Resumen del informe de cumplimiento del RGPD

Sitio web auditado:
https://www.ejemplo-clinica-demo.com/

Responsable del tratamiento:

Nombre	**Clínica Ejemplo Salud, S.L.**
CIF	**B12398745**
Localización	Avenida de la Salud, 18, bajo, 28040 – Madrid, España
Teléfono	**+34 600 987 654**
Email	**privacidad@ejemplo-clinica-demo.com**

Fecha del análisis:
27/12/2025

Consultor:
Sanjiv Sharma,
Data Protection and Digital Risk Consultant
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:

1.1 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

Buenas prácticas técnicas observables desde el exterior

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

2. Valoración global de riesgo

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

2.1 Resumen de riesgos por categoría

La siguiente matriz muestra la concentración de incumplimientos y riesgos detectados por categoría.

Categoría	Nivel de cumplimiento			Nivel de riesgo		
	Cumplimiento – C	Parcialmente conforme - PC	No conforme – NC	Bajo	Medio	Alto
Cookies	3	2	9	3	1	10
Política de privacidad	7	8	2	7	9	2
Recogida de datos(Formularios)	11	17	20	20	26	2
Seguridad de los datos	4	1	5	6	1	5
TOTAL	25	28	36	36	37	19

2.2 Criterios de evaluación (C / NC / P)

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

A. Cumplimiento (C)

Se considera **Cumplido** cuando:

- El requisito del RGPD/LOPDGDD está **plenamente implementado**
- La información es **clara, accesible y específica**
- No se detectan desviaciones relevantes

No requiere acción correctiva inmediata.

B. Parcialmente conforme (PC)

Se considera **Parcialmente conforme** cuando:

- El requisito está implementado **de forma incompleta**
- Existe información, pero es **genérica, ambigua o desactualizada**
- La medida existe, pero **no cumple plenamente** los criterios de la AEPD

Requiere corrección para reducir el riesgo.

C. No conforme (NC)

Se considera **No conforme** cuando:

- El requisito **no está implementado**
- Existe una infracción clara del RGPD
- El consentimiento, la base legal o la transparencia **no son válidos**

Supone riesgo regulatorio y requiere actuación prioritaria.

2.3 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

Definición de niveles

- **Riesgo Alto**
  Incumplimientos susceptibles de sanción, invalidación del consentimiento o reclamaciones formales.
- **Riesgo Medio**
  Deficiencias relevantes que requieren adecuación para garantizar el cumplimiento.
- **Riesgo Bajo**
  Aspectos mejorables sin impacto inmediato significativo.

2.4 Lectura por categoría (qué significa para la empresa)

Cookies

- Alta concentración de **No Conformidades (NC)** y **Riesgo Alto**.
- Indica problemas estructurales en:
  - consentimiento
  - configuración del banner
  - control previo a la instalación de cookies

Impacto:
Riesgo elevado de invalidez del consentimiento y sanciones frecuentes en la práctica de la AEPD.

Política de privacidad

- Predominan valores **Parcialmente conformes (PC)** y **Riesgo Medio**.
- Suele indicar:
  - información incompleta
  - redacción genérica
  - falta de adaptación a los tratamientos reales

Impacto:
Riesgo moderado, pero transversal: afecta a todos los tratamientos.

Recogida de datos (Formularios)

- Es la categoría con **mayor volumen de hallazgos**.
- Alta concentración de:
  - No conformidades
  - Riesgos medios y altos

Impacto:
Exposición directa a reclamaciones de usuarios, especialmente por:

- falta de base legal clara
- información insuficiente en el momento de la recogida

Seguridad de los datos

- Menor volumen total, pero presencia relevante de **Riesgo Alto**.
- Indica falta de evidencias visibles de medidas de seguridad.

Impacto:
Riesgo cualitativo elevado, especialmente tratándose de datos sensibles o de salud.

2.5 Qué indica el resultado global

Aunque existen elementos de cumplimiento, el análisis muestra que:

- Los **incumplimientos críticos no están aislados**
- Se concentran en áreas clave (cookies, formularios, transparencia)
- El riesgo no es puntual, sino **acumulativo**

Conclusión interpretativa

El sitio web presenta un **nivel de riesgo global alto**, no por un único incumplimiento grave, sino por la **suma de deficiencias estructurales** que afectan a derechos fundamentales de los usuarios.

Esto justifica:

- priorización de acciones correctoras
- enfoque planificado y no reactivo
- necesidad de coordinación entre medidas técnicas y documentales

---

3. Principales incumplimientos detectados (visión general)

A continuación, se resumen los **principales incumplimientos o debilidades detectadas**, sin entrar en detalle técnico o jurídico exhaustivo:

1. **Gestión de cookies no conforme**
    - Consentimiento no válido o insuficientemente granular.
2. **Deficiencias en la política de privacidad**
    - Falta de información obligatoria o redacción genérica.
3. **Recogida de datos sin base legal claramente identificada**
    - Formularios sin referencia explícita a la base jurídica aplicable.
4. **Información al usuario incompleta**
    - Incumplimiento del principio de transparencia (art. 12–14 RGPD).
5. **Ausencia de evidencias visibles de medidas de seguridad**

- Falta de indicios claros de protección adecuada de los datos.

(La lista anterior no es exhaustiva)

---

4. Impacto potencial para la empresa

Los incumplimientos detectados pueden implicar los siguientes riesgos:

4.1 Riesgo regulatorio

- Posible **exposición a sanciones por parte de la AEPD**
- Requerimientos de adecuación obligatoria
- Procedimientos sancionadores iniciados a raíz de reclamaciones

4.2 Riesgo de invalidez del consentimiento

- Cookies y tratamientos basados en consentimiento que podrían considerarse **nulos**
- Tratamientos sin base legal válida

4.3 Riesgo reputacional

- Pérdida de confianza de usuarios y clientes
- Impacto negativo en la imagen de marca
- Reclamaciones públicas o privadas

---

5. 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

---

6. Próximos pasos recomendados

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

6.1 Revisión del informe detallado de auditoría

Analizar el informe completo de auditoría RGPD, el cual desarrolla en detalle:

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

Esta revisión permite comprender con precisión el origen y la criticidad de los riesgos detectados.

6.2 Definición de un plan de adecuación

Sobre la base del informe detallado, 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 y controlada.

6.3 Seguimiento y verificación

Una vez implementadas las medidas correctoras, resulta aconsejable:

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

Este enfoque permite avanzar hacia un modelo de cumplimiento efectivo y sostenible.