

## Resumen del informe de cumplimiento del RGPD del sitio web

### Sitio web auditado:

<https://www.demo-despacho-legal.es/>

### Responsable del tratamiento:

**Nombre** Despacho Legal Demo S.L.P.

**Localización** España (ubicación anonimizada)

**Email** contacto@despacho-demo.es

### Detalles de la auditoría:

| Fecha de la auditoría | Versión de la auditoría | Método de análisis   | Base legal   |
|-----------------------|-------------------------|--|--|
| 27/12/2025            | V1.0                    | Revisión del sitio web de acceso público (sin autenticación) | RGPD • Directiva ePrivacy • Directrices de la AEPD |

### Consultor:

Sanjiv Sharma,  
Consultor en Protección de Datos y Riesgo Digital

<https://es.tickgdpr.eu>

*Documento preliminar de carácter informativo e indicativo.*

## 1. Objeto y alcance de la auditoría

La presente auditoría preliminar tiene como objetivo realizar una evaluación inicial del grado de cumplimiento del Reglamento General de Protección de Datos (RGPD) y normativa aplicable en el sitio web analizado.

El análisis se ha limitado a los siguientes ámbitos:

### A. Ámbitos analizados

- Cookies y tecnologías de seguimiento
  - Consentimiento
  - Configuración del banner
  - Gestión de preferencias
- Política de privacidad
  - Transparencia de la información
  - Contenido mínimo exigido por el RGPD
- Recogida de datos personales
  - Formularios
  - Bases legales
  - Información al interesado
- Medidas básicas de seguridad
  - Transmisión de datos

### B. Exclusiones del alcance de la auditoría

Esta auditoría no incluye revisión contractual interna, análisis de sistemas backend, ni evaluación de medidas organizativas no visibles públicamente.

---

## 2. Criterios de evaluación

Los resultados anteriores se han determinado conforme a los siguientes criterios objetivos.

## Criterios de evaluación (C / PC / NC)

| Tipo de evaluación         | Criterios de evaluación aplicables   | Implicación operativa  |
|----------------------------|--|--|
| Cumplimiento (C)           | <p>Se considera Cumplido cuando:</p> <ul style="list-style-type: none"> <li>• El requisito del RGPD/LOPDGDD está plenamente implementado</li> <li>• La información es clara, accesible y específica</li> <li>• No se detectan desviaciones relevantes</li> </ul>   | <i>No requiere acción correctiva inmediata.</i>                    |
| Parcialmente conforme - PC | <p>Se considera <b>Parcialmente conforme</b> cuando:</p> <ul style="list-style-type: none"> <li>• El requisito está implementado <b>de forma incompleta</b></li> <li>• Existe información, pero es <b>genérica, ambigua o desactualizada</b></li> <li>• La medida existe, pero <b>no cumple plenamente</b> los criterios de la AEPD</li> </ul> | <i>Requiere corrección para reducir el riesgo.</i>                 |
| No conforme (NC)           | <p>Se considera <b>No conforme</b> cuando:</p> <ul style="list-style-type: none"> <li>• El requisito <b>no está implementado</b></li> <li>• Existe una infracción clara del RGPD</li> <li>• El consentimiento, la base legal o la transparencia <b>no son válidos</b></li> </ul>   | <i>Supone riesgo regulatorio y requiere actuación prioritaria.</i> |

## Criterios de clasificación del riesgo

El nivel de riesgo asignado a cada hallazgo se basa en:

- Gravedad del incumplimiento

- Naturaleza de los datos tratados
- Impacto potencial sobre los derechos de los interesados
- Probabilidad de actuación de la AEPD

| Tipo                | Criterios aplicables   |
|---------------------|--|
| <b>Riesgo Alto</b>  | Incumplimientos susceptibles de sanción, invalidación del consentimiento o reclamaciones formales. |
| <b>Riesgo Medio</b> | Deficiencias relevantes que requieren adecuación para garantizar el cumplimiento.                  |
| <b>Riesgo Bajo</b>  | Aspectos mejorables sin impacto inmediato significativo  |

### 3. Resultados generales

La siguiente tabla resume el **resultado global del análisis preliminar**, desglosado por categoría, nivel de cumplimiento y riesgo asociado.

| Categoría                      | Nivel de cumplimiento |                            |                  | Nivel de riesgo |           |           |
|--------------------------------|-----------------------|----------------------------|------------------|-----------------|-----------|-----------|
|                                | Cumplimiento – C      | Parcialmente conforme - PC | No conforme – NC | Bajo            | Medio     | Alto      |
| Cookies                        | 4                     | 1                          | 6                | 4               | 1         | 7         |
| Política de privacidad         | 12                    | 4                          | 0                | 13              | 5         | 0         |
| Recogida de datos(Formularios) | 0                     | 5                          | 1                | 0               | 8         | 1         |
| Seguridad de los datos         | 5                     | 2                          | 3                | 6               | 2         | 4         |
| <b>TOTAL</b>                   | <b>21</b>             | <b>12</b>                  | <b>10</b>        | <b>23</b>       | <b>13</b> | <b>12</b> |

### 4. Resumen para la Alta Dirección

#### Situación global de cumplimiento

En relación con el cumplimiento del RGPD y los criterios de la AEPD, el sitio web se encuentra en una **situación de cumplimiento parcial**. Si bien cumple con los requisitos mínimos en determinados ámbitos, existen **deficiencias relevantes en áreas de alta visibilidad y especial sensibilidad regulatoria**.

Los resultados de la auditoría **no evidencian un fallo sistemático del sistema de cumplimiento**. No obstante, **los riesgos a los que está expuesto el sitio web no pueden ser ignorados**, dado su potencial impacto regulatorio y reputacional.

Las secciones siguientes **identifican y desarrollan las principales incidencias que deben ser abordadas** con el fin de **reducir el riesgo de actuaciones por parte de la autoridad de control, reclamaciones de los usuarios y posibles daños reputacionales**.

### Principales hallazgos de un vistazo

- Aspectos plenamente conformes: **21**
- Aspectos con cumplimiento parcial o no conformes: **22**
- Hallazgos clasificados como de alto riesgo: **12**

#### Interpretación:

El sitio web **se ajusta en principio a los requisitos del RGPD y a los criterios de la AEPD**, si bien **presenta inconsistencias en su implementación práctica**. La existencia de **hallazgos clasificados como de alto riesgo** sitúa a la organización en una **posición que podría atraer la atención de la autoridad de control**.

### Áreas de riesgo clave

#### A. Consentimiento de cookies y tecnologías de seguimiento (prioridad máxima)

- Mayor número de hallazgos no conformes y de alto riesgo
- Afecta a la totalidad de los usuarios del sitio web
- Área frecuentemente objeto de supervisión por parte de la autoridad de control

#### Implicaciones:

Se trata de un aspecto fácilmente perceptible tanto por los usuarios como por la autoridad de control, lo que expone a la organización a un mayor riesgo de sanciones y a posibles impactos reputacionales.

#### B. Política de privacidad y transparencia (riesgo moderado de carácter transversal):

- A nivel estructural, el sitio web cumple con los requisitos aplicables
- Existen inconsistencias en la ejecución práctica de la política de privacidad

#### Implicaciones:

Esta situación puede dar lugar a desafíos en materia de responsabilidad proactiva y credibilidad, en la medida en que la organización no aplica de forma coherente lo que declara en su documentación. Dichas inconsistencias debilitan el principio de responsabilidad proactiva en el conjunto de las actividades de tratamiento.

#### C. Formularios de recogida de datos (debilidad estructural)

- No se han identificado elementos plenamente conformes
- Consentimiento e información al interesado insuficientes en el punto de recogida de datos mediante los formularios

#### Implicaciones:

La falta de transparencia puede dificultar la generación de leads en el futuro y comprometer el uso lícito de los datos personales recogidos.

#### D. Controles de seguridad de los datos (aplicación desigual)

- Existen algunos controles de cumplimiento implementados
- No obstante, se han identificado también un número significativo y claramente visible de incumplimientos de alto riesgo

#### Implicaciones:

Esta situación debilita la capacidad de la organización para demostrar de forma clara y consistente la aplicación de medidas técnicas y organizativas adecuadas para la protección de los datos personales de los usuarios, y aumenta su nivel de exposición en caso de que se produzca un incidente de seguridad.

---

### 5. Implicaciones estratégicas

- El riesgo regulatorio es real y práctico, no meramente teórico

- Una reclamación o actuación inspectora podría escalar con rapidez
  - La situación actual debilita la capacidad de defensa de la organización conforme a los principios de responsabilidad proactiva del RGPD
  - La adopción de medidas correctoras mejoraría de forma significativa el nivel de cumplimiento y la posición de riesgo de la organización
- 

## 6. Recomendaciones para la Alta Dirección

- Corrección inmediata de los mecanismos de consentimiento de cookies
  - Alineación de la política de privacidad con las prácticas reales de tratamiento de datos
  - Estandarización y corrección de los formularios de recogida de datos
  - Cierre de las brechas de seguridad de los datos identificadas
  - Abordar el cumplimiento del RGPD como una cuestión de gestión del riesgo y no únicamente como un ejercicio documental
- 

## 7. Naturaleza indicativa del presente informe

Este informe constituye una **evaluación preliminar e indicativa**, basada exclusivamente en:

- Observaciones externas del sitio web
- Análisis funcional y documental visible públicamente
- Buenas prácticas generalmente aceptadas en materia de protección de datos

No sustituye:

- Una auditoría RGPD completa
  - Un análisis jurídico detallado
  - Una revisión técnica interna de sistemas y procesos
-

## 8. Recomendaciones y próximos pasos

A partir del análisis realizado y de los resultados reflejados en el presente resumen, se recomienda a la entidad responsable valorar la adopción de los siguientes pasos:

### A. Revisión del informe detallado de auditoría

Analizar el informe completo de auditoría RGPD, elaborado como parte de una evaluación profesional, en el que se desarrollan en detalle:

- Cada uno de los incumplimientos y deficiencias identificadas
- Las evidencias técnicas y documentales asociadas (capturas, pruebas funcionales)
- Los artículos del RGPD y los criterios de la AEPD aplicables en cada caso
- El contexto, alcance real y nivel de impacto de cada hallazgo

La revisión del informe detallado permite comprender con precisión el origen y la criticidad de los riesgos detectados, así como su posible impacto regulatorio.

### B. Definición de un plan de adecuación

Sobre la base del informe detallado y, en su caso, con el apoyo de asesoramiento especializado, se recomienda:

- Priorizar las acciones correctoras en función del nivel de riesgo (alto, medio, bajo)
- Definir las medidas técnicas, organizativas y documentales necesarias
- Asignar responsables internos para la ejecución de cada acción
- Establecer plazos razonables de implementación

El objetivo es reducir el riesgo regulatorio de forma progresiva, controlada y alineada con las directrices de la AEPD.

### C. Seguimiento, verificación y apoyo continuado

Una vez implementadas las medidas correctoras, resulta aconsejable:

- Verificar su correcta aplicación y efectividad

- Documentar las acciones realizadas como evidencia de cumplimiento
- Revisar periódicamente los tratamientos y configuraciones afectadas

Este enfoque, apoyado en un acompañamiento técnico-jurídico adecuado, permite avanzar hacia un modelo de cumplimiento efectivo, sostenible y defendible ante terceros.