TEMA 5. ESTÁNDARES Y NORMATIVAS LEGALES APLICABLES A LOS ENTORNOS WEB

Objetivos:

- Conocer el marco legal aplicable a los Sistemas de Información Basados en Web
- Comprender la necesidad del seguimiento de las recomendaciones y normativas de accesibilidad y usabilidad

NORMATIVAS DE ACCESIBILIDAD WEB (WCAG)

La accesibilidad Web significa que personas con algún tipo de discapacidad van a poder hacer uso de la Web. En concreto, al hablar de accesibilidad Web se está haciendo referencia a un diseño Web que va a permitir que estas personas puedan percibir, entender, navegar e interactuar con la Web, aportando a su vez contenidos. La accesibilidad Web también beneficia a otras personas, incluyendo personas de edad avanzada que han visto mermadas sus habilidad a consecuencia de la edad.

En España, las leyes a considerar en cuestión de accesibilidad web son el Real Decreto 1494/2007 , de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social y la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, donde aparecen una serie de artículos de especial trascendencia para el mundo empresarial.

Ilustración 32: El W3C ofrece una serie de herramientas para evaluar la accesibilidad de las Webs (https://validator-suite.w3.org/)

Las Pautas de Accesibilidad para el Contenido Web (WCAG) 2.0 se publicaron el 11 de diciembre de 2008, tras un largo proceso de desarrollo, revisión, debate y consenso, coordinado por uno de los grupos de trabajo de la Iniciativa para la Accesibilidad Web (WAI), perteneciente al W3C.

WCAG 2.0 es una evolución de la primera versión de las pautas (WCAG 1.0, publicadas en mayo de 1999). Como en la versión anterior, su objetivo principal es establecer unos criterios claros que permitan tanto el desarrollo de contenidos accesibles como la evaluación de la accesibilidad de contenidos ya existentes. No obstante, aunque WCAG 2.0 contiene muchos de los criterios recogidos en WCAG 1.0, existen algunas diferencias importantes, tanto en su filosofía como en su estructura.

La más notable de estas diferencias es la denominada "neutralidad tecnológica", es decir, la independencia de las pautas respecto de la tecnología usada para crear contenidos web. Así, mientras las WCAG 1.0 estaban orientadas sólo a aquellas tecnologías desarrolladas por el W3C (principalmente HTML y CSS), las WCAG 2.0 pueden aplicarse a cualquier tecnología de contenidos que disponga de características de accesibilidad. Esta independencia no sólo permite evaluar o desarrollar contenidos con otras tecnologías presentes, sino que también permite que las WCAG 2.0 puedan ser aplicadas a tecnologías futuras aún no desarrolladas.

La Norma **UNE 139803:2012: Requisitos de Accesibilidad para contenidos en la Web** , es una norma española de reciente aprobación (julio de 2012) que establece los requisitos de accesibilidad para los contenidos web. En cuanto a sus requisitos, referencia completamente a las Pautas de Accesibilidad para el contenido web WCAG2.0 de la Iniciativa para la Accesibilidad Web (WAI) del Consorcio de la Web (W3C) por lo tanto hay una equivalencia directa entre ellas.

Además, en la redacción de los criterios recogidos en WCAG 2.0 se partió de la idea de que todos ellos debían ser verificables, es decir, se han redactado de forma que puedan ser verificados con fiabilidad mediante una combinación de análisis automatizados y comprobaciones manuales. Para facilitar esta labor, en lugar de redactarse como instrucciones del tipo "para cumplir X, debe hacerse B", se describen como implicaciones lógicas del tipo "si ocurre Y, entonces se cumple B". Este cambio, que en apariencia conduce al mismo resultado, permite sin embargo verificar el cumplimiento de un determinado criterio bajo un abanico mucho más amplio de circunstancias: por ejemplo, al aplicar distintas técnicas para resolver un mismo problema; al usar distintas tecnologías de contenidos (donde las técnicas aplicables pueden variar); o bajo distintos entornos de uso (sistema operativo, aplicaciones de usuario, productos de apoyo, etc.).

Los cuatro principios de la accesibilidad

WACG 2.0 se organiza en torno a cuatro principios teóricos que buscan garantizar el acceso a los contenidos. Cualquier usuario que use la Web debe obtener un contenido:

1. **Perceptible**. Es decir, que la información y los elementos del interfaz de usuario deben ser presentados a los usuarios de forma que ellos puedan percibirlos mediante al menos uno de los sentidos.
2. **Operable.** Es decir, que cualquier usuario pueda realizar la interacción necesaria para actuar sobre el contenido.
3. **Comprensible**. Es decir, que la información y el manejo de la interfaz de usuario debe ser comprensible (legible, entendible, predecible…)
4. **Robusto,** que quiere decir que el contenido debe estar suficientemente descrito para poder ser leído con distintos lectores y con distintas tecnologías de asistencia.

Si no se cumple alguno de estos principios, los usuarios con discapacidad sensorial o motora no podrán usar la web.

Pautas generales de accesibilidad

WACG 2.0 ofrece doce pautas generales que proporcionan los objetivos básicos que se deben lograr para crear un contenido accesible, organizadas por los distintos principios:

Perceptibilidad

Pauta 1.1: Alternativas textuales. Se deben proporcionar alternativas textuales para cualquier contenido no textual.

Pauta 1.2: Alternativa para multimedia tempo-dependientes. Se deben proporcionar alternativas para el contenido multimedia basado en el tiempo.

Pauta 1.3: Adaptable. El contenido se debe crear de varias formas pero sin perder información o estructura.

Pauta 1.4: Distinguible (vista y oído). Se debe facilitar a los usuarios el ver y escuchar el contenido, incluyendo distinción entre lo más y menos importante.

Operatibilidad

Pauta 2.1: Acceso mediante teclado. Toda la funcionalidad debe estar disponible desde el teclado.

Pauta 2.2: Suficiente tiempo. La información debe permanecer durante suficiente tiempo para leer y usar el contenido.

Pauta 2.3: Destellos. No se debe diseñar con formas que puedan provocar ataques epilépticos.

Pauta 2.4: Navegable. Se debe proporcionar a los usuarios medios que ayuden a navegar, localizar el contenido y determinar dónde se encuentran.

Comprensibilidad

Pauta 3.1: Legible y entendible. El contenido debe ser legible y comprensible.

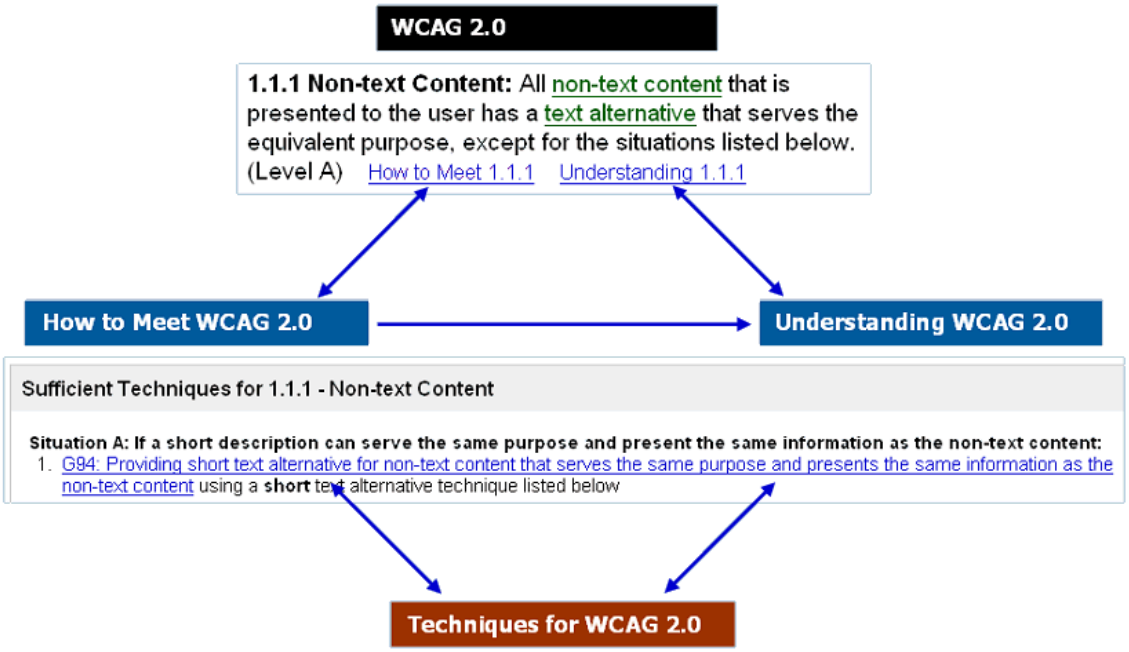
Pauta 3.2: Predecible. La apariencia y la operabilidad de las páginas Web deben ser predecibles.

Pauta 3.3: Ayuda a la entrada de datos. Se debe ayudar a los usuarios a evitar y corregir los errores.

Robustez

Pauta 4.1: Compatible. La compatibilidad con los agentes de usuario debe ser máxima (tanto con los actuales como con los futuros).

Cada una de estas pautas tiene una serie de técnicas que ayudan al cumplimiento de las mismas:



En la URL http://www.w3.org/TR/2008/REC-WCAG20-20081211/#guidelines puede usted leer todas y cada una de las pautas y las técnicas recomendadas para su cumplimiento. En http://www.sidar.org/recur/desdi/traduc/es/wcag/wcag20/ hay una traducción al castellano.

Niveles WCAG2.0

Cada Pauta WCAG 2.0 se desarrolla en una serie de criterios de éxito. En total se han definido 60 criterios de éxit o puntos de comprobación y verificación que determinan el nivel de accesibilidad (A,AA o AAA).

Para que una página Web sea conforme con las Pautas WCAG 2.0 debe satisfacer todos y cada uno de sus requisitos de conformidad:

- **Nivel de Conformidad "A".** Se cumplen los puntos de verificación de prioridad 1.
  - no especifican cómo se representa la información
  - son razonablemente aplicables a cualquier sitio web
  - son comprobables de forma automática. Algunos requieren la evaluación de forma manual. Los criterios de cumplimiento que requieren comprobación manual producen resultados consistentes bajo múltiples verificaciones por personas distintas.
- **Nivel de Conformidad "AA"**. Se cumplen los puntos de verificación de prioridades 1 y 2 .
  - puede requerir que los autores presenten el contenido de una cierta manera
  - son razonablemente aplicables a cualquier sitio web
  - son comprobables de forma automática. Algunos requieren la evaluación de forma manual. Los criterios de cumplimiento que requieren comprobación manual producen resultados consistentes bajo múltiples verificaciones por personas distintas.
- **Nivel de Conformidad "AAA"**. Se cumplen los puntos de verificación de prioridades 1,2 y 3
  - son criterios que van más allá de los niveles 1 y 2 y pueden aplicarse para hacer sitios accesible a más personas con cualquier discapacidad o un tipo concreto de discapacidad

Cuando una página cumple con las pautas WCAG 2.0 puede incluir en ella una declaración que indique a los usuarios que cumple con el W3C mediante un logotipo

También se debe indicar:

- fecha en que se revisó el cumplimiento
- título, versión y URI de las pautas WCAG 2.0
- Nivel de conformidad alcanzado
- Alcance (enumeración de las páginas que lo cumplen)
- Listado de las tecnologías de las que depende el contenido.

Herramientas de validación de la accesibilidad

A la hora de evaluar la accesibilidad de una página Web, hay una serie de pasos que habría que seguir para realizarlo de una forma ordenada:

1. Determinar el alcance de la evaluación
2. Establecer la muestra representativa de las páginas que se van a analizar

3. Evaluación automática
4. Evaluación manual
5. Resumir los problemas. Realizar informe.

Para la evaluación automática se pueden utilizar herramientas como :

- http://www.tawdis.net/
- http://examinator.ws/

Aunque las herramientas de validación automáticas resuelven muchos de los problemas de accesibilidad que pudiesen aparecer en las páginas Web, dicha revisión hay que completarla con una revisión manual.

El análisis manual presenta algunas ventajas sobre el realizado mediante herramientas automáticas. Hay problemas que sólo pueden ser detectados mediante métodos de verificación manuales y suelen ser más intuitivos que los automáticos.

A pesar de sus ventajas, también se pueden encontrar algunos inconvenientes:

- Requieren más tiempo.
- Es necesario utilizar más herramientas o probar configuraciones distintas.
- Requiere del juicio personal de la persona que revisa.
- Algunas situaciones son difíciles de simular.
- Algunos fallos puede no detectarlos.

Las tareas a realizar en un proceso manual son tan diversas como:

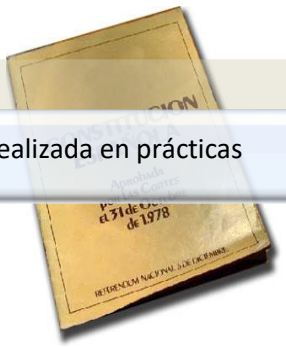
- Aplicar un listado de puntos de comprobación de las pautas o un checklist de accesibilidad a las páginas web.
- Probar múltiples configuraciones de distintos navegadores existentes.
- Técnicas de filtrado: Realizar las siguientes revisiones en los anteriores navegadores gráficos:
    - Desactivar las imágenes y comprobar que el texto alternativo es adecuado.
    - Desactivar el sonido y comprobar que el contenido del audio está disponible a través de texto equivalente (subtitulado, trascripción).
    - Comprobar que se puede aumentar el tamaño de fuente y que la página no pierde precisión en el diseño y continúa siendo usable con un tamaño de fuente grande.
    - Comprobar que no es necesario el desplazamiento horizontal con diferentes resoluciones de pantalla y/o con diferentes tamaños de ventana.
    - Visualizar la pantalla en escala de grises y observar si el contraste es suficiente.
    - Comprobar que hay acceso en la navegación y funcionalidad sólo con teclado. Navegar a través de los enlaces y controles de formulario, además comprobar que los vínculos indican claramente el destino o dónde conducen.
    - Comprobar que hay acceso en la navegación y funcionalidad desactivando plugins, scripts, etc
- Acceder y examinar las páginas con un lector de pantalla y navegadores especiales como sólo texto para comprobar que toda la información está disponible y en un orden lógico significativo.

- Leer y evaluar el contenido de las páginas, comprobar que el texto es claro, sencillo y adecuado al propósito del sitio.

Para llevar a cabo esta evaluación manual, hay herramientas orientadas al desarrollo y evaluación que proporcionan soporte como: algunas funcionalidades de las barras de accesibilidad, lectores de pantalla, magnificadores de pantalla, navegadores con opciones especiales, navegadores alternativos, simuladores de personas con discapacidad visual, simuladores de personas con discapacidad cognitiva, herramientas orientadas a la epilepsia, evaluadores de texto, evaluadores de color, herramientas para niños con discapacidades motrices, etc. Algunas de estas herramientas pueden ser:

- **Web Accessibility Toolbar (Internet Explorer y Ópera)** Se instala en el propio navegador y permite realizar una serie de pruebas para comprobar la accesibilidad Web. Entre sus funciones se encuentran:
  - Activar/desactivar hojas de estilo.
  - Localizar características desaconsejadas.
  - Listar o resaltar las imágenes presentes y sustituirlas por texto alternativo.
  - Hacer pruebas estructurales y semánticas.
  - Hacer pruebas de color.
- **Web Developer Toolbar (Mozilla Firefox).** Extensión que añade una barra de herramientas. Entre sus funciones más destacadas se encuentran:
  - Deshabilitar javascript y hojas de estilo.
  - Reemplazar imágenes por texto alternativo.
  - Identificar encabezados en tablas de datos, elementos estructurales desaconsejados, marcos, enlaces, etc.
- **Internet Explorer Developer Toolbar:** Barra de herramientas que permite evaluar la accesibilidad Web. Las funciones que ofrece son:
  - Desactivar selectivamente opciones del navegador.
  - Seleccionar elementos específicos de la Web.
  - Comprobar el código HTML, CSS.
  - Mostrar información de imágenes, tablas y tamaños.
- **Firefox Acessibility Extension:** Extensión que añade una barra de herramientas. Tiene opciones que facilitan la navegación por los contenidos de usuario con discapacidad y realiza comprobaciones de accesibilidad.

LA PROTECCIÓN DE DATOS



Ejercicio 42. Valide el nivel de accesibilidad de la página web realizada en prácticas

La Constitución Española establece (art. 18.4) que:

> *La ley limitará el uso de la informática para garantizar le honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

El Parlamento Europeo y el Consejo de la Unión Europea adoptaron en 1995 una Directiva relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Es una consecuencia de la libre circulación de personas, mercancías, servicios y capitales, pero este intercambio de datos personales deberá realizarse desde la óptica de un tratamiento equivalente de la protección de la intimidad en los distintos estados miembros.

En nuestro país existe normativa referente a la protección jurídica de las personas en lo que concierne al tratamiento automatizado de sus datos personales. En este sentido, se entiende la protección de datos *"el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad"*.

En primer lugar, se trata de proteger a las personas ante el manejo o manipulación, no autorizada, de sus datos personales, bien cuando sean susceptibles de un tratamiento automatizado o no, o se encuentren en un soporte lógico susceptible de tratamiento automatizado o no. No tiene sentido, por tanto, la aplicación de esta normativa a ficheros manuales no indexados.

En segundo lugar, el resultado de la elaboración de los datos debe ser identificable con el titular de los mismos, o que se pueda identificar a la persona con el resultado.

En tercer lugar, tiene que darse un manejo o acceso a los datos sin consentimiento de su titular, o para fines diferentes a los que autorizó o se vio obligado a dar los datos.

La Agencia de Protección de Datos

La Agencia de Protección de Datos es un ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada. Actua con plena independencia de las AAPP, aunque está sometida al control financiero del Tribunal de Cuentas. Su finalidad principal es velar por el cumplimiento de la legislación sobre protección de datos personales y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos.

Sus funciones son:

- Atender las peticiones y reclamaciones presentadas por los afectados
- Proporcionar información acerca de sus derechos
- Ejercer la potestad sancionadora
- Ordenar el cese o inmovilización de los ficheros que proceda
- Inspeccionar los ficheros
- Ejercer el control y adoptar las autorizaciones que procedan para los movimientos internacionales de datos.

Ejercicio 43. Dése una vuelta por la web de la Agencia Española de Protección de Datos (www.agpd.es) y comente con dos o tres párrafos el contenido de una de las guías publicadas (a escoger por el alumno de entre las disponibles)

Ley Orgánica 15/1999. de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)

La LOPD pretende garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. Se aplica tanto a los ficheros públicos como privados que contengan datos de carácter personal. Sin embargo el régimen de protección de datos no será de aplicación:

- A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas
- A los ficheros sometidos a la normativa sobre protección de materias clasificadas
- A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

Hay otro tipo de ficheros que se regirán por sus disposiciones específicas:

- Ficheros regulados por la legislación electoral
- Ficheros con fines estadísticos amparados por legislación nacional o autonómica
- Ficheros de informes personales de calificación del Régimen del personal de las Fuerzas Armadas
- Ficheros derivados del Registro Civil y del Registro Central de Penados y Rebeldes

- Los ficheros procedentes de imágenes y sonidos obtenidos mediante el uso de cámaras por las Fuerzas y Cuerpos de Seguridad.

La LOPD da una serie de definiciones que hay que tener claro. Exponemos las más importantes, si bien todas se encuentran en la URL:

a) **Datos de carácter persona**l: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
b) **Tratamiento de datos**: cualquier operación o procedimiento técnico, sea o no automatizado, que implique la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, bloqueo, modificación, o cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
c) **Fichero**: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
d) **Responsable del fichero o del tratamiento**: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.
    a. En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará responsable del tratamiento a la persona o personas integrantes de los mismos.
e) **Encargado del tratamiento**: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.
f) **Afectado o interesado**: Persona física titular de los datos que sean objeto del tratamiento.
g) **Consentimiento del interesado**: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
h) **Cancelación**: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.
i) **Cesión o comunicación de datos**: Tratamiento de datos que supone su revelación a una persona distinta del interesado.
j) **Procedimiento de disociación**: Todo tratamiento de datos personales que permita la obtención de datos disociados (aquellos que no permite la identificación de un afectado o interesado)
k) **Fuentes accesibles al público**: A los efectos de la LOPD se consideran fuentes accesibles al público aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no

impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

l) **Responsable de seguridad**: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

¿Qué entiende la LOPD por **calidad de los datos?** Se hace referencia a que los datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimas para las que se hayan obtenido. Si son inexactos o están incompletos deben ser cancelados o sustituidos por los correctos. Serán cancelados cuando dejen de ser necesarios.

Los datos personales. Clasificación.

Los datos personales se clasifican en dos categorías de acuerdo con el mayor o menor grado de secreto que tengan asociados por su propia naturaleza; esto es, atendiendo a su confidencialidad.

Entendemos por públicos aquellos datos personales que son conocidos por un número cuantioso de personas sin que el titular pueda saber, en todos los casos, la fuente o la forma de difusión del dato. En este sentido, serían públicos el nombre, apellidos, edad o la profesión.

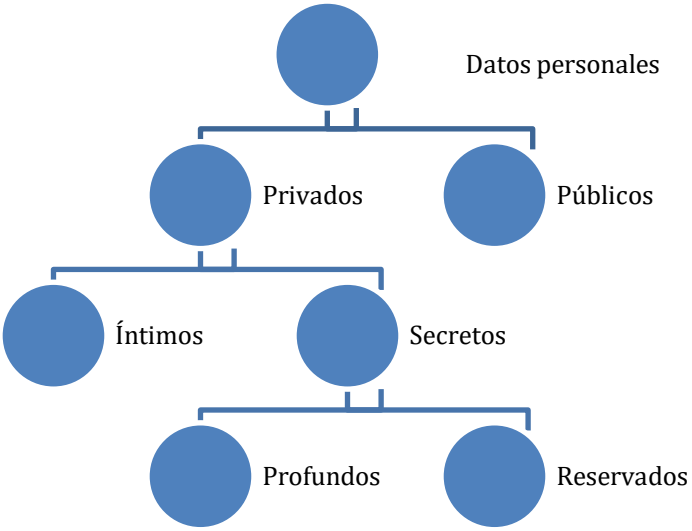


Ilustración 33 Clasificación de los datos personales.

Por privados se entiende aquellos datos personales que la persona se ve obligada a proporcionar en ciertas circunstancias reguladas. A su vez, los datos privados pueden ser íntimos o secretos. Los datos íntimos son aquellos datos que el individuo puede proteger de su difusión frente a cualquiera pero que, de acuerdo con un fin determinado, esté obligado –por mandato legal- a dar periódica o regularmente en cumplimiento de sus obligaciones cívicas. Los datos secretos son aquellos datos que el ciudadano no estará obligado a dar a nadie salvo casos excepcionales, expresamente regulados en las leyes.

Por último, los datos secretos serán a su vez profundos o reservados, siendo los reservados aquellos que bajo ningún concepto, ni por ningún motivo, está obligado el titular a darlos a conocer a terceros si no es así su voluntad. Los datos secretos profundos admiten excepciones a esta exención de obligación.

Los datos denominados secretos se conocen también como datos “sensibles”, “sensibilísimos” o de una “sensibilidad especial”.

Medidas de seguridad en función del tipo de datos

Conocer qué tipo de datos son más sensibles que otros es vital para cumplir con más o menos obligaciones y deberes exigidos la normativa. Para ello, el Real Decreto de la LOPD ha mantenido la tipología de datos personales que se recogían en el antiguo Reglamento de Medidas de Seguridad (RMS).

Las medidas de seguridad exigibles a los ficheros y tratamientos de datos personales se clasifican en tres niveles:

- BÁSICO
- MEDIO y
- ALTO.

Los niveles de seguridad son acumulativos de modo que un fichero de nivel alto deberá aplicar también las medidas previstas en los niveles, básico y medio.

NIVEL ALTO. Ficheros o tratamientos con datos:

- Que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
- Que contengan datos derivados de actos de violencia de género.

NIVEL MEDIO. Ficheros o tratamientos con datos:

- Relativos a la comisión de infracciones administrativas o penales.
- Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre. (Solvencia Patrimonial y Crédito)
- Aquellos de los que sean responsables las Administraciones Tributarias y se relacionen con el ejercicio de sus potestades tributarias.
- Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
- Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias, y aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
- Aquellos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los de localización. Estos ficheros aplicarán además lo previsto en el artículo 103 RDLOPD respecto del registro de accesos.
- Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

NIVEL BÁSICO. Cualquier otro fichero que contenga datos de carácter personal.

Como casos excepcionales, en cuanto al nivel de seguridad aplicar, tenemos que en caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual será suficiente la implantación de las medidas de seguridad de **nivel básico** cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
- Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.
- Se trate de ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

Nivel	Debemos cumplir los art. Del RDLOPD
Básico	Art. 89 Funciones y obligaciones del personal
	Art. 90. Registro de incidencias
	Art. 91. Control de acceso
	Art. 92. Gestión de soportes y documentos
	Art. 93. Identificación y autenticación
	Art. 94. Copias de respaldo y recuperación
Medio	Arts. 95 y 109: Responsable de seguridad
	Arts. 96 y 110: Auditoria
	Art. 97. Gestión de soportes
	Art. 98. Identificación y autenticación
	Art. 99. Control de acceso físico
	Art. 100. Registro de incidencias
Alto	Art. 101. Gestión y distribución de soportes–Cifrado de datos.
	Art. 102. Copias de respaldo y recuperación
	Art. 103. Registro de accesos
	Excepción: Responsable persona física y único usuario
	Art. 104. Telecomunicaciones
	Cifrado en redes públicas o inalámbricas

El documento de seguridad

El "documento de seguridad" es un documento de carácter interno que debe reflejar por escrito todo lo relacionado con las medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar la seguridad de los datos en una organización determinada. Dicho documento debe ser elaborado por el responsable del fichero y, en su caso, por el encargado del tratamiento, y es de obligado cumplimiento para todo el personal que tenga acceso a los sistemas de información.

El documento de seguridad debe ser elaborado por el responsable del fichero y, en su caso, por el encargado del tratamiento, teniendo en cuenta que, tal y como establece al artículo 88.2 del Real

Decreto 1720/2007, este podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable.

Una vez elaborado el documento de seguridad, hay que ponerlo en conocimiento de todo el personal que tenga acceso a los sistemas de información quienes tienen la obligación de tratar los datos cumpliendo con todas y cada una de las normas y procedimientos contenidos en dicho documento.

Tal y como establece el artículo 88.3 del Reglamento de la LOPD (Real Decreto 1720/2007), el Documento de Seguridad deberá contener, como mínimo, los siguientes aspectos:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
- Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados
- Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, el documento de seguridad deberá contener además:

- La identificación del responsable o responsables de seguridad.
- Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

Inscripción de ficheros

Siempre que se proceda al tratamiento de datos personales, definidos en el art. 3,a) de la Ley Orgánica 15/1999, como "cualquier información concerniente a personas físicas identificadas o identificables," que suponga la inclusión de dichos datos en un fichero, considerado por la propia norma (artículo 3.b).), como "conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso," el fichero se encontrará sometido a la Ley, siendo obligatoria su inscripción en el Registro General de Protección de Datos, conforme dispone el artículo 26.

Artículo 26. Notificación e inscripción registral.

- "*Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos.*
- *Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.*
- *Deberán comunicarse a la Agencia Española de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.*
- *El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.*
- *Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia Española de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.*"

Sanciones por incumplimiento LOPD

El incumplimiento de la Ley Orgánica de Protección de datos puede dar lugar a sanciones económicas, que se establecen en función de la infracción cometida. Existen tres tipos de infracciones: leves, graves y muy graves.

- **Leves (de 900€ a 40.000€)**
  - No remitir a la AGPD las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo
  - **No solicitar la inscripción del fichero** de datos de carácter personal en el Registro General de Protección de Datos.
  - El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.
  - La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artc. 12 de la LOPD.
- **Graves (de 40.001€ a 300.000€)**
  - Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el BOE o diario oficial correspondiente.

  - Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en la Ley LOPD y sus disposiciones de desarrollo.
  - Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el art. 4 de la Ley LOPD y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave.
  - La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el art. 10 de la Ley LOPD.
  - El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
  - El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.
  - El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por la Ley LOPD y sus disposiciones de desarrollo.
  - Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
  - No atender los requerimientos o apercibimientos de la AGPD o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.
  - La obstrucción al ejercicio de la función inspectora.
  - La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en la Ley LOPD y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave.
- **Muy graves (de 300.001€ a 600.000€)**
  - La recogida de datos en forma engañosa o fraudulenta.
  - Tratar o ceder los datos de carácter personal especialmente protegidos salvo en los supuestos en que la Ley LOPD lo autoriza.
  - No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la AGPD para ello.
  - La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la AGPD salvo en los supuestos en los que conforme a la Ley LOPD y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

TEXTOS LEGALES EN LA WEB

A la hora de hacer pública una web hay una serie de información que la legislación obliga a que tengan un acceso permanente, fácil, directo y gratuito, es decir, siempre visible por el usuario. Es por ello que casi siempre se ubican en el footer de la página. Hablamos del Aviso Legal, la Politica de Privacidad y las Condiciones Generales de Venta.

Aviso Legal.

El aviso legal es el documento que recoge las cuestiones que la Ley de Servicios de la Información –LSSI en adelante- obliga a incluir prácticamente en todas las webs, concretamente en aquellos "*prestadores de servicios de la sociedad de la información*", es decir personas físicas o jurídicas, que realicen actividades económicas por internet u otros medios telemáticos siempre que la dirección y gestión de su negocio esté centralizada en España o posea una sucursal, oficina o cualquier otro tipo de establecimiento permanente situado en España. Por ejemplo

- Web corporativa de una empresa
- Tienda ecommerce.
- Autónomo con una web corporativa independientemente de si es usada como página informativa sobre sus negocios o como tienda online.
- Blog particular si incluye publicidad.

Dice el art. 10 de la LSSI,

> *Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:*
>
> *a. Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.*
> *b. Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.*
> *c. En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.*
> *d. Si ejerce una profesión regulada deberá indicar*
> *i. Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado*
> *ii. El título académico oficial o profesional con el que cuente.*
> *iii. El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento*
> *iv. Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.*
> *e. El número de identificación fiscal que le corresponda.*
> ***f. Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.***

g. *Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.*

Aparte de esta información obligatoria, habrá que incluir información, siempre que sea aplicable, sobre:

- los derechos de los contenidos mostrados en la web. Quién es el propietario de los mismos, el uso que se cede, la responsabilidad sobre los textos mostrados, etc.
- Ley aplicable y jurisdicción para la resolución de controversias o cuestiones relacionadas con la web
- Responsabilidad del titular ante la caida del servicio, mal funcionamiento o links externos.

Política de privacidad

Hay que informar a los usuarios del procedimiento llevado a cabo por la Web para recoger los datos personales, permitiendo ver a los usuario el uso que se les da. Por ejemplo, la jurisprudencia indica que el email de cada usuario es un dato personal, por ello para la suscripción a una newsletter el usuario debe expresamente aceptar la Política de Privacidad.

Esta Política de Privacidad será aceptada por los usuarios de manera previa en los formularios de recogida de datos, y deberán de ser informados de manera inequívoca, según el artículo 5 de la LOPD:

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

Condiciones Generales de Contratación y/o Uso

Si tenemos algún tipo de herramienta, asesoramiento online o comercio electrónico, debemos mostrar obligatoriamente un texto legal denominado “Condiciones Generales de Contratación y/o del Uso”, que el usuario deberá aceptar previo a la formalización de la compra, donde se indique:

1. Información clara y detallada de los precios de compra, con mención expresa de si incluyen los impuestos correspondientes y gastos de envío. De no ser así se deberá decir a cuánto ascienden estos.
2. Descripción del proceso de compra.
3. Obligaciones tanto para el vendedor y el comprador.
4. Condiciones de la compra, cuales son los plazos, la forma de entrega, la forma de pago…
5. Soluciones en el caso de que el pedido sea defectuoso.
6. Idioma en el que se va a celebrar el contrato.

Además, la LSSICE obliga a confirmar al comprador la realización de la operación, puede ser expuesta por dos vías:

1. Mediante correo electrónico remitido en un máximo de 24 horas después de la realización de la compra.
2. Mediante una pantalla de confirmación que aparezca cuando se haya finalizado el proceso de compra.

Política de cookies

La llamada Ley de Cookies no es una ley tal cual, sino que se trata del texto correspondiente al apartado segundo del artículo 22 de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (o LSSI), una vez modificado por el Real Decreto-ley 13/2012 por el cual se transponían una serie de directivas europeas. El texto en concreto dice lo siguiente:

> *2. Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*
>
> *Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones, siempre que aquél deba proceder a su configuración durante su instalación o actualización mediante una acción expresa a tal efecto.*
>
> *Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.*

Como vemos, cuando un usuario visita nuestra web por primera vez, éste debe consentir la instalación de nuestras cookies. Para facilitar dicho consentimiento, los propietarios de webs deben poner a disposición del usuario un procedimiento por el cual informen sobre los siguientes aspectos:

- Tipo de cookies que se instalarán al visitar nuestra web
- Utilización de dichas cookies: para qué y por quién
- Forma de desactivarlas

Así, el usuario debe tener la posibilidad de impedir la instalación de las cookies o incluso optar por no navegar por la web. De igual modo, se debe incluir en las páginas un enlace claramente identificable en el que el usuario pueda informarse sobre la política de cookies que se lleva a cabo.

Sin embargo, la implementación de esta 'ley' ha llevado en muchos casos a una interpretación interesada de la misma. Así, muchas webs han desarrollado una metodología por la cual se informa al usuario de que se le han instalado una serie de cookies en su navegador y que si quiere desinstalarlas tiene que hacer tal o cual cosa. Obviamente, esto incumple claramente la ley.

Se consideran **cookies exentas**, sobre las que no se aplica la ley, es decir, sobre las que no es necesario informar ni obtener el consentimiento las siguientes:

- Cookies estrictamente necesarias para prestar un servicio expresamente solicitado por el usuario

- Cookies necesarias únicamente para permitir la comunicación entre el equipo del usuario y la red

Ejemplos de cookies **exentas** son las que se emplean con la exclusiva finalidad de:

- Cookies de entrada del usuario
- Cookies de sesión/autenticación/identificación de usuario
- Cookies de seguridad del usuario
- Cookies de sesión de reproductor multimedia
- Cookies de carga
- Cookies de personalización de la interfaz de usuario
- Cookies de complemento (plug-in) para intercambiar contenidos sociales
- Cookies de cesta de la compra
- Cookies para rellenar un formulario

Es muy posible que en el desarrollo de una web usemos cookies no exentas sin saberlo, por ejemplo:

- si hay publicidad de terceros
- si usamos Google Analytics o cualquier otro contador de visitas externo

Es muy importante que la política de Cookies esté accesible permanentemente a través de un enlace que puede situarse de forma diferenciada junto a la política de privacidad, el aviso legal o las condiciones generales y de uso de tu web o en la parte superior de la web. El texto del enlace deberá tener relación con el contenido de la página, por ejemplo, puedes emplear expresiones como “Cookies” o “Política de cookies”.

BIBLIOGRAFÍA:

http://www.w3c.es/Traducciones/es/WAI/intro/accessibility

http://cuestionesderecho.es/creacion-del-aviso-legal-y-cumplimiento-de-la-lopd-desde-cero/

E. Santos et I. López-Vidriero, “Protección de Datos Personales. Manual Práctico para Emprsas”, ICEF Consultores. FC Editorial.

M.A. Davara Rodríguez, “Manual de Derecho Informático 10ª edición”, Thomson-Aranzadi 2008

TABLA DE CONTENIDO