CHECKOUT 3.0 / HTML ESTÁTICO

Manual Técnico - Checkout 3.0

KONEBE Checkout Fácil para Sitios - widget HTML con backend KONEBE

1. Qué es Checkout 3.0

Checkout Fácil para Sitios proporciona un widget de pago para páginas HTML estáticas. El comercio no necesita desarrollar backend propio, pero debe activar una conexión comercial autorizada en KONEBE.

> El HTML público solo contiene un identificador de widget. Nunca incluya la PDV Key, frases de recuperación ni privilegios administrativos en el HTML externo.

2. Configurar y activar el widget

• En Peuro Pay > Conexiones, abra Checkout Fácil para Sitios 3.0. Si hace falta, configure el TPV, guarde preferencias y active la conexión comercial.

• Elija nombre, descripción, donación (importe libre) o pago (importe fijo), moneda comercial, activos habilitados y dominios HTTPS autorizados.

• Guarde y copie el HTML generado. Desactivar el widget impide nuevos pagos, pero no cancela obligaciones ya iniciadas.

3. Incorporar en HTML estático

```
<div class="konebe-checkout"
 data-widget-id="<PUBLIC_WIDGET_ID>"></div>
<script async
 src="https://app.konebe.com/app/checkout-widget-embed.js">
</script>
```

El script carga un iframe alojado en KONEBE. Use el identificador público real generado en el panel. Compruebe el comportamiento en sitios con política CSP y restricciones de origen HTTPS.

4. Operaciones de la API Checkout

Operación	Permiso
widget-list / widget-save	Sesión de billetera autenticada; guardar requiere conexión activa.
widget-disable	Puede desactivar incluso con la conexión inactiva.
widget-get	Lectura pública limitada a datos de presentación.
widget-start	Inicia un intento público con límites e identificación.

Todas usan POST /api/merchant-checkout. El backend controla destinatarios, monedas, límites y permisos. El visitante no puede sustituir la billetera de destino.

5. Donaciones e importe fijo

• Importe fijo: el backend utiliza el precio guardado por el comercio; el visitante no puede modificarlo mediante HTML.

• Donación: el visitante introduce un importe sujeto a las reglas autorizadas y a los límites del cobro convertido cuando corresponda.

• Cada intento de pago tiene su identificador. Los reintentos del mismo intento deben ser idempotentes; las donaciones independientes reciben identificadores propios.

6. Seguridad y límites de uso público

• Los dominios autorizados son una protección adicional: Origin y Referer por sí solos no autentican. Compruebe CSP, iframe, límites de solicitudes y revocación.

• El frontend no puede decidir billetera, comisiones, conversión ni confirmar pagos. El backend comprueba red, transacción y estado financiero.

7. Cuándo preferir Checkout 2.0

Para pedidos con inventario y entregas automáticas integradas con el backend del comercio, utilice Checkout 2.0 o la API TPV. Checkout 3.0 está pensado para cobros sencillos en sitios sin backend.

Seguridad y límites financieros

• Nunca comparta frases de recuperación, claves privadas, la PDV Key ni credenciales de tesorería con el comprador; nunca las incluya en HTML público.

• Solo status=paid, confirmado por el backend, autoriza la entrega automática. Abrir el enlace, escanear el QR u obtener HTTP 200 no demuestra el pago.

• Cobro convertido: mínimo equivalente a 1 PEURO y máximo configurable de hasta 10.000 PEURO por cobro; comisiones definidas en el backend.

• Cobro directo: billeteras previamente autorizadas, direcciones exclusivas por cobro y límites técnicos de cada red; no se aplica el límite comercial de la reserva PEURO.

Verificación directamente en producción

KONEBE verifica operaciones directamente en producción, tras una publicación autorizada, con seguimiento e importes controlados. Este documento no certifica la publicación ni pagos reales.

• Antes de probar, compruebe el origen real de la API, el checkout, los bindings de Cloudflare y el esquema D1. No ejecute migraciones automáticamente por este manual.

• Utilice referencias de pedido identificables, supervise la conciliación blockchain y registre resultados sin secretos.