

# API pasarela de pago tefpay versión 2.0 (noviembre 2023)

NCN Customer Projects

Exported on 03/05/2025



Version 3.01

New Computing Netservices S.L.  
C/ Ferran Valls i Taberner, 5  
08006 Barcelona, España  
[info@tefpay.com](mailto:info@tefpay.com)  
[tefpay.com](http://tefpay.com)

## Aspectos generales operativos y funcionales de las transacciones

Cada e-commerce tiene unas características muy concretas, por eso se requiere de una gran variedad de transacciones para realizar pagos.

En tefpay se intenta dar solución a esta diversificación de necesidades con distintas transacciones y el comercio podrá combinarlas según más le convenga.

En este apartado se describen las transacciones más comunes, si requiere de alguna transacción adicional consulte con tefpay

### Pago estándar.

`Ds_Merchant_TransactionType = "201"`

Esta es la transacción más genérica. Al realizar esta transacción el titular tiene que estar presente y Tefpay solicitará la entrada de datos de la tarjeta (número, caducidad y CVV). Posteriormente, se intentará autenticar al cliente usando los mecanismos 3DSecure y MastercardCode si están accesibles. Si la autenticación del titular es correcta se procederá al cobro de la transacción.

En el proceso de autenticación el resultado puede ser negativo (no autenticado), con lo que no se procede al cobro de la operación o puede ser positivo (autenticado), con distintos niveles de garantías de cobro o sin garantías de cobro según la respuesta. Los e-commerce pueden configurar en tefpay que tipo de autenticación y garantías desean aceptar.

Todo este proceso se realiza en tiempo real, es decir, se produce un cargo en la tarjeta de crédito o débito.

### Devolución Parcial o Total

`Ds_Merchant_TransactionType = "4"`

Esta transacción será enviada por el e-comercio a tefpay, el cliente no necesita estar presente. Es una transacción iniciada por el comercio.

Al recibir esta transacción tefpay verifica que la autorización original esté aprobada y en tal caso se procederá a la devolución. Sólo se podrá realizar una devolución como máximo por el importe total de la autorización.

Aunque esta transacción se ejecuta en tiempo real puede demorarse que el titular reciba el abono en su cuenta por motivos exclusivamente de proceso bancario de las mismas. También en función de la entidad.

### Devolución online

`Ds_Merchant_TransactionType = "204"`

Esta transacción será enviada por el e-comercio a tefpay, el cliente no necesita estar presente. Es una transacción iniciada por el comercio.

Al recibir esta transacción tefpay verifica que la autorización original esté aprobada y en tal caso se procederá a la devolución. Sólo se podrá realizar una devolución como máximo por el importe total de la autorización.

Esta transacción se ejecuta en tiempo real el titular recibirá el abono en su cuenta inmediatamente.

## Autenticación

`Ds_Merchant_TransactionType = "203"`

Permite al comercio validar la tarjeta de crédito o débito y se utiliza para securizar una transacción validando el titular. No es necesario que el cargo posterior vinculado a la autenticación sea por importe igual al autenticado.

Es importante remarcar que en esta operación no se realiza ningún cobro en tiempo real. Posteriormente, el comercio deberá realizar el cobro de la autenticación en un periodo máximo de hasta 90 días naturales.

La operativa es similar a la de preautorizaciones, aunque en este caso no se produce solicitud de autorización, por lo que la transacción no es contable y no provoca retenciones en cuenta al titular. No se valida ni CVV2, ni la fecha de caducidad de la tarjeta ni si el titular tiene saldo. Sólo se valida que existe aquella numeración de tarjeta, y en el caso de que la operación se procese por 3D Secure la identidad del titular.

## Confirmación de autenticación

`Ds_Merchant_TransactionType = "209"`

Es el complemento a la transacción de autenticación, es decir, es el cobro de la autenticación realizada previamente.

El titular de la tarjeta no está presente, por lo tanto, la envía el e-commerce a tefpay.

El cobro se realiza en 3D Secure/SecureCode si la autenticación fue aprobada con este modo de seguridad. Cabe recordar que el plazo máximo para el cobro son 180 días naturales y dicho cobro no puede superar al importe autenticado.

Con esta transacción el e-commerce puede fraccionar pagos securizados hasta llegar al máximo del importe en la autenticación.

## Cobro recurrente

`Ds_Merchant_TransactionType = "208"`

Esta transacción será enviada por el e-comercio a tefpay, por eso, se requiere de una transacción previa dónde el cliente estuviera presente (transacciones tipo 201, 203, etc...).

Se considera una operación recurrente aquella compra a partir de la cuál el titular acepta cargos posteriores en su tarjeta, ya sean estos de carácter periódico, por tratarse de un bien o servicio de prestación regular, como es una compra de suscripción a un periódico, o bien el uso de los datos de la tarjeta para compras regulares repetidas en el mismo ecommerce. Por ejemplo los procedimientos de compra rápida o "one click buying" donde el cliente ya está identificado en compras anteriores. Un caso particular es el de una compra con pagos aplazados fraccionados.

Esta transacción no se procesa mediante 3D Secure/SecureCode, por eso, se considera no segura. Con la excepción de una compra con pago fraccionado que si puede securizarse porque se conoce el importe total a pagar, el número exacto de plazos de pago y su importe.

## Cobro sin 3D Secure/SecureCode

`Ds_Merchant_TransactionType = "22" o "27"`

Son dos transacciones de cobro no securizado con 3D. Se utilizará preferentemente la nueva transacción tipo 27 reservando la T22 para operativas especiales a consultar con Tefpay.

Transacción análoga a la transacción tipo 1, pero sin autenticación del titular de la tarjeta.

Al realizar esta transacción el titular tiene que estar presente y Tefpay se solicitará la entrada de datos de la tarjeta (número, caducidad y CVV). Posteriormente, se procederá al cobro de la transacción.

Los e-commerce pueden configurar en tefpay que tipo de autenticación desean aceptar para sus pagos.

Todo este proceso se realiza en tiempo real, con cliente presente, y para validar la tarjeta de crédito o débito se ejecuta un cargo o preautorización en la misma por un importe usualmente reducido que luego se procede a anular.

## Preautorización

Ds\_Merchant\_TransactionType = "202"

Suele utilizarse cuando en el momento de la compra no se puede determinar el importe exacto o, por alguna razón, el comercio no desea que el importe sea cargado en la cuenta del cliente de forma inmediata.

La solicitud de preautorización se lleva a cabo en tiempo real y produce una retención por el importe de la venta en la cuenta del titular. Algunos bancos emisores SI efectúan apuntes contables al titular que anulan automáticamente pasados unos días.

Toda preautorización debe tener una Confirmación de Preautorización en un período máximo de 7 días naturales. En caso contrario perderá su validez como garantía de pago.

## Confirmación de Preautorización

Ds\_Merchant\_TransactionType = "207"

Es el cobro de la preautorización. En este caso, el titular ya no es necesario que esté presente. Al igual que la confirmación de la autenticación el importe no puede superar al importe preautorizado y el plazo máximo para realizar el cobro se recorta a los 7 días naturales.

## Preautorización diferida.

Ds\_Merchant\_TransactionType = "216"

Transacción enviada por el e-commerce a tefpay. El titular no está presente. Revisar documentación e implementación específica para preautorizaciones.

## Anulación de preautorización.

Ds\_Merchant\_TransactionType = "218"

Transacción enviada por el e-commerce a tefpay y debe ser enviada antes de los 7 días naturales.

## Pagos mediante transferencia bancaria.

Ds\_Merchant\_TransactionType = "41"

Permite al titular realizar pagos mediante transferencias bancarias al e-commerce.

En esta operativa el titular debe estar presente y tefpay solicitará la entrada de los datos requeridos.

## Pagos mediante llamada telefónica.

`Ds_Merchant_TransactionType = "11"`

Los datos son introducidos por el comercio aunque son facilitados vía telefónica por el titular de la tarjeta. Los datos que el comercio debe solicitar al cliente únicamente es el número de tarjeta y la caducidad.

La toma de datos debe realizarse por la operadora en un formulario securizado o mediante operadora automatizada en la propia centralita con IVR.

## Suscripciones

`Ds_Merchant_TransactionType = "6"`

Permite la suscripción del titular de la tarjeta a un servicio ofrecido por el e-commerce.

Tefpay realizará cobros automáticamente y se notificará al comercio del resultado.

El e-commerce deberá indicar a tefpay importe a cobrar recurrentemente, finalización de la suscripción así como su periodicidad.

Si su comercio quiere este tipo de operación contacte con tefpay y solicite el documento de suscripciones: "Remote Subscription API (Merchant Interface)"

## Consulta de totales

`Ds_Merchant_TransactionType = "210"`

Solicitar consulta de totales (número e importe) de la sesión en curso y/o de previas (hasta 7 días).

Si su comercio quiere este tipo de operación contacte con tefpay y solicite el documento: "Consulta de totales"

## Cobro recurrente con Stripe

`Ds_Merchant_TransactionType = "25"`

Tefpay soporta sólo cobros recurrentes con Stripe. Es análoga a la operación descrita anteriormente, `Ds_Merchant_TransactionType = "208"`.

Esta transacción no se procesa mediante 3DSecure/SecureCode, por eso, se considera no segura.

Si su comercio requiere de este tipo de operación contacte con tefpay y solicite el documento: "Cobros recurrentes con Stripe".

## Preautorización Validación AVS importe cero

`Ds_Merchant_TransactionType = "33"`

Esta transacción será enviada por el e-commerce a tefpay, por eso, se requiere de una transacción previa dónde el cliente estuviera presente (transacciones tipo 201, 203, etc...).

Se considera una transacción para validación de la tarjeta, por ejemplo se hace una Transacción tipo 201 y al cabo de un mes se quiere realizar una carga sobre esa misma tarjeta (operación recurrente) pero queremos asegurarnos que la tarjeta está aún activa, usamos una transacción tipo 33 con importe 0 euros y si es ok lanzamos una tipo 208 para cobrar.

## Cobro sin autenticación ACS

`Ds_Merchant_TransactionType = "227"`

Esta transacción será enviada obligando al cliente a no autenticar por el método challenge (es cuando la entidad emisora envía clave por sms o la app de la entidad para confirmar la operación, también llamada autenticación ACS), este tipo de operación no es segura. Este tipo de transacción es creada principalmente para operaciones con tarjetas no europeas, ya que estas en su mayoría no tienen activa la nueva normativa PSD2.

## Resumen características de las operaciones.

Tipo de transacción	Produce cargo en la cuenta	Securización 3DSecure/SecureCode	Notas
Pago estándar.	SI	Aplica	
Devolución Parcial o Total	SI	No aplica	No puede superar el importe de la venta original.
Autenticación	NO	Aplica	
Confirmación de autenticación	SI	Aplica	Tiene un plazo máximo de 180 días para realizar el cobro.
Cobro recurrente	SI	No aplica	
Cobro sin 3DSecure/SecureCode	SI	No aplica	
Preautorización	NO	No aplica	
Confirmación de Preautorización	SI	No aplica	Tiene un plazo máximo de 7 días

Tipo de transacción	Produce cargo en la cuenta	Securizacion 3DSecure/SecureCode	Notas
			para realizar el cobro.
Anulación de preautorización.	NO	No aplica	
Preautorización importe 0.	NO	No aplica	
Validación de tarjeta de crédito/débito	NO	No aplica	Se realiza una preautorización y una anulación automática.
Almacenar tarjeta	NO	No aplica	No se realiza ninguna validación de la tarjeta.
Pagos mediante transferencia bancaria	SI	No aplica	Sólo requiere num. tarjeta y caducidad.
Pagos mediante llamada telefónica	SI	No aplica	
Suscripciones	Depende el caso.	Depende el caso.	



## Backoffice de tefpay.

### Introducción.

El backoffice es una aplicación web que permite el control en tiempo real sobre las transacciones de su empresa. Pudiendo consultar las operaciones realizadas por periodos, tipos de transacción, moneda, importe, numero de pedido, o incluso medios de pago.

Para acceder solicite a tefPay su cuenta de acceso y URL en función de si se desea acceder al entorno de producción o de integración.

### Consulta de operaciones.

Una vez logeado en el backoffice podrá consultar las operaciones realizadas tal y como se muestra en la siguiente imagen:

Transacciones

Total de transacciones

Cuentas de Clientes

Anti-Fraude

Administración

Administración Backoffice

Correos enviados

Transacciones realizadas

FILTROS

PERIODO:  
01/05/2016 a 12/05/2016

SERVIDOR:  
Todas

COMERCIO:  
V99000105 (Default)

TIPO TRANSACCIÓN:  
Todas

ESTADO:  
☒ V ☐ X ☐ AMBOS

Actualizar transacciones

Descargar CSV

Imprimir

Descargar PDF

Vista de Transacciones

Db.ID	Servidor	Fecha	Operación	Comercio	NºPedido	Nombre	Teléfono	Dirección	Ciudad	País	NºTrans.	NºTarjeta	Autorización	Estado	Importe	Mon	Acción
				- x	- x	- x	- x				- x	- x	- x	- x			
4555797	ccppslinte2	12/05/2016 16:00:21	Devolución	V99000105	160505000000070000001						230	424242*****4242	796328	V	-50,00 EUR		
4555737	ccppslinte2	05/05/2016 18:18:57	Venta	V99000105	160505000000070000003						229	424242*****4242	596347	V	100,00 EUR		Devolución
4555736	ccppslinte2	05/05/2016 18:16:35	Venta	V99000105	160505000000070000003						228	424242*****4242	365243	V	100,00 EUR		Devolución
4555735	ccppslinte2	05/05/2016 18:02:32	Venta	V99000105	160505000000070000003						227	424242*****4242	356964	V	50,00 EUR		Devolución
4555734	ccppslinte2	05/05/2016 17:56:46	Autenticación	V99000105	160505000000070000003	GS						424242*****4242		V	250,00 EUR		Venta
4555733	ccppslinte2	05/05/2016 17:47:36	Venta	V99000105	160505000000070000002						223	424242*****4242	504558	V	50,00 EUR		Devolución
4555732	ccppslinte2	05/05/2016 17:37:47	Autenticación	V99000105	160505000000070000002	GS						424242*****4242		V	250,00 EUR		Venta
4555731	ccppslinte2	05/05/2016 17:12:35	Venta	V99000105	160505000000070000001						219	424242*****4242	185977	V	50,00 EUR		Devolución
4555730	ccppslinte2	05/05/2016 17:02:37	Autenticación	V99000105	160505000000070000001	GS						424242*****4242		V	250,00 EUR		Venta
4555728	ccppslinte2	05/05/2016 16:19:45	Venta	V99000105	160505000000060000001						215	424242*****4242	842125	V	166,67 EUR		Devolución
4555727	ccppslinte2	05/05/2016 16:17:51	Venta	V99000105	160505000000060000001						214	424242*****4242	593458	V	83,33 EUR		Devolución
4555726	ccppslinte2	05/05/2016 15:42:35	Venta	V99000105	160505000000060000001						213	424242*****4242	139733	V	100,00 EUR		Devolución
4555725	ccppslinte2	05/05/2016 15:35:49	Autenticación	V99000105	160505000000060000001	GS						424242*****4242		V	350,00 EUR		Venta
4555724	ccppslinte2	05/05/2016 15:22:35	Venta	V99000105	160505000000050000008						209	424242*****4242	884214	V	50,00 EUR		Devolución

Actualizar transacciones

Mostrando 1 - 23 de 23

11	Autenticaciones	4.600,00 EUR
11	Ventas Total	823,00 EUR
1	Devoluciones	50,00 EUR
	Cobros netos	773,00 EUR

Esta pantalla visualizará las operaciones que se están procesando en tiempo real en su e-commerce.

## Funcionamiento.

En este apartado se describirá el funcionamiento de las operaciones citadas en el apartado 1.

A las operaciones con "clientes presente" suelen llamarse operaciones iniciadas por el titular (cliente de su e-commerce) ya que debe introducir los datos de tarjeta de crédito y es quien da la conformidad a realizar el pago, análogamente, las operaciones con "cliente no presente" suelen llamarse operaciones iniciadas por el comercio ya que no requiere intervención del titular y las envía directamente el servidor de su e-commerce a tefpay. Este último tipo de operaciones son, por ejemplo devoluciones, cobro recurrentes, etc ...

Tipo de transacción	Tipo de transacción	Presencia del cliente
Pago estándar con 3D secure + EMV3DS	201	cliente presente
Devolución Parcial o Total	4	cliente no presente
Devolución online Parcial o Total	204	cliente no presente
Autenticación	203	cliente presente
Confirmación de autenticación	209	cliente no presente
Cobro recurrente	208	cliente no presente
Cobro sin 3DSecure/SecureCode	22 y 27	cliente presente
Cobro no seguro	227	cliente presente
Preautorización	202	cliente presente
Confirmación de Preautorización	207	cliente no presente
Anulación de preautorización.	218	cliente no presente
Almacenar tarjeta	21	cliente presente
Preautorización importe 0	29	cliente presente
Pagos mediante transferencia bancaria	41	cliente presente
Pagos mediante llamada telefónica	11	cliente presente
Suscripciones	6	cliente presente

Para las operaciones con cliente presente, tefpay proporciona al e-commerce tres métodos de implementación.

- Método usando página hospedada.
- Método usando formulario de pago integrado con iFrame.
- Método usando formulario de pago con Javascript.

## Método usando página hospedada.

El e-commerce mostrará un boton en su página de e-commerce que al ser pulsado por el cliente será enviado a **tefpay** y este **solicitará los datos de la targeta en una página securizada.**

Al finalizar el pago esta transacción devolverá en la respuesta unos datos, llamados tokens que deberán ser reutilizados por el comercio para realizar operaciones con cliente no presente, es decir, serán las transacciones que se enviarán directamente desde su servidor de e-commerce a tefpay.

Tefpay proporciona varias páginas hospedadas o plantillas en función de las características de la operación o de las características de su e-commerce:

- Plantilla de página hospedada genérica.

Pasarela de pago seguro tefpay™

tefPAY  
payment services

Carro de compra

Pedido

160512151237123456789

Descripción

Lorem ipsum dolor sit amet, an dicta laudem philosophia nec, mel in prima oporteat consequat. An oblique accommodare mei, est id esse populo commune. Sit ei meliore accusam fabellas, eam cu oratio abhorreant, ne audire meliore usu.

Importe

1.00 EUR

Verified by MasterCard.  
VISA SecureCode.

Verified by Visa y MasterCard SecureCode protegen los datos de sus tarjetas de crédito y débito.

Completar la información de su pago

Nombre en la tarjeta

Número de tarjeta

Fecha de caducidad

Mes

Año

Código seguridad

SSL Secure Connection

Finalizar Pago

Cancelar

El Código seguridad (CVV) es el código de 3 dígitos en el reverso de su tarjeta de crédito. Lo puede encontrar en el espacio en blanco designado para su firma.

**En la siguiente URL podrá visualizar rápidamente todas plantillas de páginas hospedadas que tefpay proporciona por defecto:** <https://intepayments.tefpay.com/simu/>

Requerimiento PCI : SAQ A

El requerimiento PCI mediante presentación de formulario SAQ A a la entidad titular de la cuenta merchant cuando esta lo requiera es de simple cumplimiento dado que los requerimientos PCI recaen sobre la infraestructura de Tefpay y el comercio queda en la prácticamente exento. Solicitar caso de no disponer del mismo formulario PCI SAQ A para presentar a la entidad titular de la cuenta merchant.

❗ Las páginas hospedadas en tefpay pueden ser personalizadas con la apariencia de su página de e-commerce aunque tefpay proporciona las plantillas anteriores por defecto. Si su e-commerce quiere personalizar una página hospedada solicite a tefpay el documento: "**Hosted: Personalización página hospedada y T.P.V.**"

## Método usando formulario de pago integrado con iFrame.

Con este método su comercio puede incrustar una página hospedada en su e-commerce mejorando considerablemente la integración de la plataforma de pagos en con su e-commerce.

La implementación usando página hospedada con iFrame queda fuera del alcance de este documento. Solicite a tefpay un documento específico de cómo integrar su plataforma con este método llamado: "**Hosted usando iFrame**". En ese documento sólo se describe una sencilla API en javascript para implementar con tefpay un iFrame, las variables requeridas para procesar pagos se describen en el presente documento.

**\*Importante en la siguiente URL podrá visualizar un ejemplo básico de un pago usando un iFrame** <https://intesecure02.tefpay.com/iframe/index.phtml>

Requerimiento PCI : SAQ A

El requerimiento PCI mediante presentación de formulario SAQ A a la entidad titular de la cuenta merchant cuando esta lo requiera es de simple cumplimiento dado que los requerimientos PCI recaen sobre la infraestructura de Tefpay y el comercio queda en la prácticamente exento. Solicitar caso de no disponer del mismo formulario PCI SAQ A para presentar a la entidad titular de la cuenta merchant.

Personalización iFrame : Solicitar información adicional a Tefpay caso de querer personalizar iFrame. Ver documento

## Método usando formulario de pago con Javascript .

En las transacciones iniciadas por el cliente/titular, su e-commerce puede también usar la pasarela tefpay sin reenviar el titular de la tarjeta a una página hospedada en tefpay, dicho de otro modo, **el titular introduce los datos de la tarjeta en su e-commerce.**

La implementación sin usar página hospedada queda fuera del alcance de este documento aunque si su e-commerce requiere esta característica, tefpay deberá recibir los datos de la tarjeta cifrada. Solicite a tefpay un documento específico de cómo cifrar correctamente la tarjeta llamado: "**Hosted: Cifrado por RSA**". En ese documento sólo se describe como cifrar la tarjeta, es decir, es un complemento a esta documentación con unos pequeños cambios que afectan al cifrado.

Tenga en cuenta que todas las transacciones realizadas con este método serán sin usar 3DSecure/SecureCode ya que el cliente no será autenticado en la entidad bancaria correspondiente.

- **Importante .En la siguiente URL podrá visualizar rápidamente el funcionamiento básico de un pago sin usar una página hospedada en tefpay:** <https://intesecure02.tefpay.com/simupayweb/hostedrsa/index.phtml>.
- Observará que el cifrado se produce en el navegador del cliente y en ningún caso la tarjeta viajará en claro por los servidores de su e-commerce.

En este procedimiento es requisito fundamental que el comercio controle que no se puedan ejecutar cobros repetidos. Para ello debe bloquearse siempre la tecla de pago después de pulsada por el cliente. Una vez pulsada la tecla de PAGAR debe visualizarse un mensaje que indique que la transacción se está procesando. La respuesta ok/ko llega al navegador del cliente y también por callback. Es responsabilidad del comercio visualizar los mensajes de error que puedan producirse así como controlar que no se produzcan duplicados por compras repetidas. Por parte de Tefpay se prestará la ayuda y validación necesaria.

#### Requerimiento PCI DSS : SAQ A-EP

El requerimiento PCI mediante presentación de formulario SAQ A-EP a la entidad titular de la cuenta merchant cuando esta lo requiera es de cumplimiento más complejo que en los casos anteriores dado que los requerimientos PCI recaen en parte sobre la infraestructura del comercio y para asegurar su cumplimiento el alcance del formulario SAQ A-EP es bastante extenso. Asimismo por el mismo motivo el comercio puede quedar sujeto a escaneos periódicos de la infraestructura.

En caso de duda consultar con Tefpay.


### Transacciones iniciadas por el cliente.

En la página de pago de su e-commerce usted tiene que implementar un botón de "Pagar" que al ser pulsado por el titular será redireccionado a la página hospedada de tefpay.

Cuando el titular pulse en dicho botón se le mostrarán los datos más relevantes al pago como pueden ser:

Dato	Significado
Importe	El importe que se le cobrará al cliente.
Número de pedido	Es el identificador la compra.
Descripción del pedido	Una breve descripción del pedido que está comprando.

Por otro lado, se le solicitarán los datos pertinentes para realizar el cargo en su cuenta:


**Carro de compra**


**Pedido** 160510170340123456789

---

**Descripción** Lorem ipsum dolor sit amet, an dicta laudem philosophia nec, mel in prima oporteat consequat. An oblique accommodare mei, est id esse populo commune. Sit ei meliore accusam fabellas, eam cu oratio abhorreant, ne audire meliore usu.


---

**Importe** 1.00 EUR



**Verified by MasterCard. VISA SecureCode.**

Verified by Visa y MasterCard SecureCode protegen los datos de sus tarjetas de crédito y débito.


**Completar la información de su pago**


**Nombre en la tarjeta**

**Número de tarjeta**

**Fecha de caducidad**

**Código seguridad**

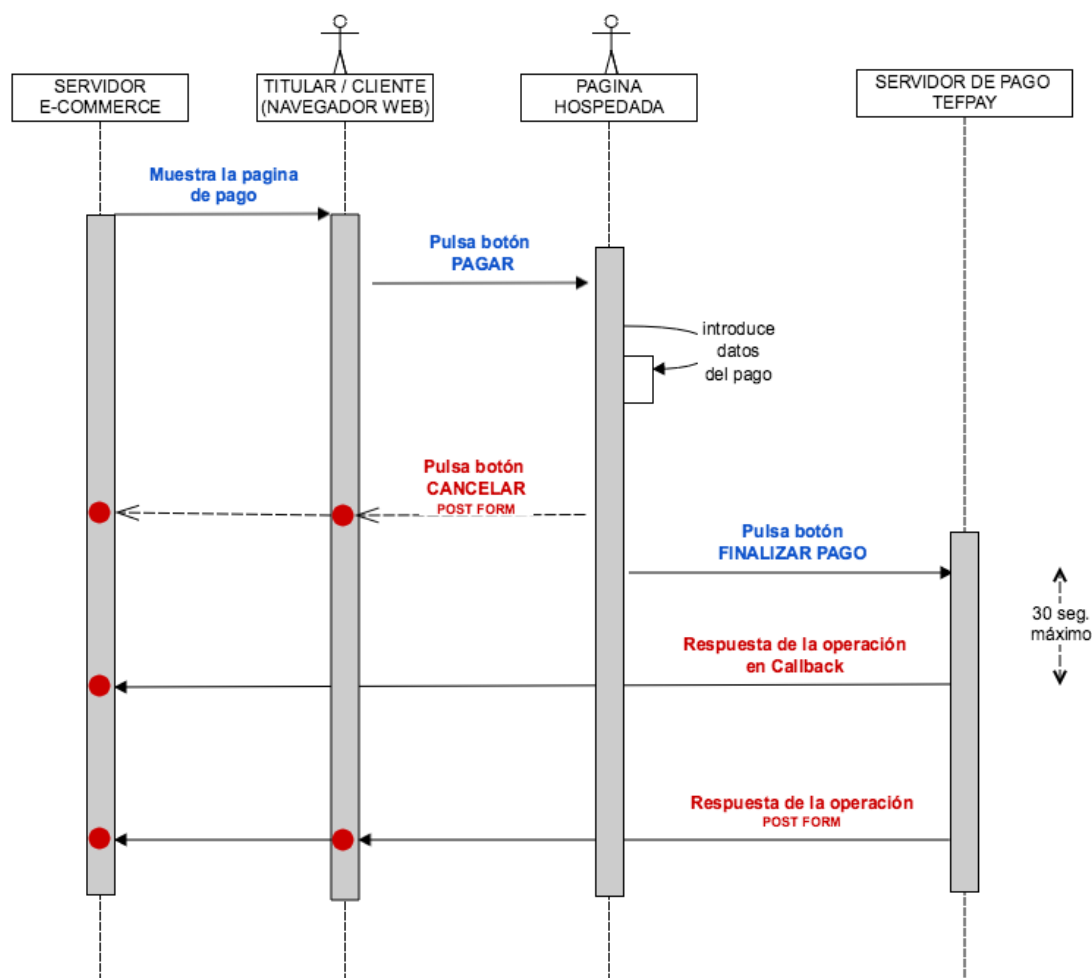
El Código seguridad (CVV) es el código de 3 dígitos en el reverso de su tarjeta de crédito. Lo puede encontrar en el espacio en blanco designado para su firma.



Una vez el cliente introduce los datos y pulse en el botón "**Finalizar Pago**", tefpay ejecutará la operación en el banco y devolverá al titular a su e-commerce con los resultados de la operación.

Tefpay también enviará a su servidor de e-commerce una petición con el resultado de la transacción. Esta petición, llamada respuestas en **callback**, contendrá un identificador (**token**) para realizar operaciones iniciadas por el comercio: como la devolución, cobro recurrente, etc.

Resumen del flujo de la operación en transacciones iniciadas por el cliente:



## Transacciones iniciadas por el comercio.

En estas transacciones el comercio inicia la transacción sin necesidad de la interacción de su cliente ya que no está presente.

Para ejecutarlas se utilizan tokens creados previamente en una transacción iniciada por el cliente.

El token es una referencia securizada a la base de datos de tarjetas y permite siempre una referencia de cuando se creó y a que transacción original queda vinculado. Incluye el token los datos de fecha, matchdata del pedido, 4 últimos dígitos de la tarjeta para un comercio o agrupación de referencia.

El comercio usando los siguientes datos podrá efectuar operaciones sobre una transacción aceptada inicialmente por el cliente:

Dato	Significado
Número de pedido Ds_Merchant_MatchingData	Es el identificador de la compra original que el cliente aceptó.

Dato	Significado
Fecha de la operación Ds_Date	Es la fecha cuando el cliente realizó el pago.
Cuatro últimos dígitos de la tarjeta Ds_PanMask	Son los cuatro últimos dígitos que el cliente usó para realizar el pago

En el siguiente cuadro se detallan las transacciones que el comercio puede realizar a partir del *token* obtenido de una transacción iniciada por el cliente.

Tipo de transacción iniciada por el cliente	Tipo de transacción disponibles para el comercio
201. Pago estándar.	<ul style="list-style-type: none"> <li>• 4 – Devolución Parcial o Total</li> <li>• 204 – Devolución online Parcial o Total</li> <li>• T33 - Validacion de tarjeta</li> <li>• 208 – Cobro recurrente</li> <li>• 216 – Preautorización diferida</li> </ul>
203. Autenticación	<ul style="list-style-type: none"> <li>• 209 – Confirmación de autenticación</li> <li>• T33 - validacion de tarjeta</li> <li>• 208 – Cobro recurrente</li> <li>• 216 – Preautorización diferida</li> </ul>
22. Cobro sin 3DSecure/SecureCode	<ul style="list-style-type: none"> <li>• 4 – Devolución Parcial o Total</li> <li>• 204 – Devolución online Parcial o Total</li> </ul>
27. Cobro sin 3DSecure/SecureCode (Online)	<ul style="list-style-type: none"> <li>• 4 – Devolución Parcial o Total</li> <li>• 204 – Devolución online Parcial o Total</li> <li>• T33 - Validacion de tarjeta</li> <li>• 208 – Cobro recurrente</li> <li>• 216 – Preautorización diferida</li> </ul>
202. Preautorización	<ul style="list-style-type: none"> <li>• 207 – Confirmación de Preautorización</li> <li>• 218 – Anulación de preautorización</li> <li>• 216 – Preautorización diferida</li> <li>• T33 - validacion de tarjeta</li> <li>• 208 – Cobro recurrente</li> </ul>
21. Almacenar tarjeta	<ul style="list-style-type: none"> <li>• 208 – Cobro recurrente</li> </ul>
41. Pagos mediante transferencia bancaria	<i>No hay disponibles</i>
11. Pagos mediante llamada telefónica	<ul style="list-style-type: none"> <li>• 4 – Devolución Parcial o Total</li> </ul>

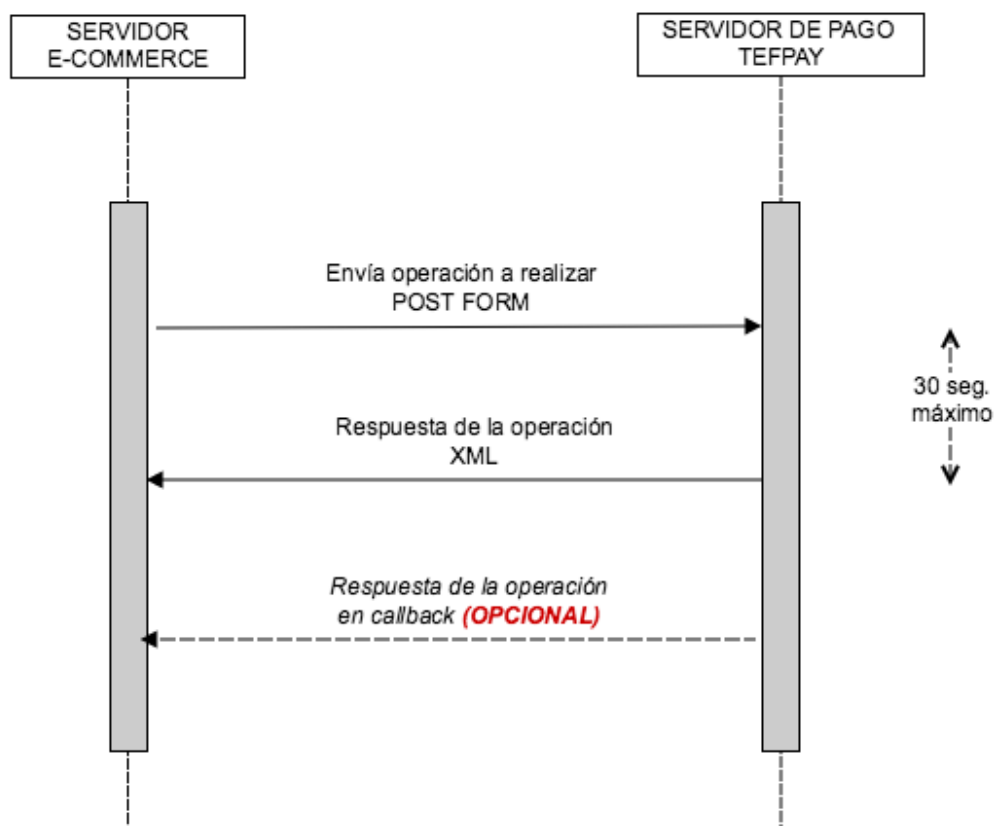


Tipo de transacción iniciada por el cliente	Tipo de transacción disponibles para el comercio
	<ul style="list-style-type: none"> <li>• 33 – Validacion de tarjeta</li> <li>• 208 – Cobro recurrente</li> <li>• 208 – Cobro recurrente</li> </ul>
6. Suscripciones	<ul style="list-style-type: none"> <li>• 4 – Devolución Parcial o Total</li> <li>• 204 – devolución online Parcial o Total</li> <li>• 33 – Validacion de tarjeta</li> <li>• 208 – Cobro recurrente</li> </ul>

Estas transacciones son enviadas por el servidor de su e-commerce y en la misma conexión recibirá los datos del resultado de la transacción. Opcionalmente, en este tipo de transacciones se puede recibir la respuesta en la url de **callback**.

Tefpay estima un tiempo máximo de espera no superior a 30 segundos para realizar la transacción con la entidad bancaria. Transcurrido este tiempo más un margen razonable la transacción se cancelará automáticamente.

Flujo de la operación en transacciones iniciadas por el comercio:



## Respuestas en callback

En los apartados anteriores se ha explicado el funcionamiento de como Tefpay notifica las respuestas de las transacciones de pago. En este apartado nos centraremos en como su e-commerce debe gestionar las respuestas en **callback** que envía Tefpay.

Para implementar la respuesta en callback el e-commerce debe indicar en las peticiones una URL donde recibir dichas respuestas (campo Ds\_Merchant\_Url). Esta URL será un CGI, Servlet o similar, desarrollado en el lenguaje que se considere adecuado para que el servidor del e-comercio sea capaz de interpretar la respuesta que le envíe los servidores de pago de tefpay. Será una página transparente al usuario (es decir, no se cargará en el navegador). En ella podrá recibir y recoger los datos de la respuesta de la operación y de esta forma introducirlos en su base de datos.

En las transacciones iniciadas por el comercio esta URL de callback es opcional y en la mayoría de casos innecesaria ya que la respuesta se recibe en la misma conexión y entre servidores de pasarela y el comercio. En las transacciones de cliente presente aunque la variable es opcional es necesaria por motivos de seguridad.

El protocolo utilizado en las respuestas vía URL de callback se recomienda usar HTTPS aunque al no contener datos sensibles puede usarse HTTP, el formato de este mensaje es un formulario HTML, enviado con el método POST.

*La respuesta call back se envía desde el mismo servidor. Si no puede entregarse tras un time-out máximo de 5 segundos se corta la comunicación y se reintentará posteriormente su entrega en hasta 5 reintentos.*

## Especificaciones de mensajes y variables en las transacciones.

### Transacciones iniciadas por el cliente.

En este tipo de operaciones el comercio deberá enviar un POST FORM HTML.

A continuación se muestra un ejemplo sencillo de un formulario con el método POST y con el botón de "PAGAR" correspondiente que debe introducir en su página de e-commerce:

```
<form id="pay" action="https://intepayments.tefpay.com" method="post" >
  <input id="Ds_Merchant_UrlOK" name="Ds_Merchant_UrlOK" type="hidden"
value="" />
  <input id="Ds_Merchant_Url" name="Ds_Merchant_Url" type="hidden"
value="" />
  <input id="Ds_Merchant_UrlKO" name="Ds_Merchant_UrlKO" type="hidden"
value="" />
  <input id="Ds_Merchant_MerchantCode" name="Ds_Merchant_MerchantCode"
type="hidden" value="" />
  <input id="Ds_Merchant_MerchantSignature"
name="Ds_Merchant_MerchantSignature" type="hidden" value="" />
  <input id="Ds_Merchant_TransactionType"
name="Ds_Merchant_TransactionType" type="hidden" value="" />
  <input id="Ds_Merchant_Amount" name="Ds_Merchant_Amount" type="hidden"
value="" />
  <input id="Ds_Merchant_MatchingData" name="Ds_Merchant_MatchingData"
type="hidden" value="" />
  <input id="Ds_Merchant_Lang" name="Ds_Merchant_Lang" type="hidden"
value="" />
  <input id="Ds_Merchant_Description" name="Ds_Merchant_Description"
type="hidden" value="" />
  <button type="submit" form="pay" value="Submit">Pago</button>
</form>
```

Si su e-commerce utiliza las páginas hospedadas en tefpay por defecto debe considerar que estas usan la codificación UTF-8. Si su e-commerce usa la codificación ISO-8859-1 debe convertir los textos para que se muestren correctamente en las páginas hospedadas. En PHP puede usar la función: [utf8\\_encode](#). Ejemplo:

```
...
<input id="Ds_Merchant_Description" name="Ds_Merchant_Description" type="hidden"
value="<?php echo utf8_encode('mostrar correctamente textos: ó ñ á í')" />
...
```

Las variables que debe enviar se detallan a continuación:

Dato	Variable	Característica	Descripción
Nombre y apellidos del titular	Ds_Merchant_UserName	Opcional	Titular de la tarjeta. Ej: 'Alfonso Gonzalo'

Dato	Variable	Característica	Descripción
			Longitud máxima 45 caracteres.
URL de OK	Ds_Merchant_UrLOK	Sólo en cliente presente	URL dónde el usuario será redirigido en caso de transacciones correctas. Ej: <a href="https://www.ecom.com/payok.php">https://www.ecom.com/payok.php</a> (No usar IP, usar dominios, puerto 443/80, en integración se permiten IP's)
URL de KO	Ds_Merchant_UrLKO	Sólo en cliente presente	URL donde el usuario será redirigido en caso de transacciones incorrectas no aceptadas o con error. Ej: <a href="https://www.ecom.com/payko.php">https://www.ecom.com/payko.php</a> (No usar IP, usar dominios, puerto 443/80, en integración se permiten IP's)
URL	Ds_Merchant_Url	Recomendada	URL del comercio. Dirección en la que se recibirá la respuesta de la transacción enviada por tefpay al comercio Ej: <a href="https://www.ecom.com/resp.php">https://www.ecom.com/resp.php</a> (No usar IP, usar dominios, puerto 443/80, en integración se permiten IP's)
Tipo de transacción	Ds_Merchant_TransactionType	Obligatoria	<ul style="list-style-type: none"> <li>• 201 – Pago estándar</li> <li>• 202 – Preautorización</li> <li>• 203 – Autenticación</li> <li>• 6 – Suscripciones</li> <li>• 11 – Pagos mediante llamada telefónica.</li> <li>• 19 – Validación de tarjeta de crédito/débito</li> <li>• 21 – Almacenar tarjeta</li> </ul>

Dato	Variable	Característica	Descripción
			<ul style="list-style-type: none"> <li>• 22 – Cobro sin 3DSecure/ SecureCode</li> <li>• 41 – Pagos mediante transferencia bancaria.</li> </ul>
Nombre del comercio	Ds_Merchant_Name	Opcional	<p>Este campo se mostrará al titular en el proceso de autenticación: 3DSecure/SecureCode.</p> <p>Ej: "Ecommerce"</p> <p>Longitud máxima 25 caracteres.</p>
Template de página hospedada a mostrar	Ds_Merchant_Template Number	Opcional	<ul style="list-style-type: none"> <li>• 00 – Pago con tarjeta de crédito/débito (por defecto)</li> <li>• 01 – Pago mediante transferencia bancaria</li> <li>• 02 – Pago con tarjeta de crédito/débito con aceptación de condiciones.</li> <li>• 03 – Pago con tarjeta de crédito/débito con importe introducido en tefpay.</li> <li>• 04 – Pago con tarjeta de crédito/débito con carro de compra completo</li> <li>• 05 – Renovar tarjeta de crédito/débito</li> </ul>
Logo del comercio a mostrar en template de página hospedada	Ds_Merchant_Logo	Opcional	<p>URL con el Logo del comercio.</p> <p>Se aconseja usar HTTPS para evitar problemas con certificado SSL en su pagina hospedada.</p>
Identificación de comercio código FUC	Ds_Merchant_Merchant Code	Obligatoria	<p>Número de comercio facilitado por la entidad bancaria al comercio.</p> <p>Para integración solicitar a Tefpay.</p>
Descripción del Producto	Ds_Merchant_Descriptio n	Recomendada	<p>Este campo se mostrará al titular en la página hospedada.</p>

Dato	Variable	Característica	Descripción
Código de pedido	Ds_Merchant_MatchingData	Obligatoria	Numero de pedido único compuesto de 21 caracteres numéricos.
Referencia de pedido	Ds_Merchant_OrderReference	Opcional	8 caracteres alfanuméricos. Tiene como objetivo cuadrar operaciones con la entidad bancaria. Ejemplo: A1234567
Idioma	Ds_Merchant_Lang	Opcional	Idioma a mostrar en la pagina hospedada. <ul style="list-style-type: none"> <li>• en – inglés</li> <li>• es – español (por defecto)</li> <li>• fr – francés</li> <li>• ru – ruso</li> <li>• ca – catalán</li> <li>• cs - checo</li> <li>• it - italiano</li> <li>• de - aleman</li> <li>• pt - portuguez</li> <li>• pl - polaco</li> <li>• da - danés</li> </ul> seguimos la ISO_639-1
Identificador de cliente	Ds_Merchant_CustomerNumber	Opcional	Número de cliente compuesto de 6 caracteres numéricos.
Moneda	Ds_Merchant_Currency	Opcional, enviar únicamente si su comercio usará distintas monedas.	Moneda con la que se realiza el pago. <ul style="list-style-type: none"> <li>• 978 – Euro (EUR)</li> <li>• 840 – Dólar (USD)</li> <li>• 826 – Libra Esterlina (GBP)</li> <li>• 124 – Dólar canadiense (CAD)</li> <li>• 392 – Yen</li> <li>• 032 – Austral Argentino</li> <li>• 052 – Peso Chileno</li> <li>• 170 – Peso Colombiano</li> <li>• 356 – Rupia India</li> <li>• 484 – Nuevo Peso Mejicano</li> <li>• 604 – Nuevos Soles</li> <li>• 756 – Franco Suizo</li> <li>• 986 – Real Brasilenõ</li> </ul>

Dato	Variable	Característica	Descripción
			<ul style="list-style-type: none"> <li>937 – Bolívar Venezolano</li> <li>949 – Lira Turca</li> </ul>
Referencia de cliente	Ds_Merchant_ClientRef	Opcional	La referencia del comercio para identificación interna del cliente.  Compuesta de 12 caracteres alfanuméricos.
Referencia de su aplicación	Ds_Merchant_Application	Opcional	Número de la aplicación compuesto de 6 caracteres numéricos.
Importe	Ds_Merchant_Amount	Obligatoria	Importe de la transacción a realizar. Las dos últimas posiciones se consideran decimales.  Ej: 1000 = 10.00
Datos opcionales	Ds_Merchant_Op1...Op10	Opcional	Variable alfanumerica opcional para el comercio. De Op1 a OP10.
Firma	Ds_Merchant_MerchantSignature	Obligatoria	Algoritmo de verificación SHA-1.
Terminal bancario	Ds_Merchant_Terminal	Opcional	Número de terminal asignado por su entidad bancaria.  Compuesto de 8 caracteres numéricos.
Terminal de autenticación	Ds_Merchant_TerminalAuth	Opcional	Número de terminal asignado por su entidad bancaria para la autenticación  Compuesto de 8 caracteres numéricos.
COF	Ds_Merchant_Subscription_Enable	Obligatoria Opcional	Campo de datos adicionales para la autenticación EMV3DS  Obligatoria si se quieren realizar operaciones recurrentes después  Opcional si solo se hará una operación

Dato	Variable	Característica	Descripción
RTS	Ds_Merchant_Preauth_RTS	Opcional	Referencia de Transacción de Sistema  ES necesaria en la transaccion T207 o T218, hace referencia a la operacion que quieres anular o confirmar

## Respuesta de una transacción iniciada por el cliente

El comercio recibirá un POST FORM HTML en la dirección indicada en el Ds\_Merchant\_UrlOK o Ds\_Merchant\_UrlKO dependiendo de la respuesta de la transacción.

En Ds\_Merchant\_Url también se enviará un POST FORM HTML con los mismos valores de respuesta que a las url's anteriores. Recomendamos usar esta url para guardar la respuesta en base de datos.

Variable	Valor de ejemplo	Descripción
Ds_Amount	'1000'	Importe de la transacción que se ha realizado. <i>Los dos últimos dígitos se consideraran decimales.</i>
Ds_Merchant_MatchingData	'091222152933123456789'	Número de pedido de la transacción que se ha realizado. <i>Los 2 ultimos dígitos pueden haberse modificado respecto a los enviados.</i> <i>Corresponden a la referencia realmente procesada.</i>
Ds_AuthorisationCode	020441	Número de autorización bancaria alfanumérico.
Ds_Bank	2100	Código Banco por el cual se ha procesado la transacción.
Ds_Merchant_TransactionType	201	Mismo valor que la transacción solicitada.
Ds_Message	Aceptada	Mensaje de respuesta.
Ds_Code	'0190'	Código de la respuesta de la entidad



<b>Ds_PanMask</b>	XXXX	Últimos cuatro dígitos de la tarjeta.
<b>Ds_Expiry</b>	2012	Caducidad de la tarjeta. Formato: YYMM
<b>Ds_Date</b>	091222152950	Fecha de la transacción. Formato: YYMMDDHHMMSS
<b>Ds_Merchant_MerchantCode</b>	Mismo que la transacción solicitada	Número de comercio.
<b>Ds_Merchant_Guarantees</b>	100	Resultado 3DSecure/SecureCode de la transacción. <ul style="list-style-type: none"><li>• 100: Cliente autenticado. Comercio seguro.</li><li>• 50: Cliente no autenticado. Comercio seguro.</li><li>• 0: Cliente no autenticado.</li></ul>
<b>Ds_Signature</b>	'e463ertg572f18873df54353b094fe2aswq147a7'	Firma de la respuesta.

Los siguientes campos (a la que llamamos token) son los necesarios para enviar posteriormente transacciones iniciadas por el comercio:

- Ds\_Merchant\_MatchingData
- Ds\_Date
- Ds\_PanMask

**i** Si el usuario pulsa en el botón cancelar de la página hospedada será redireccionado a la URL de KO (Ds\_Merchant\_UrlKO) con Ds\_Code = 208 y **con las variables que el comercio envió a la pasarela de pagos tefpay.**

Exemplo:

Ds\_Code = 208

Ds\_Message = Cancelado por el usuario

Ds\_Merchant\_MerchantCode = V99008980

Ds\_Merchant\_MatchingData = 160519152416123456789

Ds\_Merchant\_TransactionType = 1

Ds\_Merchant\_Amount = 100

Ds\_Merchant\_Url = <https://intepayments.tefpay.com/simu/simut1x.phtml>

Ds\_Merchant\_MerchantSignature = f194a86020dacda6d2f26a8611dd23119cc30ad9

## Transacciones iniciadas por el comercio

Estas peticiones se realizan con una referencia (token), de modo que pueden vincularse a una operación previa de cliente presente la cual tiene que estar aprobada por la entidad bancaria.

Es importante que los *headers* de la petición HTTP sean correctos ya que sino se mostrará una página de "Not found". A continuación se muestran los *headers* para realizar la petición:

❗ POST / HTTP/1.1  
Host: intesecure02.tefpay.com  
Connection: keep-alive  
Content-Length: 1083  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/535.1 (KHTML, like Gecko) Chrome/13.0.782.220 Safari/535.1  
Content-Type: application/x-www-form-urlencoded  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8  
Accept-Encoding: gzip,deflate  
Accept-Language: es-ES,es;q=0.8 Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.3

Las variables que debe enviar se detallan a continuación:

Variable	Valor de ejemplo	Descripción
Ds_Merchant_TransactionType	208	<ul style="list-style-type: none"> <li>4 – Devolución</li> <li>204 – Devolución online</li> <li>207 – Confirmación de Preautorización</li> <li>209 – Confirmación de autenticación</li> <li>208 – Cobro recurrente</li> <li>218 – Anulación de preautorización</li> <li>216 – Preautorización diferida</li> <li>33 – Validacion AVS</li> </ul>
Ds_Merchant_MatchingData	'091222152933123456789'	Número de pedido de la transacción original.
Ds_Merchant_MerchantCode	'V99008980'	Número de comercio
Ds_Merchant_Amount	'1000'	Importe de la transacción a realizar. Las dos últimas posiciones se consideran decimales.
Ds_Date	'091222152950'	Fecha recibida en la respuesta aceptada de la transacción original. Formato: YYMMDDHHMMSS
Ds_Merchant_PanMask	'4242'	Valor recibido de la respuesta aceptada de la transacción original.
Ds_Merchant_MerchantSignature	'fgh3...4d56'	Algoritmo verificación SHA-1.

Variable	Valor de ejemplo	Descripción
Ds_Merchant_Recurrency	'1'	<p>Permite pagos fraccionados en una transacción tipo 9 securizada</p> <ul style="list-style-type: none"> <li>• 1 – Indica que se efectuarán cargos posteriores (pago fraccionado).</li> <li>• 0 – Indica que es el último cargo.</li> </ul> <p>Viene de una autenticación (tipo 3) previa sin usar Ds_Merchant_SecureInitialAmount.</p>
Ds_Merchant_Url (opcional)	<a href="https://www.web.com/trans.php">https://www.web.com/trans.php</a>	Url para recibir la respuesta en background.

Recuerde que esta petición se realiza en tiempo real en su entidad bancaria y este puede demorarse en la respuesta como máximo 30 segundos. Por lo tanto, mantenga la conexión abierta durante unos 40 segundos. La demora habitual es de 1 o 2 segundos.

Si utiliza PHP puede usar la siguiente función para enviar los datos a tefpay:

```

/* -----
Envío de datos en POST, $postData, a una URL, $url.
----- */
function send_trans($url, $postData) {

    $headers = array( 'Connection: Keep-Alive',
                     'Content-Type: application/x-www-form-urlencoded' );
    $ch = curl_init( $url );
    curl_setopt( $ch, CURLOPT_USERAGENT, 'Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.13) Gecko/20080311 Firefox/2.0.0.13' );
    curl_setopt( $ch, CURLOPT_URL, $url );
    curl_setopt( $ch, CURLOPT_RETURNTRANSFER, true );
    curl_setopt( $ch, CURLOPT_FOLLOWLOCATION, true );
    curl_setopt( $ch, CURLOPT_CONNECTTIMEOUT, 60 );
    curl_setopt( $ch, CURLOPT_TIMEOUT, 40 ); // timeout en 40 segundos
    curl_setopt( $ch, CURLOPT_POST, true );
    curl_setopt( $ch, CURLOPT_POSTFIELDS, $postData );
    curl_setopt( $ch, CURLOPT_HTTPHEADER, $headers );
    curl_setopt( $ch, CURLOPT_SSL_VERIFYHOST, 2 );
    curl_setopt( $ch, CURLOPT_SSL_VERIFYPEER, true );
    $xml = curl_exec( $ch );
    curl_close($ch);
    return ($xml);
}

/* -----
Valores de acceso a pagos con tefpay.
----- */
$url = "https://inteseccure02.tefpay.com/paywebv1.7.0/INPUT.php";
$key = "XXXXXXXXXXXX";
$merchantCode = "V99000XXXX";

```

```
/* -----
Configuramos variables para realizar el cobro
----- */
$postData2['Ds_Merchant_MerchantCode'] = $merchantCode;
$postData2['Ds_Merchant_MatchingData'] = $originalPayment['Ds_Merchant_MatchingData'];
$postData2['Ds_Merchant_PanMask'] = $originalPayment['Ds_PanMask'];
$postData2['Ds_Date'] = $originalPayment['Ds_Date'];
$postData2['Ds_Merchant_TransactionType'] = "8";
$postData2['Ds_Merchant_Amount'] = "188";
$postData2['Ds_Merchant_MerchantSignature'] = sha1($postData2['Ds_Merchant_Amount'].
$postData2['Ds_Merchant_MerchantCode'].$postData2['Ds_Merchant_MatchingData'].$key);

/* -----
Lanzamos el pago y obtenemos la respuesta
----- */
$paymentResponse = send_trans($url, $postData);
print_r($xml);
```

## Respuesta de una transacción iniciada por el comercio

El comercio en la misma petición recibirá los siguientes campos: (destacar que son los mismos campos que la variables recibidas en una petición iniciada por el cliente)

Variable	Valor de ejemplo	Descripción
Ds_Amount	'1000'	Importe de la transacción que se ha realizado. 2 últimos dígitos son decimales.
Ds_Merchant_MatchingData	'091222152933123456789'	Número de pedido de la transacción que se ha realizado.
Ds_AuthorisationCode	020441	Número de autorización.
Ds_Bank	2100	Código del Banco por el cual se ha realizado la transacción.
Ds_Merchant_TransactionType	208	Mismo valor que la transacción solicitada.
Ds_Message	Aceptada	Mensaje de respuesta.
Ds_Code	'0190'	Código de la respuesta.

Variable	Valor de ejemplo	Descripción
Ds_PanMask	'424242'	Últimos cuatro dígitos de la tarjeta.
Ds_Expiry	2012	Caducidad de la tarjeta. Formato: YYYY
Ds_Date	091222152950	Fecha de la transacción. Formato: YYMMDDHHMMSS
Ds_Merchant_MerchantCode	'V99008980'	Número de comercio.
Ds_Merchant_Guarantees	100	Resultado de la transacción. Resultado de la transacción. <ul style="list-style-type: none"> <li>100: Cliente autenticado. Comercio seguro.</li> <li>000: Cliente no autenticado.</li> </ul>
Ds_Signature	'e463...47a7'	Firma de la respuesta.

El formato será un XML (*eXtensible Markup Language*). Ejemplo:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<Ds_Message>Aceptada</Ds_Message>
<Ds_Merchant_MatchingData>110705123619123456789</Ds_Merchant_MatchingData>
<Ds_Bank>2100</Ds_Bank>
<Ds_Date>110705124046</Ds_Date>
<Ds_AuthorisationCode>059334</Ds_AuthorisationCode>
<Ds_PanMask>0004</Ds_PanMask>
<Ds_Merchant_TransactionType>9</Ds_Merchant_TransactionType>
<Ds_Amount>1200</Ds_Amount>
<Ds_Code>100</Ds_Code>
<Ds_Merchant_Guarantees>100</Ds_Merchant_Guarantees>
<Ds_Merchant_MerchantCode>999008980</Ds_Merchant_MerchantCode>
<Ds_Signature>7cc5e91cf9bdd063c06f8676ca6aa68d575b357e</Ds_Signature>
</response>
```

Si usa PHP puede usar esta función:

```
/* -----
Esta función parsea un string xml, $xmldata, y retorna un array con
los valores devueltos por la pasarela de pagos.
----- */
function parse_xml($xmldata)
```

```
{
    if (empty($xmldata))
        return false;
    $reader = new XMLReader();
    if ($reader->xml($xmldata) == false){
        return false;
    }
    $data = array();
    $ack = false;
    while ($reader->read()) {
        if ($reader->nodeType == XMLREADER::ELEMENT) {
            $name = $reader->localName;
            if ($name == "response"){
                $ack = true;
                continue;
            }
            if ($reader->isEmptyElement) {
                $data[$name] = "";
                continue;
            }
            if ($reader->read() == false)
                continue;
            $value = $reader->value;
            if (empty($name) || is_null($value))
                continue;
            $data[$name] = $value;
        }
    }
    return ($ack?$data:$ack);
}
```

## Transacción recurrente iniciada por el comercio

En el caso de transacciones recurrentes se recomienda utilizar, aunque es opcional, la variable Ds\_TransactionID. Esta variable se recibe en la transacción presencial y debe enviarse en la solicitud de la recurrente.

Variable	longitud	ejemplo
Ds_Merchant_TransactionID	128	dn270cfj4ed89sarrk98eopt5

## Firma en los mensajes intercambiados. Ejemplo cálculo firma.

Se facilitará al comercio de una **clave**, que se utilizará para firmar los datos. De este modo se puede verificar la identificación del comercio y que los datos no han sido alterados en ningún momento. Se utilizará como protocolo

de securización el algoritmo público Hash SHA-1, que garantiza los requisitos mínimos de seguridad en cuanto a la autenticación del origen. La clave será enviada por tefpay al comercio en el proceso de alta en tefpay.

Para la creación en la petición HTTP se utilizarán los siguientes campos y el resultado debe ser asignado a la variable `Ds_Merchant_MerchantSignature`:

**i** `Ds_Merchant_Amount + Ds_Merchant_MerchantCode + Ds_Merchant_MatchingData + Ds_Merchant_Url + CLAVE`

La respuesta de la transacción aprobadas o denegadas por la entidad bancaria también irá signada y se usan los siguientes campos:

**i** `Ds_Amount + Ds_Merchant_MatchingData + Ds_AuthorisationCode + Ds_Merchant_TransactionType + Ds_Date + CLAVE.`

En el caso de que la operación sea cancelada en tefpay, la respuesta de la transacción irá signada los los siguientes campos:

**i** `Ds_Message + Ds_Code + Ds_Merchant_MatchingData + CLAVE.`

**!** La clave nunca debe ser transmitida, ni debe aparecer en el código fuente de la web del comercio. Por ello, el cálculo del algoritmo hash SHA-1 debe implementarse en la parte del servidor de Internet del comercio. Si el comercio reside en un servidor ajeno bajo una hosting, deberá ponerse en contacto con la empresa proveedora para que le informe del modo de implementar el algoritmo criptográfico.

Ejemplo en PHP de como generar la firma:

```
$cadena = $Ds_Merchant_Amount . $Ds_Merchant_MerchantCode . $Ds_Merchant_MatchingData  
.  
          $Ds_Merchant_Url . (CLAVE compartida proporcionada por tefPAY);  
$Ds_Merchant_MerchantSignature = sha1($cadena);
```

## Gestión de errores

Tefpay proporciona dos variables para determinar los errores producidos en la transacción: `Ds_Code` y `Ds_CodeBank`.

1) El **`Ds_Code`** es la variable principal para la gestión de errores (aunque es más genérico que el **`Ds_CodeBank`**). Su valor es un número catalogado en 4 ramas:

- 1XX = Aprobadas por el banco.
- 2XX = Denegadas / Canceladas por el banco.
- 3XX = Error en la petición de entrada.
- 5XX = Filtros que introduce tefpay.

2) El **`Ds_CodeBank`** es el error "exacto" que proporciona el banco en caso de que deniegue la operación.

Este campo estará presente sólo si `Ds_Code` = 2XX (Denegadas / Canceladas por el banco) y no están catalogados siguiendo un patrón.

## Lista de códigos Ds\_Code

Ds_Message	Ds_Code	Significado	Acción	Mensaje recomendado a mostrar.
Aceptada	100	La transacción se ha realizado correctamente.		Transacción aceptada.
Pendiente	101	La transacción no ha sido autorizada, pero el cliente ha sido autenticado correctamente.	Realizar un cobro periódico pasado unos minutos. En caso de error continuado contactar con tefpay.	Transacción pendiente de cobro.
Autorizada	102	Transacción de comercio electrónico autorizada por el banco sin autenticación.	Revisión manual de la venta.	Transacción autorizada aunque atención al cliente requiere revisión manual de la operación.
Aceptada para proceso diferido	103	Transacción para proceso diferido una vez validada	En cola para proceso diferido	En cola
Entidad bancaria inaccesible	200	La transacción no se ha completado ya que a fallado la conexión con el banco.	Reintentar la conexión pasados unos minutos.	Entidad bancaria inaccesible.
Operación denegada	201	La transacción no ha sido procesada.	Reintentar realizar la transacción.	Operación denegada.
Error en autenticación	202	Los valores especificados para la autenticación del titular de la tarjeta son incorrectos.	Reintentar realizar la transacción.	Error en autenticación.



Error del sistema	203	Error en algún modulo del sistema .	Reintentar realizar la transacción.	Operación cancelada por error del sistema.
Error de formato	204	Los datos introducidos para iniciar la transacción son incorrectos.	Reintentar realizar la transacción y contactar con tefpay.	Operación cancelada por error de formato.
Tarjeta caducada	205	La tarjeta introducida está caducada.	Reintentar realizar la transacción con la caducidad correcta.	Tarjeta caducada
Tarjeta no válida	206	La tarjeta no es válida	Reintentar realizar la transacción.	Tarjeta no válida
Error en proceso	207	Error desconocido no catalogado	Reintentar la transacción y reportar soporte tefpay si permanece	Transacción cancelada por error desconocido no catalogado
Cancelado por el usuario	208	El usuario ha cancelado la transacción.		Transacción cancelada. Error proceso.
Fraude	209	El banco ha retornado error 202	Reintentar realizar la transacción.	Operación denegada.
Error comunicaciones	210	Error comunicaciones	Reintentar posteriormente	Operación a verificar puede estar cargada al cliente
Error en proceso	211	El campo Ds_Date es incorrecto.	Verificar el campo Ds_Date	Transacción cancelada.
Error en proceso	212	Transacción ya existe no se puede crear token	Transacción ya existe en tefpay.	Transacción cancelada., error proceso.

Error en proceso	215	Targeta en lista negra	Desactivar el token ya que está en lista negra.	Transacción cancelada.
Sistema ocupado	216	Sistema ocupado en la entrada	Reintentar más tarde	Operación cancelada en la entrada. Intentelo más tarde.
Token inconsistente transactionID	217	transactionid con error en el campo Ds_Date, Ds_MatchingData	No coinciden datos de token	Error en datos token no coinciden
Operación no disponible cancelada	218	Sistema ocupado	Reintentar más tarde	Operación cancelada. No se puede enviar al procesador de pagos.
Error conexión Procesador	219	Error conexión	No se puede conectar. Reintentar más tarde	Error de conexión con Procesador de pago. No se ha enviado transacción.
Transacción Pendiente	220	Transacción en proceso	Esperar resultado por callback	La transacción esta en proceso. La respuesta se recibirá por call back.
Sistema en mantenimiento .	221	Se están realizando tareas de mantenimiento.	Reintentar más tarde.	Sistema en mantenimiento. Inténtelo más tarde.
Hash incorrecto	300	Error en el cálculo del hash.	Contactar con soporte tefpay.	Transacción cancelada
Transacción no encontrada	302	La transacción previa sobre la cual se pretende realizar una operación no existe.	Contactar con soporte tefpay.	Transacción cancelada
Número de pedido	303	Este número de pedido ya ha sido utilizado en el proceso 3DSecure.	Contactar con soporte tefpay.	Transacción cancelada

no encontrado				
Importe excedido	304	Importe excedido		Transacción cancelada
Pan incorrecta	305	La tarjeta tiene un error de formato.	Contactar con soporte tefpay.	Transacción cancelada
Tipo de transacción incorrecta.	306	El tipo de transacción no existe, es incorrecto o su comercio no tiene activada este tipo de transacción	Contactar con soporte tefpay.	Transacción cancelada
Importe incorrecto	307	El formato del importe introducido es incorrecto.	Contactar con soporte tefpay.	Transacción cancelada
Csv incorrecto	308	El CVV entrado es incorrecto.	Contactar con soporte tefpay.	Transacción cancelada
Caducidad recibida incorrecta	309	Datos token caducado	Contactar con soporte tefpay.	Transacción cancelada
Fecha incorrecta.	310	El formato de la fecha es incorrecto.	Contactar con soporte tefpay.	Transacción cancelada
Número de pedido incorrecto	311	El formato del número de pedido es incorrecto.	Contactar con soporte tefpay.	Transacción cancelada
Comercio incorrecto	312	El formato del comercio es incorrecto.	Contactar con soporte tefpay.	Transacción cancelada
Url's incorrectas	313	La url/urls enviadas tienen un formato erróneo.	Contactar con soporte tefpay.	Transacción cancelada
Devoluciones excedidas	314	Devoluciones excedidas		Transacción cancelada
Datos opcionales incorrectos	315	Datos opcionales incorrectos.	Contactar con soporte tefpay.	Transacción cancelada

Transacción de referencia incorrecta	316	La transacción de referencia no se encuentra o es incorrecta.	Contactar con soporte tefpay.	Transacción cancelada
Terminal incorrecto	317	Numero de terminal bancario incorrecto	Revise longitud y formato del campo Ds_Merchant_Terminal.	Transacción cancelada
Datos opcionales incorrectos	318	Se excede del tamaño de datos opcionales.	Limite longitud de los campos opcionales.	Transacción cancelada
Error del Batch :Datos enviados incorrectos	319	Las variables recibidas no son correctas	Revisar variables y datos	Transacción rechazada para batch diferido
Faltan datos para realizar la transacción	320	Faltan datos para realizar la transacción	Revisar variables requeridas del pago.	Transacción cancelada
Error en IDtransaction	321	Error en ID transacción	Revisar gestión datos, no se ha podido leer	Identificador de transacción incorrecto
Pais denegado	500	Pais denegado		Transacción cancelada
Transacción cancelada	501	La transacción no cumple con los criterios (filtros) definidos por el comercio.		Transacción cancelada
Transacción cancelada	502	Tarjeta pais origen denegada		Transacción cancelada
Consulta de totales correcta	600	La transacción se ha realizado correctamente.		N/A
Consulta de totales incorrecta	604	No es posible encontrar los totales que se solicitan.		N/A

## Lista de códigos Ds\_CodeBank

	Ds_CodeBank	Significado
1	101	Tarjeta caducada
2	102	Tarjeta en Lista Negra o sospechosa de fraude, incluir en fichero de Lista Negra
3	106	Excedido el número de intentos del PIN
4	107	Llamar al Emisor
5	172	Denegada, no repetir
6	173	Denegada, no repetir sin actualizar antes
7	174	Denegada, no repetir antes de 72 horas
8	180	Tarjeta no soportada por el sistema
9	190	Denegada por diversos motivos
10	192	Denegada. No es posible verificar autenticación por Referencia
11	193	Denegada. Excedido importe de la autenticación
12	201	Tarjeta caducada
13	202	Tarjeta en Lista Negra o sospechosa de fraude
14	290	Denegada diversos motivos
15	400	Aceptación de la anulación.
16	480	No encontró la operación que se quiere anular por no estar procesada o autorizada.
17	481	No encontró la operación que se quiere anular por no estar procesada o autorizada.

	<b>Ds_CodeBank</b>	<b>Significado</b>
18	600	Aceptación consulta de totales
19	604	No es posible encontrar los totales que se solicitan
20	904	Mensaje erróneo
21	909	Error de sistema.
22	912	Centro Resolutor no disponible
23	913	Recibido mensaje duplicado
24	914	No se acepta la anulación.
25	916	MAC erróneo
26	948	Fecha y Hora no sincronizada
27	949	Fecha de Caducidad de la tarjeta no coincide con la que el Emisor tiene en sus archivos
28	950	Violación de las normas existentes para realizar una autorización local
29	965	Violación de norma existentes para realizar una devolución

## Entorno de integración de tefpay.

El comercio dispone de un entorno de pruebas para verificar el correcto funcionamiento antes de la puesta en marcha en producción.

### Datos necesarios

Para activar el entorno de integración tefpay requiere la siguiente información:

- Definir transacciones necesarias.
- URL del logo a mostrar en paginas hospedadas
- Nombre contacto técnico
- Email contacto técnico
- Teléfono contacto técnico
- Importe inferior aceptado
- Importe máximo aceptado
- Comercio seguro autenticado : indicar si, no, mixto
- Moneda de cobro
- Tarjetas aceptadas o denegadas por país.
- Ventas aceptadas o denegadas por país.
- No permitir uso de tarjetas fuera de su país
- Limites de número de operaciones por tarjeta, por IP
- Limites de compra en importe por tarjeta, por IP
- En caso necesario otras reglas personalizadas (Consultar)

Cuando tefpay disponga de la información solicitada, procederá a la alta de una cuenta de pruebas y facilitará al e-commerce los siguientes datos:

Dato	Significado
Ds_Merchant_MerchantCode	Número de comercio
Clave	Clave necesaria para firmar los mensajes
URL hosted	Dirección de la página hospedada (transacciones iniciadas por el cliente)
URL Servidor de pagos	Dirección del servidor de pagos (transacciones iniciadas por el comercio)
URL Backoffice	Dirección del backoffice de pruebas

### Tarjetas de pruebas

Las tarjetas disponibles para simular transacciones correctas o incorrectas se detallan a continuación:

Num. tarjeta	Caducidad	CVV2	Resultado	Característica tarjeta
4548812049400004	2020/12	123	Operaciones aprobadas	VISA SPAIN CREDIT
4475555555555557	Cualquiera	Cualquiera	Operaciones aprobadas	VISA SPAIN CREDIT
4379000000000005	Cualquiera	Cualquiera	Operaciones aprobadas	VISA SPAIN CREDIT
4273399999999996	Cualquiera	Cualquiera	Operaciones aprobadas	VISA SPAIN CREDIT
4918011111111118	Cualquiera	Cualquiera	Operaciones aprobadas	VISA SPAIN DEBIT
6712111111111119	Cualquiera	Cualquiera	Operaciones aprobadas	MAESTRO SPAIN DEBIT
5020303030303039	Cualquiera	Cualquiera	Operaciones aprobadas	MAESTRO SPAIN DEBIT
5331833333333337	Cualquiera	Cualquiera	Operaciones aprobadas	MASTERCARD SPAIN CREDIT
5341244444444450	Cualquiera	Cualquiera	Operaciones aprobadas	MASTERCARD SPAIN CREDIT
4444444444444448	Cualquiera	Cualquiera	Operaciones aprobadas / cancelada	VISA POLAND
4444424444444440	Cualquiera	Cualquiera	Operaciones aprobadas / cancelada	VISA USA DEBIT PREPAID
4242424242424242	Cualquiera	Cualquiera	Operaciones aprobadas / cancelada	VISA USA CREDIT
375604007001007	Cualquiera	Cualquiera	Operaciones aprobadas / cancelada	AMERICAN EXPRESS SPAIN CREDIT
5555555555555557	Cualquiera	Cualquiera	Operaciones aprobadas / cancelada	MASTERCARD USA CREDIT
4940000001018436	2020/12	Cualquiera	Operaciones denegadas	VISA SPAIN CREDIT



Num. tarjeta	Caducidad	CVV2	Resultado	Característica tarjeta
4940000001018436	2020/10	Cualquiera	Operaciones denegadas	VISA SPAIN CREDIT
4940000001018436	2020/11	Cualquiera	Operaciones denegadas	VISA SPAIN CREDIT
2323232323232	Cualquiera	Cualquiera	Operaciones canceladas	

## Pruebas a realizar

A continuación se detallan las pruebas sugeridas que se realicen en integración antes del paso previo a un entorno de producción.

Num. tarjeta	Caducidad	CVV2	Propósito de la prueba	Ds_Code	Significado error	Ds_CodeBank
447555555555557	Cualquiera	Cualquiera	Tratar con operaciones aceptada	100		No existe
4242424242424242	Cualquiera	Cualquiera	Tratar con operaciones aceptada (si tiene configurado aceptar tarjetas de USA)	100		No existe
4940000001018436	2022/12	Cualquiera	Tratar con operaciones denegada	201	Operación denegada	0190
4940000001018436	2022/10	Cualquiera	Tratar con operaciones con transacciones abortada	210	El sistema está ocupado	No existe. La transacción enviada pero sin respuesta del banco.
4940000001018436	2022/11	Cualquiera	Tratar con una tarjeta fraudulenta	209	Tarjeta con posible fraude	0202
4940000001018436	Cualquiera	Cualquiera	Tratar con tarjetas no validas	206	Tarjeta no válida	0180
4242424242424242	Cualquiera	Cualquiera	Prueba de errores 3XX. (Importe = 55,000 €)	307	Importe incorrecto	No existe

Num. tarjeta	Caducidad	CVV2	Proposito de la prueba	Ds_Code	Significado error	Ds_CodeBank
232323232323232	Cualquiera	Cualquiera	Manejar operaciones 5XX	502	La tarjeta país origen denegada	No existe
4940000001018436	2022/10	Cualquiera	Probar timeouts a 10 segs con respuesta de 30segs	210	El sistema está ocupado	No existe
4507670001000009	Cualquiera	Cualquiera	Tratar con operaciones con transacciones abortada	210	Transaccion abortada	No existe. La transacción enviada pero sin respuesta del banco.
454881290888885	Cualquiera	Cualquiera	Tratar con operaciones denegadas por datos erroneos.	20X	Error de formato	904
4599830100494019	Cualquiera	Cualquiera	Tratar con una tarjeta fraudulenta	209	Tarjeta con possible fraude	0202

## Ejemplos en integración.

Descripción	URL
Método usando página hospedada (Con varias plantillas predefinidas)	<a href="https://intepayments.tefpay.com/simu/">https://intepayments.tefpay.com/simu/</a>
Método usando formulario de pago con Javascript	<a href="https://intesecure02.tefpay.com/simupayweb/hostedrsa/index.phtml">https://intesecure02.tefpay.com/simupayweb/hostedrsa/index.phtml</a>
Método usando formulario de pago integrado con iFrame	<a href="https://intesecure02.tefpay.com/iframe/index.phtml">https://intesecure02.tefpay.com/iframe/index.phtml</a>

## Datos adicionales.

En este apartado se definen las variables adicionales que tefpay devuelve en las respuestas a las peticiones de cobro. Estas variables no se envía por defecto, por lo tanto, si desea recibirlas contacte con tefpay.

## Datos de tarjeta crédito/débito.

En este apartado se definen las variables adicionales que tefpay devuelve referentes a la tarjeta de crédito/débito cuando una operación es iniciada por el cliente y está aprobada por la entidad bancaria.

Estas variables no se envía por defecto, por lo tanto, si desea recibirlas contacte con tefpay.

Variable	Valor ejemplo
Ds_CostumerCreditCardCountry	SPAIN
Ds_CostumerCreditCardCountryCode	ESP
Ds_CostumerCreditCardCountryNumber	724
Ds_CostumerCreditCardOrganization	SERVIED SOCIEDAD ESPANOLA DE MEDIOS DE PAGO, S.A.
Ds_CostumerCreditCardBrand	VISA
Ds_CostumerCreditCardType	CREDIT
Ds_CostumerCreditCardCategory	CLASSIC

## Identificador de tarjeta.

En este apartado se definen una variable que se usa como identificador de tarjeta de crédito/débito del cliente.

Esta variable no se envía por defecto, por lo tanto, si desea recibirla contacte con tefpay.

Variable	Valor de ejemplo
Ds_CostumerCreditCardId	f50523515d23d0ad4377bd0.....

## Número de identificación bancaria (BIN)

En este apartado se definen la variable que representa los 6 primeros dígitos de la tarjeta de crédito/débito del cliente.

Esta variable no se envía por defecto, por lo tanto, si desea recibirla contacte con tefpay.

Variable	Valor ejemplo
Ds_CostumerCreditCardBin	454881 (Seis primeros dígitos de la tarjeta de crédito)

## Nombre del titular.

En este apartado se definen la variable que contiene el nombre que el cliente ha introducido en la página hospedada, por lo tanto, esta variable estará presente en las transacciones iniciadas por el cliente.

Esta variable no se envía por defecto, por lo tanto, si desea recibirla contacte con tefpay.

Variable	Valor ejemplo
Ds_Merchant_UserName	Juan Pérez Rubio