GUIA DE CERTIFICACIÓN API

Guía certificación Implementación

Aval Pay

Medellin, 2025

Versión 1.1

USO CONFIDENCIAL

Declaración del documento

Para uso confidencial

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

El cliente acuerda por su aceptación o uso de estos documentos, devolverlos a solicitud de Aval Pay® 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.

Guía de Certificación PSE

PSE ofrece una solución eficiente y segura para realizar transferencias bancarias en línea. Para implementar este servicio, es necesario integrar el **API Gateway**, asegurando que el lenguaje de programación utilizado pueda comunicarse con un servicio **REST**.

Este botón de pagos permite a empresas e individuos realizar transferencias de manera rápida y sencilla. A nivel general, el flujo de funcionamiento del servicio es el siguiente:

- **Inicio de la transacción:** A través del servicio **Information**, se obtiene la lista de bancos disponibles asociados al comercio. El usuario selecciona su entidad financiera y el código del banco elegido se envía en el campo **bankcode** del instrumento **redirection**.
- **Creación de sesión:** Se genera una sesión en estado *pendiente*, devolviendo una URL para redirigir al cliente al portal del banco seleccionado.
- **Finalización del pago:** Tras completar la transacción en la plataforma bancaria, el usuario es redirigido de vuelta a la página del comercio.

A continuación, se detallan los aspectos clave a considerar para el proceso de certificación del sitio del comercio con la pasarela de pagos **AvalPay**

.

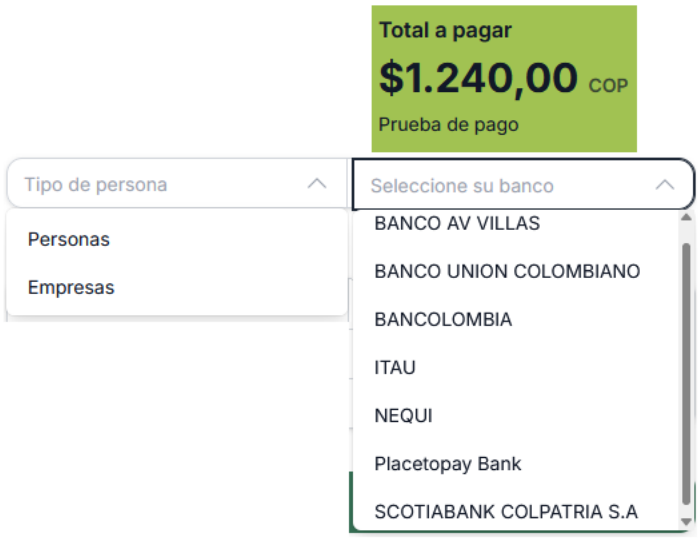
1. USO DEL IVA O IMPUESTOS (OPCIONAL)

- El comercio tiene la opción de discriminar el **IVA** o cualquier otro impuesto aplicable a los productos dentro de la transacción.
- Esta información debe ser enviada en la **solicitud (Request)** de la transacción.
- Es fundamental revisar la documentación correspondiente para conocer el procedimiento detallado sobre cómo realizar esta discriminación correctamente.
- https://docs.placetopay.dev/gateway/api/reference/transaction#process-request

2. LISTADO DE BANCOS Y TIPO DE PERSONA

- En este ítem se evaluará la manera en cómo a un usuario final se le desglosará el listado de bancos, el tipo de persona (Person o Company) y al momento de seleccionar uno de los bancos, si tome el respectivo código, adicional a eso que se evidencie el listado completo de bancos correspondientes. Como sugerencia, recomendamos al comercio almacenar esta información en caché durante un periodo de 24 horas.


```
"bankList": [
    {
        "description": "BANCO AV VILLAS",
        "code": "1052"
    },
    {
        "description": "BANCOLOMBIA",
        "code": "1007"
    },
    {
        "description": "BANCO UNION COLOMBIANO",
        "code": "1022"
    },
    {
        "description": "ITAU",
        "code": "1014"
    },
    {
        "description": "NEQUI",
        "code": "1507"
    },
    {
        "description": "Placetopay Bank",
        "code": "9999"
    },
    {
        "description": "SCOTIABANK COLPATRIA S.A",
        "code": "1019"
    }
],
```



3. PROCESAMIENTO TRANSACCIONAL

- **CONTROL DEL BOTÓN DE REDIRECCIÓN**

  Para este ítem se evaluará que al momento que el usuario de varias veces clic al botón para proceder a pagar, solo se realice una petición al servicio esto con el fin de evitar que se creen dobles peticiones, que pueden llegar a generar confusión

- **VALIDACIÓN CAMPOS:**
  - El Código de Referencia tiene una longitud máxima de 32 caracteres.
    - El Código de Referencia es alfanumérico.
    - Para una transacción con estado Aprobado, la referencia usada no puede repetirse.
  - Se debe solicitar al usuario los siguientes campos para enviar como pagador y comprador: nombres, apellidos, email, teléfono, dirección.
    - El campo nombre no permite caracteres especiales o números a excepción de la tilde o la Ñ.
    - Para el documento se debe seguir el siguiente patrón de validación. Tipos de documento - Placetopay Docs
    - El campo email debe contener la estructura de un email válido.
  - La dirección IP debe ser la del equipo del usuario final
  - El agente de navegación debe tomarse con una propiedad dependiendo del lenguaje de programación.

- **CONSISTENCIA DE LA INFORMACIÓN**

  En este ítem se evaluará la información que se envía en cada una de las peticiones que, si sea correcta y de acuerdo a lo que el usuario está pagando, a continuación, se describe el detalle de estos:

- La Fecha y hora de la transacción presenta un valor consistente entre la base de datos del desarrollo del comercio, y la consulta de la consola de Aval Pay y el comprobante de venta generada por el desarrollo cuando se realizan transacciones.
- Al realizar una transacción, se envía al aplicativo Aval Pay API el mismo Total, IVA, Base de Devolución que fueron digitados o seleccionado en la interfaz de usuario.
- El banco seleccionado por el usuario debe aparecer de manera única y coincidente entre la base de datos del desarrollo del comercio, la consulta de la consola de Aval Pay.

- **RESÚMEN DE PAGO.**

  Este es el que debe visualizar el usuario al momento de finalizar la transacción, los datos mínimos que, de contener dicho comprobante, son los siguientes:

  - Se incluye en el soporte de respuesta el estado del pago.
  - Se muestra la fecha y hora en que se realizó la transacción.
  - Se detalla el banco seleccionado por el usuario.
  - Se especifica la referencia de la transacción.

- **CONTROL DE DOBLE PAGO:**
  - Cuando el usuario intente realizar una transacción y cuenta con una operación en estado pendiente debe presentarse un mensaje informativo que permita identificar que se tiene una transacción pendiente, su referencia y datos de contacto del establecimiento comercial, a continuación, compartimos una estructura de ejemplo, en la cual se podrían basar para construir este:
    - 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>***.

En este momento su orden # 292706 presenta un proceso de pago cuya transacción se encuentra PENDIENTE de 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 mayor información sobre el estado actual de su operación puede comunicarse a nuestras líneas de atención al cliente o enviar un correo electrónico a digital@herson.com.co y preguntar por el estado de la transacción

NOTA: Para los ítems de procesamiento transaccional, dirigirse al punto 10 de la guía llamada consideraciones finales, donde podrá visualizar los datos requeridos en cada una de las peticiones que deben generar, adicional a eso validar en la documentación publica https://docs.placetopay.dev/gateway/api/reference/information

4. CRONJOB O SONDA

- El comercio puede tener en su base de datos una transacción en estado pendiente por los siguientes motivos, por respuesta directa de la entidad financiera o por no recepción de respuesta por parte de Aval Pay (TimeOut), para esto debe implementar un cronjob o tarea programada, donde realizará las respectivas consultas de las transacciones con este estado y si ya se actualizo este, para esta creación, deberá tener en cuenta lo siguiente:
    - Recuerde configurar en su servidor una tarea programada implementando este método y que corra cada 12 minutos verificando las transacciones que tengan más de 7 minutos en estado pendiente.
    - Cuando al consumir el servicio se genere timeout en la conexión a Aval Pay (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 cumplir con el comportamiento general de este estado (control de doble pago y proceso sonda)

5. WEBHOOK O NOTIFICACIÓN

- **El comercio nos debe proporcionar una URL/URI expuesta públicamente en donde se realizará un llamado por medio de un POST con la siguiente estructura JSON:**
- **El comercio debe escuchar el request enviado en donde se notificará de manera asíncrona las transacciones realizadas. Se relaciona documentación:** Notificación - Placetopay Docs

6. 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 cinco (5) 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. (opcional)
- Estado de la transacción.
- Valor (debe estar concatenado con el tipo de moneda según ISO 4217).

Fecha y Hora	Referencia	Estado	Autorización/Cus	valor
31-12-2023 6:50 p.m	ORDEN_521	PENDIENTE	58985	COP $18000
31-12-2023 6:50 p.m	ORDEN_522	APROBADO	58986	USD $200
31-12-2023 6:50 p.m	ORDEN_523	RECHAZADO	58987	COP $8000
31-12-2023 6:50 p.m	ORDEN_524	APROBADO PARCIAL	58988	USD $800

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 la razón o motivo para que sea analizada y dar la excepción sobre este.

7. MULTICREDITO

Si se requiere realizar una dispersión de fondos por el medio de pago PSE, se requiere que se implemente esta funcionalidad, para esto deberá tener las siguientes consideraciones:

- Se debe contar con una cuenta padre y con mínimo 2 o máximo 9 cuentas hijas para que esta funcionalidad se habilite de manera correcta, estas se deben gestionar con ACH.
- Se debe enviar en el request un objeto llamado **dispersión** con los arrays que contengan la información de las cuentas hijas a las cuales se va a realizar la dispersión de los fondos, como se evidencia en los ejemplos de petición.

GUIA DE CERTIFICACIÓN BOTON AVAL

El botón aval brinda la facilidad para realizar transferencias de forma rápida y segura. Para implementar este botón, se debe consumir el servicio Api Gateway, el cual se debe tener en cuenta que el lenguaje de programación utilizado pueda comunicarse con un servicio REST.

Un servicio de botón que permite realizar transferencias bancarias es una herramienta que puede ser utilizada por empresas o individuos que necesitan realizar pagos o transferencias de forma rápida y sencilla.

En términos generales, el flujo y funcionamiento del servicio es de la siguiente manera:

- Para iniciar una transacción con Botón Aval, se entregará por medio del servicio **Information** la lista de bancos disponible asociada al comercio; esto para que el usuario elija la entidad financiera de su preferencia, el código del banco seleccionado debe ser enviado en el campo **bankcode** del instrumento **redirection**.

- Se creará una sesión en estado pendiente y se retorna una URL para realizar la redirección del cliente al servicio externo del banco seleccionado del grupo Aval.

- Realizado el pago en la URL proporcionada, el usuario será retornado a la página del comercio.

A continuación, se describen los diferentes aspectos para tener en cuenta para proceso de certificación de sitio del comercio con la pasarela de pagos Aval Pay.

1. USO DEL IVA O IMPUESTOS (OPCIONAL)

- El comercio debe discriminar el IVA o impuesto de los productos en la transacción, esta información se envía el Request, se debe tener validar el apartado de la documentación la cual explica esta como se discrimina.
  https://docs.placetopay.dev/gateway/api/reference/transaction#process-request

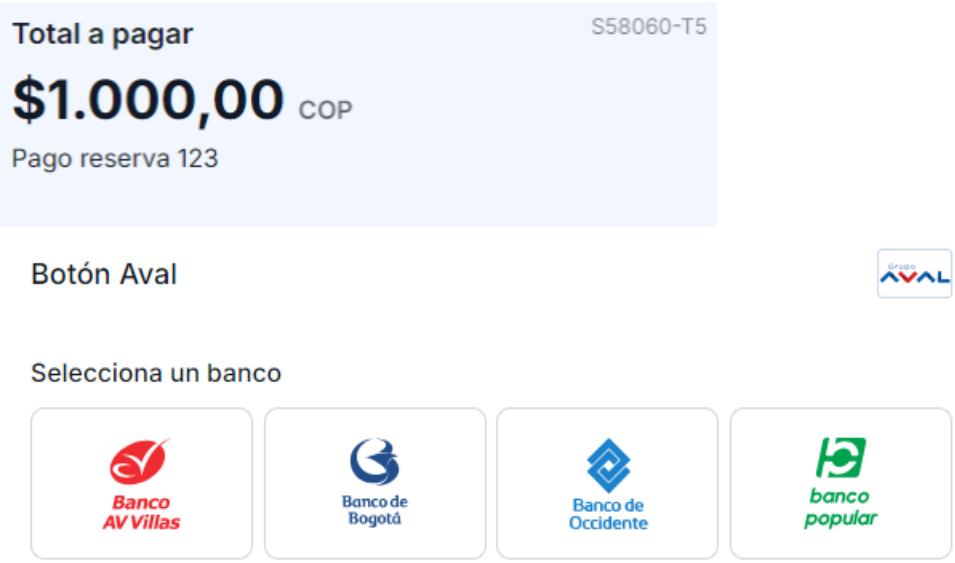
2. CREDENCIALES DE CONEXIÓN

- Los datos de configuración de conexión de Aval Pay (Login y SecretKey) deben ser almacenados como parámetros ya sea en la base de datos o en algún archivo .ini, .json, xml, etc.

3. LISTADO DE BANCOS

- En este ítem se evaluará la manera en cómo a un usuario final se le desglosará el listado de bancos y al momento de seleccionar uno de los bancos, si tome el respectivo código, adicional a eso que se evidencie el listado completo de bancos correspondientes. Como sugerencia, recomendamos al comercio almacenar esta información en caché durante un periodo de 24 horas.


```
"bankList": [
    {
        "id": "1",
        "code": "0052",
        "description": "Banco AV Villas"
    },
    {
        "id": "3",
        "code": "0001",
        "description": "Banco Bogota"
    },
    {
        "id": "5",
        "code": "0023",
        "description": "Banco Occidente"
    },
    {
        "id": "4",
        "code": "0002",
        "description": "Banco Popular"
    }
],
```



4. PROCESAMIENTO TRANSACCIONAL

- **Validación campos:**
  - El Código de Referencia tiene una longitud máxima de 32 caracteres.
    - El Código de Referencia es alfanumérico.
    - El Código de Referencia no almacena el número de la tarjeta.
    - Para una transacción con estado Aprobado, la referencia usada no puede repetirse.
  - Se debe solicitar al usuario los siguientes campos para enviar como pagador y comprador: nombres, apellidos, email, teléfono, dirección.
    - El campo nombre no permite caracteres especiales o números a excepción de la tilde o la Ñ.
    - Para el documento se debe seguir el siguiente patrón de validación. Tipos de documento - Placetopay Docs
    - El campo email debe contener la estructura de un email válido.
  - La dirección IP debe ser la del equipo del usuario final
  - El agente de navegación debe tomarse con una propiedad dependiendo del lenguaje de programación.

- **Consistencia de la información**
  En este ítem se evaluará la información que se envía en cada una de las peticiones que, si sea correcta y de acuerdo a lo que el usuario está pagando, a continuación, se describe el detalle de estos:
  - La Fecha y hora de la transacción presenta un valor consistente entre la base de datos del desarrollo del comercio, y la consulta de la consola de Aval Pay y el comprobante de venta generada por el desarrollo cuando se realizan transacciones.
  - Al realizar una transacción, se envía al aplicativo Aval Pay API el mismo Valor Total, IVA, Base de Devolución que fueron digitados o seleccionado en la interfaz de usuario.

- El banco seleccionado por el usuario debe aparecer de manera única y coincidente entre la base de datos del desarrollo del comercio, la consulta de la consola de Aval Pay.

- **Resúmen de pago.**

Este es el que debe visualizar el usuario al momento de finalizar la transacción, los datos mínimos que, de contener dicho comprobante, son los siguientes:

- Se incluye en el soporte de respuesta el estado del pago.
- Se muestra la fecha y hora en que se realizó la transacción.
- Se detalla el banco seleccionado por el usuario.
- Se especifica la referencia de la transacción.

- **Control de doble pago:**
  - Cuando el usuario intente realizar una transacción y cuenta con una operación en estado pendiente debe presentarse un mensaje informativo que permita identificar que se tiene una transacción pendiente, su referencia y datos de contacto del establecimiento comercial, a continuación, compartimos una estructura de ejemplo, en la cual se podrían basar para construir este:
    - 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>***.

En este momento su orden # 292706 presenta un proceso de pago cuya transacción se encuentra PENDIENTE de 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 mayor información sobre el estado actual de su operación puede comunicarse a nuestras líneas de atención al cliente o enviar un correo electrónico a digital@herson.com.co y preguntar por el estado de la transacción

NOTA: Para los ítems de procesamiento transaccional, dirigirse al punto 10 de la guía llamada consideraciones finales, donde podrá visualizar los datos requeridos en cada una de las peticiones que deben generar, adicional a eso validar en la documentación publica https://docs.placetopay.dev/gateway/api/reference/information

5. CRONJOB O SONDA

- El comercio puede tener en su base de datos una transacción en estado pendiente por los siguientes motivos, por respuesta directa de la entidad financiera o por no recepción de respuesta por parte de Aval Pay (TimeOut), para esto debe implementar un cronjob o tarea programada, donde realizará las respectivas consultas de las transacciones con este estado y si ya se actualizo este, para esta creación, deberá tener en cuenta lo siguiente:
    - Recuerde configurar en su servidor una tarea programada implementando este método y que corra cada 12 minutos verificando las transacciones que tengan más de 7 minutos en estado pendiente.
    - Cuando al consumir el servicio se genere timeout en la conexión a Aval Pay (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 cumplir con el comportamiento general de este estado (control de doble pago y proceso sonda)

6. Webhook o notificación (Opcional)

- **El comercio nos debe proporcionar una URL/URI expuesta públicamente en donde se realizará un llamado por medio de un POST con la siguiente estructura JSON:**
- **El comercio debe escuchar el request enviado en donde se notificará de manera asíncrona las transacciones realizadas. Se relaciona documentación: https://docs.placetopay.dev/checkout/notification**

7. 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 cinco (5) 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. (opcional)
- Estado de la transacción.
- Valor (debe estar concatenado con el tipo de moneda según ISO 4217).

Fecha y Hora	Referencia	Estado	Autorización/Cus	valor
31-12-2023 6:50 p.m	ORDEN_521	PENDIENTE	58985	COP $18000
31-12-2023 6:50 p.m	ORDEN_522	APROBADO	58986	USD $200
31-12-2023 6:50 p.m	ORDEN_523	RECHAZADO	58987	COP $8000
31-12-2023 6:50 p.m	ORDEN_524	APROBADO PARCIAL	58988	USD $800

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 la razón o motivo para que sea analizada y dar la excepción sobre este.

8. INICIO DE PAGO Y USO DE IMAGEN CORPORATIVA

Antes de realizar el pago, se debe visualizar un resumen de pago y en este apartado se debe visualizar el logo de Aval Pay, este lo deben tomar de la siguiente ruta: placetopay-static-test-bucket.s3.us-east-2.amazonaws.com/avalpaycenter-com/logos/Logo Avalpay.svg y de los bancos listado en el ítem 3, este lo deben tomar de la guía de estilos alojada en ese enlace AvalPay
Antes de efectuar la operación, el usuario debe aceptar la política de tratamiento de datos de su establecimiento comercial.
El sitio únicamente debe realizar venta de productos y/o servicios relacionados a las actividades comerciales establecidas al inicio de la negociación, en caso de ser evidenciado actividades comerciales no permitidas por Aval Pay el sitio no será certificado.

9. RECOMENDACIONES PARA LA IMPLEMENTACIÓN

1. PREGUNTAS FRECUENTES Y TERMINOS Y CONDICIONES

Se debe contar con un apartado en el aplicativo, el cual contenga las preguntas frecuentes sobre un proceso de pago, Aval Pay comparte una guía de estas.

El usuario debe aceptar los términos y condiciones antes de ser redireccionado a la pasarela de pagos o debe brindarle la opción de visualizarlo en un apartado del aplicativo.

2. CREDENCIALES DE CONEXIÓN

- Los datos de configuración de conexión de Aval Pay (Login y SecretKey) deben ser almacenados como parámetros ya sea en la base de datos o en algún archivo .ini, .json, xml, etc.

10. CONSIDERACIONES FINALES

Para el proceso de certificación se debe de enviar la información al analista asignado de Aval Pay 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.
- Todos los métodos que se generan y la información que viaja en cada uno de estos, se explica más a detalle en el siguiente enlace: https://docs.placetopay.dev/gateway

GUIA DE CERTIFICACIÓN TARJETA DE CREDITO

Una vez realizada la integración con Aval Pay 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:

1. 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 dichos impuestos de los productos en la transacción. Se debe enviar la base, el tipo de impuesto y el valor del impuesto.

En caso de enviarse se valida que el comercio incluya dichos valores correspondientes dentro de la solicitud de pago, el request enviado, el desglose de IMPUESTOS, donde se le debe mostrar al usuario.

Para hace uso de este deben enviarse cada tipo de impuesto según lo descrita la documentación https://docs.placetopay.dev/gateway/api/reference/transaction#process-request

2. PROCESAMIENTO TRANSACCIONAL

2.1. Control del botón de redirección

Para este ítem se evaluará que al momento que el usuario de varias veces clic al botón para proceder a pagar, solo se realice una petición al servicio esto con el fin de evitar que se creen dobles peticiones, que pueden llegar a generar confusión

2.2. Validación campos:

- El Código de Referencia tiene una longitud máxima de 32 caracteres.
- El Código de Referencia es alfanumérico.
- Para una transacción con estado Aprobado, la referencia usada no puede repetirse.

Se debe solicitar al usuario los siguientes campos para enviar como pagador y comprador: nombres, apellidos, email, teléfono, dirección.

- El campo nombre no permite caracteres especiales o números a excepción de la tilde o la Ñ.
- Para el documento se debe seguir el siguiente patrón de validación, que compartimos en la documentación. Tipos de documento - Placetopay Docs
- El campo email debe contener la estructura de un email válido, en caso de que el campo no contenga una estructura valida, se debe alertar al usuario.
- La dirección IP debe ser la del equipo del usuario final.
- El agente de navegación debe tomarse con una propiedad dependiendo del lenguaje de programación.

En el proceso de pago 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 Aval Pay, para que la información que se envié en estos campos sea consistente y correcta se debe hacer de la siguiente forma:

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 comprador y dejar que Aval Pay solicite los datos del titular.

3. VALIDACION ALGORITMO LUHN, VALIDACION CVV.

El sistema debe validar que el número de tarjeta ingresado cumpla con el algoritmo de Luhn. Este algoritmo es utilizado para verificar la autenticidad del número de tarjeta de crédito o débito.

Requisitos:

- Al ingresar un número de tarjeta, el sistema debe ejecutar la validación con el algoritmo de Luhn.
- Si el número no es válido según el algoritmo, el sistema debe impedir que el usuario continúe con la operación.

- Si el número es válido, el sistema debe identificar y mostrar la marca de la tarjeta (Visa, Mastercard, etc.), ya sea visualmente o reflejada en el váucher de la transacción (opcional).

Validación de CVV

El sistema debe validar que el código CVV ingresado cumpla con los siguientes criterios:

- Solo se aceptan caracteres numéricos.
- El campo debe estar configurado como tipo "password" para ocultar los valores ingresados.

Requisitos:

- El sistema debe restringir el ingreso de caracteres no numéricos en el campo CVV.
- El campo debe mostrarse como un campo de contraseña (ocultando los caracteres ingresados).
- Si el usuario intenta ingresar caracteres no permitidos, se debe mostrar un mensaje de error.

4. PROCESAMIENTO DE LA INFORMACIÓN

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

- Número de tarjeta
- CVV
- Fecha de Vencimiento
- Valor Total
- Moneda
- Referencia
- Descripción
- Impuesto (opcional)
- Base de Devolución (Opcional si no se usan impuestos)
- Información del usuario
- Información de los protocolos de seguridad

5. COHERENCIA DE LA INFORMACIÓN

La información enviada a Aval Pay 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 Aval Pay 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 Aval Pay.

6. MANEJO DE RESPUESTAS PARA ESTADOS TRANSACCIONALES

Al momento que el usuario culmine su proceso de pago ya sea Aprobado, Rechazado o Pendiente, se debe mostrar el detalle de la transacción, como recomendación deben visualizarse los siguientes datos:

- Referencia.
- Estado final de transacción
  - Aprobado
  - Rechazado
  - Pendiente
  - Fallido
- Fecha y hora.
- Valor total.
- Moneda con la cual se realizó el pago.

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).

7. CONTROL TRANSACCIÓN PENDIENTE

Se puede visualizar una transacción en estado pendiente por los siguientes motivos:

Por respuesta directa de la entidad financiera o la no recepción de respuesta por parte de Aval Pay.

El segundo caso ocurre cuando el usuario final al seleccionar pagar es redireccionado a la plataforma de pago, en ese momento en la base de datos del comercio se marca la transacción con estado pendiente, con el fin de esperar un resultado final al terminar el proceso transaccional. Cuando el usuario culmina el proceso, la plataforma de pago no obtiene el estado final de la transacción, por lo cual, se debe ejecutar la operación para obtener la información del pago realizado.

Se cuenta con dos formas para obtener el estado final de una transacción, mediante la URL de notificación (webhook) y la sonda o tarea programada (cronjob):

7.1. CONTROL DE DOBLE PAGO:

Cuando el usuario intente realizar una transacción y cuenta con una operación en estado pendiente debe presentarse un mensaje informativo que permita identificar que se tiene una transacción pendiente, su referencia y datos de contacto del establecimiento comercial, a continuación, compartimos una estructura de ejemplo, en la cual se podrían basar para construir este:

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>***.

7.2. URL DE NOTIFICACIÓN

Este proceso tiene la finalidad de informar a su sistema cuando las transacciones cambian de estado pendiente a un estado final. La url de notificación es configurada por el comercio en los puertos 80 o 443 y debe estar programada para recibir una petición tipo POST por parte de Aval Pay, tiene una estructura similar a la siguiente:


```
{
  "status": {
    "status": "APPROVED",
    "reason": "00",
    "message": "Aprobada",
    "date": "2024-07-11T15:22:37-05:00"
  },
  "internalReference": 1,
  "reference": "5834381",
  "signature": "9c0f8ff164d0af4a795f71ee127d8926f56d05fb"
}
```


En ella se suministra el internal reference, la referencia proporcionada por el comercio y el estado de la petición que puede ser (APPROVED, REJECTED) para esta notificación.

7.3. CRONJOB O SONDA

Este proceso es una contingencia a la url de notificación, para esto se debe implementar un cronjob o tarea programada, donde en caso de mantener un estado PENDIENTE mediante el método **query** con la referencia interna se realiza la consulta y como última opción en caso de pérdida de comunicación al crear la transacción con el **processtransaction** a través del servicio de search el cual es una contingencia

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 Aval Pay (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)

Nota: 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 12 horas verificando las transacciones que tengan en estado pendiente.

8. 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 cinco (5) 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).

FECHA Y HORA	REFERENCIA	ESTADO	AUTORIZACIÓN/CUS	VALOR
31/01/2022 6:50 p. m.	ORDEN_515	PENDIENTE	5555	USD $200
31/01/2022 1:00 p. m.	ORDEN_501	APROBADO	5439	USD $289
30/01/2022 10:59 a. m.	ORDEN_459	RECHAZADO	5276	USD $76
29/01/2022 3:05 p. m.	ORDEN_420	APROBADO PARCIAL	5002	USD $526

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 Aval Pay, la razón o motivo para que sea analizada y dar la excepción sobre este.

9. GENERACIÓN Y VALIDACIÓN DE 3DS

En caso de contratar el servicio 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 **Solicitud de información**:

Una vez el usuario retorna de la validación se debe consultar la información de la autenticación mediante el **3DSquery,** 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: Placetopay Docs

10. CONTROL DE IDEMPOTENCIA

La validación para evitar transacciones duplicadas debe realizarse durante el Flujo del Proceso de Pago. El keyword de Idempotencia “IdempotenceKey”, es un valor único definido por el comercio para cada transacción, debe enviarse dentro de la Solicitud de Pago.

{

...

"idempotenceKey": "ABCD1234",

"instrument": {

...

}

Para más detalles por favor basarse en la documentación oficial: Control de Idempotencia - Placetopay Docs

NOTA: El Comercio generará y enviará el Parámetro IdempotenceKey con un valor único basado en la Lógica de Negocio del Comercio, para cada transacción. El sistema impedirá que se procesen transacciones con la misma IdempotenceKey.

11. 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.

12. 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"
   },
…
```

13. REVERSO & REEMBOLSO DE TRANSACCIONES

13.1. REVERSO

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 Aval Pay, 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: El reverso solo será posible antes de la hora de conciliación, en caso tal se requiera realizar este proceso posterior a la hora definida, se debe de realizar un reverso extemporaneo, de la misma forma se debe de informar si los reversos se realizaran mediante la API o mediante la consola administrativa.

13.2. REVERSO EXTEMPORÁNEO

El reverso solo será posible antes de la hora de conciliación la cual es a las 8 de la noche hora Colombia, en caso tal se requiera realizar este proceso posterior a la hora definida, se debe de realizar un reverso extemporáneo con la red procesadora.

14. FUNCIONALIDAD DE SUSCRIPCION/TOKENIZACIÓN

Para integrar la funcionalidad de pago suscripción es importante tener en cuenta los siguientes puntos adicionales a los anteriores ya mencionados en este documento:

TIPO DE FLUJO TRANSACCIONAL

En la guía de certificación de tokenización, se describen varios flujos de pago que garantizan la seguridad y comodidad de las transacciones. A continuación, se presentan los principales escenarios:

14.1. SUSCRIPCIÓN RECURRENTE (Cobro Sin Presencia del Usuario)

A continuación, se explican cada uno de los escenarios por el cual se presenta este escenario:

- El usuario no está presente en cada transacción:
- Primera transacción y almacenamiento del token: En la primera transacción, se solicita información de la tarjeta y se almacena el token generado.
- Cobros: Para cada cobro subsecuente, el comerciante utiliza el token almacenado en lugar de los datos de la tarjeta.
- Solicitud de autorización: El token es enviado al procesador de pagos, que a su vez solicita la autorización al banco emisor.
- Autorización y confirmación: El banco valida y autoriza la transacción, devolviendo la confirmación al comerciante.

- Notificación al usuario: El usuario es notificado del cobro, generalmente a través de un correo electrónico o notificación en la app del servicio.

14.2. TRANSACCIÓN CON PAGO A UN CLIC

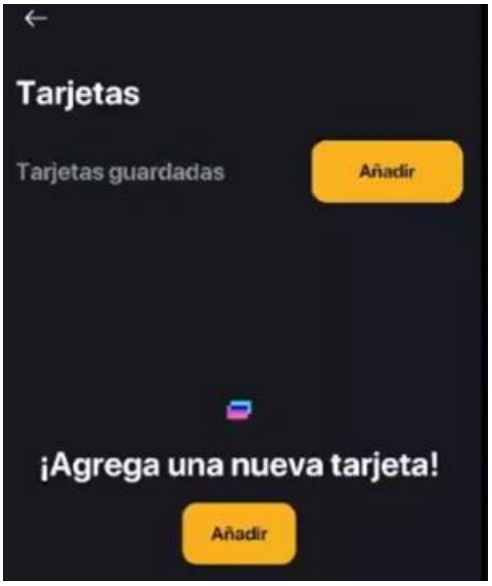
- A continuación, se explican cada uno de los escenarios por el cual se presenta este escenario:
- El usuario dispone de una billetera digital donde en cliente selecciona la tarjeta tokenizada con la que desea realizar la transacción
- Usuario selecciona método de pago: El usuario elige una tarjeta almacenada en la billetera digital para realizar la compra.
- Autorización de la transacción: El token es enviado al banco emisor para la validación. autoriza la transacción.
- Confirmación y notificación: El resultado de la autorización se devuelve al comerciante, quien completa la transacción y notifica al usuario

14.3. PROCESO DE PAGO

El sistema le debe permitir al usuario comprador, visualizar el monto total a pagar antes de que se vaya a generar un cobro inmediato sobre el servicio, este valor debe de coincidir con el valor enviado a Aval Pay.

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

En caso de que la experiencia de pago sea pago a un clic, es decir, se tokeniza la tarjeta y ésta quede habilitada para el usuario en caso de un próximo cobro o exista un baúl para gestionar los medios de pago, la instrucción o descripción en el proceso de inscripción de las tarjetas debe ser específico de cara al usuario haciendo alusión que la tarjeta será almacenada, por ejemplo: agregar tarjeta, mis tarjetas, mis medios de pago, mi billetera.



El sistema debe ser independiente al momento de actualizar el estado de una Suscripción (Tokenización) cuando el usuario realiza el flujo de tokenización debe hacerse un consumo al método query para conocer el estado de la tokenización, de acuerdo a lo anterior en el momento que se brinda un estado de la Suscripción(Tokenización) y se actualiza el estado en el sistema del comercio, se debe hacer de forma general en BD manteniendo la trazabilidad acorde al estado dado por Aval Pay.

Para el caso de los cobros mediante el token una vez se realiza la petición hacia Aval Pay. Se responde inmediatamente con la información de la transacción, de este modo siempre que el estado sea diferente de PENDIENTE no debe volverse a consultar a Aval Pay sino tomar inmediatamente el estado y actualizarlo en el sistema del comercio, de forma general en BD manteniendo la trazabilidad acorde al estado dado por Aval Pay.

Nota: Tener en cuenta que en la sonda (Cronjob) y notificación Webhook) únicamente se debe depender de ellos cuando la transacción se encuentra bajo estado PENDIENTE, de lo contrario siempre que haya un estado final APROBADO o RECHAZADO, el sistema debe hacer la actualización de acuerdo con lo especificado en el párrafo anterior

14.4. CAMPOS ENVIADOS EN EL PROCESAMIENTO CON EL COLLECT

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

Datos del pagador(payer):

- Tipo de documento.
- Número de documento.
- Nombre del pagador.
- Apellido del pagador.
- Email del pagador.
- Teléfono celular del pagador.

Datos del pago(payment):

- Referencia
- Descripción
- Moneda
- Valor.
- IVA (opcional)

- Base de devolución (opcional)
- Dispersión (En caso de habilitar el servicio)
    - Convenio
    - Tipo de convenio
    - Moneda
    - Total

Instrument

- token
- Token/Subtoken

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: PlacetoPay Checkout - Placetopay Docs

14.5. INVALIDACIÓN Y ELIMINACIÓN DE TOKEN

En este punto se evalúa el servicio de inhabilitar token, esto permite realizar la invalidación de un token almacenado con el fin de no ser más utilizado a nivel transaccional.

Es necesario implementar un control de rechazos para garantizar que, si el mensaje de la transacción indica que fue rechazada por razones como robo o BIN bloqueado, el token sea invalidado de inmediato.

Si el mensaje recibido corresponde a otras razones, como fondos insuficientes, se permitirá un máximo de tres intentos de cobro antes de proceder con la invalidación del token. En caso de no aplicar lo anteriormente mencionado la pasarela de pagos no se hará responsable de multas o sanciones impuestas por las marcas.

- Respuestas invalidación inmediata:
- Negada, Tarjeta vencida con orden de retención
- Negada, Tarjeta bloqueada o cancelada
- Negada, Tarjeta vencida
- Tarjeta robada
- Negada, Tarjeta inválida
- Tarjeta perdida
- Negada, La tarjeta está bloqueada en el archivo de tarjetas de uso restringido
- Tipo de tarjeta inválida

https://docs.placetopay.dev/gateway/api/reference/tokenize#tokenize-invalidate-request

Nota: En caso de no aplicar el máximo intento de cobro o inactivar ese servicio en entorno productivo, la pasarela de pago no se hace responsable de multas, sanciones que las marcas puedan imponer al comercio.

15. FUNCIONALIDAD DISPERSION DE FONDOS

Para integrar la funcionalidad de pago con dispersión de fondos es importante tener en cuenta los siguientes puntos adicionales a los anteriores ya mencionados en este documento y recordar que solo se pueden hacer 3 dispersiones contando al sitio autenticado:

15.1. MANEJO DE ESTADOS PARCIALMENTE APROBADOS.

Al momento que un usuario realice un flujo transaccional pero no pague el valor completo del producto o servicio, el servicio de Placetopay al momento de consultar la transacción con dicho escenario devolverá el siguiente estado:
APPROVED_PARTIAL, PARTIAL_EXPIRED.

15.2. CONTROL TRANSACCION APROBADA PARCIALMENTE.

Se debe de implementar un control cuando la transacción queda en un estado parcialmente aprobada, lo cual quiere decir que un monto fue recaudado exitosamente resta el faltante, para esto el comercio debe definir el flujo para recaudar el dinero restante o realizar el proceso de devolución del dinero recaudado.

15.3. CONTROL RECHAZO POR FLUJO TRANSACCIONAL

Al momento de que el usuario realice una transacción de dispersión, existe un escenario en el cual las transacciones, una de este rechace al momento del cobro, por lo cual al momento de consultar la sesión de pago. En el array Payments solo devolverá el objeto de pago hasta donde se procesó, es decir si se realiza una dispersión de 3 sitios y la transacción se rechaza al momento de hacer el segundo cobro, en el array Payments solo devolverá dos objetos de pago los cuales fueron los que se realizaron.

15.4. REVERSO TRANSACCIONAL

Cuando la dispersión adopta un flujo de **parcialmente expirado**, el sistema de la pasarela de pagos ejecuta un proceso de reversión de las transacciones aprobadas. Esto permite que el comercio pueda reiniciar el flujo transaccional completo.

Es importante tener en cuenta que el proceso de reversión podría quedar en estado **rechazado**. En ese caso, será responsabilidad del comercio gestionar nuevamente la reversión de la(s) transacción(es) afectada(s).

16. FUNCIONALIDAD RECURRENCIA

Para integrar la funcionalidad de pago con recurrencia es importante tener en cuenta los siguientes puntos adicionales a los anteriores ya mencionados en este documento:

16.1. NOTIFICACIÓN

Al momento de enviar el campo“notificationUrl”, la estructura del request de la notificación cambia ya que este se notificara cuando se realicen los pagos posteriores al primer cobro, es decir cuando la recurrencia empiece a ejecutarse.

La estructura es la siguiente:


```
{
  "status": {
    "status": "APPROVED",
    "reason": "00",
    "message": "Transacción aprobada",
    "date": "2019-01-01T12:00:00-05:00"
  },
  "internalReference": 1598634446,
  "reference": "564555",
  "signature": "a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7r8s",
  "recurring": {
     "tries": 2,
     "enabled": 0
  }
}
```

16.2. VALIDACION ENVIO DE RECURRENCIA

Se debe de validar al momento de crear la petición de pago que los datos de periodicidad (Dia, Mes, Año), intervalo (cada tiempo de ejecución), máximo de periodos (cantidad máxima de cobros), fecha de próximo pago, fecha de finalización.

Doc: https://docs.placetopay.dev/checkout/create-session#recurring-payment
Nota: Tener presente para cancelar la recurrencia se debe realizar desde el panel administrativo, no es posible modificar el valor de la recurrencia o su periodicidad luego de la creación de la recurrencia.

17. RECOMENDACIONES A IMPLEMENTAR

17.1. REQUISITOS DE SEGURIDAD

Los datos de configuración de la conexión de Aval Pay 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.

17.2. PREGUNTAS FRECUENTES, TERMINOS, CONDICIONES Y POLÍTICAS DE PRIVACIDAD

Se debe incluir dentro de un apartado del sitio, una sección de Preguntas Frecuentes (FAQ) y mencionar los pagos a través de Aval Pay. 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, adicionalmente estas preguntas frecuentes se compartirán al inicio de la integración.

Para garantizar la transparencia y el cumplimiento de las normativas aplicables, el comercio debe establecer Términos y Condiciones claros y una política de gestión de información del usuario accesible adicionalmente estos de deben añadir en un apartado por ejemplo en el pie de página, etc... Estos deben cumplir con los siguientes lineamientos:

- Los T&C deben ser visibles para el usuario antes de procesar el pago.
- El comercio debe permitir al usuario consultar y aceptar las condiciones generales de manera explícita antes de finalizar la compra.
- El comercio es responsable de definir los términos y condiciones generales que regulen sus operaciones.

17.3. LOGOS DE AVAL PAY

El sistema donde se realizó la integración debe de mostrar al usuario el logo de Aval Pay, este logo se puede tomar de alguna de las siguientes URL's:

- https://placetopay-static-test-bucket.s3.us-east-2.amazonaws.com/avalpaycenter-com/logos/Logo Avalpay.svg

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.

18. INFORMACIÓN RELEVANTE

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 Aval Pay 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.

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: Números de tarjeta de pruebas - Placetopay Docs

Nota: Para todas las franquicias:

- Código de verificación: 123
- Fecha de vencimiento de la tarjeta: Seleccione una fecha vigente