



Manual técnico de FRIDA

Arquitectura, seguridad, datos, integraciones, despliegue, pruebas y operación.

Edición 2026.08.22.1

Documento operativo y formativo



Contenido

Índice generado a partir de los capítulos y procedimientos del documento.

Manual técnico de FRIDA	4
1. Propósito y alcance	4
2. Arquitectura	4
Mapa de arquitectura	4
3. Entornos y aislamiento	5
4. Modelo de datos	5
5. Seguridad	5
6. Transacciones y consistencia	6
Perímetro RRSIF/VERI*FACTU	7
Importación documental y stock	7
7. Integraciones	7
Google Calendar	7
Correo	7
WhatsApp Business	8
8. Rendimiento	8
9. Despliegue	8
10. Respaldo y recuperación	9
11. Pruebas y observabilidad	9
12. Mantenimiento	9
13. Incidencias frecuentes	10
Agenda lenta	10
Evento sin color correcto	10
Recordatorio no enviado	10
Correo aceptado pero no recibido	10
Facturación bloqueada	10
Documento de compra sin correspondencia	10
Stock duplicado tras una factura	10
14. Datos que nunca deben publicarse	10
WhatsApp Business para notificaciones de citas	12
Alta en Meta	12
Configuración privada	12
Parámetros de las plantillas de Meta	13
Plantillas recomendadas	13
Webhook de estados	14
Ejecución	14

Fuentes oficiales	14
-----------------------------	----

Manual técnico de FRIDA

Versión documentada: 2026.08.22.1

1. Propósito y alcance

FRIDA es una aplicación web multiusuario para negocios de servicios. Integra agenda, expedientes de clientes, recursos, ventas, caja, inventario, bonos, tarjetas regalo, facturación, privacidad, marketing e integraciones externas.

Cada cliente debe disponer de una instancia y una base de datos independientes. No se comparte información operativa entre centros. El código común se despliega mediante releases verificadas y la configuración sensible permanece fuera de la raíz pública y del repositorio.

2. Arquitectura

Mapa de arquitectura

Presentación

Vistas PHP, CSS, JS y accesibilidad

Servicios de aplicación

Agenda, clientes, caja, inventario, facturas, privacidad

Persistencia e integraciones

PDO + MySQL | Google Calendar | Correo | WhatsApp Cloud API

Operación

Migraciones, workers, respaldos, healthcheck, contratos y E2E

Las dependencias fluyen hacia servicios y adaptadores; los secretos se resuelven fuera de la raíz pública.

La aplicación usa PHP con PDO y MySQL/MariaDB. La interfaz se sirve desde `views/`, las reglas de negocio se concentran en `src/Service/`, las integraciones en `src/Integration/` y la configuración común en `config/`.

Capas principales:

- Presentación: vistas PHP, componentes parciales, CSS y JavaScript progresivo.
- Aplicación: servicios transaccionales para citas, cobros, caja, facturas, inventario, prepagados, privacidad, soporte y campañas.
- Dominio: normalización de medios de pago, estados y reglas compartidas.
- Persistencia: PDO con consultas preparadas, transacciones e índices.
- Integraciones: Google Calendar, correo y WhatsApp Cloud API mediante adaptadores y colas idempotentes.
- Operación: migraciones, respaldo, healthcheck, despliegues y pruebas.

La aplicación no utiliza secretos incluidos en el código. Los ficheros privados se resuelven desde `/home/u196349093/.config/sandstudio/` o mediante variables de entorno.

3. Entornos y aislamiento

Los entornos actuales son:

- Producción de Sand Studio: <https://sandstudio.finnos.es>.
- Showroom demostrativo: <https://showroom.finnos.es>.
- Web comercial: <https://finnos.es>.

El showroom contiene exclusivamente información ficticia. Sus integraciones pueden usar una configuración compartida expresamente marcada para demostración. Una implantación nueva debe crear una base de datos, credenciales, dominio, copias de seguridad e integraciones propios.

Las constantes APP_ENV, IS_PRODUCTION_ENV, IS_TEST_ENV e IS_SHOWROOM_ENV gobiernan las protecciones de cada entorno. La aplicación rechaza configuraciones incompatibles, muestra la identificación del showroom y bloquea la emisión fiscal mientras falten datos revisados.

4. Modelo de datos

El modelo cubre:

- Identidad y acceso: usuarios, perfiles, áreas profesionales y actividad.
- Clientes: expediente, contactos, categorías, notas, imágenes y privacidad.
- Agenda: citas, lista de espera, recursos, relaciones profesional-especialidad y bloqueos de solapamiento de profesional, cliente, cabinas y equipos.
- Comercio: ventas, productos, inventario, lotes, proveedores, pedidos, documentos de compra y correspondencias de catálogo por proveedor.
- Prepago: bonos, tarjetas regalo, transferencias y movimientos trazables.
- Tesorería: cajas, movimientos, cierres y acreditación por medio de pago.
- Facturación: series independientes, facturas ordinarias, simplificadas y rectificativas, líneas con origen, IVA incluido e IRPF por base elegible.
- Catálogo fiscal: reglas de especialidad, herencia de tratamiento, producto, excepción por cargo, instantáneas y eventos de resolución.
- Gobierno fiscal: perfiles versionados, evaluación restrictiva del alcance, transiciones y registro separado de estado jurídico e implementación.
- RRSIF: configuración por entorno, certificados cifrados, registros de alta y anulación, transmisiones y eventos inmutables.
- Integraciones: OAuth, tokens cifrados, colas de calendario y notificaciones.
- Gobierno: configuración, consentimientos, soporte y logs de actividad.

Las migraciones de migrations/ son idempotentes. Cada despliegue ejecuta bin/migrate.php, que registra las migraciones aplicadas y omite las ya existentes. Las relaciones críticas usan claves foráneas, restricciones e índices sobre fechas, estados, propietarios y claves de búsqueda.

5. Seguridad

Controles implantados:

- Autenticación con password_hash y password_verify.
- Regeneración del identificador de sesión al autenticar.
- Cookies HttpOnly, SameSite Lax y modo estricto cuando PHP aún no inició sesión.
- Revalidación de la cuenta activa en cada petición.
- RBAC por capacidades para administración, recepción y profesionales.
- Token CSRF en formularios con cambio de estado.
- Consultas preparadas y validación de identificadores.
- Escape HTML de datos mostrados.
- Ficheros privados fuera de la raíz pública.
- Restricción de tipos, tamaño y nombres de adjuntos.
- Adjuntos de soporte transitorios: se envían por correo y no se conservan.
- Tokens OAuth cifrados y acceso de Google con ámbitos mínimos.
- Firmas de consentimiento y galerías cifradas con AES-256-GCM y claves fuera de la web.
- Certificados fiscales PKCS#12/PFX cifrados con AES-256-GCM, acceso administrativo y validación previa de vigencia y NIF.
- Normalización de imágenes para retirar metadatos EXIF antes de cifrar.
- Eventos de privacidad y firmas de solo adición; la retirada crea un evento nuevo.
- Logs canónicos de operaciones sensibles.
- CSP, protección frente a framing, nosniff, política de referente y permisos.

La consola SQL es administrativa y de solo lectura. No sustituye las migraciones ni debe habilitar escrituras arbitrarias.

La configuración privada privacy-crypto.php -y su equivalente de showroom- declara la clave activa, el histórico de claves, la región y la fecha de verificación. Perder todas las copias de una clave hace irre recuperables los medios y firmas asociados; no debe almacenarse junto a una única copia del servidor.

6. Transacciones y consistencia

Los servicios que cambian saldos, stock, asistencia, cobros o facturas usan transacciones. Las filas sensibles se bloquean con FOR UPDATE antes de calcular y guardar un nuevo estado.

Principios:

- Una cita no puede solaparse con el profesional, el cliente o los recursos seleccionados, y el tratamiento debe ser compatible con una especialidad del profesional.
- Una asistencia que consume bono o tarjeta genera un movimiento trazable.
- Una anulación reintegra saldo y consumibles cuando corresponde.
- Los ajustes de cobro no reescriben el histórico económico: generan un ledger.
- Las facturas emitidas son inmutables; se corrigen con rectificativas.
- Los precios de factura contienen IVA y se desglosan, no se incrementan.
- Una operación cobrada solo puede aparecer en un borrador o factura; la clave

única de origen impide duplicarla.

- La simplificada usa serie propia, valida 400/3.000 €, receptor cualificado e incompatibilidad entre anonimato y retención.
- Los cierres de caja acreditan efectivo, TPV, Bizum y transferencia por separado.

Perímetro RRSIF/VERI*FACTU

La capa RRSIF está desacoplada del agregado de factura y se apoya en cinco grupos de tablas: configuración por entorno, certificados cifrados, registros, intentos de transmisión y eventos. La emisión crea el alta dentro de la transacción fiscal; una anulación crea otro registro y nunca elimina el anterior.

El servicio canónico serializa los campos reglados, calcula la huella SHA-256, encadena sobre el registro precedente y conserva XML, versión de esquema y estado. Los XML se validan contra XSD y la implementación del hash se contrasta con los casos oficiales. El PDF obtiene los datos de QR desde el registro inmutable, no desde valores reconstruidos en la vista.

Producción opera en shadow: crea registros y QR interno claramente rotulado, pero dos guardas independientes bloquean los transportes de pruebas y real. El showroom admite preparar mTLS contra el entorno externo de pruebas solo tras instalar un certificado propio del centro, verificar vigencia y NIF y superar los contratos de esquema, idempotencia, respuesta y reintento.

La activación real requiere una decisión administrativa separada, la declaración responsable de la versión y pruebas documentadas. FRIDA no afirma homologación, recepción AEAT ni condición VERI*FACTU antes de esos hitos.

Importación documental y stock

El contrato frida.procurement-document.v1 desacopla FRIDA de cualquier OCR o proveedor de inteligencia artificial. Solo se admiten JSON o CSV normalizados, con un máximo de 2 MB y 500 líneas. El fichero se lee de forma transitoria; se persisten los datos normalizados, la huella SHA-256 y las decisiones humanas, no el PDF o fotografía original.

La correspondencia propone productos mediante alias confirmado, referencia del proveedor, EAN, SKU y similitud de texto. La propuesta nunca actualiza stock por sí sola: cada línea debe validarse, descartarse con trazabilidad o vincularse a un producto creado desde el contexto de la revisión.

La finalización serializa el documento con FOR UPDATE y aplica en una única transacción pedido, línea, coste efectivo, lote, caducidad, saldo y movimiento. Las claves únicas proveedor-tipo-número y proveedor-huella impiden recargar el mismo documento. Una factura posterior a una recepción previa se concilia sin alterar existencias; una línea descartada queda excluida de pedido, lote y stock. Las salidas con lote siguen FEFO.

7. Integraciones

Google Calendar

OAuth usa autorización web, PKCE, state, tokens cifrados y ámbitos mínimos. Cada profesional puede tener un calendario privado asignado desde backend. Las citas se sincronizan mediante una cola idempotente.

La vista de agenda combina la base de datos local con eventos de Google. La base local se renderiza primero y prevalece durante el breve intervalo anterior a la sincronización; la lectura externa se completa de forma asíncrona sin bloquear tabla, formularios ni navegación.

Correo

El transporte usa el servicio de correo del alojamiento. Una aceptación por el relay confirma recepción técnica, no entrega ni lectura final. Soporte envía a equipo@finnos.es y añade copia al buzón del centro cuando es diferente.

WhatsApp Business

El modo manual genera un enlace compatible con dispositivos que puedan abrir WhatsApp. El modo automático usa exclusivamente WhatsApp Cloud API, plantillas aprobadas, opt-in acreditable y una cola con reintentos exponenciales.

Los secretos necesarios son token de usuario del sistema, identificador del teléfono y versión activa de Graph API. Nunca deben almacenarse en Git ni en una tabla visible desde la aplicación.

8. Rendimiento

La prueba del 28 de julio de 2026 realizó ocho solicitudes autenticadas, secuenciales y con caché caliente por ruta en el showroom.

Ruta	Media	p95
Agenda diaria	0,879 s	1,135 s
Agenda semanal	0,870 s	1,138 s
Clientes	0,018 s	0,021 s
Detalle de cliente	0,021 s	0,026 s
Ventas	0,019 s	0,024 s
Caja	0,016 s	0,017 s
Estadísticas	0,023 s	0,027 s
Inventario	0,017 s	0,020 s
Marketing	0,017 s	0,023 s
Facturación	0,023 s	0,026 s
Integraciones	0,320 s	0,394 s
Soporte	0,015 s	0,018 s

La base de datos y el alojamiento responden con margen en los módulos internos. La medición histórica identificó Google Calendar como punto a vigilar. Desde la versión 2026.08.01.1, la respuesta interactiva ya no espera esas consultas: la agenda interna llega primero y los cuatro calendarios vinculados se fusionan en segundo plano. El coste externo puede crecer, pero queda fuera de la ruta crítica de formularios y tablas.

Siguiente optimización si aumenta la escala: cachear por calendario y rango durante 30-60 segundos y configurar los workers como tarea programada. La agenda local ya se renderiza sin esperar a proveedores externos. El diagnóstico CLI reproducible está en `bin/agenda_performance.php`.

9. Despliegue

El flujo obligatorio es:

- 1 Comprobar que Git no contiene cambios sin registrar.
- 2 Sincronizar a un candidato privado.
- 3 Ejecutar auditoría estática y lint PHP.
- 4 Ejecutar healthcheck y contratos de negocio.
- 5 Crear respaldo de ficheros y base de datos.

- 6 Aplicar migraciones idempotentes.
- 7 Sincronizar el candidato con la raíz pública.
- 8 Reinstalar .htaccess y permisos.
- 9 Ejecutar smoke tests públicos y E2E.

Scripts disponibles:

- scripts/deploy_production.sh
- scripts/deploy_showroom.sh
- scripts/deploy_finnos_site.sh

Nunca debe desplegarse directamente editando la raíz pública.

10. Respaldo y recuperación

Antes de cada despliegue se genera un respaldo versionado. Debe comprobarse:

- Que el archivo existe y no está vacío.
- Que incluye código, configuración pública y dump de datos.
- Que los secretos continúan fuera del respaldo público.
- Que existe una política de retención externa al mismo alojamiento.

Una recuperación debe hacerse primero en un dominio temporal, ejecutar migraciones, healthcheck y E2E, y solo entonces conmutar tráfico.

11. Pruebas y observabilidad

La suite cubre las vistas públicas y autenticadas mediante auditoría estática, tres perfiles RBAC y contratos de negocio. También prueba ciclos de vida de citas, lista de espera, ventas, caja, inventario, compras, importación documental, bonos, tarjetas, facturas, privacidad, marketing, integraciones y soporte.

Comandos principales:

```
./tests/static_audit.sh
php bin/healthcheck.php production
./tests/e2e_test.sh URL FICHERO_PRIVADO_DE_CUENTAS
./tests/performance_smoke.sh URL FICHERO_PRIVADO_DE_CUENTAS 12
```

Los indicadores operativos recomendados son:

- p95 de agenda, clientes, ventas y estadísticas.
- errores HTTP 5xx y fallos de autenticación anómalos.
- tamaño y edad de las colas de Calendar y WhatsApp.
- fallos de correo, Calendar y WhatsApp por proveedor.
- duración y resultado de respaldos, migraciones y workers.
- crecimiento de tablas de logs, movimientos e históricos.

12. Mantenimiento

Para cada cambio:

- 1 Reproducir el caso con datos ficticios.
- 2 Añadir o actualizar una prueba.

- 3 Mantener reglas de negocio en servicios reutilizables.
- 4 Aplicar cambios de esquema mediante migración idempotente.
- 5 Revisar RBAC, CSRF, validación, transacciones y auditoría.
- 6 Medir rutas afectadas.
- 7 Desplegar con respaldo y smoke test.

Las decisiones fiscales, jurídicas o de proveedor no deben codificarse por suposición. Deben parametrizarse, revisarse y quedar bloqueadas de forma segura hasta disponer de información suficiente.

El alcance del copiloto fiscal, sus exclusiones y la arquitectura del ledger futuro se definen en [docs/fiscal/phase-0-scope-and-architecture.md](#). El copiloto no presenta modelos, no usa certificados, no representa al centro y no confecciona la declaración anual de la renta.

13. Incidencias frecuentes

Agenda lenta

Comprobar latencia de Google, número de calendarios, errores OAuth y llamadas síncronas. La agenda interna debe seguir siendo la fuente operativa.

Evento sin color correcto

Revisar estado de la cita, cola calendar_sync_outbox, token OAuth y resultado del worker.

Recordatorio no enviado

Comprobar opt-in, automatización de la plantilla, nombre aprobado por Meta, teléfono normalizado, estado de cola y worker.

Correo aceptado pero no recibido

Revisar logs del relay, SPF, DKIM, DMARC, carpeta de spam y rebotes.

Facturación bloqueada

Validar identidad fiscal, series, regla fiscal revisada por especialidad y habilitación explícita. No eliminar el bloqueo sin completar la configuración.

Documento de compra sin correspondencia

Revisar referencia, EAN y descripción, buscar en el catálogo completo o crear el producto desde la línea activa. El producto nuevo debe conservar stock cero hasta confirmar **Registrar entrada de stock**.

Stock duplicado tras una factura

Comprobar si la mercancía ya se recibió con el albarán. En ese caso, vincular el pedido y usar **Conciliar sin alterar stock**; no registrar una segunda recepción.

14. Datos que nunca deben publicarse

- Contraseñas, tokens, claves OAuth o secretos de webhook.
- Dumps de producción.
- Ficheros privados de configuración.
- Adjuntos de soporte.
- Datos de clientes en documentación, capturas o showroom.

- Domicilios privados no necesarios para la información legal publicada.

WhatsApp Business para notificaciones de citas

FRIDA separa dos canales:

- **Manual:** abre WhatsApp con el texto configurado y funciona desde cualquier navegador compatible en iOS, Android, macOS, Linux y Windows.
- **Automático:** usa exclusivamente WhatsApp Cloud API. Permanece bloqueado hasta configurar las credenciales privadas y una plantilla aprobada por Meta para cada tipo.

Alta en Meta

- 1 Crear o seleccionar el portfolio empresarial del centro en Meta Business

Suite y completar su información.

- 1 Crear una aplicación de tipo Business en Meta for Developers, asociarla al

portfolio y añadir el producto WhatsApp.

- 1 Crear o seleccionar la cuenta de WhatsApp Business, WABA.

- 2 Añadir el número emisor. Se recomienda un número dedicado. Si el panel ofrece

coexistencia oficial con WhatsApp Business App, debe seguirse exclusivamente ese flujo; no debe desregistrarse un número operativo sin plan de reversión.

- 1 Verificar la propiedad por SMS o llamada, aprobar el nombre visible y registrar el teléfono con un PIN de verificación en dos pasos de seis cifras.

- 1 Anotar, sin enviarlos por correo o chat:

- identificador del portfolio;
- WABA ID;
- Phone Number ID;
- número emisor;
- versión de Graph API soportada por la aplicación.

- 1 Crear un usuario del sistema en Business Settings, asignarle la aplicación y

la WABA, y generar un token con:

- whatsapp_business_messaging;
- whatsapp_business_management, necesario para administración y

suscripción de webhooks.

- 1 Guardar el token únicamente en el fichero privado del servidor.

El token temporal de la pantalla de inicio solo sirve para validar el alta. La operación estable debe usar un token de usuario del sistema y un procedimiento de rotación controlado.

Configuración privada

La sección whatsapp del fichero privado /home/u196349093/.config/sandstudio/integrations.php debe seguir esta estructura, sin copiar valores reales al repositorio:

```
'whatsapp' => [
    'enabled' => true,
    'mode' => 'production',
```

```

    'credentials' => [
      'transport' => 'cloud_api',
      'access_token' => 'TOKEN_DE_USUARIO_DEL_SISTEMA',
      'phone_number_id' => 'ID_NUMERICO_DEL_TELEFONO',
      'api_version' => 'v23.0',
      'public_base_url' => 'https://centro.example',
    ],
  ],

```

Cada plantilla se crea y aprueba en WhatsApp Manager antes de escribir su nombre en Administración → Notificaciones de citas.

Antes de activar el envío automático, el centro debe poder acreditar el opt-in exigido por WhatsApp para ese destinatario y canal. Las plantillas de citas son comunicaciones operativas asociadas a una reserva y no pueden incorporar promociones. El consentimiento para marketing se gestiona de forma independiente.

Parámetros de las plantillas de Meta

Las tres plantillas deben declarar siete parámetros de cuerpo, en este orden:

- 1 centro
- 2 cliente
- 3 servicio
- 4 profesional
- 5 fecha
- 6 hora
- 7 dirección

FRIDA no intenta crear ni aprobar plantillas en nombre del negocio. El texto personalizable del panel controla el mensaje manual; en los envíos automáticos, Meta controla el texto aprobado y FRIDA aporta estos valores.

Si se activa «Adjuntar evento de calendario» para la cita confirmada, esa plantilla de Meta debe incorporar una cabecera de tipo documento. FRIDA enviará en ella un .ics mediante un enlace aleatorio temporal servido desde public_base_url. El archivo omite el nombre del cliente y funciona con Apple Calendar, Google Calendar, Outlook y clientes compatibles con iCalendar.

WhatsApp recupera el adjunto como text/plain, uno de los tipos documentales admitidos por Cloud API, conservando el nombre cita-frida.ics. El acceso directo fuera del transporte de WhatsApp se sirve con el MIME estándar text/calendar.

Plantillas recomendadas

Crear tres plantillas de categoría Utility y en idioma español:

- frida_cita_creada: registro de la cita.
- frida_cita_confirmada: confirmación de la cita.
- frida_recordatorio_24h: recordatorio previo.

Las tres deben declarar los siete parámetros de cuerpo en el orden anterior. La plantilla confirmada debe incluir una cabecera de documento si se activa el adjunto .ics. No deben mezclarse promociones con estas plantillas operativas.

Después de la aprobación:

- 1 Abrir Administración → Notificaciones de citas.
- 2 Informar nombre e idioma exactos de Meta para cada marco.

- 3 Mantener desmarcado el envío automático.
- 4 Enviar una prueba a un destinatario ficticio controlado con opt-in.
- 5 Comprobar que Meta devuelve un identificador wamid.
- 6 Activar cada automatización por separado.

Webhook de estados

El envío inicial puede funcionar sin webhook, pero no es suficiente para conocer entrega, lectura o fallo final. Para trazabilidad completa:

- 1 Publicar un endpoint HTTPS específico con token de verificación.
- 2 Verificar la firma de cada notificación antes de procesarla.
- 3 Configurar la URL de callback en el producto Webhooks de la aplicación.
- 4 Suscribirse la aplicación a la WABA mediante `/WABA-ID/subscribed_apps`.
- 5 Procesar los estados sent, delivered, read y failed.
- 6 No guardar el contenido del mensaje si no es necesario para el servicio.

FRIDA aún no expone este endpoint. Hasta incorporarlo, el estado aceptada significa únicamente que Meta aceptó el mensaje para procesamiento.

Ejecución

`bin/appointment_notification_worker.php` siembra recordatorios de 24 horas y procesa la cola idempotente. La misma tarea se ejecuta como parte de `bin/calendar_sync_worker.php`. El despacho oportunista queda limitado a operaciones que modifican citas y no bloquea la carga GET de la agenda.

En Hostinger debe crearse una tarea programada cada minuto, con las variables privadas del entorno y sin imprimir secretos:

```
cd /home/u196349093/domains/sandstudio.finnos.es/public_html && \
APP_ENV=production \
SANDSTUDIO_DB_CONFIG=/home/u196349093/.config/sandstudio/database.php \
SANDSTUDIO_INTEGRATIONS_CONFIG=/home/u196349093/.config/sandstudio/integrations.php \
php bin/appointment_notification_worker.php 25
```

El resultado se dirige a un log privado con rotación. Debe alertarse ante mensajes en error, seis reintentos o una cola que aumente de forma sostenida.

Un resultado aceptada solo confirma que Meta devolvió un identificador wamid. Para distinguir enviado, entregado, leído o fallido se deberá habilitar posteriormente el webhook de estados de WhatsApp.

Fuentes oficiales

- <https://www.postman.com/meta/whatsapp-business-platform/overview>
- <https://www.postman.com/meta/whatsapp-business-platform/documentation/wlk6lh4/whatsapp-cloud-api>
- <https://www.postman.com/meta/whatsapp-business-platform/folder/zuoeksl/registration>
- <https://www.postman.com/meta/whatsapp-business-platform/folder/ypn8q0n/webhook-subscriptions>
- <https://www.postman.com/meta/whatsapp-business-platform/folder/huymv7d/templates>