

Documento de Integración
Formulario "Pago Web"

Índice

1. Introducción
2. Objetivo
3. Beneficios del nuevo formulario
4. Definiciones
5. Características de la tienda virtual
 - a. Requisitos obligatorios
 - b. Recomendaciones
6. Guía de uso e implementación de logos Visa y Verified by Visa
7. Integración
 - a. Consideraciones
 - b. Implementación
 - i. Crear un token de seguridad
 - ii. Crear una sesión de comunicación
 - iii. Configurar el botón de pago
 - iv. Concretar transacción
 - v. Comportamiento del formulario
 - vi. Integración, certificación y salida a producción
8. Botón “Pagar”
 - a. Botones VisaNet
 - b. Colocación del botón en la tienda virtual
9. Anexos
 - a. Códigos ECI
 - b. Códigos de acción (denegaciones)
 - c. Transición de estados para una venta
 - d. API de autorización de venta
 - e. API de anulación de venta
 - f. API de confirmación de venta
 - g. API de consulta de venta
 - h. API de antifraude para la venta

Integración del formulario web VisaNet

1. Introducción

El proceso de afiliación a Comercio Electrónico tiene una serie de etapas por las cuales debe pasar todo comercio, en el orden indicado, sin excepción alguna y cumpliendo con los requisitos que conlleva cada una de ellas.

El proceso es el siguiente:

- a) Creación de código VisaNet
- b) Integración
- c) Certificación
- d) Pase a producción

2. Objetivo

Este documento tiene como objetivo dar lineamientos generales, a los comercios y/o a los proveedores encargados del desarrollo web, para la integración y adecuación de las páginas web o tiendas virtuales de los comercios afiliados al servicio de Comercio Electrónico.

3. Beneficios del formulario de pagos VisaNet

El formulario de VisaNet simplifica y asegura los pagos online con los siguientes beneficios:

- Sin re direccionamiento hacia una nueva página
- Personalizable con el logo (imagen y texto) y color del botón “Pagar”
- Permite la tokenización de tarjetas para compras frecuentes
- Garantía de transacciones seguras con la plataforma antifraude Cybersource
- Adaptable a PC, Tablet y Móviles

El comercio podrá integrar rápidamente este formulario a su tienda virtual y brindar una experiencia fácil, rápida y segura a sus clientes.

4. Definiciones

- **Integración:** Adecuaciones de la plataforma, web o móvil, del comercio para conectar la pasarela de pagos de VisaNet.
- **Página Inicial:** Página principal de la web del comercio.
- **Página de Pagos:** Sección de la plataforma, web o móvil, del comercio en la que será exhibido el formulario de pagos que conecta con la pasarela de pagos de VisaNet.
- **Tarjetahabiente:** Persona titular de una tarjeta, en este caso, de la marca VISA.
- **Tienda Virtual:** Aplicación web o móvil desde la cual los clientes pueden adquirir productos o contratar los servicios ofrecidos por el comercio a través de un carrito de compras.
- **TLS (Transport Layer Security):** Es un protocolo de seguridad que utilizan los navegadores web y los servidores web para ayudar a los usuarios a proteger la transferencia de sus datos. Se debe considerar utilizar la versión de TLS 1.2
- **CIP:** Es un código de 8 dígitos que le sirve a tu cliente para la identificación de su pago.

5. Características de la tienda virtual

Los puntos presentados en esta sección se encuentran divididos en “Requisitos Obligatorios” y “Recomendaciones”.

Los requisitos obligatorios deben encontrarse necesariamente implementados en la tienda virtual del comercio ya que serán revisados por VisaNet Perú a lo largo del proceso de Integración y su implementación y cumplimiento son estrictamente necesarios pues condicionan el pase a producción del comercio y por consiguiente la certificación. Adicionalmente VisaNet podrá revisar en cualquier momento, mientras el comercio siga afiliado al servicio de Comercio Electrónico, que dichos requisitos se sigan cumpliendo.

Las recomendaciones permiten utilizar el servicio con mayor seguridad y eficiencia tanto para el comercio como para los tarjetahabientes que requieran realizar compras a través de la tienda virtual por lo que se recomienda sean implementados.

a. Requisitos obligatorios

A. Página Inicial (Home):

- Se debe colocar el logo de Visa según lo especificado en el punto [6. Guía de uso e implementación de los logos de Visa para comercios virtuales.](#)
- Se debe colocar el siguiente texto: esta tienda está autorizada por Visa para realizar transacciones electrónicas.

B. Página de Pagos (Checkout – Medios de pago):

- Se debe colocar sólo el logo de Visa según lo especificado en el punto [6. Guía de uso e implementación de los logos de Visa para comercios virtuales.](#)
- El país del local del comercio, de manera clara y prominente, en cualquiera de las siguientes:
 - En la misma pantalla de pago utilizada para presentar el monto final de transacción.
 - Dentro de la secuencia de páginas a las que el tarjetahabiente accede durante el proceso de checkout.

C. Sección “Contáctenos”:

- La tienda virtual deberá contar con una sección “Contáctenos” donde indique una dirección de correo electrónico, el teléfono y/o fax y la dirección física del comercio la cual debe incluir la ciudad y el país de ubicación.

D. Sección “Regístrese”:

- Se recomienda que la tienda virtual cuente con una sección “Regístrese” desde la cual los clientes del comercio (tarjetahabientes) se puedan registrar para poder realizar compras en la tienda virtual. Los datos que se deben solicitar al tarjetahabiente como mínimo son los siguientes:
 - Nombre y apellidos
 - Tipo de documento (DNI, carnet de extranjería, pasaporte, etc.)
 - Número de documento
 - Correo electrónico
 - Teléfono o fax (opcional)
 - Usuario y contraseña de registro

E. Enlaces

- La tienda virtual debe estar libre, en su totalidad, de enlaces (links) que direccionen a webs que promocionen, comercialicen o muestren contenido relacionado a los giros prohibidos por VisaNet y la marca Visa que se podrán encontrar en la “Adenda al Contrato de Afiliación al Sistema VisaNet Perú para Comercio Electrónico” publicada en www.visanet.com.pe.

F. No diferenciación entre medios de pago.

- La marca VISA, sus logos y la indicación de poder pagar con medios de pago VISA no deben tener menor prominencia que otras marcas o medios de pago.
- Las tarjetas VISA no deben diferenciarse ni clasificarse en el flujo de pago. Es decir para el flujo de pago no deben existir pasos diferentes para tarjetas de débito, crédito o prepagadas de la marca VISA tal y como se muestra en la figura 1.

Figura 1. Error de diferenciación entre tipo de tarjetas.



G. Certificado SSL

- El comercio debe contar con un certificado SSL de un mínimo de 256 bits el cual debe estar vigente durante toda la permanencia del comercio en el sistema VisaNet.

H. Términos y Condiciones¹:

- El comercio debe definir y notificar los términos y condiciones de compra a través de la tienda virtual. La política debe contener como mínimo los siguientes puntos:
 - Descripción general de los bienes y/o servicios comercializados.
 - Políticas de entrega, las cuales deben contener información sobre lo siguiente (si aplica):
 - ✓ Plazos de entrega
 - ✓ Horarios de entrega
 - ✓ Cobertura de la entrega
 - ✓ Medios de entrega (descripción del medio y forma por el cual se entregará la mercadería o se brindará el servicio)
 - ✓ Modo de confirmación de la entrega
 - ✓ Costos relacionados a la entrega
 - Políticas relacionadas a la devolución, reembolso y cancelación de los productos o servicios adquiridos:
 - ✓ Políticas de cambios. Cuándo aplican, condiciones, plazos, etc.
 - ✓ Políticas de cancelación. Declaración si se aceptan devoluciones de mercadería o cancelaciones de servicios y bajo qué condiciones y plazos.
 - ✓ Los cuales deberán colocarse:
 - En la secuencia de las páginas finales antes del checkout, un “clic para aceptar” u otro botón de aceptación, casilla, o lugar para una firma electrónica.
 - En la pantalla de salida cerca del botón “Enviar”

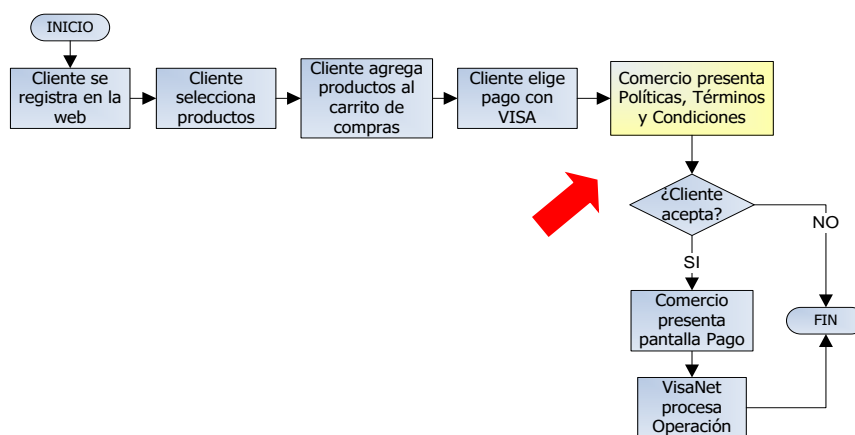
¹ Los Términos y Condiciones se incluyen dentro del proceso de compra debido a que es el estándar de la marca Visa a nivel internacional. De esta manera, se evita un desconocimiento por parte del cliente de los criterios de venta y de devolución establecidos por el comercio.

- Un enlace a una página web separada no cumple con este requerimiento.
- Políticas de recepción de reclamos.
 - ✓ Descripción del procedimiento que deben seguir aquellos clientes que quieran presentar un reclamo relacionado al servicio.
- Políticas de entrega de múltiples envíos
- Políticas de privacidad de la información del consumidor.
- Restricciones
 - ✓ Restricciones de exportación (si se conocen).
 - ✓ Restricciones legales (si se conocen).
 - ✓ Otras restricciones aplicables.
- Datos de contacto del comercio (los mismos incluidos en la sección “Contáctenos”).
- Verificación de Mayoría de Edad.
 - ✓ Incluir términos de aceptación del tarjetahabiente (checkbox) en la tienda virtual indicando que es mayor de edad (mayor a 18 años) en el momento de la compra aquellos comercios que vendan los siguientes productos:
 - Bebidas alcohólicas
 - Cigarrillos
 - Material con contenido para adultos
 - Juegos en línea
 - Armas

Importante:

- Los Términos y Condiciones de la compra deben mostrarse en la misma pantalla que se utiliza para presentar el monto total de la compra (o dentro de la secuencia de páginas web a las cuales ha tenido acceso el cliente antes de ingresar los datos del medio de pago en el formulario correspondiente del proceso de pago) con un botón de aceptación (vistobueno), que confirme la lectura y aceptación de los términos y condiciones, antes de concluir la compra. En la figura 2 se muestra un esquema como ejemplo considerando la integración a una Página Web.

Figura 2: Ejemplo de ubicación de los Términos y Condiciones dentro del flujo de pago



- Se deberá incluir los términos y condiciones, es decir; las políticas de venta y cancelación, las mismas que deberán publicarse en Inglés y Español.

- Los términos y condiciones deberán mostrarse como parte del proceso de compra (un link no es válido).
- Para seguridad y control; el ticket de la compra (boleta electrónica o detalle) deberá ser enviado al e-mail que el cliente proporcionó en su registro, además se recomienda validar la confirmación de la recepción del mismo.

b. Recomendaciones

La falta de interacción física entre vendedor y comprador en una tienda online hace que aumenten las posibilidades de que se genere una transacción fraudulenta. No se puede examinar la tarjeta de crédito del cliente físicamente para asegurarse que es válida, ni se puede pedir la identificación para comprobar la identidad del titular de la tarjeta. Afortunadamente, existen excelentes herramientas para superar estos y otros obstáculos, previniendo así los efectos perniciosos de los fraudes para su negocio online. Si va a vender por canales virtuales, es imprescindible que cuente con una herramienta de calificación de transacciones, que podrá ser de VisaNet o propia. Si es una herramienta propia deberá ser previamente aprobada por el área de Prevención de Fraudes de VisaNet.

Es recomendable que la tienda virtual cuente con los puntos indicados en esta sección ya que esto permitirá que se reduzcan las posibilidades de fraudes y/o controversias.

A. Seguimiento de la Entrega:

- Es recomendable que todas las empresas que realizan comercio electrónico y cuyo giro de negocio implique la posterior entrega de un producto o prestación de un servicio, brinden información que permita a los tarjetahabientes realizar el seguimiento a la entrega y conocer el estado de su pedido.
- Este sistema de monitoreo puede realizarse a través de un operador logístico, pero en la tienda virtual se debe especificar cómo acceder al sistema de monitoreo.
- Este sistema de monitoreo en línea debería ofrecer la siguiente información básica (cuando aplique):
 - Orden de compra:
 - ✓ Fecha de la compra
 - ✓ Nombre del cliente
 - ✓ Dirección del cliente
 - ✓ Dirección de entrega
 - ✓ Detalle de la compra
 - Despacho y entrega:
 - ✓ Fecha de despacho.
 - ✓ Medio utilizado para el despacho.
 - ✓ Datos sobre la unidad de despacho (tipo de unidad, marca, modelo, número de placa).
 - ✓ Fecha estimada de la entrega.
 - ✓ Nombre del chofer y documento de identidad de la persona encargada de la entrega.
 - ✓ Número de guía de entrega.
 - Estado del pedido:
 - ✓ Se debe indicar en qué parte del proceso de despacho y entrega se encuentra el pedido del tarjetahabiente.

- Entregar siempre la mercadería en un domicilio y oficina. Nunca entregarlo en la calle.
- Conservar siempre la guía de entrega de los productos debidamente firmada

B. Características del Carrito de Compras:

- Producto seleccionado
- Cantidad
- Monto y Moneda
- Cálculo del IGV (si es necesario)
- Cálculo del Flete (si es necesario)
- Cálculo de cambio de moneda (si es necesario)
- Opción de Seguir Comprando
- Opción de Eliminar

C. Medidas de Seguridad adicionales

- En el sistema de registro:
 - Se sugiere que el cliente complete siempre un formulario de registro.
 - Crear validaciones, como por ejemplo, no permitir el mismo correo electrónico para diferentes usuarios.
 - Confirmar la existencia del correo electrónico previamente a la aceptación del registro del tarjetahabiente. Por ejemplo, enviar un mail al correo electrónico informado en el formulario de registro para que el tarjetahabiente confirme sus datos y registro.
 - De ser factible, validar los datos del comprador. Por ejemplo: número de teléfono del comprador incluyendo el código de ciudad / dirección de entrega (distrito / provincia) incluyendo el código postal.
- En el proceso de compra:
 - Utilizar correos electrónicos de confirmación de la compra solicitada por el cliente. Es decir, obligar al tarjetahabiente a ingresar al correo electrónico para confirmar el pedido (digitar una palabra clave, seguir un link de confirmación, etc.).
 - Identificar y notificar a quien corresponda (VisaNet) para evaluar compras inusuales o sin comportamiento lógico, tales como:
 - ✓ Compras por grandes cantidades (artículos-productos y montos).
 - ✓ Múltiples transacciones del mismo cliente y con una misma tarjeta enmascarada.
 - ✓ Múltiples transacciones con una misma tarjeta enmascarada y diferentes clientes.
 - ✓ Múltiples transacciones con un mismo cliente con diferentes tarjetas enmascaradas.
 - ✓ Compras realizadas en horas inusuales, por ejemplo, en la madrugada.
 - ✓ Solicitud de múltiples entregas en una misma dirección de entrega.
 - ✓ Múltiples transacciones con una sola dirección de facturación y diferentes direcciones de entrega.
 - ✓ Múltiples transacciones con una misma dirección IP (ya sea con una misma tarjeta o diferentes tarjetas).
- Post venta:
 - Mantener un registro de operaciones fraudulentas o altamente sospechosas.
 - Solicitar a VisaNet capacitación en seguridad para su personal.

6. Guía de uso e implementación de logos Visa y Verified by Visa

- Los logos oficiales de la marca Visa y Verified by Visa deben ser descargados desde página web de VisaNet www.visanet.com.pe.
- Los logos Visa o alguna porción de éstos; nunca deben ocultarse, distorsionarse, desfigurarse ni alterarse de manera alguna, ni aparecer con menor prominencia que otras marcas de medios de pagos.
- El nombre la marca Visa como texto tiene que utilizarse para indicar la aceptación (en la página de checkout) solamente cuando no sea posible utilizar una representación visual del logotipo de la marca en la tienda virtual.
- Los comercios afiliados no podrán usar las marcas ni logos propiedad de Visa de una manera que pudiera perjudicar la reputación de Visa Inc., VisaNet del Perú o cualquiera de sus afiliadas y de las Marcas Propiedad de Visa.
- Los comercios que no cumplan con los requisitos para la implementación y uso de los logos Visa no podrán completar la integración ni ser pasados a producción.
- VisaNet del Perú podrá revisar periódicamente el cumplimiento de los lineamientos para la implementación de logos.

7. Integración

El proceso de integración consta principalmente de cuatro pasos:

1. Crear un token de seguridad.
2. Crear una sesión de comunicación.
3. Configurar el Botón de Pago.
4. Solicitar autorización de transacción.

a. Consideraciones

- El comercio afiliado recibirá un **Usuario** y una **Contraseña** para poder invocar al API de Seguridad para la creación del token. Además, es importante mencionar que el comercio es responsable de custodiar dichas credenciales y estas nos deben estar dentro del código fuente de su aplicación dado que se trata de información sensible.
- El botón de pagos funciona en los siguientes navegadores actualizados al protocolo TLS versión 1.2:
 - IE 11+
 - Chrome 30+
 - Firefox 27+
 - Safari 7+
- El formulario de pagos se adapta a todos los dispositivos móviles (smartphones y tablets) con los siguientes sistemas operativos:
 - Android
 - iOS
- En el botón “Pagar” del formulario de pagos no se debe utilizar un color hexadecimal bajo, dado que el color del texto será siempre blanco.

b. Implementación

i. Paso 1: Crear un token de seguridad

Para poder insertar el botón de pago y el formulario en el web del comercio, por temas de seguridad, es necesario crear un token el cual permitirá la comunicación con las diferentes API. Para ello, será necesario consumir la API de seguridad:

Endpoint para conexión con la API:

Ambiente	URL API de Seguridad
Desarrollo	https://apitestenv.vnforapps.com/api.security/v1/security
Producción	https://apiprod.vnforapps.com/api.security/v1/security

Request

POST <https://apitestenv.vnforapps.com/api.security/v1/security>

HEADER

Authorization: Basic { credenciales }

(*) credenciales = String(GetBytes(Usuario:Password))

Successful Response

STATUS CODE 201 Created

HEADERS

Content-Type: text/plain

{ tokenSeguridad }

Los parámetros de respuesta de la API se explican a continuación:

Parámetro	Descripción
tokenSeguridad	Token generado para invocar a las siguientes APIs

ii. Paso 2: Crear una sesión de comunicación

Previo a invocar al formulario es necesario crear un token de sesión, para esto se debe invocar a la **API de Sesión** de la siguiente manera:

Endpoint para conexión con la API:

Ambiente	URL API de creación de sesión
Desarrollo	https://apitestenv.vnforapps.com/api.ecommerce/v2/ecommerce/token/session/{merchantId}
Producción	https://apiprod.vnforapps.com/api.ecommerce/v2/ecommerce/token/session/{merchantId}

Request

POST <https://apitestenv.vnforapps.com/api.ecommerce/v2/ecommerce/token/session/{merchantId}>

```

HEADER
Content-Type: application/json
Authorization: { tokenSeguridad }

BODY
{
  "amount":{ amount },
  "antifraud":{
    "clientIp":"{ clientIp }",
    "merchantDefineData":{
      "MDD{Nºx}":"{ valMDD }",
      "MDD{Nºx+1}":"{ valMDD }",
      "MDD{Nºx+2}":"{ valMDD }"
    }
  },
  "channel":"{ channel }",
  "recurrenceMaxAmount":{ recurrenceMaxAmount }
}

```

Los parámetros necesarios para la invocación de la API se explican a continuación:

Parámetro	Descripción
merchantId	Código de Comercio, creado al momento de la afiliación al producto Comercio Electrónico Pago Web
tokenSeguridad	Token generado con la API de seguridad en el paso 1
amount	Importe de la transacción Formato #####.## (dos decimales separados por punto) Ejemplo: 1000.00
antifraud	Objeto antifraude
clientIp	Dirección IP del cliente
merchantDefineData	Objeto MDD (Estos valores se deben ingresar para ayudar a la herramienta de prevención de fraude a realizar una mejor calificación a las transacciones)
MDD{Nºx}	MDD número x a registrar en antifraude
MDD{Nºx+1}	MDD número x + 1 a registrar en antifraude
MDD{Nºx+2}	MDD número x + 2 a registrar en antifraude
...	En el objeto MDD se pueden insertar varios MDD
channel	Canal de registro (web, callcenter, recurrent)
recurrenceMaxAmount	Importe máximo del cargo

	Formato #####.## (dos decimales separados por punto) Ejemplo: 1000.00 Es opcional, cuando no que quiere trabajar con este campo se debe enviar null.
--	--

Successful Response

STATUS CODE 200 OK

HEADERS

Content-Type: application/json

BODY

```
{
  "sessionKey": "{ sessionKey }",
  "expirationTime": { expirationTime }
}
```

Los parámetros de respuesta de la API se explican a continuación:

Parámetro	Descripción
sessionKey	Identificador único generado por el sistema
expirationTime	Vigencia de la sesión formato UNIX (30 min)

iii. Paso 3: Configuración del botón de Pago

Para colocar el botón de pago en la página del comercio se requiere configurar múltiples parámetros los cuales se explican en la siguiente tabla.

Campo	Tipo/Valor	Obligatorio	Descripción
FORMULARIO DE PAGOS			
action	URL	Sí	Indica el URL al que debe hacer post el formulario. Ejemplo: https://www.dominio.com/paginaRespuesta
method	"POST"	Sí	Indica el método a utilizar que en este caso debe ser POST
data-sessiontoken	TEXTO	Sí	Identificador único por transacción generado por el sistema (atributo "sessionKey" en respuesta de API de sesión)
data-channel	TEXTO	Sí	Canal de registro
data-merchantid	NUMÉRICO (9 MÁX.)	Sí	Código del comercio, generado durante la afiliación
data-buttonsize	<input checked="" type="checkbox"/> "SMALL" <input checked="" type="checkbox"/> "MEDIUM" <input checked="" type="checkbox"/> "LARGE"		Tamaño del Botón de Pago. Valor por defecto: DEFAULT

	✓ "DEFAULT"		
data-buttoncolor	✓ "NAVY" ✓ "GRAY"		Color del Botón de Pago (Navy = Azul, Gray = Gris). Valor por Defecto: NAVY
data-merchantlogo	URL	Condicional	URL del logo del comercio. Altamente recomendable incluir un logo, caso contrario se mostrará el nombre del comercio. El tamaño sugerido es 187x40px. Nota: Si no inserta este valor, por no contar con una imagen como logo, es obligatorio colocar un texto en el campo "data-merchantname"
data-merchantname	TEXTO	Condicional	Nombre del comercio (se mostrará en caso se omita el logo en el campo data-merchantlogo). La longitud sugerida es de veinticinco caracteres. Nota: Si no inserta este valor es obligatorio colocar la dirección URL de una imagen en el campo: "data- merchantlogo"
data- formbuttoncolor	HEXADECIMAL		Define el color del botón "Pagar" en el formulario. Valor por Defecto: Rojo (#FF0000)
data-showamount	✓ "TRUE" ✓ "FALSE"		Indica si se muestra el monto a pagar en el botón Pagar del formulario. Por defecto: TRUE Por ejemplo: 
data-amount	NUMÉRICO	Sí	Importe a pagar Formato #####.## (dos decimales separados por punto) Ejemplo: 1000.00
data-purchasenum	NUMÉRICO (9 MÁX.)	Sí	Número de Pedido, este valor debe ser creado por el comercio y es único por intento de autorización. La longitud máxima es de nueve caracteres y debe ser de tipo numérico. Por ejemplo: "000000001" o "1"
data-cardholdername	TEXTO		Nombre del cliente. No permite caracteres especiales.
data-cardholderlastname	TEXTO		Apellido del cliente. No permite caracteres especiales
data-cardholderemail	EMAIL		Email del cliente con formato x@x.x por ejmplo: micorreo@mail.com
data-expirationminutes	NUMÉRICO	Sí	Tiempo de duración de la sesión de pago expresado en minutos
data-timeouturl	URL	Sí	Dirección URL de la aplicación del comercio para re dirección en caso de que exista un timeout, durante el pago, en el formulario de VisaNet

TARJETA FRECUENTE			
data-usertoken	TEXTO		Id del token de usuario para recuperar las tarjetas recordadas por el tarjetahabiente
RECURRENCIA			
data-recurrence	TEXTO		Indica si en el registro de la transacción existirá un proceso de recurrencia. Admite los siguientes valores: - TRUE - FALSE
data-recurrencetype	TEXTO		Indica el tipo de recurrencia a mostrar en el formulario de pagos. Admite los siguientes valores: - FIXED - VARIABLE - FIXEDINITIAL - VARIABLEINITIAL
data-recurrencefrequency	TEXTO		Indica la frecuencia para pagos recurrentes. Admite los siguientes valores: - MONTHLY - QUARTERLY - BIENNIAL - ANNUAL
data-recurrenceamount	TEXTO		Importe máximo a cargar como pago recurrente. Opcional, si no se envía nada se manda como null.
data-recurrenceamount	TEXTO		Monto a pagar en recurrente. Aplica cuando el data-recurrencetype es FIXED y FIXEDINITIAL

A continuación, se muestran algunos ejemplos de configuración del botón de pago:

Librería JS:

Ambiente	URL librería JS para invocar el formulario
Desarrollo	https://static-content-qas.vnforapps.com/v2/js/checkout.js?qa=true
Producción	https://static-content.vnforapps.com/v2/js/checkout.js

Formulario de pagos regular

Es el comportamiento básico del botón de pago y permite realizar una transacción con la información del cliente.

```
<form action='paginaRespuesta' method='post'>
  <script src='js/checkout.js'
    data-sessiontoken='123456ABCD789'
    data-channel='web'
    data-merchantid='123456789'

    data-merchantlogo='img/comercio.png'
    data-formbuttoncolor='#D80000'

    data-purchasenumber='123'
    data-amount='20.98'

    data-expirationminutes='5'
    data-timeouturl='timeout.html'
  ></script>
</form>
```



Formulario de pagos con recordar tarjeta

El siguiente escenario es idéntico al anterior. La diferencia es que en la configuración obtenida a partir del Merchant Id (data-key) la API configura el formulario para presentar "Recordar Tarjeta".

```
<form action='paginaRespuesta' method='post'>
  <script src='js/checkout.js'
    data-sessiontoken='123456ABCD789'
    data-channel='web'
    data-merchantid='123456789'

    data-merchantlogo='img/comercio.png'
    data-formbuttoncolor='#D80000'

    data-purchasenumber='123'
    data-amount='20.98'

    data-expirationminutes='5'
    data-timeouturl='timeout.html'
  ></script>
</form>
```



Formulario de pagos (recordar tarjeta + ocultando datos del cliente)

En el siguiente ejemplo el comercio inyecta el nombre, apellido y el email del cliente por lo que no se muestran en el formulario. Esta configuración también se obtiene del Merchant Id. Si los datos enviados por el comercio no tienen formato válido, se mostrarán en el formulario con opción a edición.

```
<form action='paginaRespuesta' method='post'>
  <script src='js/checkout.js'
    data-sessiontoken='123456ABCD789'
    data-channel='web'
    data-merchantid='123456789'

    data-merchantlogo='img/comercio.png'
    data-formbuttoncolor='#D80000'

    data-purchasenumero='123'
    data-amount='20.98'

    data-expirationminutes='5'
    data-timeouturl='timeout.html'

    data-cardholdername='Juan'
    data-cardholderlastname='Perez'
    data-cardholderemail='jperez123@correo.com'
  ></script>
</form>
```



Formulario de pagos con tarjeta recordada

En el formulario se muestra la lista de tarjetas asociadas a un usertoken y se despliegan como se muestra en la figura. El sistema de comercio configura el campo "data-usertoken" con un token guardado y asociado al usuario que está realizando el pago.

```
<form action='paginaRespuesta' method='post'>
  <script src='js/checkout.js'
    data-sessiontoken='123456ABCD789'
    data-channel='web'
    data-merchantid='123456789'

    data-merchantlogo='img/comercio.png'
    data-formbuttoncolor='#D80000'

    data-purchasenumero='123'
    data-amount='20.98'

    data-expirationminutes='5'
    data-timeouturl='timeout.html'

    data-usertoken='token123456'
  ></script>
</form>
```



Formulario de pagos mostrando cuotas

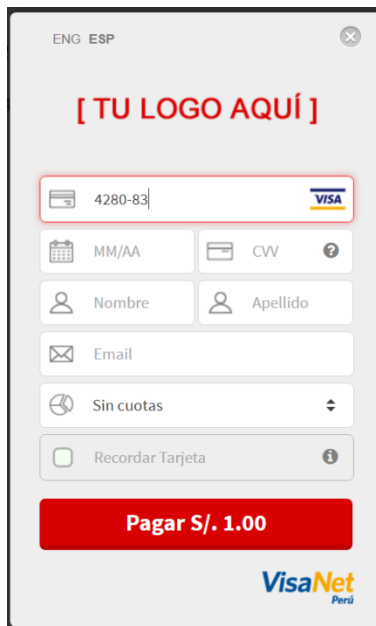
En este ejemplo la ventana incluye la funcionalidad de cuotas por estar activa en la configuración obtenida a partir del Merchant Id (data-key).

```
<form action='paginaRespuesta' method='post'>
  <script src='js/checkout.js'
    data-sessiontoken='123456ABCD789'
    data-channel='web'
    data-merchantid='123456789'

    data-merchantlogo='img/comercio.png'
    data-formbuttoncolor='#D80000'

    data-purchasenummer='123'
    data-amount='1.00'

    data-expirationminutes='5'
    data-timeouturl='timeout.html'
  ></script>
</form>
```



The screenshot shows a mobile checkout interface for VisaNet Perú. At the top, there's a language selector (ENG ESP) and a close button. Below is a placeholder for the merchant logo "[TU LOGO AQUÍ]". The card number field contains "4280-83" and is highlighted with a red border. Below the card number are fields for the expiration date (MM/AA), CVV, and a question mark icon. There are also fields for "Nombre" and "Apellido". An "Email" field is present. A dropdown menu shows "Sin cuotas" with a downward arrow. Below that is a checkbox for "Recordar Tarjeta" with an information icon. At the bottom, a large red button says "Pagar S/. 1.00". The VisaNet Perú logo is in the bottom right corner.

Formulario de pagos con tarjeta foránea

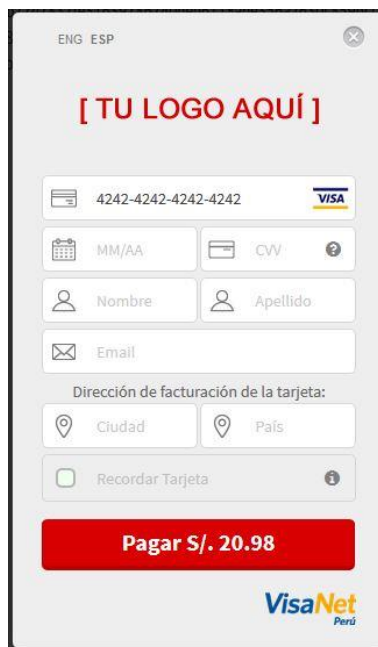
Este comportamiento es automático y se activa cuando el usuario digita una tarjeta con BIN que no pertenece a Perú.

```
<form action='paginaRespuesta' method='post'>
  <script src='js/checkout.js'
    data-sessiontoken='123456ABCD789'
    data-channel='web'
    data-merchantid='123456789'

    data-merchantlogo='img/comercio.png'
    data-formbuttoncolor='#D80000'

    data-purchasenummer='123'
    data-amount='20.98'

    data-expirationminutes='5'
    data-timeouturl='timeout.html'
  ></script>
</form>
```



The screenshot shows a mobile checkout interface for VisaNet Perú. At the top, there's a language selector (ENG ESP) and a close button. Below is a placeholder for the merchant logo "[TU LOGO AQUÍ]". The card number field contains "4242-4242-4242-4242" and is highlighted with a red border. Below the card number are fields for the expiration date (MM/AA), CVV, and a question mark icon. There are also fields for "Nombre" and "Apellido". An "Email" field is present. Below that is a section titled "Dirección de facturación de la tarjeta:" with fields for "Ciudad" and "País". There is a checkbox for "Recordar Tarjeta" with an information icon. At the bottom, a large red button says "Pagar S/. 20.98". The VisaNet Perú logo is in the bottom right corner.

Formulario de pagos ocultando en monto en “Pagar”

Si el comercio no desea mostrar el monto en el botón pagar se deberá enviar `data-showamount='false'`.

```
<form action='paginaRespuesta' method='post'>
  <script src='js/checkout.js'
    data-sessiontoken='123456ABCD789'
    data-channel='web'
    data-merchantid='123456789'

    data-merchantlogo='img/comercio.png'
    data-formbuttoncolor='#D80000'
    data-showamount='false'

    data-purchasenummer='123'
    data-amount='20.98'

    data-expirationminutes='5'
    data-timeouturl='timeout.html'

    data-cardholdername='Juan'
    data-cardholderlastname='Perez'
    data-cardholderemail='jperez123@correo.com'
  ></script>
</form>
```



Formulario de pagos con recurrencia fija

Para pagos recurrentes son obligatorios los campos `data-recurrence = TRUE`, `data-recurrencetype = FIXED`, `data-frequency`, `data-recurrencemaxamount` y `data-recurrenceamount`; donde el primero de ellos es recuperado de la configuración del comercio y el resto se deberá indicar el valor en el script de configuración.

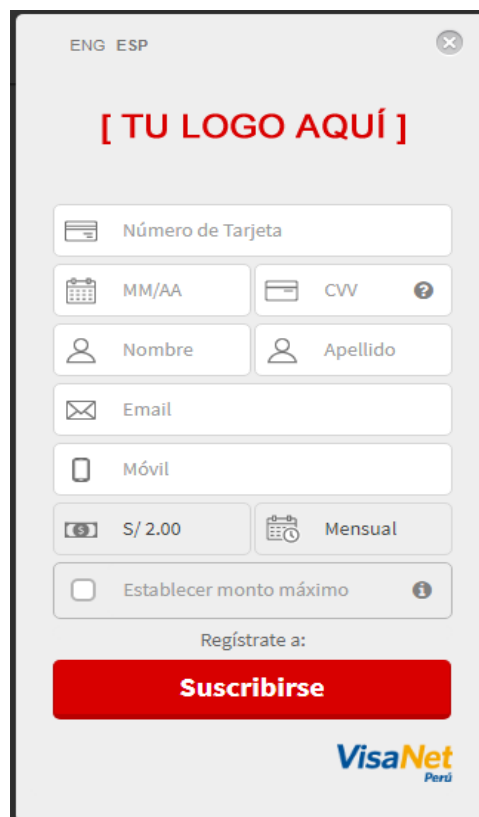
```
<form action='paginaRespuesta' method='post'>
  <script src='js/checkout.js'
    data-sessiontoken='123456ABCD789'
    data-channel='web'
    data-merchantid='123456789'

    data-merchantlogo='img/comercio.png'
    data-formbuttoncolor='#D80000'

    data-purchasenummer='123'
    data-amount='1.00'

    data-expirationminutes='5'
    data-timeouturl='timeout.html'

    data-recurrence='TRUE'
    data-recurrencetype='FIXED'
    data-recurrencefrequency='MONTHLY'
    data-recurrencemaxamount='12.00'
    data-recurrenceamount='2.00'
  ></script>
</form>
```



Formulario de pagos con recurrencia variable

Para pagos recurrentes son obligatorios los campos data-recurrence = TRUE, data-recurrencetype = VARIABLE, data-frequency y data-recurrencemaxamount; donde el primero de ellos es recuperado de la configuración del comercio y el resto se deberá indicar el valor en el script de configuración.

```
<form action='paginaRespuesta' method='post'>
  <script src='js/checkout.js'
    data-sessiontoken='123456ABCD789'
    data-channel='web'
    data-merchantid='123456789'

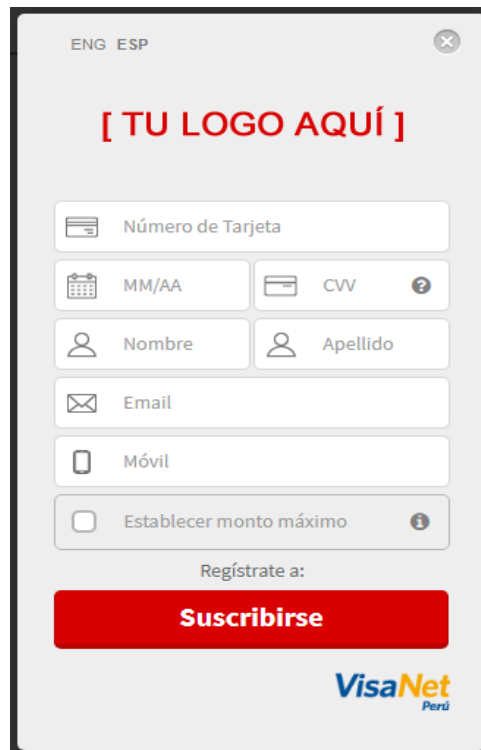
    data-merchantlogo='img/comercio.png'
    data-formbuttoncolor='#D80000'

    data-purchasenummer='123'
    data-amount='1.00'

    data-expirationminutes='5'
    data-timeouturl='timeout.html'

    data-recurrence='TRUE'
    data-recurrencetype='VARIABLE'
    data-recurrencefrequency='MONTHLY'
    data-recurrencemaxamount='12.00'

  ></script>
</form>
```



Formulario de pagos con recurrencia fija + pago inicial

Para pagos recurrentes son obligatorios los campos data-recurrence = TRUE, data-recurrencetype = FIXEDINITIAL, data-frequency, data-recurrencemaxamount y data-recurrenceamount; donde el primero de ellos es recuperado de la configuración del comercio y el resto se deberá indicar el valor en el script de configuración.

```
<form action='paginaRespuesta' method='post'>
  <script src='js/checkout.js'
    data-sessiontoken='123456ABCD789'
    data-channel='web'
    data-merchantid='123456789'

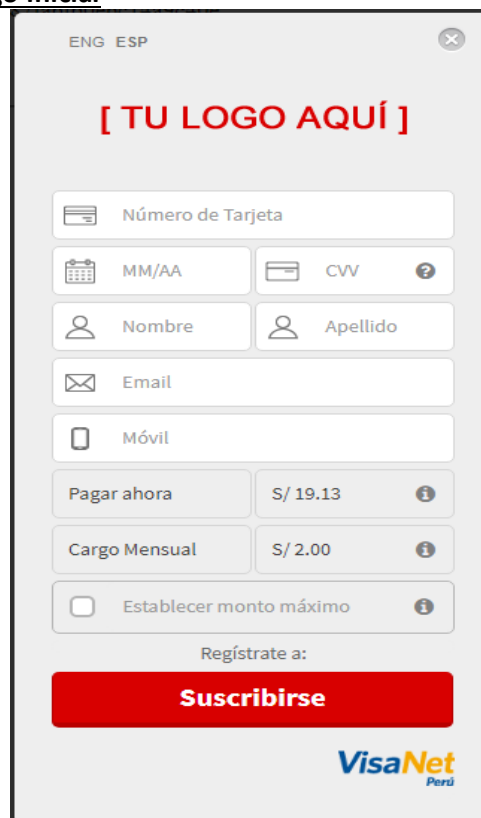
    data-merchantlogo='img/comercio.png'
    data-formbuttoncolor='#D80000'

    data-purchasenummer='123'
    data-amount='19.13'

    data-expirationminutes='5'
    data-timeouturl='timeout.html'

    data-recurrence='TRUE'
    data-recurrencetype='FIXEDINITIAL'
    data-recurrencefrequency='MONTHLY'
    data-recurrencemaxamount='12.00'
    data-recurrenceamount='2.00'

  ></script>
</form>
```



Formulario de pagos con recurrencia variable + pago inicial

Para pagos recurrentes son obligatorios los campos data-recurrence = TRUE, data-recurrencetype = VARIABLEINITIAL, data-frequency y data-recurrencemaxamount; donde el primero de ellos es recuperado de la configuración del comercio y el resto se deberá indicar el valor en el script de configuración.

```
<form action='paginaRespuesta' method='post'>
  <script src='js/checkout.js'
    data-sessiontoken='123456ABCD789'
    data-channel='web'
    data-merchantid='123456789'

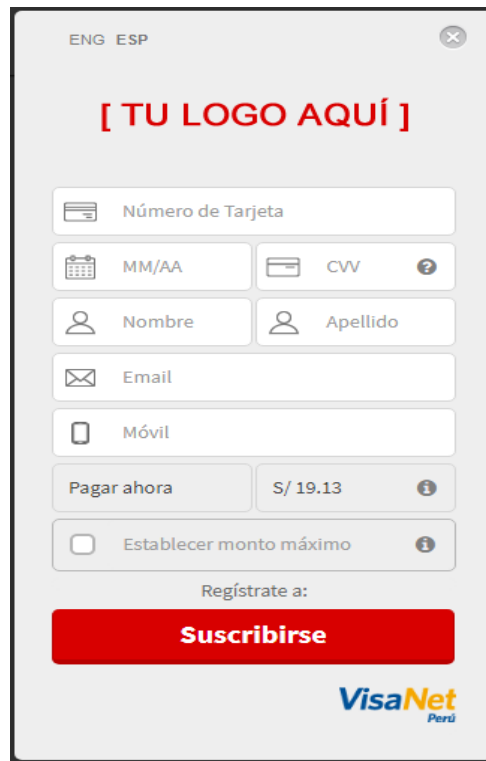
    data-merchantlogo='img/comercio.png'
    data-formbuttoncolor='#D80000'

    data-purchasenummer='123'
    data-amount='19.13'

    data-expirationminutes='5'
    data-timeouturl='timeout.html'

    data-recurrence='TRUE'
    data-recurrencetype='VARIABLEINITIAL'
    data-recurrencefrequency='MONTHLY'
    data-recurrencemaxamount='12.00'

  ></script>
</form>
```



The screenshot shows a mobile payment interface for VisaNet Perú. At the top, there are language options (ENG, ESP) and a close button. Below is a placeholder for the merchant logo "[TU LOGO AQUÍ]". The form contains several input fields: "Número de Tarjeta", "MM/AA", "CVV", "Nombre", "Apellido", "Email", and "Móvil". There are two buttons: "Pagar ahora" (Pay now) and "Establecer monto máximo" (Set maximum amount). The current amount is displayed as "S/ 19.13". Below the form, there is a "Regístrate a:" (Sign up to:) section with a large red "Suscribirse" (Subscribe) button. The VisaNet Perú logo is at the bottom right.

Formulario de pagos con PagoEfectivo

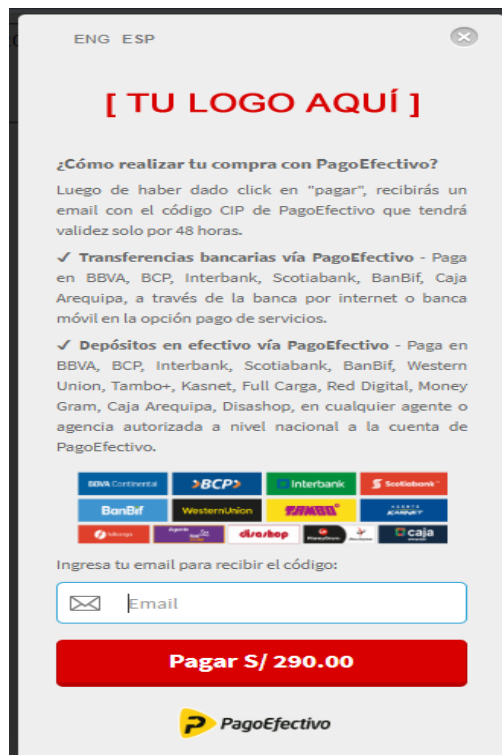
Estos son los campos mínimos a mandar, adicionales al formulario de pago elegido arriba (esto para cuando el Pago Habiente seleccione Pago con tarjeta).

Para los pagos con PagoEfectivo son obligatorios los campos los campos data-merchantid y data-amount, datos de los que se deberá indicar el valor en el script de configuración. Esta opción se activará siempre y cuando el comercio tenga habilitada la opción de PagoEfectivo desde el módulo web del comercio y el Pago habiente haya seleccionado esta opción.

```
<form action='paginaRespuesta' method='post'>
  <script src='js/checkout.js'
    data-sessiontoken='123456ABCD789'
    data-channel='web'
    data-purchasenummer='123'
    data-merchantid='123456789'
    data-amount='290.00'

    data-merchantlogo='img/comercio.png'
    data-formbuttoncolor='#D80000'

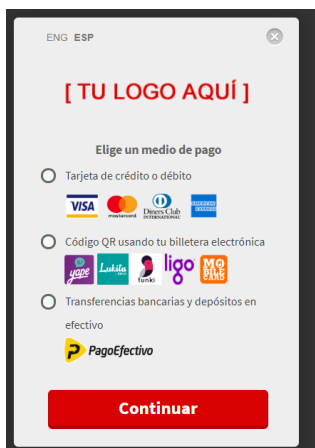
    data-expirationminutes='5'
    data-timeouturl='timeout.html'
  ></script>
</form>
```



The screenshot shows a mobile payment interface for VisaNet Perú, specifically for the "PagoEfectivo" (Cash Payment) option. At the top, there are language options (ENG, ESP) and a close button. Below is a placeholder for the merchant logo "[TU LOGO AQUÍ]". The form contains a section titled "¿Cómo realizar tu compra con PagoEfectivo?" (How to make your purchase with PagoEfectivo?). It explains that after clicking "pagar", the user will receive an email with a CIP code that is valid for 48 hours. There are two main options: "Transferencias bancarias vía PagoEfectivo" (Bank transfers via PagoEfectivo) and "Depósitos en efectivo vía PagoEfectivo" (Cash deposits via PagoEfectivo). Below these options, there is a grid of logos for various banks and payment providers: BBVA, BCP, Interbank, Scotiabank, BanBif, Western Union, and others. There is a field for "Ingresa tu email para recibir el código:" (Enter your email to receive the code:). At the bottom, there is a large red button labeled "Pagar S/ 290.00" and the PagoEfectivo logo.

Nota: si no se envían todos los campos obligatorios el formulario emitirá un mensaje de alerta indicando los datos faltantes.

Si el comercio tiene habilitada la opción de PagoEfectivo se mostrará esta pantalla inicial para seleccionar el medio de pago antes de todos los formularios anteriores.



iv. Paso 4: Concretar transacción

Dependiendo del método de pago (tarjeta o PagoEfectivo), habrán dos caminos para concretar la transacción

a. Pago con Tarjeta: Solicitar autorización de transacción

En este caso, el paso final de la integración es solicitar la autorización de la transacción. Para ello es necesario consumir la API de autorización, la cual de ser invocada de la siguiente manera:

Endpoint para conexión con la API:

Ambiente	URL API de creación de sesión
Desarrollo	https://apitestenv.vnforapps.com/api.authorization/v3/authorization/ecommerce/{merchantId}
Producción	https://apiprod.vnforapps.com/api.authorization/v3/authorization/ecommerce/{merchantId}

Request

POST <https://apitestenv.vnforapps.com/api.authorization/v3/authorization/ecommerce/{merchantId}>

HEADER

Content-Type: application/json

Authorization: { tokenSeguridad }

BODY

```
{
  "antifraud": null,
```

```

"captureType": "manual",
"cardHolder": {
  "documentNumber": "{ documentNumber }",
  "documentType": "{ documentType }"
},
"channel": "{ channel }",
"countable": { countable },
"order": {
  "amount": { amount },
  "currency": "{ currency }",
  "productId": "{ productId }",
  "purchaseNumber": "{ purchaseNumber }",
  "tokenId": "{ tokenId }"
},
"recurrence": {
  "amount": "{ amount }",
  "beneficiaryId": "{ beneficiaryId }",
  "frequency": "{ frequency }",
  "maxAmount": "{ maxAmount }",
  "type": "{ type }"
},
"sponsored": null
}

```

Los parámetros necesarios para la invocación de la API de autorización se explican a continuación:

(*) Campos mínimos obligatorios para la solicitud de autorización

() Campo obligatorio que el comercio deben enviar en caso de solicitar autorizaciones con registros en el sistema recurrentes (Pago programado)**

Parámetro	Descripción
merchantId (*)	Código de comercio
tokenSeguridad (*)	Token generado con la API de seguridad
captureType (*)	Constante, siempre es el valor "manual"
cardHolder	Objeto tipo de documento
documentNumber (**)	Número de documento del tarjeta habiente
documentType (**)	Tipo de documento del tarjeta habiente. Debe ser: "0" DNI, "1" Carnet extranjería, "2" Pasaporte
channel (*)	Canal de registro. En este caso el valor a enviar es "web"

countable (*)	Este campo indica si la venta a realizar tendrá liquidación automática o manual. Acepta los siguientes valores: true – Para liquidación automática false – Para liquidación manual Revisar anexo “c”
Order	Objeto orden
amount (*)	Importe de la transacción Formato ####.## (dos decimales separados por punto) Ejemplo: 1000.00
currency (*)	Moneda de la transacción
productId (**)	Código de producto registrado en el sistema pagos recurrentes VisaNet
purchaseNumber (*)	Número de pedido
tokenId (*)	Token retornado del formulario de pagos
Recurrence	Objeto recurrente
amount (**)	Monto a cargar para la afiliación recurrente. Aplica cuando el “recurrencetype” es FIXED o FIXEDINITIAL
beneficiaryId (**)	Código de identificación del beneficiario
frequency (**)	Frecuencia de la afiliación recurrente, debe ser los siguientes valores: - MONTHLY - QUARTERLY - BIENNIAL - ANNUAL
maxAmount	Monto máximo a cargar para la afiliación recurrente. Si no se va a ingresar data se envía como null.
type (**)	Tipo de afiliación recurrente a realizar, debe ser los siguientes valores: - FIXED - VARIABLE - FIXEDINITIAL - VARIABLEINITIAL

Successful Response

STATUS CODE 200 OK

HEADERS

Content-Type: application/json

BODY

```
{
  "header": {
    "ecoreTransactionUUID": "3bfe5a37-570c-49cf-bebd-588d7066a33a",
    "ecoreTransactionDate": 1522528900672,
    "millis": 3867
  }
}
```

```

},
"order":{
  "tokenId":"44BDC4D1500F4927BDC4D1500F7927D6",
  "purchaseNumber":"8078",
  "productId":"321",
  "amount":147.02,
  "currency":"PEN",
  "authorizedAmount":147.02,
  "authorizationCode":"153831",
  "actionCode":"000",
  "traceNumber":"3713",
  "transactionDate":"180331154140",
  "transactionId":"991180900182558"
},
"dataMap":{
  "CURRENCY":"0604",
  "TRANSACTION_DATE":"180331154140",
  "TERMINAL":"00000001",
  "ACTION_CODE":"000",
  "TRACE_NUMBER":"3713",
  "ECI_DESCRIPTION":"Transaccion no autenticada pero enviada en canal seguro",
  "ECI":"07",
  "BRAND":"visa",
  "CARD":"402160*****4513",
  "MERCHANT":"341198210",
  "STATUS":"Verified",
  "ADQUIRENTE":"570002",
  "ACTION_DESCRIPTION":"Aprobado y completado con exito",
  "ID_UNICO":"991180900182558",
  "AMOUNT":"147.02",
  "PROCESS_CODE":"000000",
  "RECURRENCE_STATUS":"Registered",
  "TRANSACTION_ID":"991180900182558",
  "AUTHORIZATION_CODE":"153831"
}

```



```
}
}
```

Los parámetros de respuesta de la API se explican a continuación:

Parámetro	Descripción
header	Objeto cabecera
ecoreTransactionUUID	Código de la transacción dentro de las API de VisaNet
ecoreTransactionDate	Fecha y hora de la transacción. Formato: millis
millis	Tiempo de duración de la transacción
order	Objeto orden
tokenId	Token retornado del formulario de pagos
purchaseNumber	Número de pedido generado por el comercio
productId	Código de producto registrado en el sistema pagos recurrentes VisaNet
amount	Importe de la transacción Formato #####.## (dos decimales separados por punto) Ejemplo: 1000.00
currency	Moneda de la transacción
authorizedAmount	Importe autorizado
authorizationCode	Código de autorización
actionCode	Código de denegación y aprobación. El Código de aprobación: 000
traceNumber	Número de orden de la transacción generada en los sistemas de VisaNet
transactionDate	Fecha y hora de la transacción. Formato UNIX TimeStamp
transactionId	ID único de la transacción del sistema VisaNet (i)
token	Objeto tarjeta
tokenId	Número de tarjeta tokenizada
dataMap	Objeto datos complementarios
CURRENCY	Moneda de la transacción
TRANSACTION_DATE	Fecha y hora de la transacción. Formato UNIX TimeStamp
TERMINAL	Id de Terminal
ACTION_CODE	Código de denegación y aprobación. El Código de aprobación: 000
TRACE_NUMBER	Número de orden de la transacción generada en los sistemas de VisaNet
ECI_DESCRIPTION	Descripción del ECI (Electronic Commerce Indicator). Revisar anexo "a"
ECI	Código de ECI (Electronic Commerce Indicator). Revisar anexo "a"
BRAND	Marca de la tarjeta usada en el pago. Puede ser: visa, amex, mastercard, dinersclub
CARD	Número de tarjeta Visa. Está enmascarado. Se puede visualizar el BIN y los 4 últimos dígitos como si siguiente ejemplo: 491914*****9067
MERCHANT	Código de Comercio, creado al momento de la afiliación al producto Comercio Electrónico Pago Web
STATUS	Estado de la transacción
ADQUIRENTE	Código de adquirente
ACTION_DESCRIPTION	Descripción del código de acción, permite identificar el motivo de rechazo de una operación
QUOTA_AMOUNT	Importe aproximado del valor de cuota, este valor es devuelto por el emisor
ID_UNICO	Identificador único de la transacción generado por el sistema transaccional de VisaNet. Este permite rastrear la operación en los diferentes sistemas de VisaNet. Además, puede ser utilizado para procesos de conciliación automáticas. (i)
AMOUNT	Importe autorizado
PROCESS_CODE	Código de proceso
QUOTA_NUMBER	Número de cuotas
VAULT_BLOCK	Token generado por el tarjetahabiente al marcar la opción de recordar tarjeta
RECURRENCE_STATUS	Estado de registro en recurrentes
TRANSACTION_ID	ID de la transacción del sistema VisaNet (i)
AUTHORIZATION_CODE	Código de autorización
QUOTA_DEFERRED	Indica si el pago en cuotas debe procesarse con pagos en diferido

	0 = el pago no se procesa en diferido 1, 2 = el pago se procesa en diferido
SIGNATURE	UUID generado para el proceso de venta, el cual es utilizado en la reversa de la operación. Ejemplo: f9303580-8402-438f-bf52-f48c3cdc90ff
EXPIRATION_MONTH	Mes de vencimiento de la tarjeta. Ejemplo: 09
EXPIRATION_YEAR	Año de vencimiento de la tarjeta. Ejemplo: 2026
RECURRENCE_MESSAGE	Mensaje de respuesta de la afiliación a Pago Programado
RECURRENCE_MAX_AMOUNT	Monto máximo de la afiliación a Pago Programado. Se devuelve solo si se ha ingresado este campo en el botón.

Error Response

STATUS CODE 400 ERROR

HEADERS

Content-Type: application/json

BODY

```
{
  "errorCode": 400,
  "errorMessage": "Not Authorized",
  "header": {
    "ecoreTransactionUUID": "3bfe5a37-570c-49cf-bebd-588d7066a33a",
    "ecoreTransactionDate": 1522528900672,
    "millis": 3867
  },
  "data": {
    "CURRENCY": "0604",
    "TRANSACTION_DATE": "180331152444",
    "TERMINAL": "00000001",
    "ACTION_CODE": "180",
    "TRACE_NUMBER": "3711",
    "ECI_DESCRIPTION": "Transaccion no autenticada pero enviada en canal seguro",
    "ECI": "07",
    "CARD": "400310****6160",
    "BRAND": "visa",
    "MERCHANT": "341198210",
    "STATUS": "Not Authorized",
    "ADQUIRENTE": "570002",
    "ACTION_DESCRIPTION": "Tarjeta no valida",
  }
}
```

```

        "ID_UNICO": "991180900182558",
        "AMOUNT": "125.34",
        "PROCESS_CODE": "000000",
        "TRANSACTION_ID": "991180900182558"
    }
}

```

b. Pago con PagoEfectivo

i. Redireccionamiento a URL de PagoEfectivo

El formulario de pagos de PagoEfectivo, devolverá la siguiente estructura

```

STATUS CODE 200 OK

HEADERS

Content-Type: application/x-www-form-urlencoded

BODY

transactionToken={ transactionToken }&customerEmail={ customerEmail }&channel={ channel
    }&url={ url }

```

Los parámetros de respuesta de la API se explican a continuación:

Parámetro	Descripción
transactionToken	Es el código CIP generado por PagoEfectivo.
customerEmail	El correo del tarjeta habiente, a este correo se envía la confirmación de PagoEfectivo y la información para completar la compra.
channel	El canal en este caso siempre será "pagoefectivo"
url	URL con la misma información que se envía al correo.

Se deberá redireccionar a la URL obtenida en donde se detallarán los pasos a seguir para completar la compra y las condiciones involucradas del método seleccionado.

ii. Actualización del estado de la venta

Para este caso el paso final de la integración es el actualizar el estado de la venta y confirmar si se realizó el pago por esta o expiró el tiempo de reserva. Para ello es necesario como comercio se exponga un API callback, la cual de ser invocada de la siguiente manera:

Endpoint para conexión con la API Callback:

Ambiente	URL API Callback
Desarrollo	https://ambiente.comercio.com/api.pagoeffectivocallback/v1/callback

Producción	https://ambiente.comercio.com/api.pagoefectivocallback/v1/callback
------------	--

Request

POST https://ambiente.comercio.com/api.pagoefectivocallback

HEADER

Content-Type: application/json

BODY

```
{
  "operationNumber":"{ operationNumber }",
  "cip":"{ cip }",
  "status":"{ status }",
  "amount":{ amount }
}
```

Los parámetros necesarios para la invocación del API callback se explican a continuación :

(*) Campos mínimos obligatorios para la solicitud de autorización

Parámetro	Descripción
operationNumber (*)	Número de compra o código de transacción
Cip (*)	Código CIP.
status (*)	Estado de la venta. Puede ser "Paid" Pagado o "Expired" Expirado
amount (*)	Monto registrado de la venta

Successful Response

STATUS CODE 200 OK

HEADERS

Content-Type: application/json

Respuesta final al tarjetahabiente:

Una vez obtenido el resultado del proceso de pago, el comercio deberá mostrar la pantalla final de respuesta al cliente.

La pantalla final de compra debe mostrar la siguiente información:

- Dominio
- Logo de la empresa
- Nombre de la Tienda
- Teléfono
- Dirección Comercial
- Número de pedido

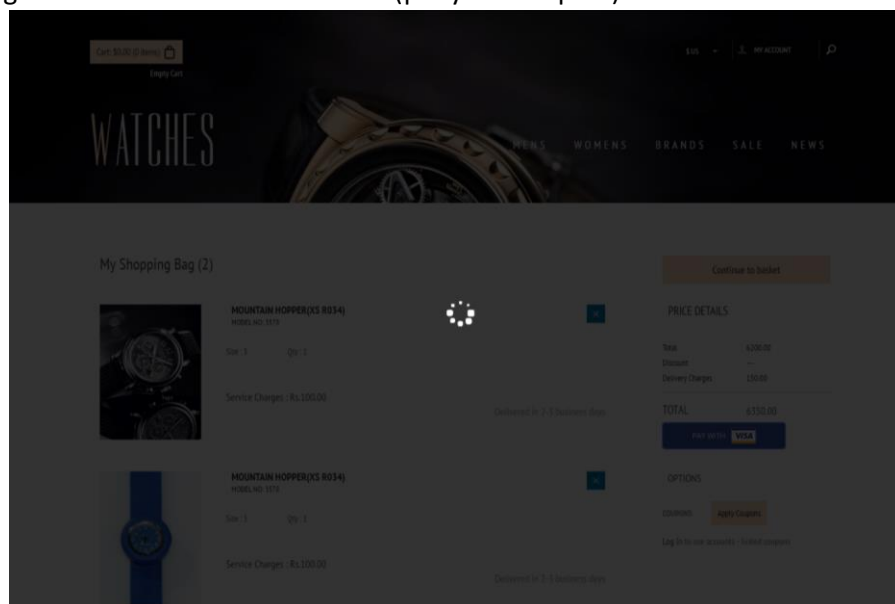
- Número de Tarjeta enmascarada: Ej: 4444 XXXX XXXX 3333
- Fecha y hora del pedido
- Importe de la transacción
- Moneda
- Descripción del producto
- Nombre del tarjetahabiente
- Descripción del código de acción
- Políticas de devolución (o el link a las mismas)
- Términos y Condiciones (o el link a la página)
- Incluir un texto indicando al cliente que debe imprimir y guardar el recibo de transacción.

Para el caso de que el método de pago elegido fuese PagoEfectivo, al final de la compra deberá redireccionarse a la URL devuelta por el botón de pago.

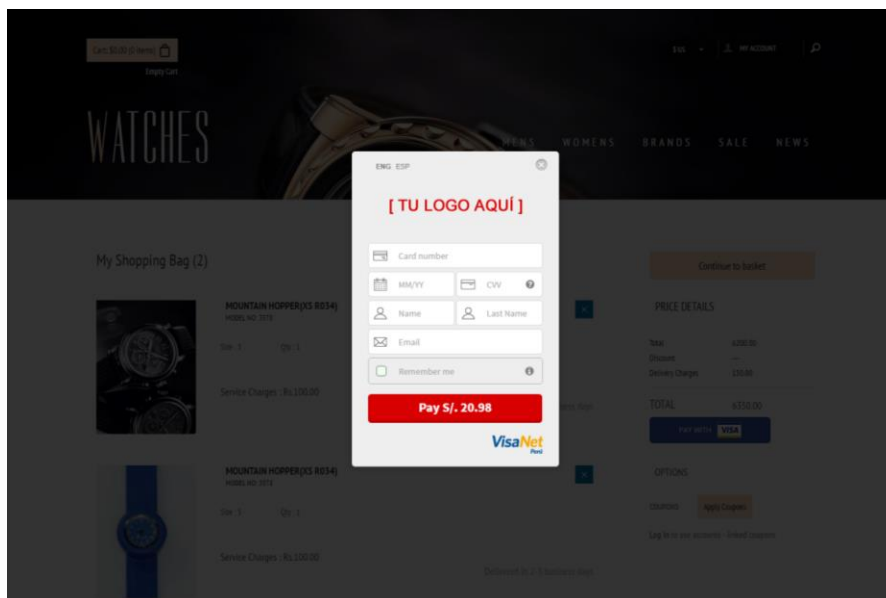
En algunos casos por un tema de reclamos, VisaNet solicitará al establecimiento el envío de una copia de esta pantalla final de compra en un plazo no mayor a 48 horas.

v. Paso 5: Comportamiento del formulario

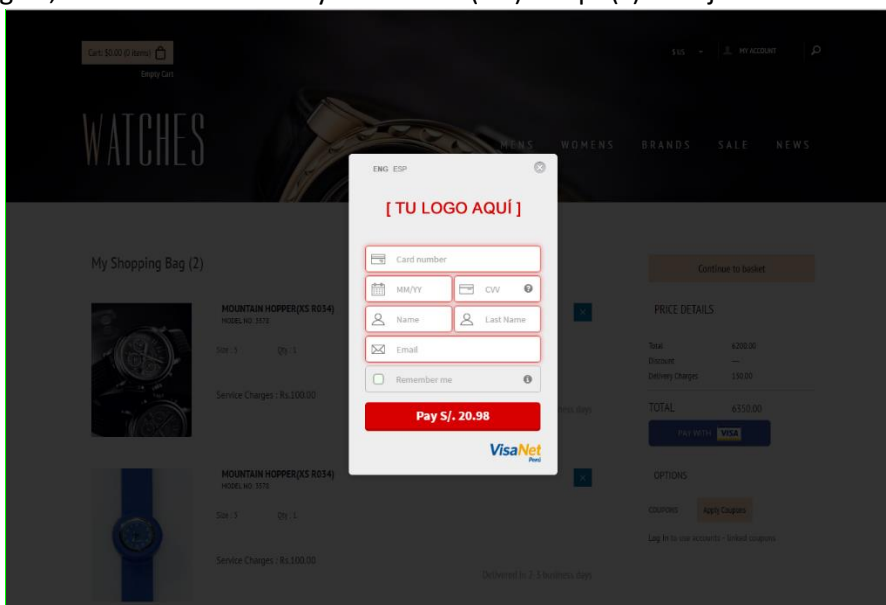
- El formulario de pagos presenta el siguiente ícono de carga (loading) al darle clic al botón “Paga con Visa” en la tienda virtual: (pre y falta el post)



- El formulario de pagos emerge sobre la tienda virtual, la cual oscurece levemente:



- Si faltase completar algún campo del formulario de pagos, al momento de dar clic en “Pagar”, el formulario vibrará y resaltará el(los) campo(s) en rojo:



vi. Paso 7: Integración, certificación y salida a producción

Para realizar las pruebas del formulario de pagos, el comercio necesitará:

- Código de comercio: código que se le asignó al comercio para pruebas.
- Llaves de autenticación: usuario y contraseña.

Las pruebas y certificación consisten en lo siguiente:

- Validación de la implementación, en la tienda virtual del comercio, de los requisitos obligatorios indicados en la sección 5.a Requisitos Obligatorios.

- Pruebas de compra para validar los diferentes escenarios de la transacción, para lo cual el comercio deberá tener cargado algunos productos y sus montos en la tienda virtual.

El comercio tiene los siguientes escenarios de pruebas disponibles:















Escenario	Tarjeta de prueba	Respuesta de Cybersource
Autorizado	<u>Nacional</u> 4919 – 1481 – 0785 – 9067 4919 – 1481 – 0785 - 9067 4500 – 3400 – 9000 – 0016	Correo (aprobado sin autenticación): accept@cybersource.com Correo (Verified by Visa): review@cybersource.com
	<u>Foránea</u> 4072 – 2102 – 9053 – 6663	
Denegado	4444 – 3333 – 2222- 1111 4111 – 1111 – 1111 – 1111	Correo (denegado por fraude): reject@cybersource.com Correo (Verified by Visa): review@cybersource.com

Si las validaciones fueron exitosas, el equipo de integración coordina el pase a producción de la tienda virtual del comercio.

8. Botón “PAGA CON VISA”

a. Botones VisaNet

Se podrá insertar en la tienda virtual cualquiera de los siguientes botones que al darles clic mostrará al formulario de pagos:

N°	Color	Tamaño	Español	Inglés
1	Azul	SMALL 86x73px		
2	Azul	MEDIUM 130x45px		
3	Azul	DEFAULT 187x40px		
4	Azul	LARGE 223x49px		
5	Gris	SMALL 86x73px		
6	Gris	MEDIUM 130x45px		
7	Gris	DEFAULT 187x40px		

8	Gris	LARGE 223x49px	PAGA CON 	PAY WITH 
---	------	-------------------	--	--

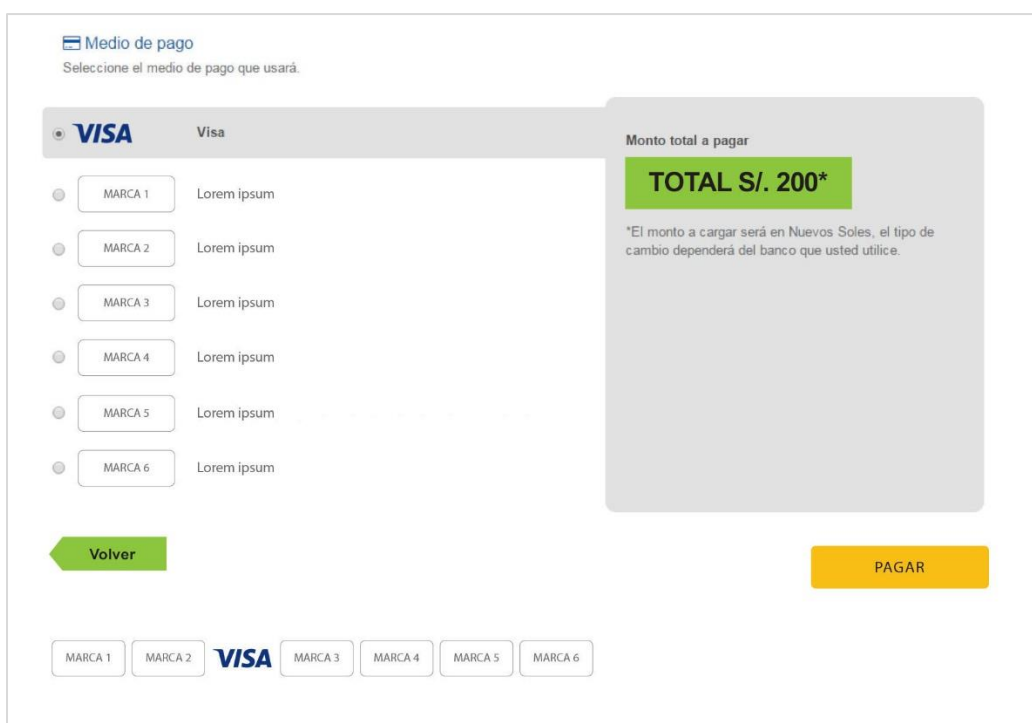
Se podrán descargar desde la página web de VisaNet: www.visanet.com.pe

b. Colocación del botón en la tienda virtual

El formulario de pagos solo podrá invocarse desde la tienda virtual desde uno de los botones VisaNet indicados previamente.

Para ello la colocación del botón debe ser de la siguiente manera:

Paso 1: Checkout del comercio



Medio de pago
Seleccione el medio de pago que usará.

VISA Visa

- MARCA 1 Lorem ipsum
- MARCA 2 Lorem ipsum
- MARCA 3 Lorem ipsum
- MARCA 4 Lorem ipsum
- MARCA 5 Lorem ipsum
- MARCA 6 Lorem ipsum

Volver

Monto total a pagar
TOTAL S/. 200*
*El monto a cargar será en Nuevos Soles, el tipo de cambio dependerá del banco que usted utilice.

MARCA 1 MARCA 2 **VISA** MARCA 3 MARCA 4 MARCA 5 MARCA 6

PAGAR

Paso 2: Checkout del comercio (botón VisaNet)

Medio de pago

Seleccione el medio de pago que usará.

VISA

Visa

MARCA 1

Lorem ipsum

MARCA 2

Lorem ipsum

MARCA 3

Lorem ipsum

MARCA 4

Lorem ipsum

MARCA 5

Lorem ipsum

MARCA 6

Lorem ipsum

Volver

MARCA 1

MARCA 2

VISA

MARCA 3

MARCA 4

MARCA 5

MARCA 6

Monto total a pagar

TOTAL S/. 200*

*El monto a cargar será en Nuevos Soles, el tipo de cambio dependerá del banco que usted utilice.

PAGA CON

VISA

9. Anexos

a. Códigos ECI

Códigos retornados en el proceso de autenticación. Sus valores significan:

ECI	Descripción
5	Transacción autenticada
6	Comercio intentó autenticación pero tarjetahabiente no está participando
7	Transacción no autenticada pero enviada en canal seguro
10	Entidad emisora no disponible para autenticación
11	Clave secreta del tarjetahabiente incorrecta
12	Tarjeta Vencida

b. Códigos de acción (denegaciones)

Códigos retornados desde el proceso de autorización para transacciones denegadas:

Código de acción	Descripción de apoyo para el comercio	Descripción a mostrar al cliente
101	Operación Denegada. Tarjeta Vencida.	Operación Denegada. Tarjeta Vencida. Verifique los datos en su tarjeta e ingréselos correctamente.
102	Operación Denegada. Contactar con la entidad emisora.	Operación Denegada. Contactar con entidad emisora de su tarjeta.
104	Operación Denegada. Operación no permitida para esta tarjeta.	Operación Denegada. Operación no permitida para esta tarjeta. Contactar con la entidad emisora de su tarjeta.
106	Operación Denegada. Exceso de intentos de ingreso de clave secreta.	Operación Denegada. Intentos de clave secreta excedidos. Contactar con la entidad emisora de su tarjeta.
107	Operación Denegada. Contactar con la entidad emisora.	Operación Denegada. Contactar con la entidad emisora de su tarjeta.

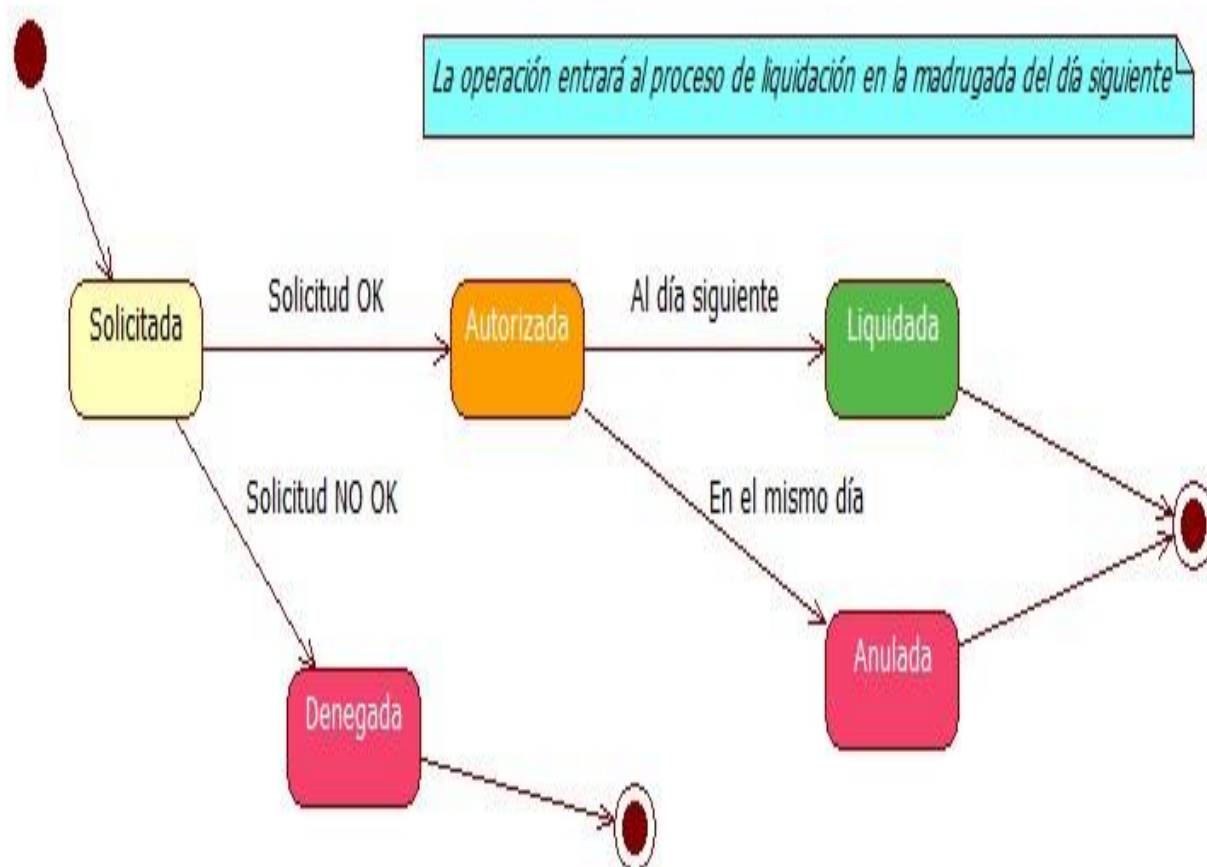
108	Operación Denegada. Exceso de actividad.	Operación Denegada. Contactar con la entidad emisora de su tarjeta.
109	Operación Denegada. Identificación inválida de establecimiento.	Operación Denegada. Contactar con el comercio.
110	Operación Denegada. Operación no permitida para esta tarjeta.	Operación Denegada. Operación no permitida para esta tarjeta. Contactar con la entidad emisora de su tarjeta.
111	Operación Denegada. El monto de la transacción supera el valor máximo permitido para operaciones virtuales	Operación Denegada. Contactar con el comercio.
112	Operación Denegada. Se requiere clave secreta.	Operación Denegada. Se requiere clave secreta.
116	Operación Denegada. Fondos insuficientes.	Operación Denegada. Fondos insuficientes. Contactar con entidad emisora de su tarjeta
117	Operación Denegada. Clave secreta incorrecta.	Operación Denegada. Clave secreta incorrecta.
118	Operación Denegada. Tarjeta inválida.	Operación Denegada. Tarjeta Inválida. Contactar con entidad emisora de su tarjeta.
119	Operación Denegada. Exceso de intentos de ingreso de clave secreta.	Operación Denegada. Intentos de clave secreta excedidos. Contactar con entidad emisora de su tarjeta.
121	Operación Denegada.	Operación Denegada.
126	Operación Denegada. Clave secreta inválida.	Operación Denegada. Clave secreta inválida.
129	Operación Denegada. Tarjeta no operativa.	Operación Denegada. Código de seguridad invalido. Contactar con entidad emisora de su tarjeta
180	Operación Denegada. Tarjeta inválida.	Operación Denegada. Tarjeta Inválida. Contactar con entidad emisora de su tarjeta.
181	Operación Denegada. Tarjeta con restricciones de Débito.	Operación Denegada. Tarjeta con restricciones de débito. Contactar con entidad emisora de su tarjeta.
182	Operación Denegada. Tarjeta con restricciones de Crédito.	Operación Denegada. Tarjeta con restricciones de crédito. Contactar con entidad emisora de su tarjeta.
183	Operación Denegada. Error de sistema.	Operación Denegada. Problemas de comunicación. Intente más tarde.
190	Operación Denegada. Contactar con entidad emisora.	Operación Denegada. Contactar con entidad emisora de su tarjeta.
191	Operación Denegada. Contactar con entidad emisora.	Operación Denegada. Contactar con entidad emisora de su tarjeta.
192	Operación Denegada. Contactar con entidad emisora.	Operación Denegada. Contactar con entidad emisora de su tarjeta.
199	Operación Denegada.	Operación Denegada.
201	Operación Denegada. Tarjeta vencida.	Operación Denegada. Tarjeta vencida. Contactar con entidad emisora de su tarjeta.
202	Operación Denegada. Contactar con entidad emisora.	Operación Denegada. Contactar con entidad emisora de su tarjeta
204	Operación Denegada. Operación no permitida para esta tarjeta.	Operación Denegada. Operación no permitida para esta tarjeta. Contactar con entidad emisora de su tarjeta.
206	Operación Denegada. Exceso de intentos de ingreso de clave secreta.	Operación Denegada. Intentos de clave secreta excedidos. Contactar con la entidad emisora de su tarjeta.
207	Operación Denegada. Contactar con entidad emisora.	Operación Denegada. Contactar con entidad emisora de su tarjeta..
208	Operación Denegada. Tarjeta perdida.	Operación Denegada. Contactar con entidad emisora de su tarjeta.
209	Operación Denegada. Tarjeta robada.	Operación Denegada. Contactar con entidad emisora de su tarjeta
263	Operación Denegada. Error en el envío de parámetros.	Operación Denegada. Contactar con el comercio.
264	Operación Denegada. Entidad emisora no está disponible para realizar la autenticación.	Operación Denegada. Entidad emisora de la tarjeta no está disponible para realizar la autenticación.
265	Operación Denegada. Clave secreta del tarjetahabiente incorrecta.	Operación Denegada. Clave secreta del tarjetahabiente incorrecta. Contactar con entidad emisora de su tarjeta.
266	Operación Denegada. Tarjeta vencida.	Operación Denegada. Tarjeta Vencida. Contactar con entidad emisora de su tarjeta.
280	Operación Denegada. Clave errónea.	Operación Denegada. Clave secreta errónea. Contactar con entidad emisora de su tarjeta.
290	Operación Denegada. Contactar con entidad emisora.	Operación Denegada. Contactar con entidad emisora de su tarjeta.
300	Operación Denegada. Número de pedido del comercio duplicado. Favor no atender.	Operación Denegada. Número de pedido del comercio duplicado. Favor no atender.
306	Operación Denegada. Contactar con entidad emisora.	Operación Denegada. Contactar con entidad emisora de su tarjeta.
401	Operación Denegada. Tienda inhabilitada.	Operación Denegada. Contactar con el comercio.

402	Operación Denegada.	Operación Denegada.
403	Operación Denegada. Tarjeta no autenticada	Operación Denegada. Tarjeta no autenticada.
404	Operación Denegada. El monto de la transacción supera el valor máximo permitido.	Operación Denegada. Contactar con el comercio.
405	Operación Denegada. La tarjeta ha superado la cantidad máxima de transacciones en el día.	Operación Denegada. Contactar con el comercio.
406	Operación Denegada. La tienda ha superado la cantidad máxima de transacciones en el día.	Operación Denegada. Contactar con el comercio.
407	Operación Denegada. El monto de la transacción no llega al mínimo permitido.	Operación Denegada. Contactar con el comercio.
408	Operación Denegada. CVV2 no coincide.	Operación Denegada. Código de seguridad no coincide. Contactar con entidad emisora de su tarjeta
409	Operación Denegada. CVV2 no procesado por entidad emisora.	Operación Denegada. Código de seguridad no procesado por la entidad emisora de la tarjeta
410	Operación Denegada. CVV2 no procesado por no ingresado.	Operación Denegada. Código de seguridad no ingresado.
411	Operación Denegada. CVV2 no procesado por entidad emisora.	Operación Denegada. Código de seguridad no procesado por la entidad emisora de la tarjeta
412	Operación Denegada. CVV2 no reconocido por entidad emisora.	Operación Denegada. Código de seguridad no reconocido por la entidad emisora de la tarjeta
413	Operación Denegada. Contactar con entidad emisora.	Operación Denegada. Contactar con entidad emisora de su tarjeta.
414	Operación Denegada.	Operación Denegada.
415	Operación Denegada.	Operación Denegada.
416	Operación Denegada.	Operación Denegada.
417	Operación Denegada.	Operación Denegada.
418	Operación Denegada.	Operación Denegada.
419	Operación Denegada.	Operación Denegada.
420	Operación Denegada. Tarjeta no es VISA.	Operación Denegada. Tarjeta no es VISA.
421	Operación Denegada. Contactar con entidad emisora.	Operación Denegada. Contactar con entidad emisora de su tarjeta.
422	Operación Denegada. El comercio no está configurado para usar este medio de pago.	Operación Denegada. El comercio no está configurado para usar este medio de pago. Contactar con el comercio.
423	Operación Denegada. Se canceló el proceso de pago.	Operación Denegada. Se canceló el proceso de pago.
424	Operación Denegada. Contactar con entidad emisora.	Operación Denegada.
666	Operación Denegada. Problemas de comunicación. Intente más tarde.	Operación Denegada. Problemas de comunicación. Intente más tarde.
667	Operación Denegada. Transacción sin autenticación. Inicio del Proceso de Pago	Operación Denegada. Transacción sin respuesta de Verified by Visa.
668	Operación Denegada.	Operación Denegada. Contactar con el comercio.
669	Operación Denegada.	Operación Denegada. Contactar con el comercio.
670	Operación Denegada. Módulo antifraude.	Operación Denegada. Contactar con el comercio.
672	Operación Denegada. Transacción sin respuesta de Antifraude.	Operación Denegada. Módulo antifraude.
673	Operación Denegada. Transacción sin respuesta del Autorizador.	Operación Denegada. Contactar con el comercio.
674	Operación Denegada. Sesión no válida.	Operación Denegada. Contactar con el comercio.
675	Inicialización de transacción	Inicialización de transacción
676	Operación Denegada. No activa la opción Revisar Enviar al Autorizador.	Operación Denegada. Contactar con el comercio.
677	Operación Denegada. Respuesta Antifraude con parámetros nos válidos.	Operación Denegada. Contactar con el comercio.
678	Operación Denegada. Valor ECI no válido.	Operación Denegada. Contactar con el comercio.
682	Operación Denegada. Intento de Pago fuera del tiempo permitido.	Operación Denegada. Operación Denegada.
683	Operación Denegada. Registro incorrecto de sesión.	Operación Denegada. Registro incorrecto de sesión.
684	Operación Denegada Registro Incorrecto Antifraude	Operación Denegada Registro Incorrecto Antifraude
685	Operación Denegada Registro Incorrecto Autorizador	Operación Denegada Registro Incorrecto Autorizador

904	Operación Denegada. Formato de mensaje erróneo.	Operación Denegada.
909	Operación Denegada. Error de sistema.	Operación Denegada. Problemas de comunicación. Intente más tarde.
910	Operación Denegada. Error de sistema.	Operación Denegada.
912	Operación Denegada. Entidad emisora no disponible.	Operación Denegada. Entidad emisora de la tarjeta no disponible
913	Operación Denegada. Transmisión duplicada.	Operación Denegada.
916	Operación Denegada. Contactar con entidad emisora.	Operación Denegada.
928	Operación Denegada. Contactar con entidad emisora.	Operación Denegada.
940	Operación Denegada. Transacción anulada previamente.	Operación Denegada.
941	Operación Denegada. Transacción ya anulada previamente.	Operación Denegada.
942	Operación Denegada.	Operación Denegada.
943	Operación Denegada. Datos originales distintos.	Operación Denegada.
945	Operación Denegada. Referencia repetida.	Operación Denegada.
946	Operación Denegada. Operación de anulación en proceso.	Operación Denegada. Operación de anulación en proceso.
947	Operación Denegada. Comunicación duplicada.	Operación Denegada. Problemas de comunicación. Intente más tarde.
948	Operación Denegada. Contactar con entidad emisora.	Operación Denegada.
949	Operación Denegada. Contactar con entidad emisora.	Operación Denegada.
965	Operación Denegada. Contactar con entidad emisora.	Operación Denegada.

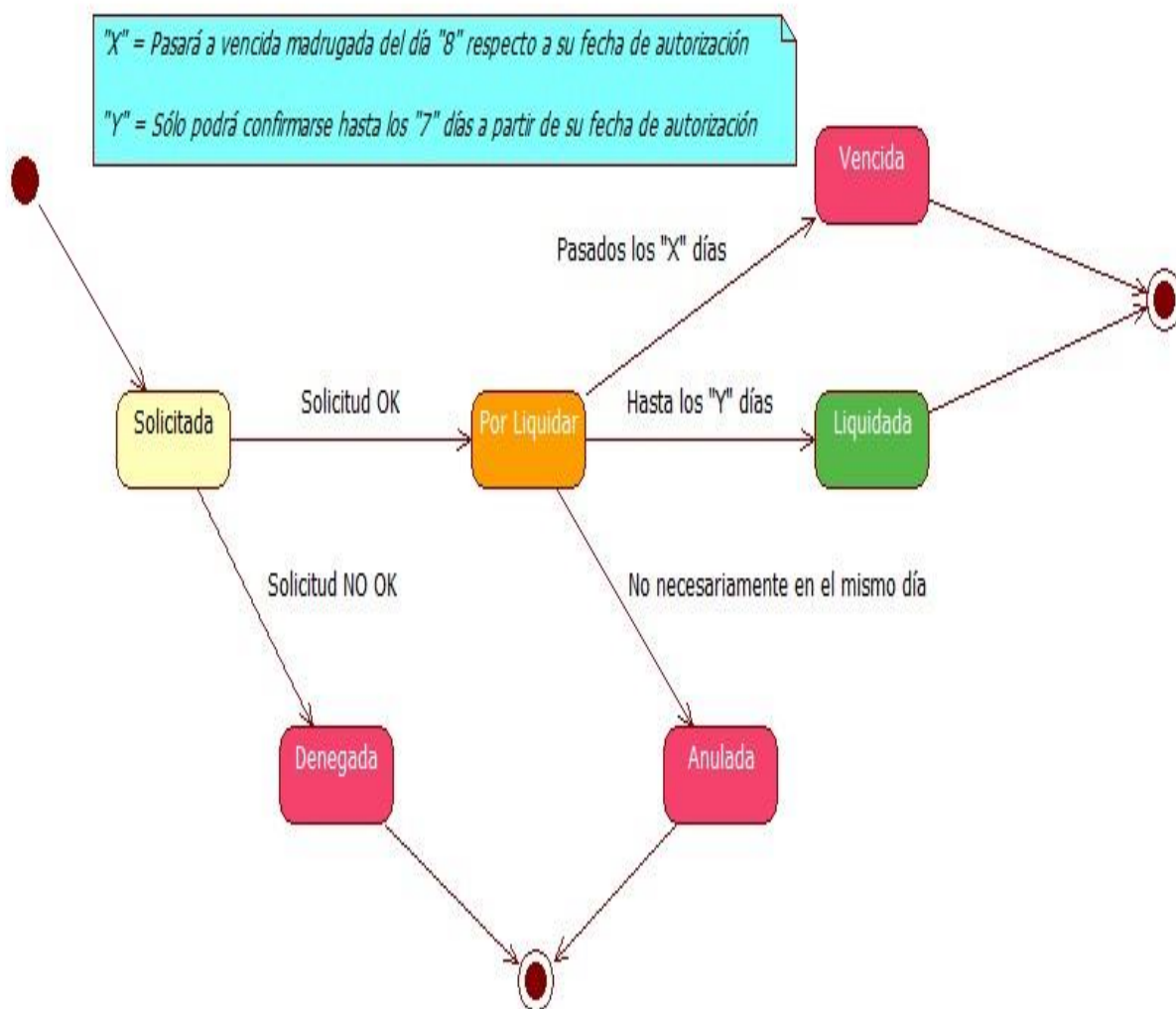
c. Transición de estados para una venta

Una venta si es <<**Contable**>> tiene la siguiente transición de estados:



Una venta <<**Contable**>> al ser aprobada pasa al estado “**Autorizada**”, caso contrario pasa al estado “**Denegada**”. La venta en estado “**Autorizada**” sólo puede ser “**Anulada**” el mismo día que su aprobación. En la madrugada del día siguiente la venta en estado “**Autorizada**” pasará en automático al estado “**Liquidada**”.

Una venta si es <<**No Contable**>> tiene la siguiente transición de estados:



Una venta <<**No Contable**>> al ser aprobada pasa al estado “**Por Liquidar**”, caso contrario pasa al estado “**Denegada**”. La venta en estado “**Por Liquidar**” puede ser “**Anulada**” hasta que no sea confirmada. Si la venta es confirmada pasa al estado “**Liquidada**”. Si la venta no es confirmada en los 7 días de haber sido aprobada, en la madrugada siguiente (*Día 8*) pasará al estado “**Vencida**”.

d. API de autorización de venta

Tipo	Especificación
PDF	API de Autorización de Venta.pdf
SWAGGER	https://app.swaggerhub.com/apis-docs/VisaNetPeru/api.visanet.authorization/1.0.0

e. API de anulación de venta

Tipo	Especificación
PDF	API de Anulación de Venta.pdf
SWAGGER	https://app.swaggerhub.com/apis-docs/VisaNetPeru/api.visanet.void/1.0.0

f. API de confirmación de venta

Tipo	Especificación
PDF	API de Confirmación de Venta.pdf
SWAGGER	https://app.swaggerhub.com/apis-docs/VisaNetPeru/api.visanet.confirmation/1.0.0

g. API de consulta de venta

Tipo	Especificación
PDF	API de Consulta de Venta.pdf
SWAGGER	https://app.swaggerhub.com/apis-docs/VisaNetPeru/api.visanet.retrieve/1.0.0

h. API de antifraude para la venta

Tipo	Especificación
PDF	API de Antifraude para la Venta.pdf
SWAGGER	https://app.swaggerhub.com/apis-docs/VisaNetPeru/api.visanet.antifraud/1.0.0