáticos de la Guardia Civil
  - Consejos para el comercio electrónico.
    - Utilice medios de pago que ofrezcan mayores garantías.
    - Los datos de su tarjeta de crédito pueden ser utilizados fraudulentamente en otro comercio electrónico. Utilice tarjetas de crédito virtuales que limitan el importe de compra.
    - Los estafadores utilizan páginas web de empresas mediadoras ficticias (SCROLL). Verifique que existen en el mundo real.
    - Busque en internet información sobre vendedores, compradores, productos y terceros. Existen foros de víctimas de fraude que trasladan su experiencia para prevenir.

Situaciones de Fraude en el Comercio Electrónico

- Consejos del Grupo de Delitos Telemáticos de la Guardia Civil
  - Consejos para el comercio electrónico.
    - Desconfíe de precios ridículos, gangas o superofertas sin garantías y fuera de la lógica comercial.
    - Si puede escoger método de pago utilice el reembolso, con derecho a la apertura del paquete previa a su aceptación.
    - Conserve todos los justificantes y resguardos hasta recibir y verificar el producto.

Situaciones de Fraude en el Comercio Electrónico

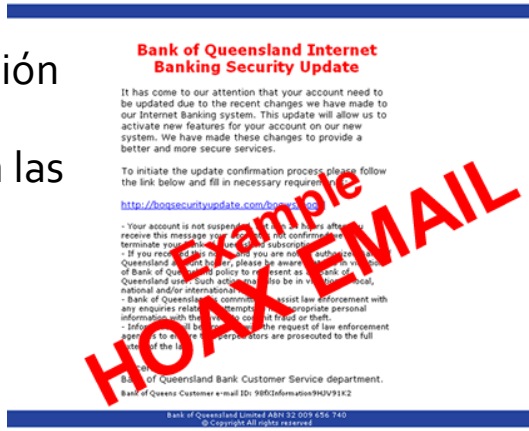
- Consejos del Grupo de Delitos Telemáticos de la Guardia Civil
  - Consejos para el comercio electrónico.
    - Si en el plazo establecido no recibe el producto y no hay respuesta del vendedor, denúncielo. El tiempo corre a favor del estafador.
    - Si el producto recibido es de características inferiores, exija su reposición. No lo conserve amparado en falsas promesas. Si no lo repone, denúncielo.
    - Si compra o vende en el extranjero, las posibilidades de perseguir un fraude se reducen.

Situaciones de Fraude en el Comercio Electrónico

- Consejos del Grupo de Delitos Telemáticos de la Guardia Civil
  - Consejos para usuarios de internet
    - Actualice constantemente el sistema operativo y el software utilizado, especialmente el navegador.
    - Con sistemas Windows, trabaje con una cuenta SIN privilegios de administrador. Evitará la instalación de programas maliciosos.
    - Utilice antivirus. Actualícelo periódicamente. Rehúse copias piratas.
    - Instale un cortafuegos o firewall.
    - No abra mensajes de correo electrónico no solicitados o de procedencia desconocida. Elimínelos directamente.
    - Especial cuidado con las redes P2P. Son fuentes de infección malware. Analice cada descarga con el antivirus.

Situaciones de Fraude en el Comercio Electrónico

- Consejos del Grupo de Delitos Telemáticos de la Guardia Civil
  - Consejos para usuarios de internet
    - Al navegar por Internet, busque páginas de confianza, avalados por sellos o certificados de calidad, evitando contenidos dudosos.
    - Utilice siempre software legal. Evite las descargas de programas de sitios no seguros.
    - Desconfíe de los mensaje que piden reenvío a conocidos, informando de noticias llamativas o por motivos filantrópicos. Muchos buscan captar direcciones de correo electrónico para prospectivas comerciales y son un engaño (HOAX)
    - Desconfíe de emails de supuestas entidades bancarias. Confirme telefónicamente o en su sucursal cualquier petición de datos de banca electrónica.
    - Limite el acceso a su información a personas conocidas en las redes sociales.



Situaciones de Fraude en el Comercio Electrónico

- Tipos de fraude en la Red.
  - Phishing
    - Consiste en la recepción de mensajes de correo falsos de entidades bancarias, en los que se solicita por distintos motivos que facilitemos nuestros datos e introduzcamos el código PIN.
    - Posteriormente se utilizan de forma fraudulenta estos datos para obtener un beneficio.
    - Características comunes:
      - Copia exacta de páginas bancarias oficiales y sus correos.
      - Solicitud de datos personales
      - Petición del código PIN.
    - A tener en Cuenta:
      - No introducir ningún dato en formularios de origen desconocido
      - No hacer click en enlaces bancarios recibidos por email
      - Asegúrese de estar en un servidor seguro antes de cualquier operación
      - Mantenga actualizado su navegador web.
      - No abrir emails de origen desconocido.
    - Ojo: El Phishing no se limita al fraude bancario.

Situaciones de Fraude en el Comercio Electrónico

- Tipos de fraude en la Red.
  - Comercio Electrónico.
    - Ventas Trampa
      - Tenemos un anuncio en internet y recibimos ofertas por una cantidad superior al precio de venta.
      - Se ofrecen a pagar inmediatamente por medio de Talones nominativos, transferencias bancarias o empresas de envío de dinero.
      - Le comunican que por error han ingresado una cantidad mayor a la acordada, enviándole un falso email del banco notificando el ingreso (o vía sms)
      - Se le propone que devuelva la diferencia a través de empresas de envío de dinero. Todo es un engaño.

Situaciones de Fraude en el Comercio Electrónico

- Tipos de fraude en la Red.
  - Email.
    - SCAM
      - Captación de personas por email, anuncios en foros, páginas de empleo o similares, con ofertas de trabajo muy ventajosas.
      - Facilitarán números de teléfono, direcciones e incluso es posible que le envíen documentos con rúbricas y sellos de entidades totalmente falsos.
      - Son empresas ficticias que le pedirán una cuenta bancaria para operar con sus activos. Recibe ciertas cantidades de dinero en su cuenta y debe transferirlo a otras o remitirlo a través de empresas de envío de dinero. El trabajador se queda con un porcentaje.
      - Se utiliza para blanquear dinero.
      - Este dinero procede de phishing que al percatarse de movimientos no autorizados acuden al banco señalando a la victima del scam como destinatario del dinero, que es denunciado al no poder devolverlo.
      - Muy importante: copias de todos los correos enviados y recibidos, teléfonos, direcciones para acreditar lo sucedido realmente.

Situaciones de Fraude en el Comercio Electrónico

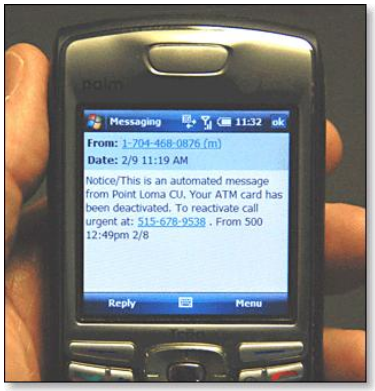
- Tipos de fraude en la Red.
  - Email.
    - Sorteos, herencias y similares.
      - Se trata de un email notificando que es el ganador de una cantidad importante de dinero, viaje, vehículo o cualquier otro bien.
      - Se le pide una cantidad de dinero para tramitación, impuestos o tasas y luego desaparecen.
      - Utilizan nombres de empresas conocidas internacionalmente.
      - Le envían enlaces a páginas idénticas al banco X, pidiendo los datos bancarios.
      - Se le solicita ayuda para cobrar una herencia o mover cantidades de dinero embargadas o retenidas a cambio de un porcentaje.
      - Pueden enviar datos personales, teléfonos, apartados de correos, fotos hasta pedirle el dinero de tramitación, abogados o similares.

Situaciones de Fraude en el Comercio Electrónico

- Tipos de fraude en la Red.
  - Otros.
    - Recarga de móviles.
      - Oferta de precios más bajos y promociones. Solicitan su tarjeta de crédito para uso fraudulento.
    - Vishing.
      - Variante del Phishing, mediante telefonía a través de internet (VoIP) se le ofrece la posibilidad de llamar a cualquier parte.
      - Recibe un email o mensaje de voz en el buzón, comunicando que existe un problema con su cuenta bancaria y que llame al teléfono gratuito adjunto.
      - Cuando llama el usuario, una centralita telefónica simulando la entidad bancaria pide los datos de su cuenta.

Situaciones de Fraude en el Comercio Electrónico

- Tipos de fraude en la Red.
  - Otros.
    - Smishing
      - Phishing para móviles. Objetivo: conseguir los datos bancarios mediante un SMS en el móvil.
      - Se informa de un cargo en cuenta o la suscripción de un servicio que necesita darlo de baja accediendo a la dirección web indicada.
      - Mediante ingeniería social intentan conseguir datos bancarios o personales.
      - Una variante es mediante la comunicación de un premio dándole un teléfono con tarificación adicional para enviar un sms con sus datos.
    - Casinos en línea
      - El fraude está relacionado con la obtención de las tarjetas de crédito para operar.
      - Los juegos están amañados y se perderá más dinero que otra cosa.
      - Existen casinos prestigiosos sometidos a control fiscal para jugar con total seguridad.



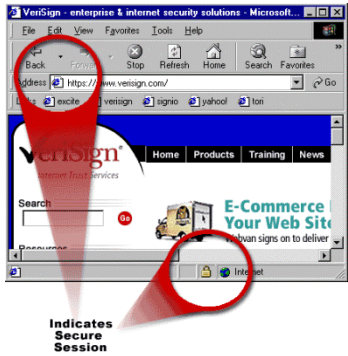
Seguridad

Seguridad

- Introducción a la seguridad en entornos de Comercio Electrónico
- Reglas para una compra segura por Internet
- Consejos para una compra segura

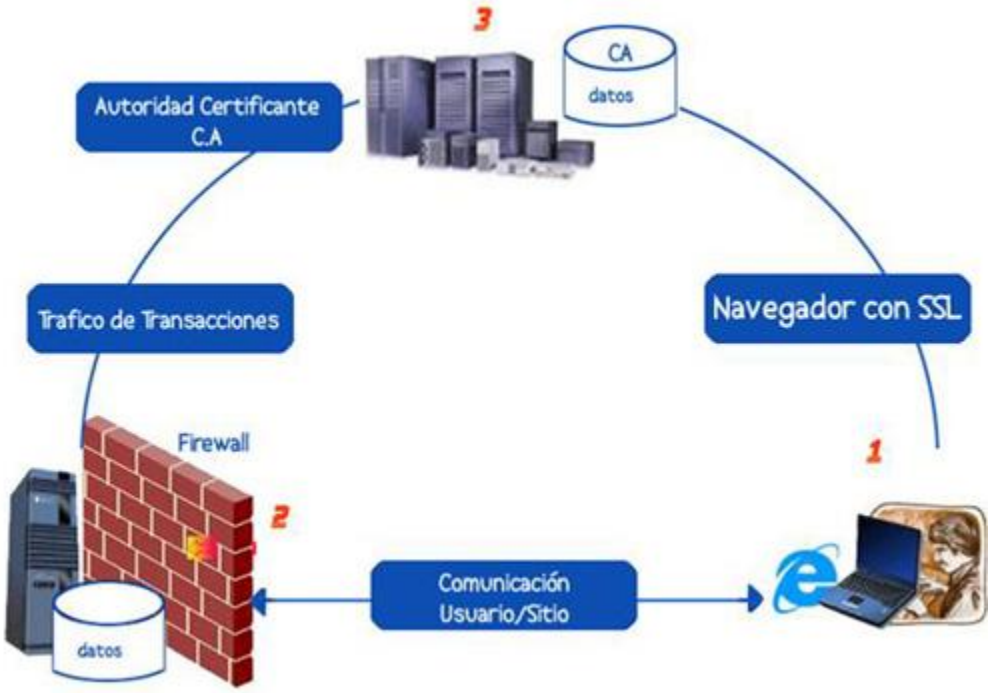
Seguridad

- Introducción a la seguridad en entornos de Comercio Electrónico
  - Existen diferentes protocolos para procesar compras de manera segura. El más utilizado es SSL.
  - La seguridad de un sitio electrónico debe ser confiable.
  - La seguridad en entornos de Comercio Electrónico consta:
    - **Privacidad**: Transacciones no visualizadas por nadie no autorizado.
    - **Integridad**: Datos o transacciones no pueden ser alterados.
    - **No Repudio**: Quien generó la transacción se hace responsable de la misma.
    - **Autenticación**: Los intervinientes son leales y válidos.
    - **Facilidad**: La transacción no debe tener dificultad



Seguridad

- Introducción a la seguridad en entornos de Comercio Electrónico
  - Herramientas para proteger un sitio E-commerce.

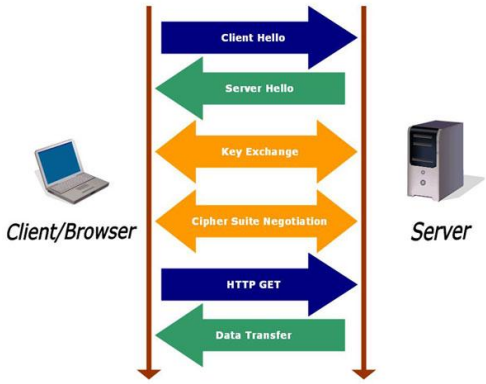


Seguridad

- Introducción a la seguridad en entornos de Comercio Electrónico
  - Firewalls (Corta Fuegos)
    - Herramienta preventiva que realiza una inspección del tráfico entrante y saliente.
    - Impide que servicios o dispositivos no autorizados accedan a ciertos recursos protegiendo contra ataques (por ejemplo DoS – Denegación de Servicio.)

Seguridad

- Introducción a la seguridad en entornos de Comercio Electrónico
  - SSL
    - Secure Sockets Layer (Protocolo de Capa Segura).
    - Se compone de 2 capas y funciona de la siguiente manera:
      - La primera capa encapsula los protocolos de nivel más alto.
      - La segunda capa se encarga de la negociación de los algoritmos de encriptación y autenticación del cliente y servidor.

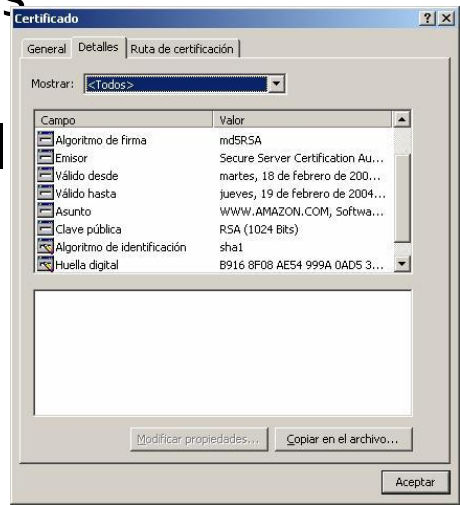


Seguridad

- Introducción a la seguridad en entornos de Comercio Electrónico
  - Certificados.
    - Una Autoridad de Certificación (CA) es una Empresa u Organismo que emite certificados.
    - Se utilizan para validar la autenticidad de un servidor o página web.
    - Un certificado contiene la siguiente información:
      - Dominio para el que se expidió
      - Dueño del certificado
      - Domicilio del dueño
      - Fecha de validez

Seguridad

- Introducción a la seguridad en entornos de Comercio Electrónico
  - Certificados.
    - Para analizar la información básica del certificado, pulsamos sobre el candado del navegador y podemos comprobar el certificado del servidor sobre el que estamos realizando la transacción.
    - Podemos acceder a la información adicional para comprobar el tipo de algoritmo, la fuerza del cifrado, etc.

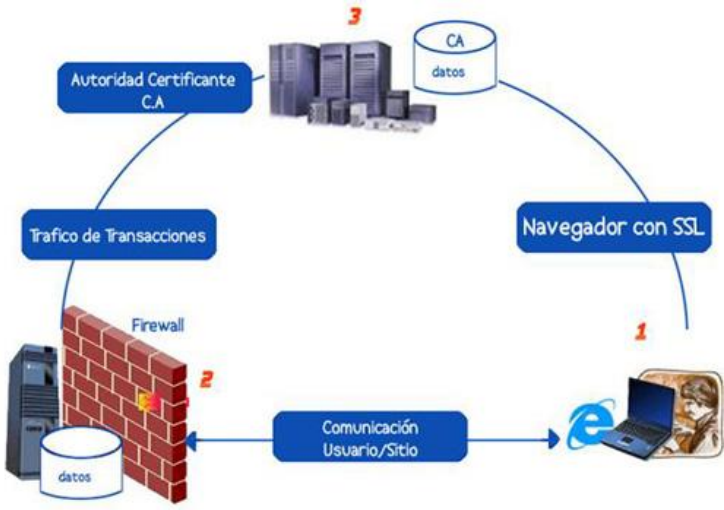


Seguridad

- Introducción a la seguridad en entornos de Comercio Electrónico

  Punto 1: El usuario que se conecta al punto 2 (servidor)

  Punto 2: Muestra los productos, los seleccionamos y procesamos la compra en el sitio seguro. El punto 2 contacta con el punto 3 (CA) y nos dice si es válido o no.

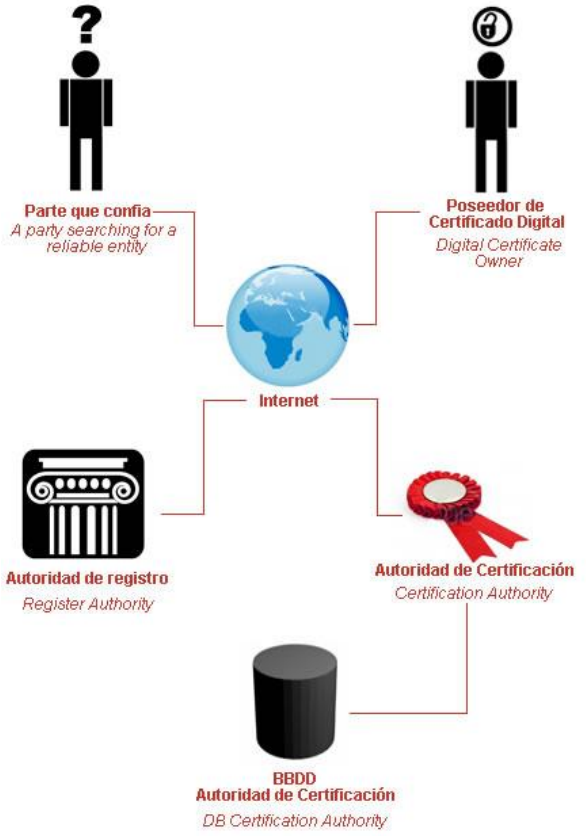


Seguridad

- Introducción a la seguridad en entornos de Comercio Electrónico
  - Infraestructura de Clave Pública (PKI)
    - Permite la gestión de certificados.
    - Soluciones hardware, software y políticas de seguridad que permiten emitir, validar, distribuir y revocar Certificados Digitales. Pueden utilizarse para la firma electrónica de documentos, email, etc.
    - Qué provee PKI:
      - Confidencialidad, Integridad de los Mensajes, Autenticación, No repudio y control de acceso.

Seguridad

- Introducción a la seguridad en entornos de Comercio Electrónico
  - Infraestructura de Clave Pública (PKI)
    - Componentes:
      - Política de Seguridad: cómo ejecutará la gestión de claves públicas y privadas.
      - Autoridad Certificadora (CA): genera los Certificados Digitales, usando una clave privada para firmarlos. Emite y revoca Certificados y crea Listas de certificados no válidos (CRL).
      - Autoridad de Registro (RA): gestiona altas y bajas de peticiones de certificación y revocaciones.
      - Autoridad de Validación (VA): proporciona información sobre el estado de los certificados. Consultas a las CRLs.
      - Sistema de Distribución de Certificados.
      - Aplicaciones habilitadas por PKI: comunicación servidores, correo electrónico, EDI, transacciones de tarjetas de créditos, VPN, ...



Seguridad en las Compras

- Reglas para una compra segura por Internet
  - **Verifique los sistemas de pago** utilizados por el portal y la fecha de cargo del pago.
  - **Lea la descripción del producto** controlando si los datos son completos.
  - **Conozca el sitio bien antes de comprar**. Investigue. Pruebe con producto barato para asegurarse que el sitio es confiable. Compruebe por teléfono si es legítimo.
  - **Lea la política de privacidad y seguridad del sitio**. Todo sitio confiable ofrece información sobre su transacción.
  - **Proporcione la mínima cantidad de información posible**. El nombre y dirección deben proveerse. Pueden pedirle más información con fines comerciales, correos masivos (spam), correspondencia directa o llamadas. No conteste preguntas no apropiadas para la transacción.

Seguridad en las Compras

- Reglas para una compra segura por Internet
  - **Su contraseña es sólo para usted**. La mayoría de sitios requieren usuario y contraseña. No revele su contraseña a otra persona y no utilice combinaciones comunes como la fecha de cumpleaños, carnet de conducir o seguridad social. No utilice la misma contraseña en otros sistemas.
  - **Mantenga fotocopias de sus transacciones.** Al final de la compra debe aparecer el resumen de la transacción. Guarde una copia. Imprima la página con el nombre del negocio, dirección, teléfono y términos legales de su compra. Archive esta información hasta el final de la garantía.

Seguridad en las Compras

- Reglas para una compra segura por Internet
  - **Consulte el producto a través de campos de "preguntas y respuestas"**. Procure resolver sus dudas y consultas, compatibilidades, características y funcionalidades del producto. Cuidado cuando no se responde a sus preguntas.
  - **Verifique las políticas de entrega del vendedor,** formas de pago, garantías y condiciones de cambio. Plazo de entrega, factura, forma de pago, tiempo de garantía y situaciones previstas para el cambio. Deben ser políticas razonables.
  - **Preste atención a los email que recibe**
  - **Use su intuición**
  - **No sea ingenuo,** si el precio es demasiado bajo para ser real, seguramente no lo es.

Seguridad en las Compras

- Consejos para una compra segura.
  - **¿Cómo debe ser una página de comercio electrónico segura?**
    - Tienen que garantizar que los datos de la transacción sólo sean accesibles por las partes implicadas, cifrando la información.
    - Deben mantener la integridad de la información para que no puedan manipularse los datos, empleando firmas digitales.
    - Deben verificar la identidad del comprador y vendedor mediante la emisión de certificados digitales.

Seguridad en las Compras

- Consejos para una compra segura.
  - **Protocolos de seguridad.**
    - Conjunto de especificaciones técnicas para conseguir una manera segura de realizar transacciones electrónicas. En ellas están involucrados el usuario final, comerciante, entidades financieras, compañías de tarjetas y propietarios de las marcas de tarjetas.
    - El protocolo de seguridad más utilizado es **SSL**. Se encarga de cifrar los datos introducidos y descifrarlos en destino. Si una tercera parte interceptase los datos, no podría acceder a ellos sin una clave capaz de descifrar la información. Sólo el vendedor muestra el certificado digital que verifica su identidad.

Seguridad en las Compras

- Consejos para una compra segura.
  - **Certificación del servidor.**
    - Cualquier empresas de Comercio Electrónico debe tener certificado de seguridad de sus servidores otorgada por una autoridad certificadora reconocida.
    - La empresas debe cuidar que sus servidores estén libres de virus o troyanos para preservar la integridad de los datos.
    - Las autoridades certificadoras expiden los certificados digitales a empresas o compradores.

Referencias

ontsi observatorio nacional de las telecomunicaciones y de la SI

Agencia Tributaria

AECEM fecemd

cecarm negocio electrónico en la Región de Murcia www.cecarm.com

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gracias por su atención

cecarm
negocio electrónico en la Región de Murcia

www.cecarm.com

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional

Crecemos con Europa

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

plan avanza

Región de Murcia

regiónDemurciaSI

fundación integra