

Medellín, Octubre 2023

Versión 1.4

**USO CONFIDENCIAL**

**GUÍA DE CERTIFICACIÓN API**

**Cs-**

Instructivo de uso

Declaración del Documento

Este documento fue preparado por, para y se mantendrá bajo la propiedad de *Evertec®*  
para su uso confidencial.

El cliente acuerda por su aceptación o uso de estos documentos, devolverlos a solicitud de *Evertec®* y no reproducirlos, copiarlos, prestarlos o de otra forma revelarlos o disponer de sus contenidos, directa o indirectamente y no usarlos para ningún otro propósito que no sea aquel para el cual fueron específicamente preparados.

**TABLA DE CONTENIDO**

1. ACTIVIDAD COMERCIO 4

2. PROCESO DE PAGO 4

3. IMAGEN CORPORATIVA 5

4. PREGUNTAS FRECUENTES 5

5. TÉRMINOS, CONDICIONES Y POLITICAS DE PRIVACIDAD 5

6. USO DE IMPUESTOS 6

7. REQUERIMIENTOS DE SEGURIDAD 6

8. CONTROL BOTÓN PAGAR Y REGRESO 7

9. TIPOS DE CRÉDITO Y CALCULO DE INTERESES (sólo Ecuador) 7

10. GENERACIÓN Y VALIDACIÓN DE OTP (sólo Ecuador) 8

11. GENERACIÓN Y VALIDACIÓN DE 3DS 8

12. GENERACIÓN Y VALIDACIÓN PINPAD-PINBLOCK (sólo Puerto Rico) 9

13. CONTROL DE IDEMPOTENCIA 10

14. ENVÍO DE KOUNTS (En caso de habilitar el servicio) 11

15. PROCESAMIENTO PAGOS CON PREAUTORIZACIÓN. 11

15.1. CHECKIN: 12

15.2. REAUTORIZACIÓN: 12

15.3. CHECKOUT 13

15.4. CANCELACIÓN DE UNA PREAUTORIZACIÓN 13

16. PROCESAMIENTO DE PAGOS CON TOKENIZACIÓN. 14

16.1. COBRAR MEDIO DE PAGO TOKENIZADO 14

16.2. INVALIDACIÓN DE TOKEN 15

17. VALIDACIÓN CAMPOS(PROCESSTRANSACTION) 16

18. MANEJO DE RESPUESTAS PARA ESTADOS TRANSACCIONALES 19

19. COMPROBANTE DE VENTA 22

20. HISTÓRICO TRANSACCIONAL 23

21. SEGURIDAD DE LA INFORMACIÓN 23

22. PROCESAMIENTO DE LA INFORMACIÓN 24

23. COHERENCIA DE LA INFORMACIÓN 24

24. DIRECCIÓN IP Y AGENTE DE NAVEGACIÓN 25

25. ENVIO EXTRADATA 25

26. REVERSO DE TRANSACCIONES 26

27. INFORMACIÓN RELEVANTE 26

27.1. FORMATO DE PLANTILLAS DE RESPUESTA 26

27.2. TARJETAS Y BANCOS DE PRUEBA PARA REALIZAR TRANSACCIONES: 31

27.3. CONSIDERACIONES FINALES 31

Nota: Se permite el uso de este documento exclusivamente para fines de instalación de clientes.

Una vez realizada la integración con Evertec Placetopay es necesario realizar pruebas desde la óptica del usuario final para evaluar que el proceso de pago sea correcto; por tanto, los enlaces y datos de pruebas deben estar libres de errores de programación.

A continuación, se describen los diferentes aspectos para tener en cuenta en el proceso de certificación API con la pasarela de pagos.

Para la certificación API se evalúan los siguientes puntos:

# ACTIVIDAD COMERCIO

El sitio únicamente debe procesar productos y/o servicios relacionados a las actividades comerciales establecidas al inicio de la negociación, en caso de ser productos no permitidas por Evertec Placetopay el sitio no será certificado.

# PROCESO DE PAGO

El sistema le debe permitir al usuario comprador, visualizar el monto total a pagar antes de realizar el pago hacia la pasarela de pagos, este valor debe de coincidir con el valor enviado a Evertec Placetopay.

El comercio definirá el proceso para realizar el desglose del producto o servicio donde se evalúan los valores e impuesto a cobrar al tarjetahabiente. Puede ser a través de formulario, carrito de compras, tienda virtual, selección de factura u otros.

El sistema debe evitar consumos adicionales al momento de actualizar el estado de una transacción cuando ya existe un estado final en el response del **process**, de este modo siempre que exista un estado final no debe hacerse un nuevo consumo al **query** para conocer el estado del pago a excepción del estado PENDIENTE, de acuerdo a lo anterior en el momento que se brinda un resumen de pago y se actualiza la transacción en el sistema del comercio, se debe hacer de forma general en BD manteniendo la trazabilidad y evitando consumos adicionales acorde al estado dado por Evertec Placetopay.

# IMAGEN CORPORATIVA

El logo de Evertec Placetopay debe estar en el home y en un tamaño que lo haga visible fácilmente, debe ser incluido mediante sus urls con extensión svg.

* [**https://static.placetopay.com/placetopay-logo.svg**](https://static.placetopay.com/placetopay-logo.svg)
* **https://static.placetopay.com/placetopay-logo-black.svg**
* [**https://static.placetopay.com/placetopay-logo-square.svg**](https://static.placetopay.com/placetopay-logo-square.svg)
* [**https://static.placetopay.com/placetopay-logo-square-dark-background.svg**](https://nam01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fstatic.placetopay.com%2Fplacetopay-logo-square-dark-background.svg&data=02%7C01%7CCarlos.Moreno%40evertecinc.com%7Cc8b65787e57c4ef072b008d7becc51c1%7C2b5b7d77f19b4c6db1805768c09ad43b%7C0%7C0%7C637187657154455565&sdata=wbBCIxS%2B0gqHeaeBnFrsKb5Ju6LpWMXGF%2FF4iph%2F%2B0w%3D&reserved=0)
* **https://dev.placetopay.com/web/wp-content/uploads/2020/08/LOGO-P2P-blanco-developers-1.png**

Adicional a esto, debe contener un hipervínculo a nuestra página principal informativa: **https://www.placetopay.com/web/**

También se sugiere agregar los logotipos de las franquicias disponibles para hacer pagos, a fin de que el cliente tenga conocimiento de los medios de pago habilitados para el comercio.

# PREGUNTAS FRECUENTES

Incluir dentro de la sección Preguntas Frecuentes (FAQ) del aplicativo del comercio uno o varios puntos relacionados con los pagos electrónicos y mencionar los pagos a través de Evertec Placetopay. En caso de que el comercio no cuente con una sección de FAQ, se deben incluir de igual forma las preguntas frecuentes proporcionadas en la documentación.

Nota: En las FAQ no debe mencionarse o hacer alusión a términos de pagos en línea ni pagos online

# TÉRMINOS, CONDICIONES Y POLITICAS DE PRIVACIDAD

Se debe contar con un portal o enlace, bien sea en el menú de navegación, pie de página o un check antes de realizar el proceso de pago, que establezca las causales del usuario frente alguna pregunta, queja o reclamo y adicional detallar la forma en que se tramitará la información de los usuarios que tengan interacción con la web, es decir, cómo se recopilará la información, cómo se va a almacenar, para qué se va a usar y si se va a compartir.

# USO DE IMPUESTOS

En caso de que dentro de la reglamentación del país y modelo de negocio sea obligatorio el envío de impuestos hacia los bancos, el comercio debe discriminar el IVA e ICE de los productos en la transacción. Se debe enviar la base, el tipo de impuesto y el valor del impuesto.

Este punto se validará en la visualización del resumen de pago y en el request que se envía a Evertec Placetopay.

# REQUERIMIENTOS DE SEGURIDAD

Los datos de configuración de la conexión de Evertec Placetopay deben ser almacenados como parámetros ya sea en la base de datos o en algún archivo .ini, .json, xml, etc. Esto se debe hacer por buenas prácticas de programación y para que al momento de actualizar la llave, el proceso sea más sencillo.

Para los sitios que usan validaciones con JavaScript se debe evitar que se afecte la operación cuando se ingresa desde un navegador que tiene deshabilitada la ejecución de JavaScript. Puede ser evitando la carga de la página o realizando validación del lado del servidor.

Se recomienda implementar contraseña cifrada en AES256 para realizar la autenticación de los usuarios en el sitio del comercio.

Por ningún motivo el comercio deberá almacenar o mostrar datos sensibles de las tarjetas de los tarjetahabientes. Los datos que se consideran sensibles son:

* Número de tarjeta de crédito.
* CVV (Código de verificación).

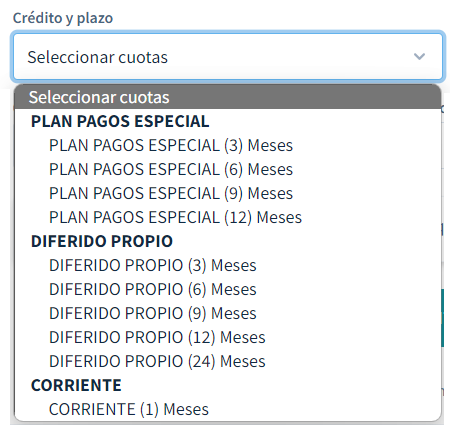
# CONTROL BOTÓN PAGAR Y REGRESO

El comercio debe parametrizar un control que prevenga al usuario y aplicativo realizar dobles peticiones al servicio de Evertec Placetopay, bien sea, porque el servicio tarde en responder al momento que se da la respuesta del pago o por interacción del usuario con el botón.

Tener en cuenta que una vez realizado el pago, en caso de que el usuario regrese a través de las instrucciones anterior y siguiente del navegador, se recomienda que se cargue nuevamente la orden, debido a que se debe evitar el envió de la misma orden al proceso de pago ya que esto incurrirá en un doble pago dependiendo de las veces que el usuario lo haga.

# TIPOS DE CRÉDITO Y CALCULO DE INTERESES (sólo Ecuador)

El comercio debe pone a disposición del usuario los tipos de crédito permitidos para su proceso de pago, de acuerdo al consumo inicial para consultar y validar la información de la tarjeta **information**:



Una vez el usuario selecciona el tipo de crédito a utilizar se debe mostrar el cálculo de los intereses según el tipo de crédito seleccionado mediante el método **interests**:

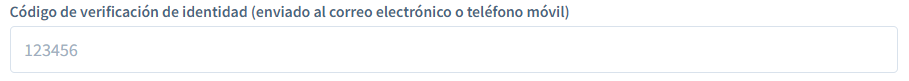
Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

El tipo de crédito seleccionado por el usuario debe ser enviado en la petición al momento que se va a realizar el **processtransaction.**

# GENERACIÓN Y VALIDACIÓN DE OTP (sólo Ecuador)

El comercio debe generar, validar y poner a disposición del usuario un campo ya sea en una modal o dentro de la misma interfaz, el cual debe estar como requerido y permitir el ingreso de únicamente valores numéricos, de acuerdo con el consumo inicial para consultar y validar la información de la tarjeta **information**:



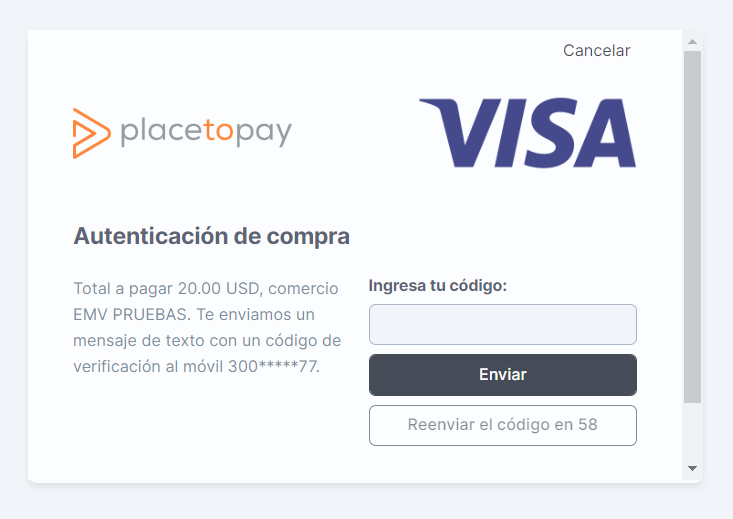
Una vez el usuario ingresa el otp y se valida contra el servicio **validate** el response brindará una firma que debe ser enviada en el **processtransaction** como otp si la respuesta ha sido satisfactoria.

En caso de que la validación del otp no se realice de forma correcta, se debe dar el detalle de error que propiamente brinda el api al realizar la validación y si se cumple el 3 intento el cual responde con bloqueo hacia lo operación, se debe bloquear o culminar la operación desde el comercio.

Adicional a esto, favor basarse en la documentación oficial:[Generación de OTP (solo Ecuador) | Gateway API (placetopay.com)](https://docs-gateway.placetopay.com/docs/api-services-docs/af61d9facbe17-generacion-de-otp-solo-ecuador)

# GENERACIÓN Y VALIDACIÓN DE 3DS

El comercio debe de levantar un flujo de autenticación de 3DS de cara al usuario ya sea en una modal o través de redirección, de acuerdo con el consumo inicial para consultar y validar la información de la tarjeta **information**:



Una vez el usuario retorna de la validación se debe consultar la información de la autenticación mediante el **query,** y el response brindará todo el detalle que debe ser enviado en el **processtransaction** como **threeDS**.

Adicional a esto, favor basarse en la documentación oficial: [3DS Lookup | Gateway API (placetopay.com)](https://docs-gateway.placetopay.com/docs/api-services-docs/069b36e2cf444-3-ds-lookup)

Una vez el usuario retorna de la validación se debe consultar la información de la autenticación mediante el **query,** y el response brindará todo el detalle que debe ser enviado en el **processtransaction** como **threeDS**.

Se debe contemplar el mandato exigido por las marcas, el cual solicita que en la trama de la transacción se envíen los siguientes parámetros obligatorios:

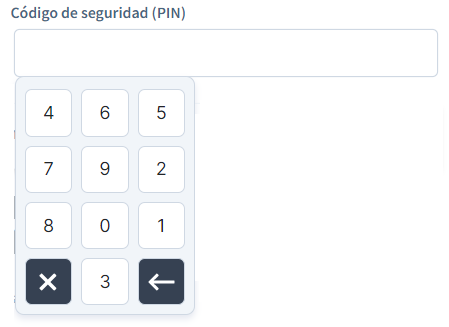
* Cardholder Email Address (Dirección de correo electrónico del titular)
* Cardholder Name (Nombre del titular)
* Cardholder Phone Number (Número de teléfono del titular)
* Common Device Identification Parameters (Device IP Address)

Por otro lado, es recomendable por parte del mandato, enviar los siguientes parámetros:

* Cardholder Billing Address City (Dirección de facturación del titular Ciudad)
* Cardholder Billing Address Country (Dirección de facturación del titular País)
* Cardholder Billing Address Line (Línea de la dirección de facturación del titular de la tarjeta)
* Cardholder Billing Address Postal Code (Código postal de la dirección de facturación del titular de la tarjeta)
* Cardholder Billing Address State (Estado de la dirección de facturación del titular de la tarjeta)

# GENERACIÓN Y VALIDACIÓN PINPAD-PINBLOCK (sólo Puerto Rico)

El comercio debe generar, solicitar y poner a disposición del usuario un PINPAD ya sea en una modal o dentro de la misma interfaz, el cual debe estar como requerido y permitir el ingreso de únicamente valores numéricos, de acuerdo con el consumo inicial para consultar y validar la información de la tarjeta **information**:



Una vez el usuario ingresa el pin, se genera el pinblock a partir de las posiciones dadas por el usuario mediante el método **pinblock** el response brindará el pinblock que debe ser enviada en el **processtransaction** como pin.

Adicional a esto, favor basarse en la documentación oficial: [Solicitud de PinPad | Gateway API (placetopay.com)](https://docs-gateway.placetopay.com/docs/api-services-docs/5b2b8c3a230f8-solicitud-de-pin-pad)

# CONTROL DE IDEMPOTENCIA

Para controlar que no realices más de una transacción aprobada para un proceso único en un periodo de tiempo predeterminado. Esto se hace identificando ese proceso con un valor único que sería enviado en el parámetro idempotenceKey

{

...

"idempotenceKey": "ABCD1234",

"instrument": {

...

}

Para mas detalles por favor basarse en la documentación oficial: <https://docs-gateway.placetopay.com/docs/api-services-docs/b61e09e4d5989-control-de-idempotencia>

# ENVÍO DE KOUNTS (En caso de habilitar el servicio)

El sistema debe de enviar en la mensajería del **processtransaction** un objeto kount con los atributos de una sesión qué es un valor aleatorio único por cada transacción y un type por default:

"kount": {

"session": "CO485",

"type": "default"

}

Adicional a esto, favor basarse en la documentación oficial:[Procesamiento de transacción | Gateway API (placetopay.com)](https://docs-gateway.placetopay.com/docs/api-services-docs/b736ea6925314-procesamiento-de-transaccion)

# PROCESAMIENTO PAGOS CON PREAUTORIZACIÓN.

Para el procesamiento con pagos preautorizados, el usuario/tarjeta habiente debe completar el proceso reservando el monto solicitado de su tarjeta de crédito, una vez se realice la reserva, este valor puede ser confirmado, modificado o cancelado.

Diagrama

Descripción generada automáticamente

## CHECKIN:

Se utiliza como depósito de garantía por la utilización de un bien o servicio. Para reservar el monto se debe enviar en la petición los siguientes datos:

"type": "checkin",

"payment": {  
 "reference": "pay\_checkin\_1",  
 "description": "Payment with pre-auth",  
 "amount": {  
 "currency": "USD",  
 "total": 10  
 }  
 }

## REAUTORIZACIÓN:

Se utilizada para modificar el monto definido como depósito de garantía separado previamente con una transacción tipo Checkin. Para modificar el valor del monto reservado se debe enviar la siguiente información:

"internalReference": 1012331, //código de referencia interna  
"authorization": "000000", //número de autorización entegado por la entidad financiera.  
 "amount": {  
 "currency": "USD",  
 "total": 15  
 },  
 "action": "reauthorization"

El internalReference se entrega en la respuesta del servicio de consulta de transacción. Es posible hacer n (varias) reauthorization, desde luego, todas antes de la operación de checkout

## CHECKOUT

Para confirmar/capturar el valor preautorizado de la reserva se debe enviar la siguiente información:

"internalReference": 11012331, //código de referencia interna  
"authorization": "000000", //número de autorización entregado por la entidad financiera.  
 "amount": {  
 "currency": "USD",  
 "total": 15  
 },  
 "action": "checkout"

El internalReference se entrega en la respuesta del servicio de consulta de sesión.

## CANCELACIÓN DE UNA PREAUTORIZACIÓN

Para anular una reserva previamente autorizada se debe enviar el action del checkout por un valor igual 0.

"internalReference": 11012331,  
"authorization": "000000",  
 "amount": {  
 "currency": "USD",  
 "total": 0  
 },  
 "action": "checkout"

La preautorización es cancelada y se libera el monto retenido en las peticiones previas.

Para más info acerca de preautorización: <https://placetopay-api.stoplight.io/docs/api-services-docs/ZG9jOjExNjAxOTc1-tipos-de-transacciones#pre-autorizaci%C3%B3n>

# PROCESAMIENTO DE PAGOS CON TOKENIZACIÓN.

Al realizar un pago con tokenización el usuario debe ingresar la información de tarjeta para que luego sean encriptados los datos de tarjeta (número y fecha de expiración), esto con el fin efectuar el cobro sobre ese medio de pago.

Para realizar la tokenización es necesario enviar los datos de tarjeta con el método del servicio *tokenize*, ver documentación: <https://placetopay-api.stoplight.io/docs/api-services-docs/967841bb68f09-tokenizacion-tokenize>

## COBRAR MEDIO DE PAGO TOKENIZADO

Al obtener el token o subtoken después de que el tarjeta habiente hizo la tokenización, se debe enviar la siguiente información:

"payment": {  
 "reference": "1122334455",  
 "description": "Testing",  
 "amount": {  
 "currency": "USD",  
 "total": 100  
 }  
 },  
 "instrument": {  
  "token": {  
 "token": "e07ca9986cf0ecac8a557fa11c07bf37ea35e9e3e3a4180c49"  
 }  
 },

El token o subtoken se podrá obtener en la respuesta del método de consulta o búsqueda de transacción (queryTransaction, searchTransation) en el arreglo instrument.

El token o la llave encriptada generada por un proceso de tokenización, este permite generar cobros sin interacción del usuario o pagos a un clic.

**Importante:** Para pagos que requieran envío de pin (Puerto Rico) es necesario solicitar al tarjeta habiente esta información de seguridad para su procesamiento:

"payment": {  
 "reference": "1234567890",  
 "description": "Token payment with pin",  
 "amount": {  
 "currency": "USD",  
 "total": 19.9  
 }  
 },  
 "instrument": {  
 "pin": "0B880E2326F6409E",  
 "card": {  
 "number": "\*\*\*\*",  
 "expiration": "\*\*/\*\*"  
 }  
 }

Es muy importante que la información del pagador sea enviada en el servicio de cobro con token, ya que esta se valida en el procesamiento en cara a la seguridad transaccional y validación de datos de tarjeta habiente.

## INVALIDACIÓN DE TOKEN

Es muy importante la administración de tokens o llaves para los instrumentos de pago, teniendo almacenada esta información de forma segura y controlar los estados de dichas llaves en bases de datos.

Para la invalidación de un token que existe en tu base datos es necesario enviar la siguiente información:

{  
 "auth": {  
 "login": "c51ce410c124a10e0db5e4b97fc2af39",  
 "tranKey": "VQOcRcVH2DfL6Y4B4SaK6yhoH/VOUveZ3xT16OQnvxE=",  
 "nonce": "NjE0OWVkODgwYjNhNw==",  
 "seed": "2021-09-21T09:34:48-05:00"  
 },  
 "locale": "en\_PR",  
 "instrument": {  
 "token": {  
 "token": "a3bfc8e2afb9ac5583922eccd6d2061c1b0592b099f04e352a894f37ae51cf1a"  
 }  
 }  
 }

Ver documentación para invalidar token: <https://placetopay-api.stoplight.io/docs/api-services-docs/90727aada9dc9-tokenizacion-invalidate>

# VALIDACIÓN CAMPOS(PROCESSTRANSACTION)

El comercio debe como mínimo enviar los siguientes campos requeridos en la solicitud de pago:

Datos del comprador y pagador(buyer-payer):

* Tipo de documento del comprador-pagador. (Opcional en Puerto Rico)
* Número de documento del comprador-pagador. (Opcional en Puerto Rico)
* Nombre del comprador-pagador.
* Apellido del comprador-pagador.
* Email del comprador-pagador.
* Teléfono celular del comprador-pagador.

Datos del pago (payment):

* Referencia
* Descripción (opcional)
* Moneda
* Valor.
* IVA (opcional)
* Base de devolución (opcional)
* Dispersión (En caso de habilitar el servicio)
* Convenio
* Tipo de convenio
* Moneda
* Total
* Recurrencia (En caso de habilitar el servicio)
* Periodicidad
* Intervalo
* Fecha próximo pago
* Número máximo de periodos
* Fecha para finalizar la recurrencia
* Url para confirmación de pagos (opcional)

Datos de la tarjeta (instrument)

* Tarjeta
  + Número o PAN
  + Expiración
  + CVV
  + Cuota
* Crédito (sólo Ecuador)
  + Código
  + Tipo
  + Código del grupo
  + Diferido
* OTP (sólo Ecuador)
* threeDS
* Id
* Enrolada
* Autenticada
* Firma valida
* Eci
* Cavv
* Xid
* Version
* Extra
  + Motivo estado de la autenticación
  + AcstransId
  + threeDSServerTransID
* Pinpad (sólo Puerto Rico)
  + TransactionId
  + Posiciones
  + PinBlock
  + Longitud
* Pin (sólo Puerto Rico)
* Kount (En caso de habilitar el servicio)
* AVS (En caso de habilitar el servicio)
  + Session
  + Tipo

Datos adicionales

* IP.
* Agente de navegación.

Importante: Debe tener en cuenta que cada uno de los campos debe contener información coherente. Adicional a esto, favor basarse en la documentación oficial en caso de cambios: [Procesamiento de transacción | Gateway API (placetopay.com)](https://docs-gateway.placetopay.com/docs/api-services-docs/b736ea6925314-procesamiento-de-transaccion)

* El sistema solicita al usuario el número de tarjeta como un campo obligatorio, sólo recibe valores numéricos. y tiene una longitud de 13 a 19 caracteres, validando el valor digitado a través del algoritmo de Luhn.
* La aplicación solicita o presenta al usuario la fecha de vencimiento como un campo obligatorio, validando que la fecha de vencimiento no esté vencida y sólo reciba el valor del mes de enero a diciembre, es decir, del 01 al 12 (Siempre a dos dígitos). Permitiendo como máximo la elección de 10 años, a partir de la fecha actual.
* El sistema solicita al usuario el CVV2 como un campo obligatorio enmascarado, sólo recibe valores numéricos y tiene una longitud máxima de 4 caracteres (American Express es la única que debe permitir como máximo 4 caracteres, Visa, Mastercard, Discover y Diners solo 3).
* La referencia debe contener una longitud máxima de 32 caracteres alfanuméricos y no debe contener o almacenar el número de la tarjeta y caracteres especiales siendo única por cada solicitud.
* Para los datos del comprador y pagador(buyer-payer) se debe validar cada uno de los campos que están siendo enviado a Evertec Placetopay como requeridos al momento que el usuario está ingresando la información.
* Para la validación del documento se deben implementar las restricciones en el campo, de acuerdo al tipo de documento seleccionado por el usuario, se puede tomar como referencia las validaciones de la documentación: [Tipos de documento | Gateway API (placetopay.com)](https://placetopay-api.stoplight.io/docs/api-services-docs/ZG9jOjExNjAxOTcz-tipos-de-documento)
* En caso de que el documento de identidad pertenezca a una persona natural, para los campos nombre y apellido no se debe de permitir el ingreso de números ni caracteres especiales, sin embargo, debe permitir el ingreso de la tilde, espacios y la letra Ñ. Caso contrario, es decir, empresas se debe enviar solo bajo nombre, la razón social o nombre comercial y para este caso si se debe permitir números.
* Para los campos numéricos como móvil o teléfono no debe permitir el ingreso de letras, ni caracteres especiales.
* Para el campo email debe contar con una estructura valida, [usuario/a]@[dominio].[Tipo de origen].[Extensión].
* La dirección IP y agente de navegación debe ser la del equipo del usuario final.

En el proceso de paga no siempre el comprador es el mismo titular, por lo que se debe tener en cuenta esta información al momento de enviar estos datos a Evertec Placetopay.

Nota: La implementación de preguntar por la propiedad de la tarjeta se considera una buena práctica y es opcional, sin embargo, si el comercio toma la determinación de no implementar esto, debe garantizar que siempre envían la información del pagador o tarjetahabiente.

# MANEJO DE RESPUESTAS PARA ESTADOS TRANSACCIONALES

Al momento que el usuario culmine su proceso de pago, se debe mostrar el detalle de la transacción, como mínimo deben visualizarse los siguientes datos:

* Referencia.
* Estado final de transacción
* Aprobado
* Rechazado
* Pendiente
* Fallido
* Aprobado Parcial (sólo en dispersión)
* Razón y mensaje
* Fecha y hora.
* Valor total.
* Intereses (sólo Ecuador)
* Tipo de crédito (sólo Ecuador)
* Cuotas
* Moneda con la cual se realizó el pago.
* Recibo.
* Autorización.
* Banco.
* Últimos 4 dígitos de la tarjeta



Si desea indicarle más información al usuario final, puedes seguir el formato de [FORMATO DE PLANTILLAS DE RESPUESTA](#_FORMATO_DE_PLANTILLAS) descrita en este documento, mostrando el estado de acuerdo con la respuesta emitida por Evertec Placetopay.

Recomendaciones alineadas a la experiencia de usuario:

* Repuesta aprobada: es posible adicionar un vínculo o botón que le permita al usuario y/o cliente ir al inicio (home) del proceso del pago, de igual forma se evaluará la recepción.

Imagen que contiene Logotipo

Descripción generada automáticamente

* Respuesta rechazada y fallida: se recomienda adicionar un vínculo o botón que le permita al usuario y/o cliente reintentar el pago.

Texto

Descripción generada automáticamente con confianza baja

**Importante:** Para el caso de dispersión se validará que no se presente ningún error bajo una transacción que haya sido rechazada por Scudo, de este modo desde el comercio se debe tener control con la interacción del arreglo tipo payment[ ] bajo la casuística del arreglo dispersion[ ], teniendo en cuenta que de acuerdo a las configuraciones de riesgo en una transacción se puede ver alterado el resultado del arreglo dispersion[ ], lo cual sino se controla adecuadamente puede generar un error en el comercio.

**Control transacción pendiente:** Se puede visualizar una transacción en estado pendiente por respuesta directa de la entidad financiera o la no recepción de respuesta por parte de Evertec Placetopay (TimeOut).

Se cuenta con tres formas para obtener el estado final de una transacción, la primera con la respuesta del servicio al momento de hacer el **processtransaction** y las otras 2 en caso de recibir un estado PENDIENTE mediante el método **query** teniendo la referencia interna y la última con el servicio de **search** el cual es una contingencia en caso de perdida de comunicación al crear la transacción con el **processtransaction**.

Nota: El consumo hacia el servicio para conocer el estado final de una transacción pendiente siempre debe hacerse mediante el método **query**, el uso del método **search** es únicamente en caso de perdida en la comunicación cuando se realiza la transacción.

Cuando al consumir el servicio **processtransaction** se genere timeout en la conexión a Evertec Placetopay (debe ser alrededor de 25 segundos) y no se obtenga ninguna respuesta por parte del servicio, la operación debe quedar marcada en estado pendiente y buscar la transacción mediante el método **search**, mientras tanto esta transacción debe cumplir con el comportamiento general de este estado (control de doble pago y proceso sonda)

* **Sonda o Cronjob:** Este proceso consiste en una tarea programada(cronjob) la cual se encarga de consumir el método **query** (consulta de transacción) sobre las transacciones que quedaron en estado pendiente en sus registros, este procedimiento se debe ejecutar cada 15 minutos verificando las transacciones que tengan más de 7 minutos en estado pendiente.

Cuando se encuentre una transacción en estado pendiente en la base de datos el sistema debe informar y presentar el siguiente evento:

* Un **mensaje control de doble pagos** informando al usuario la existencia de transacciones pendientes, antes de realizar un nuevo pago. Por ejemplo:
* “En este momento su pedido con \*#Referencia\* y valor de \*#Amount\* se encuentra en un estado de PENDIENTE de no recibir confirmación por parte de su entidad financiera, por favor espere unos minutos y vuelva a consultar más tarde para verificar si su pago fue confirmado de forma exitosa. Si desea más información sobre el estado actual de su operación puede comunicarse a nuestras líneas de atención al cliente \*000-00-00\* o enviar un correo electrónico a email@email.com y preguntar por el estado de la transacción: <#CUS/Autorización>\*\*\*”.

Cuando se encuentre una transacción en estado de aprobación parcial (sólo dispersión) en la base de datos el sistema debe informar y presentar el siguiente evento:

* Un **mensaje informativo** al usuario que indique la existencia de transacciones aprobadas parciales y el control o manejo, de acuerdo con la política del negocio que se brindará sobre esta transacción, antes de realizar un nuevo pago.

**Importante:** Para dispersión se debe definir el proceso operativo y funcional para dar control a las transacciones bajo estado APROBADO PARCIAL, de tal modo que se tenga definido un control interno en el comercio para este tipo de situaciones sobre las transacciones.

# COMPROBANTE DE VENTA

En caso de que desde el sistema se envíen comprobantes de venta (Impresión, e-mail, archivo exportado, mensaje de voz) propios de acuerdo con cada uno de los estados de transacción y se presente información relacionada al pago, se valida que la información mostrada se contraste con la información de la transacción verificando que de acuerdo con los campos mostrados la información sea coherente con relación al pago. Se recomienda que el usuario visualice la siguiente información:

* La referencia.
* Fecha y hora de la transacción.
* Estado de la transacción.
* Total pagado por el usuario.
* Tipo de crédito y diferido (Ecuador) o cuota seleccionada por el usuario final.
* Los cuatro últimos dígitos de la tarjeta
* Banco

Sino se cuenta con un comprobante de pago propio se toma como referencia el comprobante emitido por Placetopay Evertec.

# HISTÓRICO TRANSACCIONAL

En caso de que sea necesario autenticarse en el sitio del comercio para realizar un proceso de pago, se debe permitir consultar el estado de por lo menos las últimas diez (10) transacciones realizadas. Cada registro debe contener como mínimo los siguientes datos ordenados de forma descendente por fecha:

* Fecha y hora de la transacción.
* Número de referencia (emitida por el comercio).
* Autorización/CUS. (opcional)
* Estado de la transacción.
* Valor (debe estar concatenado con el tipo de moneda según ISO 4217).

Tabla

Descripción generada automáticamente

Nota: En caso de que no se haga uso de login en la página y por reglas de negocio no sea posible implementar un apartado donde se puedan consultar los pagos, se le debe informar al analista de Evertec Placetopay, la razón o motivo para que sea analizada y dar la excepción sobre este.

# SEGURIDAD DE LA INFORMACIÓN

El sistema y comercio deben de cumplir los siguientes criterios:

* El comercio debe estar certificado en PCI (vigente)
* El sistema bajo ningún motivo almacena información sensible del tarjetahabiente.
* El sistema no muestra en los resúmenes de pago, comprobantes de venta o cualquier otro apartado de cara al usuario el número de la tarjeta (como máximo BIN y últimos 4 dígitos)
* El sistema no muestra en los resúmenes de pago, comprobantes de venta o cualquier otro apartado de cara al usuario el CVV de la tarjeta.
* Se guarda en la base de datos del aplicativo la información mínima para un futuro reclamo (fecha y hora de transacción, número de recibo, valor de la transacción, número de autorización, máximo 4 últimos dígitos del número de tarjeta, referencia y pagaré, éste último si se aplica).
* El sistema debe contar con un certificado digital válido, realizando la captura de información utilizando el protocolo seguro HTTPS.
* Se debe utilizar el protocolo de TLS 1.2 o superior.
* Si el desarrollo utiliza una interfaz web (así sea intranet) la URL de captura de información no se enmascara (oculta) mediante técnicas como IFRAMES.

# PROCESAMIENTO DE LA INFORMACIÓN

Al realizar una transacción, se envía al aplicativo Evertec Placetopay los mismos datos que fueron validados,digitados o seleccionado en la interfaz de usuario:

* Número de tarjeta
* CVV
* Fecha de Vencimiento
* Cuota o Tipo de crédito (sólo Ecuador)
* Valor Total
* IVA
* Base de Devolución
* Información del usuario
* Información de los protocolos de seguridad

# COHERENCIA DE LA INFORMACIÓN

La información enviada a Evertec Placetopay no debe tener contrastes en cada interfaz en la cual se presente información referente al pago, de acuerdo con esto se debe cumplir con los siguientes aspectos:

* La fecha y hora de la transacción presenta un valor consistente entre la base de datos del desarrollo del comercio, la consulta de la consola de Evertec Placetopay y el comprobante de venta generada por el desarrollo cuando se realizan transacciones.
* Los cuatro últimos números de la tarjeta aparece de manera única y coincidente entre la base de datos del desarrollo del comercio y la consulta de la consola de Evertec Placetopay.

# DIRECCIÓN IP Y AGENTE DE NAVEGACIÓN

Cuando se envíe la petición para procesar la transacción con el método *process* es importante enviar los parámetros ipAddress y userAgent como se menciona en el punto 15 VALIDACIÓN DE CAMPOS (processTransaction). Son datos adicionales requeridos que deben enviar para el control de filtro de seguridad transaccional.

Ejemplo:

…  
"ipAddress": "192.168.1.109",  
"userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36"  
…

La dirección IP debe ser tomada del dispositivo del cliente ya sea realizando una función desde tu código o por medio de un script según tu lenguaje de programación, de igual modo con el agente de navegación, ya sea en una página web o una aplicación en donde se encuentre integrado el servicio.

# ENVIO EXTRADATA

Puedes enviar información adicional en las peticiones por medio de extrada. Si dentro del proceso de pago se necesita añadir, por ejemplo, una segunda referencia u otro dato relevante en la petición. lo puedes realizar por medio de un arreglo de objetos llamado *additional*.

Ejemplo:

…  
"additional": {

"merchantCode": "468231",

"terminalNumber": "00990101"

},  
…

Si deseas enviar particularmente información adicional sobre una cuenta de cliente donde tenga servicios y que de esta forma es identificado desde tu sistema como un número de cuenta de cliente, debes enviar la extrada de la siguiente manera:

" additional ": {

""Customer\_Account\_ID": "value": "8100312356677"

}

]

**Nota**: Las siguientes claves NO son permitidas: \_accountNumber, userAgent, fingerprint, sourcePlatform, tokenizationID, trazabilyCode, transactionCycle, RequestId, PartnerAuthCode.

# REVERSO DE TRANSACCIONES

Se debe definir el proceso de reverso de transacciones, en caso de que el comercio vaya a realizar reversos a través del api expuesto por Placetopay Evertec, se debe confirmar al analista, con el fin de que éste valide la funcionalidad y garantice el correcto funcionamiento, por otra parte, si se va a usar la consola administrativa debe ser informado a través del correo en el hilo del analista encargado.

Nota: Dependiendo de la fecha de cierre en la red, el reverso no será efectivo el mismo día llegado el escenario que se haga luego de esta hora y en su caso se deberá tramitar un reverso extemporáneo con la entidad financiera

# INFORMACIÓN RELEVANTE

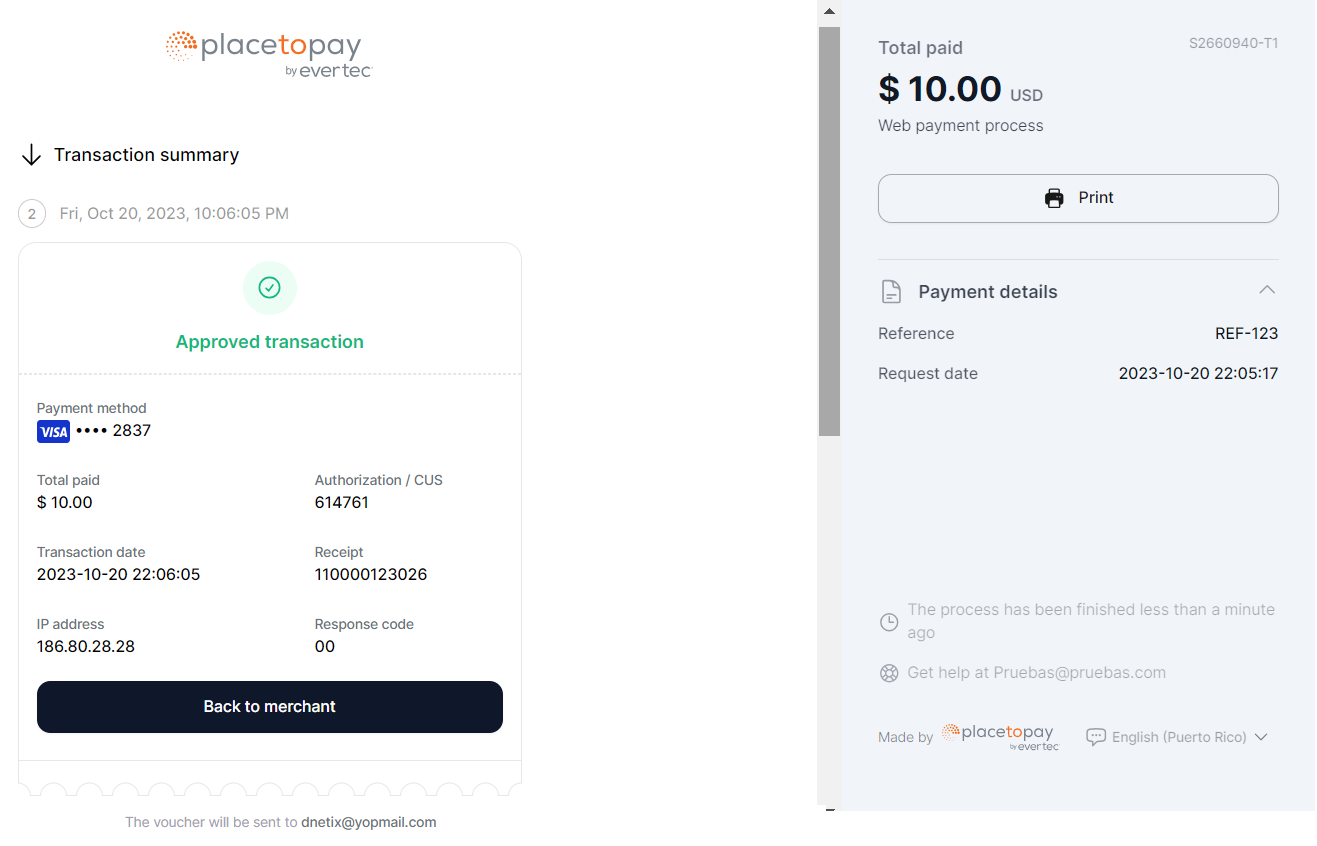
## FORMATO DE PLANTILLAS DE RESPUESTA

Las plantillas de respuesta son formatos informativos para el usuario final con respecto a su pago, por lo cual es importante mostrar los datos relevantes en las plantillas; deben de estar libres de errores ortográficos, de codificación de caracteres y sean consistentes como se describen a continuación:

* Fecha y hora de transacción.
* Valor o monto de la transacción: Tener en cuenta que deben presentarse en formato decimal a dos dígitos junto con el tipo de moneda (USD 938,99)
* IVA: Valor cobrado del IVA aplicado con el tipo de moneda (USD 25,93)
* Estado de la transacción: Los cuales son: Aprobada, Rechazada, Pendiente, Aprobada parcial (sólo en dispersión) y Fallida. (El sistema responde con los estados en inglés, se debe traducir al idioma que predomine en la página).
* Razón y Motivo: Es el mensaje de error o motivo de declinación emitido por la entidad financiera.
* Intereses (sólo Ecuador): Intereses a pagar en la transacción.
* Tipo de crédito (sólo Ecuador): Descripción del tipo de crédito seleccionado por el usuario.
* Cuotas: Número de cuotas a las cuales se difirió el pago.
* Franquicia: Nombre de la marca de la tarjeta con la cual se realizó la transacción.
* Banco: Es la entidad a la cual pertenece la tarjeta o la cuenta de la transacción
* Autorización/CUS: Es el código único de seguimiento o el # de autorización emitido por la entidad financiera.
* Recibo: Consecutivo generado por la red, emitido por Evertec Placetopay.
* Referencia: Es la referencia de pago generada por cada comercio y debe ser única para cada transacción.
* Descripción: Debe indicar de manera real el concepto o la descripción del pago.
* Dirección IP: Se debe mostrar la dirección IP del equipo donde el usuario final está realizando la transacción.
* Nombre del comprador o cliente: nombre y apellidos del comprador o cliente.
* Consulta: Teléfono, Email, o enlace a formulario de consulta, donde el usuario pueda obtener información adicional de su transacción.

Nota: el comercio deberá definir la forma y el orden para mostrar los datos, pero son obligatorias las etiquetas y la estructura de los datos. A continuación, se presentan ejemplos de aplicación para la página de respuesta en el sitio:

* Ejemplo de la plantilla de respuesta (Transacción aprobada):



* Ejemplo de la plantilla de respuesta (Transacción rechazada):

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* Ejemplo de la plantilla de respuesta (Transacción pendiente):

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* Ejemplo de la Plantilla de respuesta (Transacción aprobada parcial):

Interfaz de usuario gráfica, Aplicación, Sitio web

Descripción generada automáticamente

* Ejemplo de la plantilla de respuesta (Transacción fallida):

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

## TARJETAS Y BANCOS DE PRUEBA PARA REALIZAR TRANSACCIONES:

Por normas PCI no podemos incluir tarjetas de crédito e información adjunta en correos, sin embargo, a través del siguiente enlace pueden visualizar las tarjetas para realizar las pruebas pertinentes: <https://placetopay-api.stoplight.io/docs/api-services-docs/ZG9jOjIxNjA0MDM3-numeros-de-tarjeta-de-pruebas>

Nota: Para todas las franquicias:

* Código de verificación: 123
* Fecha de vencimiento de la tarjeta: Seleccione una fecha vigente
* Otp: 123456
* AVS: 55555

## CONSIDERACIONES FINALES

Esta información entregada junto a la evaluación de peritaje que se realiza del sitio es fundamental, dado que son tenidos en cuenta para los checklists de pruebas y si todos los puntos no se encuentran OK, el comercio NO podrá salir a producción.

Para el proceso de certificación se debe de enviar la información al analista asignado de Placetopay Evertec con los siguientes datos:

* **Url de pruebas:** El sitio habilitado para realizar la revisión y certificación
* **Usuario y clave:** Datos de acceso para el ingreso y simulación del pago.

[](https://www.facebook.com/Evertecinc/)[](https://www.instagram.com/evertec.inc/?hl=es)[](https://www.linkedin.com/company/evertec/posts/?feedView=all)[](https://twitter.com/evertec_inc/)