

Comercio Electrónico Orientado a Emprendemento

Aspectos clave da xestión dunha tenda online (4)

Dani Cerqueiro

@danicerqueiro

www.danicerqueiro.eu

5- Lexislación aplicable

LOPD

Guía sobre privacidad y seguridad en internet

La AEPD e INCIBE publican 18 fichas prácticas para concienciar a los usuarios de la importancia de proteger su información personal, ofreciendo consejos y recomendaciones prácticas.

[Vídeos de configuración de privacidad](#)

[Nota de prensa](#)



[Bienvenida a la Agencia](#)

[En qué podemos ayudarte y en qué no](#)

Ciudadanos

La protección de datos es un derecho fundamental. Conócelo.

[Conoce tus derechos](#)

[Consulta la guía del ciudadano](#)

[Canal del ciudadano](#)

Profesionales

Cumplir con la LOPD no es difícil. Descubre cómo.

[Cumple con tus obligaciones](#)

[Inscribe tu fichero](#)

[Canal del responsable](#)

1



Plan
Estratégico

PRIVACIDAD Y SEGURIDAD



Consejos y recomendaciones



Sede
electrónica

NOTIFICACIONES
ELECTRÓNICAS A
LA AEPD

Inscripción de Ficheros



Claves cumprimento LOPD:

- **Informar aos usuarios** sobre o tratamento e uso que se fará dos seus datos.
- **Consentimento expreso** dos usuarios.
- **Dereitos ARCO** (Acceso, Rectificación, Cancelación e Oposición).
- **Declaración de ficheiros** ante a AEPD.
- **Documento de Seguridade**, que describa as medidas legais, técnicas e organizativas para garantir a seguridade dos datos.
- **Firma de contrato** con Encargados de Tratamento.





Evalúa

Ferramenta tipo test de autoevaluación do cumprimento da LOPD e medidas de seguridade básicas. Unha vez rematado (45min aprox.) xera informe de resultados con suxerencias de mellora.

<http://www.servicios.agpd.es/Evalua>



Formulario NOTA

Axuda aos encargados do tratamento a inscribir a creación, supresión e/ou modificación dos ficheiros na Agencia Española de Protección de Datos. Permite cumprimentar o formulario e envíalo directamente á Agencia.

<http://sedeagpd.gob.es/sede-electronica-web/vistas/formNOTA/>




Guía modelo

Permite xerar o documento de seguridade de xeito sinxelo, simplemente cumprimentando os datos da empresa.

https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/herramientas_ayuda/common/modelo_doc_seguridad.doc

LSSI



INFORMACIÓN PRÁCTICA
En esta sección se incluye todo tipo de información relativa a aspectos prácticos de los contenidos de la Ley. 

PREGUNTAS FRECUENTES
Ámbito de aplicación, Prestación del servicio, Obligaciones, Contratación eléctrica, Responsabilidad, Comunicaciones comerciales 

 <p>PROVEEDORES Obligaciones de los proveedores de servicios.</p>	 <p>EMPRESAS Obligaciones de las empresa y ejemplos prácticos.</p>	 <p>CIUDADANOS Obligaciones de los ciudadanos y ejemplos prácticos.</p>
---	--	---

Web LSSI: <http://www.lssi.gob.es/paginas/Index.aspx>



Cookie: pequena información enviada por un sitio web e almacenada no navegador do usuario, de xeito que o sitio web pode consultar certa actividade do usuario.

Tipos de cookies:

- **Propias** (xestiónanse dende o terminal ou dominio do editor) ou de **terceiros** (enviadas por outra entidade).
- De **sesión** (só se recollen mentras o usuario navega polo sitio web) ou **persistentes** (os datos continúan almacenados na terminal durante un período de tempo determinado).
- **Técnicas** (controlan tráfico e comunicación de datos), **personalización** (recollen actividade do usuario: idioma, navegador...), **análise** (recollen datos sobre comportamento do usuario) e **publicitarias** (recollen datos sobre a xestión dos espazos publicitarios).

[Ley 34/2002, de Servicios de la Sociedad de la Información \(LSSI\)](#) obliga a informar sobre o uso de *cookies* no sitio web para que **o usuario poida aceptar ou rexeitar** expresamente o seu uso.

Recomenda sistema “doble capa”:

- **1ª capa:** aviso de cookies.
- **2ª capa:** ligazón a “aviso legal”, “política de cookies”...

Este sitio utiliza cookies para mellorar a experiencia do usuario - [Ver detalles](#)

Permitir cookies

Utilizamos cookies propias y de terceros para mejorar nuestros servicios y mostrarte publicidad relacionada con tus preferencias mediante el análisis de sus hábitos de navegación. Si continúas navegando, consideramos que acepta su uso. [ESTOY DE ACUERDO](#) [NO](#) [POLÍTICA DE COOKIES](#)

Utilizamos cookies propias y de terceros para ofrecer nuestros servicios y recoger información estadística. Si continúa navegando, acepta la instalación y el uso. [Más información](#)

¡Entendido!

6- Seguridade

Requerimentos de seguridade na rede, que deberían cumprirse en todas as operacións que supoñen un intercambio comercial, e especialmente na comunicación de datos personais, en pedidos de compra, na autorización de pagos e na realización efectiva dos mesmos.

1.- **Confidencialidade ou privacidade.** É necesario garantir que a información que se transmite por internet sea ilexible para as persoas e entidades non autorizadas.

2.- **Autenticación.** Os sistemas de comercio electrónico deben ser capaces de identificar a todos os participantes no intercambio, así como nos seus elementos.

Deben garantir que a identidade do establecemento ou comercio virtual non poderá ser suplantada, de modo que ningunha outra persona, física ou xurídica, poida realizar ataques de [*phishing*](#).

3.- Integridade. A seguridade na web tamén implica detectar alteracións introducidas no contido orixinal das mensaxes. Tamén debe asegurarse que as mensaxes recibidas coinciden coas enviadas.

O sistema será íntegro se garantiza a detección de calquera modificación na información do intercambio comercial.

4.- Non repudio. Os sistemas de seguridade en internet deben ter capacidade de garantir que a información enviada sexa recibida e lida polo seu destinatario, de forma que este non poida rexeitar a súa recepción.

O non repudio dunha información ou pago electrónico refírese á imposibilidade de que o comprador negue ter adquiridos determinados compromisos cando, en realidade, si que ten adquirido, sen que o establecemento online poida probar o que inicialmente tiñan acordado.

Esta propiedade de non repudio debe diferenciarse do dereito por lei que teñen todos os consumidores a devolver os produtos, cando estos foran comprados por internet.

Todo los requerimientos anteriores de seguridad electrónica no se cumplirían si no se acompañan de los mecanismos adecuados para proteger las aplicaciones y sistemas de información que intervienen en las compras online.

Estas técnicas recogen dos ámbitos, uno centrado en la transmisión de datos a través de internet (**Seguridad SSL**) y otro enfocado hacia el almacenamiento de los mismos (**Seguridad de Datos**).

1) Seguridad SSL en la Transmisión de Datos

A protección da información que se transfire a través de internet realízase a través de técnicas criptográficas que garantizan que os sistemas de comercio electrónico reúnen as propiedades de seguridade xa comentadas.

O protocolo de transmisión de información sensible por internet máis extendido chámase **protocolo SSL** (*secure sockets layer*). Sobre dito protocolo establécense comunicacións cifradas entre os participantes dunha transacción electrónica, o que garantiza a confidencialidade e a integridade dos datos transportados.

O usuario pode comprobar que a URL da páxina pasa a ser https:// en lugar de http:// y que o seu navegador incorpora un símbolo indicativo, como una chave ou un candado cerrado.

Por elo, é aconsellable que as entidades que ofrecen intercambios comerciais por internet implementen SSL con autenticación. Para dar de alta este proceso necesitan que unha [autoridade de certificación](#) emita un par de claves y un [certificado dixital](#).

Na práctica, os navegadores incorporan unha relación de autoridades de certificación nas que se pode confiar. Se a autoridade de certificación non ten un amplo recoñecemento, o navegador abre unha consulta ao usuario preguntándolle se confía na autoridad de certificación.

En cambio, aos usuarios non se lles soe requerir a autentificación da súa identidade, xa que facerse cos certificados e as claves supón para eles trámites adicionais. Hai excepcións en actividades que precisan dun alto nivel de seguridade, como a presentación de impostos á Axencia Tributaria.

Respecto ao repudio, a maioría de implementacións SSL proporcionan a propiedade de non repudio ás actividades dos servidores, pero non así as dos clientes. Por elo, a gran maioría de fraudes no comercio electrónico producense polo feito de que o vendedor non autentificou aos clientes de forma plenamente segura (a través de certificados).

O feito de que o pago online se realizara mediante tarxeta de crédito non significa que o usuario ou consumidor sexa verdadeiramente o titular da tarxeta bancaria.

Por iso, algunhas modalidades de pago online, como as pasarelas de pago verificadas, introduzcan elementos adicionais que permiten cumprir as propiedades de autentificación e non repudio por parte dos clientes. Para máis información: [formas de pagos online más seguras en internet](#).

2) Seguridade de datos no almacenamento

As aplicacións e datos que almacenan os ordenadores que se conectan a internet adoitan estar protexidos a través de aplicacións ou software como os [cortalumes \(firewall\)](#), sistemas de detección de intrusos ou programas antivirus, que detectan e impiden os intentos de acceso que proceden de intrusos e programas maliciosos.

Os establecementos online deben ter en conta que o almacenamento e a xestión dos datos personais dos clientes nas bases de datos da empresa debe ser acorde coa Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Personal, así como pola Lei 34/ 2002, de 11 de xullo, de Servicios de la Sociedad de la Información.

Os usuarios para realizar operacións de compra e ter acceso á base de datos da entidade que vende online deben rexistrarse para a súa identificación, o que habitualmente realízase por medio dun nome de usuario e unha contrasinal.

Na identificación, adoítase requerir o uso de mecanismos de cifrado, normalmente a través do protocolo SSL, para evitar que os datos empregados na identificación poidan ser interceptados cando son transmitidos por internet.

Graciñas

Dani Cerqueiro

@danicerqueiro

www.danicerqueiro.eu