

DOCUMENTACIÓN TÉCNICA

Integración Checkout

FECHA: 2026/01/12

VERSIÓN #: 01

REVISIÓN #: 00

Indice

INTEGRACIÓN CHECKOUT	2
1. Descripción general	2
2. Alcance de la integración	2
3. Requisitos previos.....	2
4. Flujo funcional del pago	3
5. Funcionalidades soportadas.....	3
6. Seguridad y cumplimiento	4
7. Configuración básica	4
8. Manejo de respuestas	4
9. Referencia – Checkout PCI / NO PCI.....	5
9.1 Checkout NO PCI	5
9.2 Checkout PCI	6
Conclusión	7



INTEGRACIÓN CHECKOUT

1. Descripción general

La integración **Checkout** permite a los comercios procesar pagos mediante un **flujo controlado por Nuvei**, en el cual el ingreso de los datos sensibles de la tarjeta se realiza de forma segura, reduciendo significativamente el alcance de cumplimiento PCI.

Este modelo es ideal para comercios que buscan una **integración rápida**, segura y alineada a los requerimientos bancarios y de las marcas.

2. Alcance de la integración

La integración Checkout permite al comercio:

- Procesar pagos de una sola transacción
- Redirigir o inicializar el pago desde su backend
- Delegar el manejo de datos sensibles a Nuvei
- Implementar flujos con o sin autenticación 3DS
- Reducir el alcance de cumplimiento PCI
- Recibir confirmación del estado final vía callback

3. Requisitos previos

Antes de iniciar la integración Checkout, el comercio debe contar con:

- Credenciales activas:
 - **AppCode**
 - **AppKey**
- Ambiente habilitado:
 - Sandbox / Test
 - Producción



- Dominio registrado
- Certificado SSL (HTTPS)
- URL pública para **callback / webhook**

No es obligatorio contar con certificación PCI DSS completa cuando se utiliza el flujo Checkout NO PCI.

4. Flujo funcional del pago

1. El comercio inicia la orden de pago desde su backend.
2. Se genera una referencia de pago o inicialización del checkout.
3. El cliente ingresa los datos de la tarjeta en el entorno seguro de Nuvei.
4. Se ejecutan validaciones de seguridad:
 - Antifraude
 - 3DS / OTP (si aplica)
5. Se obtiene una respuesta sincrónica.
6. El estado final se confirma vía **callback/webhook**.
7. El comercio actualiza el estado de la orden.

5. Funcionalidades soportadas

- Pagos con tarjeta de crédito y débito
- Pagos de una sola transacción
- Soporte para:
 - 3DS 2.x
- Integración con motores antifraude
- Notificación del estado transaccional vía callback

6. Seguridad y cumplimiento

- El comercio **no almacena datos sensibles**
- Comunicación cifrada TLS 1.2 o superior
- Reducción del alcance PCI
- Cumplimiento típico:
 - **PCI DSS SAQ-A** (Checkout NO PCI)

El comercio es responsable de implementar correctamente los callbacks y validaciones.

7. Configuración básica

Parámetros comunes requeridos:

- **AppCode**
- **AppKey**
- **Amount**
- **Currency**
- **Order ID**
- **Customer data**
- URLs de:
 - Callback
 - Webhook
 - Return URL (si aplica)

8. Manejo de respuestas

Estados devueltos por la transacción:

- **Approved** → pago exitoso
- **FAILURE** → pago rechazado

- **Pending / Challenge** → autenticación adicional requerida
- **Error** → error técnico o de validación

El estado final **siempre debe validarse vía webhook**.

9. Referencia – Checkout PCI / NO PCI

9.1 Checkout NO PCI

Nota:

Los establecimientos que **NO cuentan con certificación PCI DSS** deberán utilizar los siguientes endpoints.

Endpoints disponibles

- **Init Reference (Checkout):**
<https://developers.paymentez.com/api/#payment-methods-cards-init-a-reference>
- **Webhook / Callback (obligatorio):**
<https://developers.paymentez.com/api/#webhook>
- **Refund (obligatorio):**
<https://developers.paymentez.com/api/#payment-methods-cards-refund>

Notas obligatorias (NO PCI)

- Todos los comercios **deben implementar el método Refund**, por requerimiento de los Bancos.
- Es obligatorio enviar un **correo de confirmación de pago** al cliente con:
 - Detalle de la compra
 - transaction_id (DF)
 - authorization_code
- Una transacción **Aprobada** se valida con:
 - status = "success"
 - status_detail = "3"

- Todos los comercios deben implementar **callback/webhook**, proporcionando una URL pública:
<https://developers.paymentez.com/api/#webhook>
- Si estos puntos **no están implementados**, el comercio **no podrá avanzar** en su integración.

9.2 Checkout PCI

Nota:

Los establecimientos que **CUENTAN con certificación PCI DSS** pueden realizar procesamiento directo.

Endpoints disponibles

- **Pago con tarjeta:**
<https://paymentez.github.io/api-doc/#payment-methods-cards-debit-with-credit-card>
- **Webhook / Callback (obligatorio):**
<https://paymentez.github.io/api-doc/#webhook>
- **Refund (obligatorio):**
<https://paymentez.github.io/api-doc/#payment-methods-cards-refund>
- **Verify (obligatorio para OTP / 3DS):**
<https://paymentez.github.io/api-doc/#payment-methods-cards-verify>

Notas obligatorias (PCI)

- Implementación obligatoria de **Refund**.
- Envío obligatorio de **correo de confirmación de pago** al cliente.
- Validación de transacción aprobada:
 - status = "success"
 - status_detail = "3"



- Implementación obligatoria de **callback/webhook**:
<https://paymentez.github.io/api-doc/#webhook>
- Sin estos componentes, el comercio **no podrá avanzar** en su integración.

Conclusión

La integración **Checkout** es una solución segura y eficiente para comercios que requieren **pagos de una sola transacción**, permitiendo cumplir con los requerimientos bancarios y de seguridad, con o sin certificación PCI, dependiendo del flujo implementado.