Avisar y detectar al cliente cerca de la tienda SIN que instale una aplicación

Investigación técnica y legal — España, septiembre de 2026

Contexto: EcomTPV (TPV de escritorio C#/WPF) y su módulo de fidelización.

Documento de partida: `modulos IA/otras cosas/fidelizacion-wallet.html`.

---

0. Veredicto en una tabla

VÍA	¿VIVE EN 2026?	¿DE VERDAD SIN APP?	¿AVISA?	¿DETECTA?	RIESGO LEGAL
A1. Apple Wallet — `locations`	Sí	Sí (Wallet ya está instalada)	Sí, pasivo: el pase asoma en la pantalla de bloqueo, sin sonido	**No.** El comercio nunca se entera	Prácticamente nulo
A2. Google Wallet — `MerchantLocation`	Sí (aviso al usuario desde diciembre de 2025)	Sí	Sí, notificación real con sonido, **texto no editable**	**No**	Prácticamente nulo
B. Bluetooth (Eddystone / Nearby)	**MUERTO** desde el 6/12/2018; API apagada el 1/4/2021	—	—	—	—
B-bis. iBeacon dentro de un pase (`beacons`)	Sí, pero **solo iPhone** y **exige el pase ya instalado**	Sí	Igual que A1	No	Nulo
C1. Portal cautivo del wifi	Sí	Sí	Sí, por email/SMS después	Sí, pero solo de quien se conecta	**Alto**: aquí es donde la AEPD ya ha multado
C2. Detección pasiva por MAC	Técnicamente **roto** por la aleatorización	Sí	No	Malamente	**Campo de minas**
D. Pegatina NFC en el mostrador	Sí	Sí (iPhone XS o posterior, casi todo Android)	No avisa: capta	No	Nulo
E. Web Push	Sí en Android; en iOS **solo si añaden la web al inicio**	Sí	Sí	No	Bajo

Conclusión de una línea: lo único que cumple de verdad «avisar cuando está cerca, sin app y sin campo de minas legal» es **el pase del wallet con ubicaciones incrustadas**. Todo lo demás, o está muerto (Bluetooth), o está roto (MAC), o es un trámite de protección de datos serio (portal cautivo), o no avisa (NFC), o no llega al iPhone (Web Push).

Y la corrección más importante al documento de partida: el aviso de proximidad del wallet **no genera ningún evento del lado del comercio**. Ni Apple ni Google le dicen al emisor que el cliente ha pasado por delante. Sirve para *que al cliente le salte la tarjeta*, no para disparar un WhatsApp, ni para atribuir visitas, ni para medir nada.

---

1. Qué propone el documento de partida, y qué da por resuelto

Lo que propone

Un **programa de sellos que vive en Apple Wallet y Google Wallet**, sin aplicación propia. El giro conceptual: el pase deja de ser el premio y pasa a ser **el identificador** del cliente; todo lo demás (reseñas, WhatsApp, ofertas, atribución de compra) cuelga de él.

Cinco objetivos y su mecanismo:

1. **Reseñas** — petición tras la 2.ª o 3.ª visita, con enlace directo al formulario de Google. Sin incentivo.

2. **Suscripción** — NFC o QR en el mostrador → landing de tres campos → el pase entra en el wallet. Consentimientos separados por canal.

3. **Ubicación** — hasta diez coordenadas incrustadas en el pase; el sistema operativo lo muestra en la pantalla de bloqueo al acercarse.

4. **Asociación de compras** — el código del pase se escanea en el TPV. Única fuente de verdad.

5. **Puntos y sellos** — saldo actualizado por push al pase, coste cero.

Economía: hardware por local 40–150 €, coste variable 45–60 €/mes, PVP de referencia 79–149 €/mes, MVP en 6–8 semanas. Apple Developer 99 €/año, Google Wallet 0 €, push de pases 0 €. Canales ordenados por coste: pase 0 €, email 0,001 €, WhatsApp utilidad 0,008 €, SMS 0,05 €, WhatsApp marketing 0,06 €.

Descarta explícitamente: la aplicación nativa, el motor de workflows propio (se alquila Brevo/Klaviyo), premiar reseñas (ilegal, RDL 24/2021) y el NFC nativo del Wallet. Deja los sensores ToF y térmicos cenitales fuera del MVP.

Qué da por resuelto — y hasta qué punto tiene razón

LO QUE DA POR RESUELTO	VEREDICTO TRAS LA INVESTIGACIÓN
«El pase lleva hasta diez coordenadas; iOS y Android lo muestran en la pantalla de bloqueo al acercarse»	**Correcto**, y confirmado en la documentación de las dos plataformas. Ver §2.
«No se pide permiso. El geofence corre en el dispositivo. Fricción: ninguna»	**Correcto en Apple; matizable en Google.** En Android el usuario tiene que tener concedido a la app Google Wallet el permiso de ubicación **precisa y siempre**, más las notificaciones. No se lo pides tú, pero es una puerta que puede estar cerrada. Ver §2.2.
«El aviso no es una notificación push completa: es el pase asomando con una línea corta»	**Correcto para Apple**, y la propia Apple lo dice con esas palabras: *«Relevance information is passive […] It doesn't present alerts or post notifications»*. **Falso para Google**: ahí sí es una notificación de verdad, con sonido — pero **el texto lo escribe Google, no tú**.
«Apple limita a diez ubicaciones por pase»	**Correcto.** Google también: 10 por clase **más** 10 por objeto.
«Proximidad. Geofence del pase, **con tope de frecuencia**»	**No implementable tal cual.** No puedes limitar lo que no ves: no hay evento, no hay callback, no hay contador. Lo único que controlas es apagar o mover las ubicaciones por push. Ver §2.4.
Radio del geofence	**No lo dice, y es un límite real.** Para una tarjeta de sellos (`storeCard`) el radio máximo de Apple es **~100 m**, no los ~1.000 m de un billete de avión.
«Push web (PWA). Marginal: en iOS exige añadir la web a la pantalla de inicio. Casi nadie lo hace»	**Correcto y sigue siendo verdad en 2026**, incluso con el Declarative Web Push de Safari 18.4. Ver §6.
Consentimientos separados por canal, sin premarcar; art. 21 LSSI	**Correcto.** Ver §7.
Sensores ToF/térmicos «mucho más cómodos de justificar que el rastreo persistente de MAC»	**Correcto**, y la guía de la AEPD de 2024 lo respalda por la vía contraria: lo que hace inviable el rastreo de MAC es exactamente lo que estos sensores no hacen.
Fecha de nacimiento «porque la campaña de cumpleaños es la de mejor retorno»	Correcto, y **además te sirve de barrera de edad**: art. 7 LOPDGDD, 14 años. Ver §7.5.

Lo que no cubre el documento y sí pregunta el usuario: wifi, bluetooth, MAC, y el marco legal español con norma citada. Eso es lo que va a continuación.

---

2. Vía A — Wallet con relevancia por ubicación

> **Esta es la buena.** Es «sin app» de verdad: Wallet viene de fábrica en los dos sistemas operativos. El coste marginal es cero y el riesgo legal es prácticamente nulo, porque el geofence lo evalúa el teléfono (o Google) y **al comercio no le llega ningún dato de ubicación**.

2.1 Apple Wallet — la clave `locations` del `pass.json`

Apple lo dice literalmente en la guía de creación de pases:

> *«A pass can have up to ten relevant locations. In many cases, you have more than ten relevant locations, so you have to pick the best ten.»*

> *«Wallet makes relevant passes immediately accessible by integrating them with the lock screen. […] Relevance information is passive — it helps users find passes when they need them by putting relevant passes right on the lock screen. It doesn't present alerts or post notifications.»*

Límites exactos:

PARÁMETRO	VALOR
Ubicaciones por pase	**10**, máximo duro de Apple
Balizas iBeacon por pase (`beacons`)	**10** UUID distintos
`relevantDate`	**1** por pase (fecha «relevante»)
`maxDistance`	Es una `CLLocationDistance` (metros). **Tope real ~100 m** para `storeCard` , `coupon` y `generic` — es decir, la tarjeta de sellos. Hasta **~1.000 m** solo para `eventTicket` y `boardingPass`
Precisión efectiva	Se suma la `horizontalAccuracy` del GPS: con `maxDistance` 5 y precisión 10, se considera relevante hasta 15 m
Texto que se muestra	`relevantText` de cada ubicación, **tú lo escribes**, una línea corta
Sonido / vibración	**Ninguno**. Es una sugerencia pasiva
Tope de frecuencia	Apple no publica ninguno

Por qué Apple fija el tope en diez, según la documentación de PassKit: *«reducir el consumo de batería al escanear ubicaciones o balizas»* y *«mantener manejable el tamaño del fichero del pase»*.

Puertas que tienen que estar abiertas en el teléfono del cliente (por defecto lo están, pero conviene saberlas para dar soporte):

- Ajustes → Privacidad → Localización → activada, y **Wallet** en «Al usar la app» o «Siempre».
- En el propio pase: **«Sugerir en pantalla bloqueada»** activado, y «Permitir notificaciones».
- El modo de bajo consumo retrasa el disparo.

2.2 Google Wallet — `MerchantLocation` y las «nearby notifications»

Google lo llama *nearby notifications* y se configura con el campo `locations` / `MerchantLocations` de la clase y del objeto (de fidelización, oferta, genérico…), poniendo `notifyPreference` en `notifyOnUpdate` .

La referencia de `MerchantLocation` dice: *«cuando un usuario está dentro de un radio determinado de esta latitud/longitud, y permanece allí, Google dispara una notificación»*, y *«cuando el usuario sale de esa zona, la notificación se oculta»*.

PARÁMETRO	VALOR
Ubicaciones	**10 por clase + 10 por objeto** (documentación oficial de Google)
Radio	Lo decide **Google**, no tú. La documentación no publica el número; PassKit lo estima en **~150 m**
Permanencia (*dwell*)	La decide **Google**. No publicada
Texto de la notificación	**Lo escribe Google. No es personalizable.** Esta es la diferencia grande con Apple
Sonido	Sí, es una notificación normal de Android
Tope de frecuencia	La documentación de Google fija **3 notificaciones por 24 h** para las de *mensaje*; **para las de proximidad no publica tope**. PassKit habla de **4 al día en total**. Dato en conflicto: no lo des por cerrado
Requisitos en el teléfono	El usuario debe tener **notificaciones activadas** y haber concedido a la app Google Wallet **ubicación precisa y «siempre»**
Disponibilidad	La función de aviso por proximidad se desplegó a usuarios a partir de **diciembre de 2025**; España está en el mercado europeo de Google Wallet, pero conviene **probarlo con un teléfono real antes de venderlo**

Google ha añadido además interruptores por pase para que el usuario apague estos avisos, en el menú de tres puntos de la ficha del pase.

2.3 iBeacon dentro del pase — la única baliza Bluetooth que sigue viva

Es la excepción interesante al apartado B. El `pass.json` de Apple admite hasta **10 balizas** con su `proximityUUID`, su `relevantText` y su `name`. El iPhone hace saltar el pase a la pantalla de bloqueo al acercarse a una baliza con ese UUID **sin ninguna aplicación instalada**… pero **con el pase ya instalado**.

Consecuencias prácticas:

- No sirve para captar a nadie: solo funciona con quien ya es cliente del programa.
- **Solo iPhone.** Google Wallet no tiene equivalente.
- `CLBeaconRegion` está en *soft deprecation* desde iOS 18 (sigue funcionando, hay API nueva).
- Ventaja real sobre el GPS: precisión de metros dentro del local, funciona en un centro comercial o en un sótano donde el GPS no llega, y no consume batería de GPS.
- Coste: 15–40 € por baliza, con pilas que hay que cambiar.

Recomendación: no en el MVP. Guardar como opción para un local grande o un centro comercial, donde el geofence de 100 m es inútil porque cubre veinte tiendas.

2.4 Lo que el wallet NO te da (y el documento de partida da por hecho)

No hay evento de proximidad hacia el comercio. El servicio web de pases de Apple solo tiene cuatro extremos: registrar un dispositivo, listar los pases actualizados desde una fecha, entregar el pase actualizado y desregistrar (más un `/v1/log` de errores). **No existe ningún «este pase se ha mostrado» ni «este usuario está cerca».** Google, igual.

De ahí se sigue, y hay que decírselo al cliente antes de venderlo:

- El geofence del pase **no se puede medir**: no sabrás cuántas veces se ha mostrado ni a quién.
- **No se puede encadenar** con una automatización («cerca del local → mándale un WhatsApp»). El evento `cerca_del_local` que el documento propone emitir hacia Brevo **no se puede emitir**.
- **No se puede limitar la frecuencia** desde tu lado. Lo único que controlas es: quitar las ubicaciones del pase por push, o cambiar el `relevantText`.
- La única atribución real sigue siendo el escaneo del código en el TPV. Eso el documento ya lo dice bien.

---

3. Vía B — Bluetooth (iBeacon / Eddystone)

> **MUERTO.** Un móvil sin ninguna aplicación instalada **no puede** captar una baliza Bluetooth en 2026, salvo la excepción del §2.3 (iPhone con un pase de Wallet ya instalado). Google mató el sistema hace ocho años y no ha vuelto nada equivalente. Cualquier proveedor que te venda «balizas que notifican sin app» te está vendiendo un producto de 2016.

Cronología, con fuentes:

- **Octubre de 2017** — Google retira el soporte de Eddystone de Android y Chrome (el «Physical Web»).
- **25 de octubre de 2018** — Google anuncia el fin de Android Nearby Notifications. Motivo declarado: **spam publicitario**. *«These notifications did not meet our standards.»*
- **6 de diciembre de 2018** — Google deja de servir Nearby Notifications. Los usuarios dejan de ver avisos de balizas Eddystone y Physical Web.
- **1 de abril de 2021** — se apaga la Proximity Beacon API, que era lo último que quedaba para asociar un ID de baliza a un contenido.

Y en Apple **nunca existió**: iOS jamás mostró contenido de una baliza sin una app que la escuchara. Lo más cerca que estuvo fue el `beacons` del pkpass, que sigue vivo pero exige el pase.

Qué queda hoy, y qué no es:

- Balizas dentro de **tu propia app** → aquí no hay app, así que no aplica.
- **Fast Pair** de Google y el emparejamiento de Apple → son para emparejar auriculares y accesorios, no para marketing. No hay forma de meter un mensaje comercial por ahí.
- `beacons` **del pkpass** → §2.3, solo iPhone y solo clientes ya dados de alta.

Además, el legal. Aunque técnicamente funcionara: escanear direcciones Bluetooth de los que pasan por delante es exactamente el mismo tratamiento que el rastreo por MAC del §4.2, con los mismos problemas de la guía de la AEPD de 2024, y con aleatorización de la dirección Bluetooth desde Android 6 e iOS 8. Doble callejón sin salida.

Coste de oportunidad de intentarlo: hardware por local, pilas, mantenimiento, y cero alcance. No.

---

4. Vía C — Wi-Fi

4.1 Portal cautivo del wifi de la tienda

> **Funciona, es legal si se hace bien, y es exactamente donde la AEPD ya ha puesto multas de más de 40.000 €.** No es una vía «fácil»: es la más peligrosa de las que sí funcionan.

Cómo funciona. Pantalla de acceso con el logotipo del establecimiento que aparece al conectarse al wifi y obliga a identificarse antes de dar salida a internet. Se puede pedir email/móvil, o usar identificación social. A partir de ahí sabes que esa persona está *dentro* (no cerca: dentro) y puedes escribirle después.

Lo que exige el RGPD y la LSSI, punto por punto:

- **Información previa completa** — art. 13 RGPD: quién es el responsable, para qué, base jurídica, plazo, destinatarios, cómo ejercer derechos. En la propia pantalla, antes de pulsar nada.
- **Consentimiento expreso, separado y sin premarcar** para cada finalidad comercial — art. 4.11 y art. 7 RGPD, y considerando 43 (consentimiento agrupado = consentimiento inválido). **Dar el wifi no puede estar condicionado a aceptar publicidad**: eso rompe el requisito de «libremente prestado» del art. 7.4 RGPD.
- **Art. 21 LSSI** (Ley 34/2002) — para mandarle después email o SMS comerciales hace falta consentimiento previo expreso, salvo la excepción de relación contractual previa con productos similares. Conectarse al wifi **no** es una relación contractual previa de compraventa.
- **Brechas**: notificación en 72 h — art. 33 RGPD.
- **Conservación limitada** y minimización — art. 5.1.c) y 5.1.e) RGPD.

Precedentes reales: la AEPD ha sancionado por tratar sin consentimiento datos personales recogidos a través de redes wifi de negocios, con importes que arrancan en el entorno de los 40.000 € y un marco sancionador que llega a los 20 millones o el 4 % del volumen de negocio (art. 83.5 RGPD). Para un bar o una tienda, una multa así es el cierre.

Y el problema de producto, que es peor que el legal: el portal cautivo capta a quien quiere wifi gratis, que es un perfil sesgado y muy poco solapado con el cliente fiel de una cafetería de barrio. Además, la aleatorización de MAC (§4.2) ha roto la persistencia de sesión de los portales cautivos: en iOS 18 y posteriores la dirección privada **rota cada ~14 días** en redes abiertas, así que el cliente vuelve a ver la pantalla de alta una y otra vez.

Veredicto: solo si el comercio **ya tiene** wifi de invitados y quiere volumen de altas. Y aun así, es mejor usar el portal cautivo para **una sola cosa**: enseñar el botón «Añadir la tarjeta de sellos al wallet». Que el portal capte, y que el dato viva en el pase.

4.2 Detección pasiva por dirección MAC

> **Muerto por dos sitios a la vez: roto técnicamente y campo de minas jurídico.** No lo construyas y no se lo vendas a nadie.

Roto técnicamente. Las direcciones MAC que emiten los móviles al buscar redes ya no son las del fabricante:

- **Apple**: aleatorización de las tramas de sondeo desde iOS 8; «dirección wifi privada» por red desde iOS 14; y desde **iOS 18 / macOS 15 la dirección privada rota aproximadamente cada 14 días** en redes abiertas o de seguridad débil.
- **Android**: desde **Android 10** genera una MAC aleatoria distinta **por SSID**, y desde Android 12 hay aleatorización no persistente.

Efecto sobre la analítica de tienda: cualquier plataforma que cuente MAC en bruto **interpreta cada rotación como un dispositivo nuevo**. El «visitante recurrente» desaparece; lo que queda es un contador de bultos con ruido. Hay proveedores (Purple y equivalentes) que venden algoritmos de deduplicación con precisiones anunciadas del 99,8 % en aforo — pero eso es *contar*, no *reconocer*, y desde luego no *avisar*.

Y sobre todo: **una MAC no te permite escribirle a nadie.** No hay canal. Aunque la detección fuera perfecta, no puedes mandarle un mensaje a una dirección MAC. Para avisar necesitas un canal (pase, email, WhatsApp), y para tener el canal necesitas un alta consentida — o sea, la vía A.

Campo de minas jurídico. El 7 de mayo de 2024 la AEPD publicó, junto con la APDCAT (Cataluña), la AVPD (País Vasco) y el CTDPA (Andalucía), las **«Orientaciones para tratamientos que incorporen tecnologías de seguimiento Wi-Fi»**. Lo que dicen:

- La MAC es un **identificador único** que, mediante *fingerprinting*, permite detectar dispositivos y sacar patrones de movimiento → **es dato personal** y el tratamiento cae de lleno en el RGPD.
- **El consentimiento (art. 6.1.a RGPD) queda descartado** como base jurídica: es materialmente imposible pedírselo a alguien cuyo teléfono estás escuchando sin que él haga nada. Solo cabe en el escenario concreto en que el usuario se conecta voluntariamente a la red (o sea, el portal cautivo del §4.1).
- Obligación legal (6.1.c) e interés público (6.1.e) no aplican sin una ley que lo ampare. Intereses vitales (6.1.d), tampoco salvo emergencia.
- Queda el **interés legítimo (art. 6.1.f)**, y solo *con un juicio de ponderación documentado* que demuestre que no prevalecen los derechos del afectado. Las autoridades lo admiten para gestionar un espacio (aeropuerto, gran superficie) — no para hacerle marketing a un cliente de una cafetería.
- **Evaluación de Impacto obligatoria** — art. 35.3 RGPD, por observación sistemática a gran escala. Las autoridades recomiendan hacerla **incluso cuando dudes de si es obligatoria**.
- **Transparencia reforzada** — art. 13 RGPD, y en la práctica: **paneles visibles con la información, señalización pública, alertas de voz o campañas informativas**. La cartelería no es opcional.
- Medidas exigidas: **anonimizar y agregar los datos inmediatamente** tras la captura; **no asignar el mismo identificador al mismo dispositivo en visitas distintas** (es decir: prohibido justo lo que te haría falta para reconocer al cliente recurrente); limitar el ámbito del seguimiento; **no cruzar los datos de geolocalización con otras fuentes**; mecanismo de exclusión efectivo; auditorías independientes.

Traducido a producto: **la propia guía te prohíbe la funcionalidad**. «No asignar el mismo identificador en distintas visitas» y «no cruzar con otras fuentes» hacen imposible reconocer a un cliente y enlazarlo con su ficha de fidelización. Lo que queda permitido es contar bultos anónimos, que es exactamente lo que hacen mejor y más barato los sensores ToF del anexo del documento de partida.

---

5. Vía D — NFC en el mostrador

> **Funciona, cuesta céntimos, y no tiene ningún problema legal.** No sirve para avisar ni para detectar: sirve para **captar**, que es el paso previo a todo lo demás. El documento de partida ya lo tiene bien planteado.

- **iPhone**: la lectura de etiquetas NFC en segundo plano existe **desde el iPhone XS** (2018). Sin ninguna aplicación: acercas el teléfono, sale una tarjeta en pantalla y al tocarla se abre la URL en Safari. El iPhone 7, 8 y X leen NFC pero **necesitan una app**; para ellos el QR es el plan B.
- **Android**: prácticamente todos los modelos con NFC leen una etiqueta NDEF de tipo URL sin app.
- **Etiqueta**: una NTAG213 adhesiva, 0,30–0,80 € por unidad. El registro que hay que grabar es un **NDEF URI** apuntando a `https://…/alta?local=NNN`.
- **Regla práctica del documento de partida, que es correcta:** NFC y QR **en la misma placa**, nunca uno en lugar del otro. El NFC cubre a quien lo tiene activado; el QR cubre al resto y al escaparate, donde no se puede acercar el teléfono.
- **Legal**: nulo. Es el usuario el que acerca su teléfono voluntariamente y el que decide rellenar el formulario. Ni cartelería, ni EIPD, ni base jurídica que discutir más allá de la del propio formulario de alta.

---

6. Vía E — Web Push

> **Vale para Android. En iPhone es testimonial y lo seguirá siendo.** Barato de montar, pero no lo pongas en el argumentario de venta como si fuera un canal.

Android: Chrome soporta Web Push desde hace años, sin instalar nada. El usuario visita la web, se le pide permiso, acepta y ya recibe notificaciones. Coste: cero (VAPID, servidor propio).

iOS / iPadOS: Apple lo añadió en **iOS 16.4** (marzo de 2023) y la condición no ha cambiado:

> *«Web push is only supported when your site is installed as a Progressive Web App on the user's home screen.»*

- Hace falta un **manifiesto de aplicación web** y que el usuario haga **Compartir → Añadir a pantalla de inicio**. Tres toques que casi nadie da por una cafetería.
- El permiso solo se puede pedir **tras una interacción directa** del usuario.
- **Safari 18.4 / iOS 18.4** trajo el *Declarative Web Push*, que quita la necesidad de un *service worker* y simplifica mucho el código — **pero mantiene intacto el requisito de añadir a la pantalla de inicio**. En 2026 sigue igual.
- **Aviso sobre un bulo que circula:** se lee a menudo que «las notificaciones web no están disponibles en la UE desde iOS 17.4». Es **falso**. Apple anunció en febrero de 2024 que retiraría las web apps de pantalla de inicio en la UE por el DMA, y **dio marcha atrás el 1 de marzo de 2024**: las web apps y su push siguen funcionando en la Unión Europea.
- Cobertura de sistema operativo: más del 95 % de los iPhone del mundo van con iOS 16 o superior. El problema no es la versión, es el gesto de instalar.

Base jurídica: el permiso del navegador es un consentimiento válido si va acompañado de información previa (art. 13 RGPD) y de una forma de revocarlo. Como el push web usa un endpoint almacenado en el terminal, encaja además en el art. 22.2 LSSI, cuya excepción es el «servicio expresamente solicitado por el usuario» — y aquí lo está, porque él ha pulsado «Permitir». Riesgo bajo, pero pon la información delante del diálogo del navegador, nunca detrás.

Veredicto para este producto: el pase del wallet hace lo mismo, mejor, y en las dos plataformas. El Web Push es una redundancia de bajo coste, no un canal. Si se implementa, que sea en la fase 3 o más allá.

---

7. Lo legal en España, con norma citada

7.1 El marco

- **RGPD** — Reglamento (UE) 2016/679.
- **LOPDGDD** — Ley Orgánica 3/2018, de 5 de diciembre.
- **LSSI** — Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Arts. **21** (comunicaciones comerciales) y **22.2** (almacenamiento y recuperación de datos en el equipo terminal).
- **Orientaciones para tratamientos que incorporen tecnologías de seguimiento Wi-Fi** — AEPD + APDCAT + AVPD + CTDPA, **7 de mayo de 2024**.
- **Directrices 3/2019 del CEPD** sobre tratamiento de datos personales mediante dispositivos de vídeo, y la **Guía sobre el uso de videocámaras** de la AEPD, para la analítica de aforo con cámara.
- **RDL 24/2021** (transposición de la Directiva Ómnibus) — reseñas y prácticas comerciales, ya recogido correctamente en el documento de partida.

7.2 Base jurídica, vía por vía

VÍA	BASE JURÍDICA REALISTA	COMENTARIO
Alta en el programa de sellos (nombre, móvil, email, fecha de nacimiento)	**Art. 6.1.b) RGPD** — ejecución del contrato del programa de fidelización	Los datos **necesarios para el programa** no necesitan consentimiento aparte. Los que no lo son (fecha de nacimiento para la campaña de cumpleaños) sí: casilla propia
Enviarle email o SMS comercial	**Art. 6.1.a) RGPD** + **art. 21 LSSI**	Consentimiento previo, expreso, específico y **separado por canal**
WhatsApp	Igual, más la política de Meta (opt-in explícito, con independencia de la ley)	
Actualizar el saldo de sellos en el pase	**Art. 6.1.b)**	Es el servicio que pidió
Aviso de proximidad del wallet	**No hay tratamiento por tu parte**	Ver §7.3 — es el punto clave
Portal cautivo del wifi	**Art. 6.1.b)** para dar el acceso + **6.1.a)** para todo lo comercial	Y el acceso **no puede condicionarse** a aceptar publicidad (art. 7.4 RGPD)
Rastreo pasivo por MAC	**Solo art. 6.1.f)**, con ponderación documentada y EIPD	Y con las restricciones de la guía, que vacían la funcionalidad
Analítica de aforo con ToF/térmico	**Art. 6.1.f)** con datos agregados y anónimos	Mucho más defendible; procesado en el propio sensor, no sale imagen
Cámaras con analítica de comportamiento	6.1.f) + EIPD + señalización	Directrices 3/2019 del CEPD. Terreno resbaladizo

7.3 Por qué el aviso del wallet es legalmente sencillo (y esto es el argumento de venta)

El comercio no trata ningún dato de ubicación. Lo que ocurre es:

1. Tú metes unas coordenadas fijas — las de tus propios locales, que son un dato de la empresa, no de nadie — dentro de un fichero firmado.

2. Ese fichero lo instala el cliente voluntariamente en una aplicación de Apple o de Google.

3. El sistema operativo (Apple) o Google evalúan la cercanía **en su lado**.

4. **Nada vuelve hacia ti.** No hay evento, ni log, ni identificador, ni hora.

No hay recogida, ni registro, ni cesión de datos de localización del interesado por parte del responsable. Lo que sí tratas —nombre, móvil, email, historial de compras— lo tratas por el alta, no por el geofence. Entre Apple/Google y el usuario hay una relación propia, con sus propias políticas de privacidad, en la que tú no eres responsable.

Lo que sí hay que hacer, y es poco:

- Mencionarlo en la **información del alta** (art. 13 RGPD): «la tarjeta puede aparecer en la pantalla de bloqueo de tu móvil cuando estés cerca de uno de nuestros locales; puedes desactivarlo desde los ajustes del pase».
- No fingir que es una funcionalidad tuya que puedes apagar por cliente: **no puedes**, se apaga desde el teléfono.
- No usar el `relevantText` para publicidad agresiva. Es una línea corta y no hay tope de frecuencia en Apple: el abuso lo paga el cliente borrando el pase, no la AEPD.
- **Cartelería en la puerta: no hace falta ninguna.** Es la diferencia con el wifi tracking, y es la razón para elegir esta vía.

7.4 Cartelería obligatoria — cuándo sí

SITUACIÓN	¿CARTEL?	BASE
Pase de wallet con ubicaciones	**No**	No tratas datos en la puerta
Etiqueta NFC / QR de alta	**No** (pero pon un aviso de privacidad en la landing)	Art. 13 RGPD en el formulario
Portal cautivo	En la propia pantalla, sí; cartel físico no exigido	Art. 13 RGPD
Wifi tracking / rastreo de MAC	**Sí, obligatorio y reforzado**: paneles visibles, señalización, incluso avisos de voz	Orientaciones AEPD 2024 + art. 13 RGPD
Sensores ToF / térmicos de aforo	Sí, cartel informativo	Buena práctica; art. 13 si el tratamiento no es plenamente anónimo
Videovigilancia y analítica por cámara	**Sí, obligatorio**: cartel homologado en zona visible desde el acceso, con la información básica y dónde consultar la ampliada	Art. 22 LOPDGDD + Guía de videovigilancia AEPD

7.5 Menores

- **Art. 7 LOPDGDD**: el tratamiento de datos de un menor basado en su consentimiento **solo es lícito a partir de los 14 años**. Por debajo, hace falta el consentimiento del titular de la patria potestad o tutela.
- El RGPD (art. 8) deja la horquilla entre 13 y 16 años a cada Estado; **España fijó 14**.
- El consentimiento en materia de protección de datos es **siempre explícito**: no vale ninguna fórmula tácita.

Traducción a producto, y esto es una tarea concreta del formulario de alta:

- El formulario ya pide la fecha de nacimiento para la campaña de cumpleaños. **Úsala como barrera**: si sale menor de 14, no se crea el pase y se muestra un aviso.
- Mínimo **14 años** en las condiciones del programa. Si el cliente es una heladería, una tienda de golosinas o una papelería junto a un colegio, hay que decírselo por escrito antes de firmar.
- **Nunca** publicidad comportamental ni de proximidad dirigida a menores. Considerando 38 RGPD: los menores merecen protección específica en marketing y creación de perfiles.
- La campaña de cumpleaños de un menor de 14 con consentimiento paterno es posible, pero triplica el papeleo. Para un comercio pequeño, la recomendación es sencilla: **el programa es para mayores de 14 y punto**.

7.6 Resumen legal: fácil contra campo de minas

Legalmente sencillo — se resuelve con un buen formulario de alta:

1. Pase de wallet con `locations` / `MerchantLocation`.

2. Etiqueta NFC y QR.

3. Actualización del pase por push (saldo de sellos).

4. Email y WhatsApp con consentimiento separado por canal.

5. Web Push (el permiso del navegador es el consentimiento).

Campo de minas — no entrar sin abogado, EIPD y presupuesto:

1. Rastreo pasivo por MAC/Bluetooth. Además de roto, la propia guía de la AEPD te prohíbe la funcionalidad que querrías.

2. Portal cautivo mal montado. **Multas reales ya impuestas por encima de 40.000 €.**

3. Cualquier cruce entre presencia física y ficha de cliente que no venga de un acto voluntario del cliente (escanear su pase).

4. Analítica de comportamiento por cámara.

5. Menores de 14 sin consentimiento paterno.

---

8. Recomendación, en orden de esfuerzo contra beneficio

1.º — Pase de wallet con ubicaciones (Apple y Google). Hazlo.

- **En el TPV (C#/WPF):** casi nada. Un campo de latitud/longitud por local en la configuración de la tienda (o sacarlo de la dirección con geocodificación), y un campo de texto para el `relevantText` («Tienes 7 sellos, te faltan 3»). El geofence **no toca el TPV**: es un dato que viaja al generador de pases. Lo que sí toca el TPV es leer el código del pase en caja y llamar a la API de actualización.
- **Fuera:** dominio con HTTPS y certificado válido (Apple **exige** TLS en el servicio web de pases); un servicio que firme los `.pkpass` y emita los objetos de Google Wallet; APNs para las actualizaciones de Apple.
- **Certificados y coste: Apple Developer Program, 99 €/año** — una sola cuenta para toda la plataforma, no una por cliente —, con el certificado de Pass Type ID y el WWDR incluidos. **Google Wallet: 0 €**, cuenta de emisor gratuita, pero con **aprobación previa** para producción (proyecto de Google Cloud + cuenta de servicio; cuenta unos días, planifícalo).
- **Riesgo legal:** prácticamente nulo. Una frase en la información del alta.
- **Lo que hay que decirle al cliente antes de firmar:** el radio es de ~100 m en Apple para una tarjeta de sellos; en Google el texto lo escribe Google; y **no vas a poder medir cuántas veces se ha mostrado**.

2.º — NFC + QR en el mostrador. Hazlo, va con lo anterior.

- **TPV:** nada. Como mucho, un botón que muestre en pantalla el QR de alta para que el cliente lo escanee desde el otro lado del mostrador.
- **Fuera:** la landing de alta con los consentimientos separados. Etiquetas NTAG213 a 0,30–0,80 € y una placa de 5–15 €.

- **Riesgo legal:** nulo.

3.º — Web Push. Opcional, fase 3 o más allá.

- **TPV:** nada.
- **Fuera:** claves VAPID, manifiesto de aplicación web y un *service worker* (o el Declarative Web Push si solo te importa Safari moderno). Coste cero.
- **Riesgo legal:** bajo.
- **Realidad:** Android sí, iPhone testimonial. No lo vendas como canal.

4.º — iBeacon dentro del pase. Solo por encargo.

- **TPV:** nada.
- **Fuera:** balizas a 15–40 € por unidad, pilas, y un UUID por local en el pase.
- **Riesgo legal:** nulo (es el mismo mecanismo del pase).
- **Cuándo:** local muy grande, sótano, centro comercial — donde el geofence de 100 m del GPS cubre veinte tiendas y no distingue la tuya. Solo iPhone.

5.º — Portal cautivo del wifi. Solo si el comercio ya tiene wifi de invitados y lo pide.

- **TPV:** nada.
- **Fuera:** router o controlador compatible, la pantalla del portal con la información del art. 13 y los consentimientos, y el enganche con tu base de altas.
- **Riesgo legal: ALTO.** Es el único apartado de esta lista con multas de la AEPD ya firmes en España. Exige documentación de consentimiento, información completa y un responsable identificado — que sería el comercio, no tú, pero si tú se lo montas te salpica.
- **Si se hace:** que el portal solo sirva para **enseñar el botón de añadir la tarjeta al wallet**. No acumules ahí una base de datos paralela.

6.º — Rastreo pasivo por MAC / Bluetooth. NO. Ni por encargo.

- Técnicamente roto por la aleatorización (iOS 18 rota cada ~14 días; Android 10+ una MAC por SSID).
- No hay canal: una MAC no recibe mensajes.
- Y las orientaciones de la AEPD de 2024 te prohíben, con todas las letras, «asignar el mismo identificador en distintas visitas» y «cruzar los datos de geolocalización con otras fuentes» — o sea, exactamente la funcionalidad.
- Si un cliente insiste: **sensores ToF o térmicos cenitales**, que cuentan bultos sin identificar a nadie. Es otro producto, con instalación y otro ciclo de venta, y así lo dice ya el anexo del documento de partida.

7.º — Balizas Eddystone «que notifican sin app». No existe. Ver §3.

---

9. Cuatro correcciones concretas al documento de partida

1. **Quitar del plan la automatización «Proximidad … con tope de frecuencia»** o reescribirla. No hay evento hacia el comercio: no se puede contar ni limitar. Lo que sí se puede es mover o retirar las ubicaciones del pase por push.

2. **Quitar el evento `cerca_del_local` de la lista de eventos que se emiten hacia Brevo/Klaviyo.** No se puede emitir.

3. **Añadir el radio a la tabla de límites:** ~100 m en Apple para `storeCard`; el de Google lo decide Google (~150 m estimados).

4. **Matizar «no se pide permiso»:** en Android el usuario debe tener concedido a Google Wallet ubicación precisa y siempre, más notificaciones; en iOS, Localización activa para Wallet y «Sugerir en pantalla bloqueada» en el pase. No se lo pides tú, pero es una puerta que a veces está cerrada y que va a generar tickets de soporte del tipo «a mi cliente no le sale».

---

10. Fuentes

Apple Wallet

- Apple — *Wallet Developer Guide: Pass Design and Creation* (máximo de 10 ubicaciones, 10 balizas, 1 `relevantDate`, relevancia pasiva): https://developer.apple.com/library/archive/documentation/UserExperience/Conceptual/PassKit_PG/Creating.html
- Apple — *Showing a Pass on the Lock Screen*: https://developer.apple.com/documentation/walletpasses/pass/showing_a_pass_on_the_lock_screen
- Apple — *Pass.Locations*: https://developer.apple.com/documentation/walletpasses/pass/locations-data.dictionary
- Apple — *Pass.Beacons*: https://developer.apple.com/documentation/walletpasses/pass/beacons-data.dictionary
- Apple — *Adding a Web Service to Update Passes* (los únicos extremos que existen; no hay evento de proximidad): https://developer.apple.com/documentation/WalletPasses/adding-a-web-service-to-update-passes
- Apple Developer Forums — *Apple Wallet Pass Documentation - maxDistance?* (`maxDistance` es `CLLocationDistance` y se suma la `horizontalAccuracy`): https://developer.apple.com/forums/thread/666620
- Passworks — *What is the maximum value for maxDistance for Apple Wallet Pass?* (100 m en `storeCard` / `coupon` / `generic`; 1.000 m en `eventTicket` / `boardingPass`): https://help.passworks.io/maximum-distance-for-apple-wallet-passes
- PassKit — *How many locations will trigger a lock screen message?* (motivo del tope de 10): https://help.passkit.com/en/articles/2010114-how-many-locations-will-trigger-a-lock-screen-message
- PassKit — *GPS Location Notifications: Google Wallet vs Apple Wallet* (comparativa de radios y frecuencias): https://help.passkit.com/en/articles/12441270-gps-location-notifications-google-wallet-vs-apple-wallet
- PassKit — *Using Beacons with PassKit*: https://passkit.com/gemtot-beacons-eddystone-ibeacon-altbeacon/
- Passcreator — *Apple Wallet in iOS 26* y *Apple Wallet Design Update 2026*: https://www.passcreator.com/en/blog/apple-wallet-in-ios-26-what-you-need-to-know
- Apple — *WWDC26: What's new in Wallet*: https://developer.apple.com/videos/play/wwdc2026/209/
- AppleToolBox — *Boarding or Wallet Pass Doesn't Appear on Lock Screen* (ajustes de Localización y «Sugerir en pantalla bloqueada»): https://appletoolbox.com/wallet-pass-doesnt-appear-lock-screen/

Google Wallet

- Google — *MerchantLocation* (radio y permanencia los decide Google; la notificación se oculta al salir): https://developers.google.com/wallet/reference/rest/v1/MerchantLocation

- Google — *Trigger push notifications* (10 ubicaciones por clase y 10 por objeto, `notifyPreference`, texto controlado por Google, requisito de ubicación precisa y siempre): https://developers.google.com/wallet/retail/loyalty-cards/use-cases/trigger-push-notifications
- Google — *Wallet release notes*: https://developers.google.com/wallet/docs/release-notes
- 9to5Google — *Google Wallet rolling out nearby notifications* (4/12/2025): https://9to5google.com/2025/12/04/google-wallet-nearby-notifications/
- Android Authority — *Google Wallet now intuitively shows you the right pass at the right time*: https://www.androidauthority.com/google-wallet-nearby-pass-rollout-3607222/

Bluetooth / balizas

- Android Developers Blog — *Discontinuing support for Android Nearby Notifications* (25/10/2018): https://android-developers.googleblog.com/2018/10/discontinuing-support-for-android.html
- 9to5Google — *Google killing location-based Nearby Notifications on Android due to spam*: https://9to5google.com/2018/10/25/google-killing-location-notifications/
- BeaconZone — *Google Beacon Platform Shutting Down* (Proximity Beacon API, 1/4/2021): https://www.beaconzone.co.uk/blog/google-beacon-platform-shutting-down/
- VentureBeat — *Why Android Nearby, iBeacons, and Eddystone failed to gain traction*: https://venturebeat.com/business/why-android-nearby-ibeacons-and-eddystone-failed-to-gain-traction
- Apple Developer Forums — *Are several Proximity and Beacon related libraries deprecated in iOS 18?* (`CLBeaconRegion` en *soft deprecation*): https://developer.apple.com/forums/thread/757110

Wi-Fi y aleatorización de MAC

- AEPD — *Las autoridades de control de protección de datos publican unas orientaciones para tratamientos que incorporen tecnologías de seguimiento Wi-Fi* (7/5/2024): https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/autoridades-de-control-proteccion-datos-publican-orientaciones-tratamientos-tecnologias-seguimiento-wifi
- AEPD — *Orientaciones para tratamientos que incorporen tecnologías de seguimiento Wi-Fi* (guía en PDF): https://www.aepd.es/guias/orientaciones-wifi-tracking-seguimiento.pdf
- Cuatrecasas — *Nuevas orientaciones sobre los «riesgos» del Wi-Fi Tracking* (análisis de bases jurídicas y EIPD): https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/nuevas-orientaciones-sobre-riesgos-wi-fi-tracking
- PwC España — *Novedades de la Guía de orientaciones para la correcta implementación de tecnologías de seguimiento WiFi*: https://www.pwc.es/es/newlaw-pulse/regulacion-digital/novedades-guia-orientaciones-correcta-implementacion-seguimiento-wifi.html
- Lets Law — *Primeras multas de la AEPD sobre Wi-Fi tracking* (>40.000 €): https://letslaw.es/en/fines-wifi-tracking/
- Autónomos y Emprendedor — *Multas de más de 40.000 euros por utilizar los datos de los clientes que usan el wifi de los negocios*: https://www.autonomosyemprendedor.es/articulo/autonomos/multas-mas-40000-euros-aprovecharse-datos-clientes-que-usan-wifi-negocios/20240731173145037812.html
- INCIBE — *Protege tu Empresa responde: dudas legales sobre las conexiones wifi* (portal cautivo): https://www.incibe.es/empresas/blog/protege-tu-empresa-responde-dudas-legales-las-conexiones-wifi
- Purple — *MAC Address Randomization vs Device MAC: 2026 IT Guide*: https://www.purple.ai/en-us/blogs/mac-randomization-101
- Purple — *Apple iOS 18 and macOS 15 WiFi MAC randomisation guide* (rotación cada ~14 días): https://www.purple.ai/en-us/blogs/apples-ios-18-macos-15-the-impact-on-public-wifi-how-purple-can-help

- Cloud4Wi — *iOS 18 MAC randomization: key insights for IT managers*: https://cloud4wi.ai/resources/ios-18-mac-randomization/

NFC

- Apple — *Adding Support for Background Tag Reading*: https://developer.apple.com/documentation/corenfc/adding-support-for-background-tag-reading
- GoToTags — *iOS Background NFC Tag Reading on iPhone* (iPhone XS o posterior): https://gototags.com/help/ios/nfc/reading/background
- Seritag — *How to read NFC tags with an iPhone*: https://seritag.com/learn/using-nfc/how-to-read-nfc-tags-with-an-iphone

Web Push

- WebKit — *Web Push for Web Apps on iOS and iPadOS* (requisito de añadir a la pantalla de inicio): https://webkit.org/blog/13878/web-push-for-web-apps-on-ios-and-ipados/
- WebKit — *Meet Declarative Web Push* (Safari 18.4, sigue exigiendo la web app en la pantalla de inicio): https://webkit.org/blog/16535/meet-declarative-web-push/
- WebKit — *WebKit Features in Safari 18.4*: https://webkit.org/blog/16574/webkit-features-in-safari-18-4/
- MacRumors — *Apple Walks Back Decision to Disable Home Screen Web Apps in the EU* (1/3/2024): https://www.macrumors.com/2024/03/01/apple-walks-back-decision-to-disable-eu-web-apps/
- TechCrunch — *Apple reverses decision about blocking web apps on iPhones in the EU*: https://techcrunch.com/2024/03/01/apple-reverses-decision-about-blocking-web-apps-on-iphones-in-the-eu/
- MobiLoud — *Do Progressive Web Apps Work on iOS? The Complete Guide for 2026*: https://www.mobiloud.com/blog/progressive-web-apps-ios/

Protección de datos — normativa española

- AEPD — *¿Cuál es la edad para que los menores puedan prestar consentimiento?* (14 años): https://www.aepd.es/preguntas-frecuentes/10-menores-y-educacion/FAQ-1001-cual-es-la-edad-para-que-los-menores-puedan-prestar-consentimiento-para-tratar-sus-datos-personales
- Iberley — *Artículo 7 LOPDGDD*: https://www.iberley.es/legislacion/articulo-7-ley-organica-proteccion-datos-personales-garantia-derechos-digitales-lopdgdd
- Alex Barbarà — *Las obligaciones legales de las cookies: el artículo 22.2 LSSI*: https://www.alexbarbara.es/cookies-articulo-22-2-lssi/
- Legálitas — *Tengo wifi en mi negocio: cuidado con la protección de datos y las responsabilidades*: https://www.legalitas.com/actualidad/obligaciones-legales-wifi-negocio
- World Compliance Association — *La AEPD sanciona por tratar sin consentimiento datos personales recogidos a través de redes WiFi*: https://www.worldcomplianceassociation.com/1584/noticia-la-aepd-sanciona-por-tratar-sin-consentimiento-datos-personales-recogidos-a-traves-de-redes-wifi-espana.html

---

Investigación realizada el 8 de septiembre de 2026. Los límites de las plataformas (radios, topes de frecuencia, disponibilidad por país de las notificaciones de proximidad de Google Wallet) los cambian Apple y Google sin previo aviso: revalidar con un teléfono real antes de escribirlos en un contrato.