# ZenzSpa — Especificación de Requerimientos Funcionales (Unificado v2.0)

**Estado:** Borrador para revisión

**Fecha:** 12-08-2025 (America/Bogota)

**Propósito:** Unificar los requerimientos funcionales existentes del proyecto ZenzSpa con las mejoras y extensiones propuestas, en un documento único, consistente y listo para versionar/implementar.

## 0. Resumen ejecutivo

ZenzSpa es una plataforma para la gestión integral de un spa: autenticación, perfiles clínicos, servicios, horarios, citas, pagos y suscripciones VIP, marketplace, contenidos/notificaciones, analíticas y un asistente conversacional. Este documento fija **qué** debe hacer el sistema (funciones y reglas), con criterios de aceptación, permisos, errores estándar, trazabilidad y estados clave.

## 1. Alcance

**Incluye:** Frontend web/app, API backend, base de datos, pasarela de pagos, colas de tareas/notificaciones, chatbot y panel administrativo.

**Excluye:** Infraestructura física de red/telecom, hardware POS, software de terceros no integrado por API.

## 2. Convenciones y principios

* **Zona horaria operativa:** America/Bogota. Todos los datetime se almacenan en UTC y se presentan en America/Bogota.
* **Roles/Permisos (jerárquicos):** ADMIN > STAFF > VIP > CLIENT.
* **REST/JSON:** Respuestas en JSON, errores normalizados, compatibilidad con Idempotency-Key en endpoints de creación.
* **Códigos de error estándar:** 400 Validación, 401 No autenticado, 403 Sin permiso, 404 No encontrado, 409 Conflicto (concurrencia/estado), 422 Regla de negocio, 429 Límite de tasa, 5xx Fallo interno.
* **Auditoría:** Acciones administrativas y cambios críticos se registran en AuditLog (quién, qué, cuándo, desde dónde).
* **Accesibilidad/Idiomas:** UI mínimo en español; textos clave preparados para i18n.
* **Trazabilidad:** Cada requisito tiene identificador RFD-<Módulo>-NN y referencia a Historias de Usuario (HU) cuando aplique.

## 3. Actores

* **CLIENT:** Usuario registrado (no VIP) que reserva y paga.
* **VIP:** Cliente con beneficios/suscripción vigente.
* **STAFF:** Personal operativo (recepción/terapeutas) con acceso a agenda, perfiles clínicos y operaciones de caja.
* **ADMIN:** Dirección/propietario con permisos totales.
* **Pasarela de pagos:** Wompi (u otra equivalente) vía webhook y dashboards.
* **Chatbot:** Asistente conversacional (RAG) con guardrails y permisos.

## 4. Módulos y Requerimientos

A continuación se detallan los requerimientos por módulo. Para cada RFD se incluye **Descripción**, **Reglas/Restricciones**, **Criterios de Aceptación** y **Permisos**.

### 4.1 Autenticación y Gestión de Usuarios

**RFD-AUTH-01 — Verificación de identidad por OTP (SMS)** - **Descripción:** Registro/login con OTP de 6 dígitos vía SMS. Expira a los 5 minutos. - **Reglas:** Máx. 3 intentos por 10 min; en exceso → 429. Bloqueo y cooldown de 10 min; reCAPTCHA en reintentos anómalos. - **Aceptación:** - Dado un teléfono válido, cuando solicito OTP, entonces recibo código y se registra intento. - Dado un OTP correcto y vigente, cuando confirmo, entonces quedo autenticado y se emite par de tokens. - Dado intentos fallidos ≥3/10 min, cuando intento confirmar, entonces obtengo 429 y mensaje de espera. - **Permisos:** Público (solicitud OTP); autenticado tras confirmar.

**RFD-AUTH-02 — Tokens JWT con rotación y blacklist** - **Descripción:** access 15 min, refresh 7 días. Rotación segura de refresh y revocación (blacklist). - **Reglas:** Endpoint para “Cerrar sesión en todos los dispositivos”. - **Aceptación:** Revocar un refresh invalida el par anterior; acceso subsecuente requiere nuevo login. - **Permisos:** Autenticado.

**RFD-AUTH-03 — Roles/Permisos y filtrado de datos** - **Descripción:** Enmascarar datos sensibles según rol (p.ej., ocultar teléfono/email al perfil inadecuado). - **Reglas:** Control a nivel de serializador y consulta; pruebas de autorización por endpoint. - **Aceptación:** Un CLIENT no puede leer contacto de otro cliente; STAFF ve lo necesario para operar; ADMIN ve completo. - **Permisos:** Según rol.

**RFD-AUTH-04 — Cliente No Grato (CNG)** - **Descripción:** Marcar cliente como CNG bloquea nuevas citas y cancela las futuras. - **Reglas:** Operación atómica; disparo de notificaciones a ADMIN; bloqueo de registro si el teléfono coincide. - **Aceptación:** Al marcar CNG, se cancelan citas futuras (estado y slots liberados) y se audita. - **Permisos:** ADMIN.

**RFD-AUTH-05 — Recuperación de contraseña (fallback)** - **Descripción:** Flujo opcional de recuperación con OTP + nueva contraseña. - **Reglas:** Similar a RFD-AUTH-01; invalida sesiones activas al completar. - **Aceptación:** Tras éxito se obliga a reautenticación. - **Permisos:** Público (inicio), autenticado al finalizar.

**RFD-AUTH-06 — Gestión de dispositivos/sesiones** - **Descripción:** Listar y revocar sesiones activas por dispositivo. - **Reglas:** Revocar = invalidar refresh asociado. - **Aceptación:** Sesión revocada no puede refrescar tokens. - **Permisos:** Autenticado.

### 4.2 Perfil Clínico del Cliente

**RFD-CLI-01 — Modelo clínico versionado y consentimiento** - **Descripción:** Historial/condiciones, alergias, contraindicaciones, firmas de consentimiento. - **Reglas:** Versionado de cambios (changed\_by, changed\_at), acceso mínimo necesario, trazabilidad. - **Aceptación:** STAFF puede crear/editar; CLIENT ve su perfil; ADMIN puede anonimizar/eliminar bajo política. - **Permisos:** STAFF/ADMIN edición; CLIENT lectura propia.

**RFD-CLI-02 — Modo quiosco (recepción)** - **Descripción:** Captura guiada en recepción con **timeout** y bloqueo de navegación. - **Reglas:** Al salir sin guardar se descartan cambios. - **Aceptación:** Tras 5 min de inactividad, sesión vuelve a pantalla segura. - **Permisos:** STAFF.

### 4.3 Servicios y Horarios

**RFD-SRV-01 — Catálogo de servicios y categorías** - **Descripción:** CRUD de categorías y servicios con atributos (duration, price, vip\_price, is\_active). - **Reglas:** No se puede eliminar categoría con servicios activos; price\_at\_purchase se persiste en órdenes/citas. - **Aceptación:** Intento de borrar categoría con servicios → 409. - **Permisos:** ADMIN (CRUD), STAFF lectura.

**RFD-SRV-02 — Disponibilidad/horarios del spa** - **Descripción:** Bloques semanales por día, exclusión de almuerzo/descansos. - **Reglas:** Validación de solapamientos; capacidad simultánea por franja (low\_supervision\_capacity). - **Aceptación:** Crear franja que se solapa → 422; actualizar capacidad aplica a nuevas reservas. - **Permisos:** ADMIN (CRUD), STAFF lectura.

### 4.4 Citas (Agenda)

**Estados de cita:** PENDING\_PAYMENT, CONFIRMED, RESCHEDULED, COMPLETED, NO\_SHOW, CANCELLED\_BY\_CLIENT, CANCELLED\_BY\_ADMIN, REFUNDED.

**RFD-APP-01 — Creación idempotente con validación atómica** - **Descripción:** Crear cita valida bloque laboral, solapes y **buffer de limpieza** configurable. - **Reglas:** Idempotency-Key obligatorio en creación; bloqueo de concurrencia. - **Aceptación:** Cualquier conflicto → 409 con código específico; reintento con misma clave devuelve misma respuesta. - **Permisos:** CLIENT/VIP/STAFF/ADMIN.

**RFD-APP-02 — Asignación inteligente de terapeuta** - **Descripción:** API de recomendación lista solo STAFF disponibles en la franja. - **Reglas:** Considera duración, buffer, bloqueos y capacidad. - **Aceptación:** Si no hay disponibilidad, lista vacía y mensaje claro. - **Permisos:** Autenticado.

**RFD-APP-03 — Límites de citas activas** - **Descripción:** CLIENT máx. 1 activa; VIP máx. 4. - **Reglas:** Intento por encima del límite → 422. - **Aceptación:** Cambio de rol recalcula límite inmediatamente. - **Permisos:** Autenticado.

**RFD-APP-04 — Cancelación automática por no pago** - **Descripción:** Si no se paga el anticipo en advance\_expiration\_minutes, cancelar y notificar. - **Reglas:** Tarea periódica/worker; notificación por canal preferido. - **Aceptación:** Cita vuelve a estar disponible; se registra evento. - **Permisos:** Sistema.

**RFD-APP-05 — Momento Zen (multi-servicio)** - **Descripción:** Combinar servicios cortos en una única cita extendida. - **Reglas:** Validación de continuidad de bloques y duración total. - **Aceptación:** Confirmación crea un solo Appointment con subitems. - **Permisos:** Autenticado.

**RFD-APP-06 — Reagendamiento limitado de citas pagadas** - **Descripción:** Máx. 2 reagendamientos, permitidos hasta 24h antes. - **Reglas:** Cliente no puede cancelar directamente una cita pagada; debe reagendar dentro del límite. - **Aceptación:** Al exceder límite → 422. - **Permisos:** CLIENT/VIP; STAFF/ADMIN con excepciones auditadas.

**RFD-APP-07 — Cancelación por ADMIN y reembolso** - **Descripción:** ADMIN puede cancelar y disparar proceso de reembolso manual. - **Reglas:** Estados CANCELLED\_BY\_ADMIN y luego REFUNDED al aplicar nota de crédito. - **Aceptación:** Auditoría de motivo y operador. - **Permisos:** ADMIN.

**RFD-APP-08 — No-show y política de crédito** - **Descripción:** Si el cliente no llega en X min, marcar NO\_SHOW. El anticipo no es reembolsable; puede convertirse en crédito según política. - **Reglas:** credit\_expiration\_days configurable; notificación automática del resultado. - **Aceptación:** Marcar NO\_SHOW crea (o no) ClientCredit según política vigente. - **Permisos:** STAFF/ADMIN.

**RFD-APP-09 — Lista de espera** - **Descripción:** Un cliente puede unirse a la lista de espera de un horario; si se libera, se notifica FIFO. - **Reglas:** Confirmación por orden de llegada; ventana de aceptación de N minutos. - **Aceptación:** Si el cliente no confirma a tiempo, se ofrece al siguiente. - **Permisos:** Autenticado.

**RFD-APP-10 — Exportar iCal (.ics)** - **Descripción:** Agregar la cita confirmada al calendario del cliente. - **Reglas:** Archivo .ics con datos mínimos (servicio, fecha, duración, ubicación). - **Aceptación:** Descargar/adjuntar text/calendar válido. - **Permisos:** Autenticado.

**RFD-APP-11 — Bloqueo por deuda** - **Descripción:** Si existe COMPLETED con final\_payment pendiente, bloquear nuevas reservas. - **Reglas:** Intento de crear cita → 422 con detalle de deuda. - **Aceptación:** Al ponerse al día, el bloqueo se levanta automáticamente. - **Permisos:** Autenticado.

### 4.5 Pagos, Paquetes y VIP

**Entidades clave:** Order, Payment, Voucher, ClientCredit, Subscription.

**RFD-PAY-01 — Integración con pasarela (Wompi)** - **Descripción:** Checkout para anticipos/órdenes; recepción de webhooks firmados. - **Reglas:** Idempotencia por wompi\_reference; reintentos/sondeo si el webhook no llega; registro de eventos. - **Aceptación:** Estado CONFIRMED dispara confirmación de cita/orden; DECLINED limpia intentos. - **Permisos:** Sistema/Autenticado.

**RFD-PAY-02 — Precios VIP dinámicos** - **Descripción:** Cálculo al checkout; persistir price\_at\_purchase. - **Reglas:** Diferenciales aplican solo si vip\_expires\_at vigente. - **Aceptación:** Cambios de rol aplican en tiempo real.

**RFD-PAY-03 — Paquetes/Vouchers** - **Descripción:** Redimir sin nuevo pago; expiración configurable; beneficios como meses VIP. - **Reglas:** Control de saldo y usos; auditoría de redenciones. - **Aceptación:** Vencer un voucher lo vuelve no redimible; mensaje claro al usuario.

**RFD-PAY-04 — Lealtad VIP automatizada** - **Descripción:** Al cumplir condiciones (p.ej., 3 meses), emitir voucher de beneficio. - **Reglas:** Tarea programada; notificación. - **Aceptación:** SubscriptionLog registra la concesión.

**RFD-PAY-05 — Anticipo obligatorio** - **Descripción:** Porcentaje global advance\_payment\_percentage para reservar. - **Reglas:** Crear Payment tipo ADVANCE asociado a la cita. - **Aceptación:** No pagar dentro de la ventana → RFD-APP-04.

**RFD-PAY-06 — Conversión de anticipo a crédito** - **Descripción:** Al cancelar dentro de política o NO\_SHOW, convertir a ClientCredit según reglas. - **Reglas:** credit\_expiration\_days configurable. - **Aceptación:** Crédito disponible para aplicar a futuras compras.

**RFD-VIP-01 — Suscripción VIP recurrente** - **Descripción:** Cobro mensual; al aprobar cambia rol a VIP y fija vip\_expires\_at. - **Reglas:** Prorrateos/no; reintentos ante fallo; cancelación del plan. - **Aceptación:** Al fallar cobro tras N reintentos, degradar a CLIENT y notificar.

**RFD-PAY-07 — Propinas (tips)** - **Descripción:** Propina opcional en cierre de cita (efectivo o pasarela). - **Reglas:** Registro en Payment tipo TIP. - **Aceptación:** Reportes deben discriminar propinas.

**RFD-PAY-08 — Notas de débito/crédito internas** - **Descripción:** Ajustes contables post-venta con auditoría. - **Reglas:** Solo ADMIN; no alteran el price\_at\_purchase original. - **Aceptación:** Reportes de caja reflejan ajustes.

### 4.6 Marketplace de Productos

**RFD-MKT-01 — Catálogo e inventario** - **Descripción:** CRUD de productos; inventario con movimientos automáticos. - **Reglas:** Reservas de stock al checkout; disminución al confirmar pago. - **Aceptación:** Sin stock → no permite agregar al carrito.

**RFD-MKT-02 — Variantes/SKUs** - **Descripción:** Soporte para tallas/fragancias como variantes del mismo producto. - **Reglas:** SKU único por variante. - **Aceptación:** Checkout calcula stock por SKU.

**RFD-MKT-03 — Carrito y checkout** - **Descripción:** Carrito persistente, cálculo de totales VIP/CLIENT. - **Reglas:** Idempotencia al crear Order; re-cálculo de precios al pagar. - **Aceptación:** Orden queda en PAID al confirmar pago.

**RFD-MKT-04 — Entregas y estados** - **Descripción:** PENDING, PREPARING, SHIPPED, DELIVERED. - **Reglas:** Asociar entrega a una Cita existente opcionalmente (retira en spa). - **Aceptación:** Cambio de estado notifica al cliente.

**RFD-MKT-05 — Devoluciones (RMA)** - **Descripción:** Flujo de devolución con REQUESTED, APPROVED, REJECTED, REFUNDED. - **Reglas:** Políticas por tipo de producto y tiempos. - **Aceptación:** Al aprobar, generar ClientCredit o reembolso según caso.

### 4.7 Contenido y Notificaciones

**RFD-NOT-01 — Preferencias de notificación por usuario** - **Descripción:** Email/SMS/in-app; ventanas de silencio. - **Reglas:** Respeto de preferencias y horarios; fallback a canal alterno si falla principal. - **Aceptación:** Opt-out por tipo de mensaje no bloquea transaccionales críticos.

**RFD-NOT-02 — Plantillas versionadas** - **Descripción:** Plantillas transaccionales con variables y versionado. - **Reglas:** Cambios auditados; vista previa. - **Aceptación:** Envíos usan última versión activa.

**RFD-NOT-03 — Eventos principales (catálogo)** - **Descripción:** Recordatorio de cita (24h/2h), confirmación/cancelación, lista de espera disponible, pago aprobado/declinado, suscripción VIP cambios, entrega enviada. - **Reglas:** Orquestación vía cola (Celery/Jobs) y canales en tiempo real (cuando aplique). - **Aceptación:** Retries ante fallas temporales; métricas de entrega.

### 4.8 Analíticas y Reportes

**RFD-ANL-01 — KPIs definidos** - **Descripción:** Conversión a cita, tasa de no-show, % de reagendos, LTV VIP vs CLIENT, recuperación de deuda, utilización de cabinas/STAFF, AOV (carrito). - **Reglas:** Definiciones y fórmulas documentadas; consistencia de zona horaria. - **Aceptación:** Exportación CSV/XLSX y filtros por rango, rol, servicio.

**RFD-ANL-02 — Cuadros operativos** - **Descripción:** Agenda del día, cobros pendientes, créditos por vencer, suscripciones por renovar. - **Reglas:** Actualización casi en tiempo real. - **Aceptación:** Indicadores accionables (links a detalle).

### 4.9 Chatbot y Asistente Virtual

**RFD-BOT-01 — Guardrails y permisos** - **Descripción:** El bot respeta roles; no expone PII a no autenticados. - **Reglas:** Rate-limit por IP/usuario; máx. turnos por conversación. - **Aceptación:** Preguntas sobre citas/órdenes requieren sesión o verificación adicional.

**RFD-BOT-02 — Flujos principales** - **Descripción:** Consultar disponibilidad, agendar, reagendar, políticas, precios, estado de pedido. - **Reglas:** El bot siempre confirma antes de ejecutar acciones críticas. - **Aceptación:** Interacciones quedan registradas para auditoría y mejora.

### 4.10 Configuración Global

**RFD-CFG-01 — GlobalSettings** - **Descripción:** advance\_payment\_percentage, advance\_expiration\_minutes, buffer\_cleanup\_minutes, low\_supervision\_capacity, quiet\_hours, timezone\_display, credit\_expiration\_days, waitlist\_enabled. - **Reglas:** Solo ADMIN; cambios auditados. - **Aceptación:** Cambios aplican desde el siguiente evento/operación.

## 5. Catálogo de estados (texto)

* **Appointment:** PENDING\_PAYMENT → CONFIRMED → (RESCHEDULED)\* → COMPLETED | NO\_SHOW | CANCELLED\_BY\_\* → REFUNDED (si aplica)
* **Order:** CREATED → AWAITING\_PAYMENT → PAID → FULFILLING → FULFILLED | RETURN\_REQUESTED → REFUNDED
* **Payment:** INITIATED → PENDING → CONFIRMED | DECLINED → REFUNDED (si procede)
* **Subscription:** ACTIVE → PAST\_DUE → CANCELLED | EXPIRED

## 6. API (vista de alto nivel)

**Autenticación** - POST /auth/otp/request — Solicitar OTP - POST /auth/otp/confirm — Confirmar OTP → tokens - POST /auth/token/refresh — Rotar access/refresh - POST /auth/logout\_all — Revocar todas las sesiones

**Usuarios y perfiles** - GET /me — Perfil propio (enmascarado según rol) - GET /clients/{id} / PATCH /clients/{id} — Perfil clínico

**Servicios y horarios** - GET/POST /services — Listar/crear servicio - GET/POST /availability/blocks — Bloques horarios

**Citas** - POST /appointments — Crear (requiere Idempotency-Key) - GET /appointments/suggestions — Terapeutas y slots - POST /appointments/{id}/reschedule — Reagendar - POST /appointments/{id}/cancel\_by\_admin — Cancelar (ADMIN) - POST /appointments/{id}/mark\_no\_show — Marcar ausencia - GET /appointments/{id}/ics — Descargar iCal

**Pagos/VIP** - POST /checkout — Iniciar pago - POST /webhooks/payments — Webhooks pasarela - POST /subscriptions / DELETE /subscriptions/{id} — VIP

**Marketplace** - GET/POST /products — Productos/variantes - POST /cart/items — Carrito - POST /orders — Crear orden - POST /orders/{id}/return — Solicitar devolución

**Notificaciones** - GET/PATCH /me/notification-preferences — Preferencias

## 7. Catálogo de errores (extracto)

* SRV-001 Categoría con servicios activos → 409
* APP-002 Slot no disponible por solape → 409
* APP-004 Límite de citas activas superado → 422
* PAY-007 Webhook inválido/firma no verificada → 400
* VIP-003 Suscripción vencida/no vigente → 403

## 8. Catálogo de notificaciones (extracto)

* **Cita creada (pendiente de pago):** Email/SMS/in-app
* **Recordatorio 24h/2h:** SMS/in-app
* **Cita confirmada/cancelada/reagendada:** Email/SMS
* **Lista de espera disponible:** Push/SMS con ventana de N min
* **Pago aprobado/declinado:** Email
* **VIP activada/por vencer/falló cobro:** Email/SMS
* **Entrega actualizada:** Email/push

## 9. KPIs y definiciones

* **Conversión a cita:** Citas confirmadas / intentos de reserva.
* **No-show rate:** Citas NO\_SHOW / Citas confirmadas.
* **Reagendos exitosos:** Reagendos completados / intentos.
* **LTV VIP vs CLIENT:** Ingresos promedio 6–12 meses por rol.
* **Recuperación de deuda:** % de pendientes saldados en ≤7 días.
* **Utilización:** Tiempo ocupado / tiempo disponible por recurso.

## 10. Trazabilidad HU ↔ RFD (muestra)

| HU | RFD |
| --- | --- |
| HU-01/02/03 | RFD-AUTH-01/02/06 |
| HU-09–12 | RFD-CLI-01/02 |
| HU-13–15 | RFD-SRV-01/02 |
| HU-16–23 | RFD-APP-01…11 |
| HU-24–28 | RFD-PAY-01…06, RFD-VIP-01 |
| HU-29–32 | RFD-MKT-01…05 |
| HU-33–37 | RFD-ANL-01/02 |

Nota: Completar con IDs exactos y enlaces a Historias de Usuario en el repositorio/gestor.

## 11. Supuestos y decisiones

* Se adopta **un** entorno de despliegue coherente (p.ej., VPS con Nginx + Gunicorn + workers). El widget/chat puede residir en el mismo dominio detrás de reverse proxy.
* SMS vía proveedor confiable (p.ej., Twilio) para OTP y recordatorios críticos.
* Las políticas (no-show, créditos, anticipos) se parametrizan en GlobalSettings.

## 12. Pendientes y riesgos

* Definir políticas legales de datos clínicos/consentimiento y retención.
* Cerrar detalle de reintentos de cobro VIP y periodos de gracia.
* Afinar matrices de permisos por endpoint (anexo técnico).

## 13. Anexos propuestos (artefactos complementarios)

1. **OpenAPI v1** con ejemplos e idempotencia.
2. **Diccionario de datos y ERD** (tipos/índices/únicos).
3. **Diagramas de estados** de Appointment/Order/Payment/Subscription.
4. **Matriz RACI / Permisos** por rol y recurso.
5. **Política de datos personales y consentimiento** (legal + técnico).
6. **Estrategia de concurrencia e idempotencia** (locking/colisiones).
7. **Catálogo de notificaciones** (plantillas/versionado/canales/preferencias).
8. **Plan de contingencia de pagos** (reintentos/polling/caídas de webhook).
9. **Runbook de soporte y escalación** (incluye CNG).
10. **Colección Postman** (happy paths y errores).

### Formato de numeración y mantenimiento

* Los identificadores RFD-<Módulo>-NN son **estables**; toda modificación significativa implica cambio de versión menor/mayor del documento y registro en historial.

**Fin del documento**