Guía para adaptar tu web al RGPD

Ejemplo completo con OneTrust y WordPress

BLINDAJEWEB

Guía para adaptar tu web al RGPD

Ejemplo completo con OneTrust y WordPress

Javier Fernández Rivera

Lectores / Correctores

- Noelia Llera
- Samuel Parra
- Marcos Gonzalez

Temas

Índice

Prólogo

Cuando Javier contactó conmigo para pedirme escribir este prólogo, generó en mí una gran alegría, ilusión y responsabilidad. Es muy gratificante que alguien a quien admiras tanto quiera depositar su confianza en ti para algo en lo que ha puesto todo su empeño. La respuesta a la pregunta… la estás leyendo. :-)

Admiro el trabajo de Javi más allá de sus capacidades técnicas. Para mí su gran talento profesional queda a la sombra de las grandes cualidades personales que refleja en cada cosa que hace: honestidad, tenacidad y pasión.

Tengo la fortuna de llamarle amigo, y también de habernos ensuciado las manos juntos en proyectos muy bonitos y complicados. En los momentos clave es donde se comprueba la esencia de las personas, y Javi no defrauda. Nunca.

Esta guía es, sin duda alguna, una muestra de lo que te acabo de describir.

Internet se ha convertido (con un trasfondo alineado con lo que narraba George Orwell en su novela *1984*[1]) en un escaparate intrusivo de *pop-ups*, *toasts*, *banners*, modales, etc., como resultado del conflicto de intereses entre los derechos de las personas, la ambición desmesurada de algunas empresas y la incapacidad e incompetencia en muchos casos de legisladores que, en el mejor de los casos, no conocen como debieran el problema que intentan legislar.

Lo peor de todo es que la mayoría de toda esa parafernalia no consigue lo que pretende, por lo enrevesado de la norma y la complejidad en algunos casos para implementarla.

Esta guía te ayudará, de una forma clara, directa y fiable, a cumplir la RGPD en tu proyecto *online*.

Javi, con su capacidad de análisis y mimo por el detalle, nos explica con precisión y de forma comprensible cómo afecta el reglamento a nuestro proyecto *online* (puesto que cubre la práctica totalidad de aspectos relevantes) y nos muestra qué debemos hacer para cumplirlo. Si tu proyecto se basa en WordPress, cuentas, además, con un ejemplo paso a paso explicado hasta el más mínimo detalle que es oro puro.

No te entretengo más, que lo bueno empieza ahora. :-)

[1] https://es.wikipedia.org/wiki/1984_(novela) - *1984* (George Orwell)

1. Introducción

Tú eres el responsable de tu web.

Podría decirse que una web otorga un gran poder, y con un gran poder viene una gran responsabilidad, tal y como decía Peter Parker, en *Spider-Man*, aunque realmente su inspiración viene de atrás.

Franklin se dirigió al pueblo americano el 11 de abril de 1945 con un discurso que sería el último mensaje a la ciudadanía antes de morir:

> «Hoy hemos aprendido en la agonía de la guerra que un gran poder conlleva una gran responsabilidad. Nosotros, como estadounidenses, no elegimos negar nuestra responsabilidad».
>
> Franklin D. Roosevelt

Con el RGPD (Reglamento General de Protección de Datos) pasa algo parecido (salvando las distancias de la guerra), ya que, como ciudadanos europeos y propietarios de un sitio web, no podemos permitirnos negar o eludir las responsabilidades ante la protección de los datos y la seguridad en Internet. Seguridad, ese es otro elemento clave en el RGPD.

1.1. Diez razones para adaptar tu web al RGPD

1. **Por responsabilidad.** Ante la información privada se debe hacer un mejor tratamiento de los datos personales de otras personas.
2. **Por reputación.** Se tarda muchos años en conseguir la confianza de los clientes y se puede perder en unos pocos días por incumplir algunas directrices del reglamento.
3. **Por dinero.** Evitando sanciones, ya que son muchos los casos y sorprende ver las cuantías que superan a multas convencionales.
4. **Por negocio.** Conocemos lo complejo que es abrir mercados y generar beneficios, pero no somos del todo conscientes de que una desactualización nos podría dejar fuera.
5. **Por legalidad.** Para estar bajo el paraguas europeo, con todo lo que eso supone a nivel internacional.
6. **Por seguridad.** Para proteger tu mayor activo y, sin duda, el más valioso, que es tu base de datos con toda la información personal de tus clientes.
7. **Por competitividad.** Aunque todos están «poniéndose las pilas», cuanto más rápido te posiciones, mayor ventaja competitiva tendrás.
8. **Por optimización.** Para evitar recabar datos innecesarios y obligar a procesar solo la información relevante para nuestra actividad.
9. **Por transparencia.** Para procesar los datos de una forma clara, lo cual agradecerán tus usuarios y mejorará la relación con tu empresa.
10. **¡Por ti!.** Que cuando estás en el otro lado, también eres un usuario y te gustaría que tratasen adecuadamente tus datos.

> «En el momento que algo sale de tu ordenador, deja de ser privado»
> (A veces deja de serlo sin salir).
>
> Alfredo Vela

1.2. Ámbito de actuación

EL RGPD es grande y abarca muchas áreas relacionadas con la privacidad. En este libro, pondré el foco exclusivamente en la adaptación de los sitios web al reglamento. Para ello, abordaré la problemática de las *cookies* con soluciones técnicas, la mejora de los formularios, la inclusión de páginas legales y el incremento de la seguridad.

Además, también veremos las preguntas y respuestas frecuentes sobre el RGPD, las problemáticas con las estadísticas, advertencias en la implementación y una buena colección de consejos que te serán de mucha utilidad.

Con este libro te ayudaré a que tengas una web más legal y segura.

1.3. Descargo de responsabilidad

Este libro no constituye ni reemplaza un asesoramiento legal, no obstante, sirve para ayudar e informar sobre ciertos aspectos técnicos y legales.

Con la información y las herramientas propuestas en este libro, te acercarás sin duda al cumplimiento del RGPD en tu web, sin embargo, no puedes interpretar con ello que tras su aplicación tu página sea totalmente legal, ya que dependerá de cómo implementes esta información y de cada tipo de web.

Si buscas seguridad, en Blindaje Web [2] te podemos dar asistencia técnica junto con el jurista Samuel Parra [3], que es todo un referente en materia de privacidad y RGPD. Contacta ahora sin compromiso: https://blindajeweb.com/rgpd

[2] https://www.blindajeweb.com
[3] https://www.samuelparra.com

1.4 Sobre mí

Creé mi primera web en 1998 (con Notepad) y desde entonces no ha dejado de crecer mi fascinación por ese medio, ya que aúna mis dos grandes pasiones, diseño y programación.

Años más tarde, me interesé por los estándares web, la accesibilidad, la arquitectura de la información y la experiencia de usuario, temas que pude aprender de, entre otros, Emmanulle Gutierrez, Yusef Hassan y Torres Burriel, quien fue mi mentor en la universidad.

Mucho de lo que he aprendido se lo debo a Internet, y quizás por ello me siento comprometido a devolver ese conocimiento a la red en forma de artículos en mi blog, en la revista *NSU* (*No Solo Usabilidad)*, etc. También *offline*, recuerdo algunos artículos en la ya extinguida revista *@RROBA*, además de clases presenciales de programación y un curso de WordPress a periodistas.

En 2006 creé aurea.es, una iniciativa freelance de diseño web y desarrollo, que me ha permitido trabajar (desde Asturias) en proyectos de: Coca-Cola, WeblogsSL, Webedia, ING, Philips, Renault, etc. Tras quince años de experiencia y una visión más multidisciplinar, he comenzado a coordinar técnicamente proyectos web para grandes empresas. Asimismo, también he aportado soluciones técnicas y conseguido nuevos retos dentro del grupo Webedia.

Durante el año 2020 tuve la oportunidad de trabajar adaptando las webs de grandes marcas al RGPD. Este libro recopila parte de ese trabajo.

Me considero un emprendedor por convicción. Pienso que las oportunidades no llegan, se crean. ¡Y creer es crear!

blindajeweb.com es mi último proyecto, y en él ayudamos a las empresas a mantener sus webs seguras y actualizadas.

1.5. *Checklist*

En este apartado, te planteo una serie de preguntas que debes hacerte y reflexionar cuando desarrollas tu web y, a continuación, te señalo los puntos clave que tendrás que tener en cuenta para cada tema.

1.5.1. ¿Conoces realmente el RGPD y cómo adaptar tu web?

- ¿Para qué sirve?, ¿a quién aplica?, ¿obligatoriedad?, ¿sanciones?, ¿ámbito de actuación?, ¿escudo de datos?, ¿falsos mitos?
- Recursos y herramientas que ayudan con la adaptación.

1.5.2. ¿Informas adecuadamente en tu web del uso de las *cookies*?

- Información en la política de *cookies* sobre todas las *cookies* que usamos en la web, así como otras tecnologías de seguimiento. También hay que disponer de una tabla actualizada con todas las *cookies*, su tipo y finalidad.
- Presentar la información de forma detallada en la página de la política de *cookies*, también de forma más abreviada en el aviso de *cookies* y en su panel para la configuración del consentimiento.

1.5.3. ¿Gestionas el consentimiento de cookies?

- Detectar *cookies* (análisis y escaneo periódico).
- No cargar ninguna *cookie* que no sea estrictamente necesaria sin previo consentimiento del usuario.
- Solo recopilar y procesar los datos tras el consentimiento del usuario.
- Implementar *banner* de *cookies* con botón de configuración.
- Cambiar el consentimiento con el control granular de las *cookies* y el panel de preferencias. Acceso fácil a la configuración en cualquier momento.
- Bloquear y gestionar contenidos de terceros basándose en el consentimiento previo de *cookies*.

1.5.4. ¿Tienes los formularios adaptados al RGPD?

- Los formularios han de ser informativos, específicos y verificables.
- *Check* de consentimiento sobre la política de privacidad, aviso legal, términos de uso o condiciones de contratación.
- La primera capa de privacidad debe contener: el responsable, la finalidad, los derechos de los usuarios, la legitimación y el destinatario.
- Los textos han de ser claros y sencillos.
- Tras el consentimiento válido, solo se pueden recopilar y procesar datos personales para los fines que se hayan informado en ese formulario específico.
- Guardar un registro de consentimientos.
- Revisar el tratamiento de datos especialmente sensibles.

1.5.5. ¿Tienes las páginas legales necesarias?

- La mayoría de webs tendrán: aviso legal, política de privacidad y política de *cookies*. Dependiendo del tipo de web, también pueden tener: condiciones de contratación, condiciones de venta, términos de uso, etc.
- Textos legales necesarios para el *banner* ('aviso') de *cookies*, el panel de configuración de *cookies* y los diferentes grupos de *cookies*.
- La redacción ha de ser fácil y comprensible para cualquiera.
- Todas las páginas legales deberán ser fácilmente encontrables.
- Evitar textos generalistas y contar con la supervisión de un abogado especializado en privacidad y RGPD.

1.5.6. ¿Usas herramientas de terceros?

- Analiza bien las herramientas de terceros que usas, ya sean *plugins*, embebidos para crear formularios, códigos para las estadísticas, uso de APis, etc., y revisa cómo están gestionando el tratamiento de datos, qué hacen con ellos, dónde los guardan y con qué finalidad.

1.5.7. ¿Es tu web segura?

- Certificado de seguridad SSL
- WordPress, *themes* y *plugins* actualizados
- Política de usuario, permisos y roles
- Controles de acceso
- Ficheros sensibles
- Medidas de seguridad
- *Backups*, CDN, monitorización, etc.

1.5.8. ¿Los datos son tratados por empresas no europeas?

- El «escudo de datos europeo» es un punto conflictivo y si usas herramientas de terceros para el tratamiento de datos de ciudadanos europeos, puedes estar incumpliendo el RGPD. Aunque esta regulación puede cambiar, es conveniente usar un *hosting*, *newsletter*, formularios, etc. de empresas europeas, ya que están bajo el paraguas del RGPD.

Si quieres ahondar, puedes ver el *checklist* de la AEPD (Agencia Española de Protección de Datos) [4]:

> También puedes delegar la adaptación de tu web al RGPD con la ayuda técnica de **Blindaje Web** y la supervisión legal de **EGIDA**. Contacta ahora sin compromiso: https://blindajeweb.com/rgpd

[4] https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf

1.6. Recursos

- Webgrafía
    - GDPR, Guide to GDPR compliance, RGPD en EUR-Lex
    - Guía RGPD para responsables de tratamiento y uso de las *cookies*
    - Análisis de riesgos en los tratamientos de datos personales
    - Adaptación al RGPD de las políticas de privacidad en Internet
    - Listado de cumplimiento del RGPD
    - Evaluación de impacto en la protección de datos (EIPD)
    - Sanciones: Buscador AEPD y Buscador europeo
- Herramientas
    - Facilita RGPD
- *Cookies*
    - Información
        - Cookiepedia
        - Cookieserve
        - CookieMetrix
    - Servicios
        - OneTrust y CookiePro
        - Cookiebot, Quantcast, TrustArc, DIDOMI
    - *Plugins*
        - GDPR Cookie Consent y premium
        - GDPR Cookie Compliance
        - Complianz
        - AMP for WordPress
    - Estadisticas
        - Matomo, GoAccess, AWStats
- Formularios
    - Typeform
    - Contact form 7 y Advanced Contact form 7 DB
- Seguridad
    - Really Simple SSL

2. Preguntas frecuentes

He decidido incorporar en la primera parte de este libro un capítulo, a modo de FAQ (*frequently asked questions*), para definir un contexto amplio sobre el RGPD y así poder abordar mejor los siguientes capítulos.

2.1. ¿Qué es RGPD (o GDPR)?

RGPD (por sus siglas en español, Reglamento General de Protección de Datos), o GDPR (por sus siglas en inglés, *General Data Protection Regulation*), es la normativa que se encarga de proteger y regular el tratamiento y circulación de los datos de los ciudadanos europeos.

2.2. ¿Para qué sirve?

Para proteger la privacidad de los internautas de la Unión Europea y evitar que sus datos con información personal circulen por la red sin ningún tipo de seguridad ni control. Se pretende poner en valor que la persona física es el verdadero propietario de sus datos.

2.3. ¿A quién aplica?

A las organizaciones de todo el mundo (grandes y pequeñas) cuando sus actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a personas que se encuentren en la Unión Europea, independientemente de si a estos se les requiere su pago, o el control de su comportamiento, en la medida en que este tenga lugar en la Unión.
Por lo que todas las empresas que cumplan estos requisitos deben adaptar sus medios legales y técnicos, así como sus páginas web, para cumplir con el RGPD. Aunque se encuentren fuera de la Unión Europea.

2.4. ¿Cuál es su ámbito de actuación?

Afecta por igual a toda la Unión Europea y unifica las obligaciones en materia de protección de datos y privacidad, pero también atañe a cualquier otra empresa no europea que haga tratamiento de datos de ciudadanos europeos en los términos expresados anteriormente.

2.5. ¿Qué se exige?

Que las organizaciones analicen los datos que tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. Esto exige una actitud consciente, diligente y proactiva por parte de las organizaciones, empresas e individuos.

2.6. ¿Es obligatorio?

Entre otros casos, es de obligado cumplimiento si en tu web ofreces un servicio o producto, si usas publicidad o afiliados, si tienes estadísticas o analíticas o si usas algún formulario o recoges datos personales (incluido una IP, algo que es muy común).

2.7. ¿También es obligatorio para un blog?

Es una pregunta muy común, y la respuesta es sí. Por muy «personal» y «privado» que sea el blog, en realidad se trata de un sitio web que probablemente tenga comentarios o estadísticas y que, por tanto, ya incumpliría con el RGPD si no se adapta adecuadamente.

2.8. ¿Qué derechos tengo como europeo?

Bajo esta regulación, cualquier ciudadano de la Unión Europea tiene derecho, entre otros, a solicitar la información recogida por parte de una empresa, así como a la fácil eliminación, la portabilidad o la supresión total de información.

"

«Al dar derechos a otros, nos damos derechos a nosotros mismos.»

John F. Kennedy

2.9. ¿Se sanciona por incumplirlo?

No es por meter miedo, pero sí, y más de lo que imaginas. Podemos entrar en la web de AEPD (Agencia Española de Protección de Datos) [5] y localizar los procedimientos cursados en concepto de RGPD. A nivel europeo también podemos usar PRIVACY Affairs - GDPR Fines Tracker & Statistics [6], que nos mostrará las sanciones en varios países.

- 6.000.000 € a Caixabank.
- 120.000 € a Vodafone y 75.000 € a Telefónica (y no son sus únicas sanciones)
- 50.000 € a Bankia
- 5.000 € al Real Sporting de Gijón (club de fútbol)
- 4.000 € a una persona privada
- 3.000 € a un restaurante
- 2.000 € a una asociación de vecinos
- 1.500 € a una agencia de viajes
- 540 € a un bazar

Como vemos, hay de todo, desde empresas grandes a pequeños negocios. Las sanciones son reales e incluso pueden verificarse con el PDF que pone a disposición la AEPD. Ejemplo: los 5.000 € a la Federación de Baloncesto de Castilla y León [7].

[5] https://www.aepd.es/es/buscador
[6] https://www.privacyaffairs.com/gdpr-fines/
[7] https://www.aepd.es/es/documento/ps-00200-2020.pdf

2.10. ¿Se puede reclamar una indemnización?

El artículo 82 del RGPD[8] recoge que toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del reglamento tendrá derecho a recibir del responsable una indemnización por los daños y perjuicios sufridos.

2.11. ¿Hay timos en torno al RGPD?

En el siguiente artículo, «Víctimas del GDPR: Un abogado me timó y puedo perder millones por un simple mail»[9], se habla sobre ello y se deja ver cómo el nuevo reglamento de protección de datos está dejando algunas víctimas de empresas que, por un mal asesoramiento, se exponen a multas millonarias o a perder parte de su negocio.

2.12. ¿Afecta a todas las webs?

Probablemente a la inmensa mayoría. Una web debe adaptarse al RGPD:

1. Si recoge cualquier tipo de dato de un ciudadano europeo. Puede ser mediante formularios de contacto, comentarios, *newsletter*, etc.
2. Si usa *cookies* propias o de terceros, como la inmensa mayoría de servicios (Google Analytics, Typeform, Hotjar, etc.).
3. Si es un *e-commerce* donde se producen transacciones, ya sea tanto de productos físicos como digitales (infoproductos u otros).
4. Si está monetizando mediante cualquier fórmula publicitaria o afiliados.

[8] https://gdprinfo.eu/es/es-article-82

[9] https://www.elconfidencial.com/tecnologia/2018-05-28/gdpr-empresas-fraude-multas-millonarias-abogados_1569093

2.13. ¿Qué es el escudo de datos?

El *escudo de datos europeo* es un punto conflictivo, y lo más seguro es que su rumbo cambie pronto, pero en el momento de escribir esto mi consejo es:

1. Las empresas que manejan datos personales han de ser europeas.
2. Los datos manejados han de alojarse en un *datacenter* europeo.

CURIOSIDAD: Por sorprendente que parezca, estaremos infringiendo el RGPD si por ejemplo nuestra web está alojada en los servidores de GoDaddy, aunque sea esta un WordPress donde recopilamos datos de usuarios y la alojamos en servidores de un centro de datos en Alemania. Esto se explica porque las autoridades competentes de EE. UU. (de donde es la empresa GoDaddy), por ejemplo el FBI, pueden solicitar información a esta empresa sin previa diligencia judicial, y GoDaddy estará obligada a ofrecer esa información independientemente de dónde esté alojada, sea un centro de datos en EE. UU. o en Alemania. Esto entraría en conflicto con los derechos de privacidad contemplados en el RGPD europeo, por ello, te animo a que uses un proveedor de *hosting* (o cualquier otra solución) que sea una empresa de la Unión Europea.

Esto abarca a otros muchos servicios, como Mailchimp. ¿Pero entonces no puedo usar Mailchimp para mi *newsletter*? Sí, puedes, pero (al menos por ahora) no estarías cumpliendo con el RGDP, ya que los datos personales de tus suscriptores están en manos de una empresa estadounidense y no europea. Como decía al comienzo, actualmente las autoridades competentes están negociando para poner una solución a esto, ya que indudablemente implica muchos problemas y también mucho debate. No sé hasta qué punto, pero con todo esto pienso que, o bien atentas contra el libre mercado, o bien contra los derechos de privacidad, por lo que tendrán que buscar un punto intermedio y no es nada sencillo en estas cuestiones regulatorias.

2.14. ¿Estadísticas o RGPD?

Las *cookies* y las estadísticas libran una intensa guerra: por un lado, tenemos al departamento legal, que sigue a rajatabla las leyes y busca cubrirse bien las espaldas; por otro lado, tenemos al departamento de análitica junto a sus aliados (el departamento de marketing, desarrollo de producto, negocio y editorial). La superioridad númerica de los aliados es clara, pero las armas legales son duras, y es que «dura lex, sed lex» ('la ley es dura, pero es ley').

Las estadísticas forman parte de la raíz del conflicto. Toda empresa en Internet necesita crecer y, para ello, necesita información, conocer qué cosas funcionan mejor o peor, muchos negocios necesitan además justificar sus servicios basándose en las estadísticas y, en todo esto, el análisis de las métricas por parte del departamento de analítica juega un papel fundamental. Son ellos quienes pueden convertir esos números en acciones que posteriormente generarán valor.

ADVERTENCIA: Las primeras bombas llegan con una caída de tráfico en las estadísticas que suele rondar el 90 %. Lógicamente, esto sucede tras aplicar el *banner* de aviso de *cookies* junto con el bloqueo de todas ellas (Google Analytics, Tealium, etc.). No obstante, siendo rigurosos, no podríamos hablar de una «caída de tráfico», ya que en realidad el tráfico sigue estando y sigue habiendo visitas al sitio web, lo que sucede es que estas visitas no se están contabilizando y el tráfico no se está midiendo por las *cookies* bloqueadas.

Ahora bien, ponte a explicar estas batallitas al cliente que paga por publicidad. A este cliente lo que le interesa es conocer las impresiones, visitas y otras métricas. Por un lado, la explicación de esto no será entendible para algunos clientes y, por otro, aun entendiéndolo, no es relevante, ya que su inversión económica ha de estar justificada.

Pero si la ley es importante, comer también lo es, y ya se sabe que con la comida no se juega. Entonces, podemos encontrarnos ante la tesitura de no cumplir la ley, seguir con nuestro negocio y ofrecer los servicios como veníamos haciendo o cumplir la ley y asumir que perderemos una importante cuota de mercado.

Y es aquí cuando la diplomacia entra en juego para intentar solucionar el conflicto. Una diplomacia que puede estar representada por el departamento de estrategia en combinación con el departamento de UX (experiencia de usuario). Juntos deberán situarse a medio camino entre ambos bandos y proponer soluciones como puntos mínimos de encuentro. Lógicamente, nunca se podrá llegar a máximos, porque el adversario saldría perjudicado y ambos son igualmente necesarios.

El objetivo estratégico será conseguir la mayor cantidad de estadísticas posibles cumpliendo la ley. A continuación, te comparto algunas soluciones desde el punto de vista estratégico y de experiencia de usuario.

Promover la interacción del usuario

- El *banner* para el aviso de *cookies* ha de ser más notorio, esto no quiere decir más grande (que también puede ser), pero el objetivo es que el usuario se percate de su existencia. A veces, es suficiente mostrándolo con un leve movimiento para que el usuario lo vea e interactúe con él aceptando las *cookies* (con la consiguiente recopilación de estadísticas).
- Otra opción es decantarnos por la fuerza bruta de un *cookie wall*. Al visitar la web se vuelve opaca y bloquea la navegación, al mismo tiempo aparece en una ventana emergente el aviso de *cookies* como único elemento para desbloquear la navegación en la web. Esta es sin duda la opción más drástica, pero también la que repercute en mayor recopilación de estadísticas, ya que se suele ganar entre el 60 % y el 80 % de lo perdido.

Promover la aceptación de todas las *cookies*

- Con un botón de `Aceptar todas las cookies` bien diseñado centramos el foco de atención del usuario en ese elemento; en cambio, si añadimos otros como el de `Rechazar cookies`, ya estaremos creando competencia y múltiples acciones.
- Además de esto, también podemos agregar una capa de diseño CSS para mejorar el botón: su visibilidad, efecto y, por consiguiente, el uso.
    - Por ejemplo, ante un botón rojo es probable que no consigamos muchos clics, en cambio, sí con uno verde.
    - Si sombreamos un poco el botón, también resaltará más.
    - Si ampliamos esa sombra al situar el ratón por encima de este, invitaremos a que el usuario haga clic.

Alejar la posibilidad de rechazar *cookies*

- Es perfectamente legal no incorporar un botón de `Rechazar cookies` en el aviso, siempre y cuando demos acceso a esa opción. Para ello, podemos incluir un enlace de `Configuración de cookies` desde el cual el usuario podrá acceder y desde allí rechazar las *cookies*.
- He visto algunos casos que llevan esta estrategia al máximo y sitúan el enlace al final del párrafo del aviso de *cookies*. Al no situarlo al mismo nivel que el botón de aceptar, da a entender que solo cabe aceptar.

Menos elementos de interacción

- Cuantos menos elementos «cliqueables» tenga el aviso, mejor. Podemos prescindir del enlace a la política de privacidad, siempre y cuando este se encuentre dentro de la `Configuración de cookies`.
- Basta solo con dos elementos en el aviso de *cookies*: el botón `Aceptar todas las cookies` y el enlace `Configuración de cookies`.

ADVERTENCIA: En la publicación de este libro estas estrategias son acordes a la legalidad, aunque esto puede cambiar más adelante.

Otras soluciones para recopilar más estadísticas:

- Usar más fuentes de tráfico.
  - *Cloudflare*[10]*:* Que no utiliza cookies para recopilar métricas de uso.
  - *Logs* de servidor: GoAccess[11], AWStats[12], WebAlizer[13]
  - Alternativas Google Analytics
    - Matomo[14] - La alternativa de Google Analytics que protege datos y la privacidad de clientes.
- *Plugin* de contador de visitas
  - Seguramente exista algún *plugin* que simplemente cuente la visitas de los *posts* o páginas que tenemos en nuestro WordPress sin falta de cargar *cookies*. Incluso podría programarse fácilmente.

ADVERTENCIA: No hagas recargas de la página tras la interacción con el *banner,* ya que generan rebotes en las estadísticas. Las *cookies* han de cargarse de forma dinámica y transparente para el usuario una vez que acepta las *cookies*.

ADVERTENCIA: Se puede interpretar que la anonimización (o enmascaramiento) de IP en Analytics[63] es una solución para seguir cargando *cookies* de Google Analytics, ya que al no tener la IP, no se puede relacionar una métrica con una persona. Sin embargo, aunque se utilice esa versión de IP anonimizada se siguen cargando *cookies*, que es lo relevante aquí.

CONSEJO: En la adaptación al RGPD es muy importante que vayas de la mano del departamento de analítica.

[10] https://www.cloudflare.com/es-es/web-analytics/
[11] https://goaccess.io/
[12] https://awstats.sourceforge.io/
[13] http://www.webalizer.org/
[14] https://matomo.org/

2.15. ¿Es un falso mito?

Hay algunos mitos que, o bien eran correctos anteriormente y han dejado de serlo, o bien son falsos de inicio, pero como la normativa puede cambiar, podrían convertirse en verdaderos con el paso del tiempo. Es por ello que hay que estar atentos a los cambios regulatorios. En la actualidad, diciembre de 2020, voy a citar tres:

☹ **MITO 1: No se puede bloquear la navegación.**
En realidad, NO siempre es ilegal bloquear la navegación hasta aceptar las cookies. Podemos hacer esto si por razones de justificación de métricas necesitamos que nuestro consentimiento de cookies sea más estricto e incite al usuario para aceptar o irse de la web.

☹ **MITO 2: No es obligatorio un botón de `Rechazar las cookies` situado en el *banner* de consentimiento.**

1. De inicio, no se carga ninguna *cookie* que pueda ser rechazada, a excepción de las *cookies* estrictamente necesarias.
2. Es suficiente con poner un botón o enlace que lleve al panel de configuración de *cookies* y, desde allí, sí que ya es obligatorio situar un botón u otras opciones para rechazar todas las *cookies* que no sean las estrictamente necesarias.

Para clarificar aún más este asunto, la AEPD viene a decir que se debe poner un botón de rechazar o enlace o «algo» que permita la opción de rechazar las *cookies* en la primera capa (*banner* de consentimiento). Esta opción de rechazar puede estar dentro de la configuración.

☹ **MITO 3**: **No es estrictamente necesario (aunque sí recomendable) guardar un registro de consentimiento de *cookies***, sino que bastaría con probar que el sistema pide el consentimiento antes de usar las *cookies*.

Resto de capítulos disponibles

- Cookies
  - Tipos, rastreo, soluciones.
  - Servicios y plugins.
  - El top 3 de herramientas.
- WordPress plugin GDPR
  - Configuración y códigos para bloquear embebidos.
  - AMP y RGPD.
- Implementando OneTrust
  - Licencia, escaneo, plantillas, bloqueo automático y manual.
  - Códigos JS y PHP.
- Formularios
  - Capas de privacidad y datos sensibles.
  - Newsletter.
  - Consejos y advertencias.
- Textos legales
  - Textos para banner y categorías de cookies.
  - Páginas legales necesarias.
- Seguridad
  - WordPress vulnerable.
  - Herramientas, brechas y medidas de seguridad.

Comprar ahora