Pago por token y suscripciones

Guía de implementación

Versión del documento 3.15

Contenido

1. HISTORIAL DEL DOCUMENTO

Versión	Autor	Fecha	Comentario
3.15	Gestión Electrónica de Pagos y Cobranzas S.A.	19/05/23	• Actualización del capítulo *Presentación del servicio*.
3.14.2	Gestión Electrónica de Pagos y Cobranzas S.A.	20/09/22	• Actualización del capítulo *Presentación del servicio* • Actualización de la descripción de los valores del campo **vads_risk_assessment_result** en el capítulo *Tratamiento de los datos de la respuesta*.
3.14	Gestión Electrónica de Pagos y Cobranzas S.A.	26/04/22	• Adición del capítulo *Proponer intentos de pago suplementarios*. • Actualización del capítulo *Medios de pago compatibles*.
3.13	Gestión Electrónica de Pagos y Cobranzas S.A.	10/02/22	• Actualización del capítulo *Medios de pago compatibles*.
3.12	Gestión Electrónica de Pagos y Cobranzas S.A.	12/10/21	• Actualización de la definición del campo **vads_sub_effect_date**.
3.11	Gestión Electrónica de Pagos y Cobranzas S.A.	01/03/2021	• Adición del campo **vads_occurrence_type** en el capítulo *Ciclo de vida de un pago recurrente*. • Adición de un campo que describe la recurrencia en los capítulos relativos a la notificación de una creación de recurrencia. • Adición del capítulo *Pago de un vencimiento de una recurrencia*.
3.10	Gestión Electrónica de Pagos y Cobranzas S.A.	18/01/2021	• Actualización del capítulo *Presentación del servicio*. • Adición del capítulo *Unicidad de los medios de pago registrados*. • Precisión sobre las recurrencias diarias añadidas en los capítulos relativos a la recurrencia de una recurrencia. • Actualización del capítulo *Medios de pago compatibles*. • Actualización del capítulo *Dar de baja automáticamente una recurrencia por Web Services*. • Adición del capítulo *Tarjetas de test* en anexos.
3.9	Gestión Electrónica de Pagos y Cobranzas S.A.	05/05/20	• Aclaraciones sobre la creación de los pagos en caso de vencimiento del medio de pago o de purga de los datos del medio de pago. • Actualización de la configuración de las reglas de notificación.
3.8	Gestión Electrónica de Pagos y Cobranzas S.A.	21/10/19	• Actualización de los medios de pago aceptados. • Adición de un capítulo sobre la garantía de pago durante un pago por token. • Actualización de la definición del campo **vads_sub_desc** en el capítulo Generar un formulario de pago.
3.7	Gestión Electrónica de Pagos y Cobranzas S.A.	05/08/19	• Ahora el algoritmo hash está disponible en el menú **Configuración** > **Tienda**, pestaña **Claves**. • Adición del campo **vads_identifier** como parámetro de entrada para la creación de un token. • Adición de la categoría **Información sobre el análisis de riesgos** en el Diccionario de datos.

Versión	Autor	Fecha	Comentario
			• **vads_threeds_auth_type**: el campo siempre está presente en la respuesta y puede estar vacío. • Ahora el algoritmo hash está disponible en el menú **Configuración** > **Tienda**, pestaña **Claves**. • Aclaraciones proporcionadas sobre el cálculo de firma de IPN. • Aclaraciones proporcionadas sobre el formato de los campos **vads_trans_date** y **vads_presentation_date**. • Aclaración proporcionada sobre el formato de los campos **vads_product_label**, **vads_cust_zip**, **vads_order_id**, **vads_cust_first_name**, **vads_cust_last_name**, **vads_cust_phone**, **vads_cust_cell_phone**, **vads_cust_id**, **vads_cust_city**, **vads_cust_address** • **vads_auth_result**: corrección del formato del campo (an..11) • **vads_contracts**: Posibilidad de forzar la que se utilizará.
3.6	Gestión Electrónica de Pagos y Cobranzas S.A.	22/05/19	Detalles sobre los métodos de creación y de baja de la recurrencia a través de los Terminal ID web services Diccionario de datos: actualización de **vads_trans_date**

3.5	Gestión Electrónica de Pagos y Cobranzas S.A.	26/03/19	• Adición de un detalle sobre la eliminación de datos en el capítulo **Gestionar los pagos por token**.
			• Adición de las horas de creación de los pagos recurrentes en el capítulo **Gestionar los pagos por token**.
			• Actualización de las capturas en los capítulos **Crear un token en modo Test** y **Crear un token en modo Production**
			• Actualización de las capturas en **Crear una recurrencia desde el Back Office Vendedor**
			• Adición del capítulo **Definir la moneda para crear o actualizar un token**.
			• Diccionario de datos:
			  • Adición de un detalle sobre el formato del campo **vads_product_qty**
			  • Adición del campo vads_presentation_date en la sección **Información sobre la transacción**
			  • Adición de un detalle sobre el formato del campo **vads_identifier**
			  • Adición de un detalle sobre el formato del campo **vads_subscription**
			  • Eliminación de los campos **vads_ext_info_donation, vads_ext_info_donation_recipient, vads_ext_info_donation_recipient_name, vads_ext_info_donation_merchant, vads_ext_info_donation_contribution** y **vads_risk_primary_warranty**.

3.4	Gestión Electrónica de Pagos y Cobranzas S.A.	05/02/19	Versión inicial

2. PRESENTACIÓN DEL SERVICIO

Gestión de pagos por token

El servicio de gestión de pagos por token permite que los vendedores ofrezcan a sus compradores la posibilidad de asociar un token a un medio de pago para facilitar los pagos posteriores en el sitio web (sin necesidad de volver a ingresar su número de tarjeta bancaria).

Los token permiten:

- pagos rápidos y seguros.

  El comprador ya no tiene que ingresar sus datos bancarios al hacer pagos posteriores (pago con 1 solo clic).

  Los datos bancarios son almacenados en la plataforma en un entorno de alta seguridad de conformidad con la norma PCI-DSS. Solo el token pasa durante los intercambios.
- efectuar pagos recurrentes (recurrencias).

Los token pueden ser utilizados por todas las tiendas de una misma empresa.

El servicio también permite:

- Identificar las tarjetas próximas a vencer, a fin de poner en alerta al vendedor enviándole un archivo con los tokens cuya tarjeta está por vencer.
- Actualizar los datos bancarios asociados a un token, desde la página de pago o manualmente desde el Back Office Vendedor.
- Detectar automáticamente si el medio de pago ha expirado y proponer la actualización durante un pago por medio de token.
- entonces detectar la creación de un token si el medio de pago ya se ha registrado precedentemente,
- Gestionar el cambio de los otros datos correspondientes al comprador.

Conforme a las reglas de seguridad y de protección de los datos bancarios exigidas por PCI DSS, los datos del medio de pago serán eliminados si transcurrieron 15 meses sin utilizar el token asociado.

El token siempre podrá verse en el Back Office Vendedor y podrá actualizarse con nuevos datos.

Gestión de pagos recurrentes (recurrencia)

El servicio de gestión de pagos recurrentes permite a los vendedores crear suscripciones **con montos y vencimientos fijos**, también llamados “pagos recurrentes” con o sin fecha de fin, dentro del límite de validez de la tarjeta.

Al crear un pago recurrente, el vendedor define la fecha de inicio, el monto de los vencimientos y la regla de recurrencia a aplicar.

Un vez alcanzada la fecha de inicio (también llamada "fecha de efecto"), la plataforma de pago procede automáticamente a tratar los vencimientos.

Entonces el vendedor ya no tiene la posibilidad de modificar el monto de los vencimientos.

Para ser notificado del resultado de un plazo, la regla **URL de notificación al crear una recurrencia** debe estar activada y configurada desde el Back Office Vendedor (menú **Configuración** > **Reglas de notificaciones**).

En el modo PRUEBA, la transacción correspondiente al primer vencimiento se crea a más tardar 1 hora después de la suscripción, según el calendario determinado por la regla de suscripción.

En modo PRODUCTION, las transacciones se crean una vez al día entre medianoche y las 5:00 h, en la zona horaria Europa/París.

2.1. Unicidad de los medios de pago registrados

Por defecto, la plataforma autoriza al comprador registrar varias veces su medio de pago en un mismo sitio de comerciante.

Sin embargo, si el comerciante lo desea, puede activar una opción desde su Back Office Vendedor que permitirá detectar, al crear un token, si el medio de pago ya se ha registrado.

Se desaconseja activar el control de unicidad de los medios de pago registrados si no domina los impactos en su implementación.

Principio de funcionamiento

Una vez activada la opción, la plataforma verifica cada vez que se crea un token, la validez del medio de pago con el emisor y luego procede a verificar la unicidad del medio de pago.

Si nunca se ha registrado un medio de pago, entonces se crea un nuevo token asociado a este medio de pago y se devuelve su identificador al sitio del comerciante al notificar el fin de pago.

Si ya se ha registrado el medio de pago (mismo número y misma fecha de validez), entonces se utiliza el token existente y se devuelve su identificador al sitio del comerciante al notificar el fin de pago.

Los datos del comprador enviados son los transmitidos por el comerciante, no los del token precedentemente registrado.

El campo **vads_identifier_status** se valoriza en **CREATED** incluso si, en este caso, no se ha creado un token.

Entonces la notificación contiene un campo suplementario valorizado en **true**:

- **vads_identifier_previously_registered** para notificar en el formato Formulario API,
- **paymentMethodTokenPreviouslyRegistered** para notificar en formato API REST.

- No hay detección de unicidad del medio de pago al actualizar un token.
- Si el medio de pago está asociado a varios token, la notificación de fin de pago contiene el identificador del token más reciente.
- Se rechaza la creación de un token desde Back Office Vendedor si el medio de pago está asociado a otro token.
- El campo **vads_identifier_previously_registered** no se devuelve al regresar a la tienda.
- El campo **vads_identifier_previously_registered** nunca se devuelve al notificar el fin de pago si no se detecta un duplicado. Por lo tanto, el valor **false** nunca es enviado al sitio del vendedor.

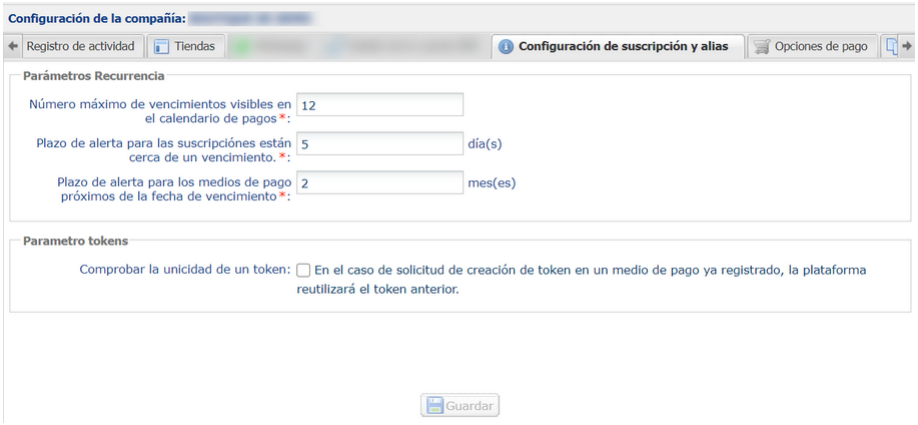
¿Qué hacer en caso de detectar un doble medio de pago?

Todo depende de sus necesidades de oficio.

- Usted puede decidir no hacer nada y brindar el servicio o suministrar el bien al comprador.
- Puede verificar si el código cliente asociado al token existente corresponde al código cliente del comprador. Si no es el caso, puede buscar si el vínculo primario entre los dos clientes explica el por qué el mismo medio de pago lo utilizan dos clientes diferentes.
- Puede verificar si la persona que solicita el registro del medio de pago es la misma que ya ha registrado este medio de pago (por ejemplo, verificando los datos de contacto, la dirección electrónica, el país, etc...).
- Si fracasan todos los controles realizados, es posible que se trate de un fraude y entonces usted puede decidir cancelar el pago.

Activación de la detección de la unicidad de los medios de pago

1. Desde el Back Office Vendedor, abra el menú **Configuración** > **Empresa** y haga clic en la pestaña **Configuración de suscripción y alias**.



2. En el marco **Parametro tokens**, marque la casilla **Comprobar la unicidad de un token.**
3. Haga clic en el botón **Guardar** para registrar sus cambios.

3. MEDIOS DE PAGO COMPATIBLES

Lista de los medios de pago compatibles con el servicio de Gestión de pagos por token:

Código Red	Medio de pago	Tipo de tarjetas (vads_payment_cards)	Acepta el pago por token
FIRSTDATA_IPG	American Express	AMEX	✓
FIRSTDATA_IPG	American Express Bansud	AMEX_BANSUD	✓
FIRSTDATA_IPG	American Express Galicia	AMEX_GALICIA	✓
FIRSTDATA_IPG	American Express HSBC	AMEX_HSBC	✓
FIRSTDATA_IPG	American Express Naranja	AMEX_NARANJA	✓
FIRSTDATA_IPG	American Express Patagonia	AMEX_PATAGONIA	✓
FIRSTDATA_IPG	American Express Santander	AMEX_SANTANDER	✓
FIRSTDATA_IPG	Cabal	CABAL	✓
FIRSTDATA_IPG	Cabal Débito	CABAL_DEBIT	✓
FIRSTDATA_IPG	Carnet	CARNET	✓
FIRSTDATA_IPG	CMR	CMR	✓
FIRSTDATA_IPG	Diners Club	DINERS	✓
FIRSTDATA_IPG	Discover	DISCOVER	✓
FIRSTDATA_IPG	Elo	ELO	✓
FIRSTDATA_IPG	Hiper	HIPER	✓
FIRSTDATA_IPG	Hipercard	HIPERCARD	✓
FIRSTDATA_IPG	JCB	JCB	✓
FIRSTDATA_IPG	Maestro	MAESTRO	✓
FIRSTDATA_IPG	Mastercard	MASTERCARD	✓
FIRSTDATA_IPG	Mastercard Débito	MASTERCARD_DEBIT	✓
FIRSTDATA_IPG	Mastercard BBVA	MC_BBVA	✓
FIRSTDATA_IPG	Mastercard Cencosud	MC_CENCOSUD	✓
FIRSTDATA_IPG	Mastercard CityBank	MC_CITYBANK	✓
FIRSTDATA_IPG	Mastercard Columbia	MC_COLOMBIA	✓
FIRSTDATA_IPG	Mastercard Comafi	MC_COMAFI	✓
FIRSTDATA_IPG	Mastercard Cordobesa	MC_CORDOBESA	✓
FIRSTDATA_IPG	Mastercard Falabella	MC_FALABELLA	✓
FIRSTDATA_IPG	Mastercard Galicia	MC_GALICIA	✓
FIRSTDATA_IPG	Mastercard HSBC	MC_HSBC	✓
FIRSTDATA_IPG	Mastercard ICBC	MC_ICBC	✓
FIRSTDATA_IPG	Mastercard Itau	MC_ITAU	✓
FIRSTDATA_IPG	Mastercard Macro	MC_MACRO	✓
FIRSTDATA_IPG	Mastercard Nación	MC_NACION	✓
FIRSTDATA_IPG	Mastercard Patagonia	MC_PATAGONIA	✓
FIRSTDATA_IPG	Mastercard Santander	MC_SANTANDER	✓
FIRSTDATA_IPG	Naranja	NARANJA	✓
FIRSTDATA_IPG	Sorocred	SOROCRED	✓
FIRSTDATA_IPG	Tuya	TUYA	✓
FIRSTDATA_IPG	Visa	VISA	✓
FIRSTDATA_IPG	Visa BBVA	VISA_BBVA	✓

Código Red	Medio de pago	Tipo de tarjetas (vads_payment_cards)	Acepta el pago por token
FIRSTDATA_IPG	Visa Chaco	VISA_CHACO	✓
FIRSTDATA_IPG	Visa Ciudad	VISA_CIUDAD	✓
FIRSTDATA_IPG	Visa Columbia	VISA_COLUMBIA	✓
FIRSTDATA_IPG	Visa Comafi	VISA_COMAFI	✓
FIRSTDATA_IPG	Visa Cordobesa	VISA_CORDOBESA	✓
FIRSTDATA_IPG	Visa Corrientes	VISA_CORRIENTES	✓
FIRSTDATA_IPG	Visa Credicoop	VISA_CREDICOOP	✓
FIRSTDATA_IPG	Visa Débito	VISA_DEBIT	✓
FIRSTDATA_IPG	Visa Electron	VISA_ELECTRON	✓
FIRSTDATA_IPG	Visa Formosa	VISA_FORMOSA	✓
FIRSTDATA_IPG	Visa Galicia	VISA_GALICIA	✓
FIRSTDATA_IPG	Visa Hipotecario	VISA_HIPOTECARIO	✓
FIRSTDATA_IPG	Visa HSBC	VISA_HSBC	✓
FIRSTDATA_IPG	Visa ICBC	VISA_ICBC	✓
FIRSTDATA_IPG	Visa Industrial	VISA_INDUSTRIAL	✓
FIRSTDATA_IPG	Visa Itau	VISA_ITAU	✓
FIRSTDATA_IPG	Visa Macro	VISA_MACRO	✓
FIRSTDATA_IPG	Visa Nación	VISA_NACION	✓
FIRSTDATA_IPG	Visa Neuquen	VISA_NEUQUEN	✓
FIRSTDATA_IPG	Visa Patagonia	VISA_PATAGONIA	✓
FIRSTDATA_IPG	Visa Provincia	VISA_PROVINCIA	✓
FIRSTDATA_IPG	Visa Santander	VISA_SANTANDER	✓
LINK	Cabal Débito	CABAL_DEBIT	✓
LINK	Maestro	MAESTRO	✓
LINK	Mastercard Débito	MASTERCARD_DEBIT	✓
LINK	Visa Débito	VISA_DEBIT	✓
PAYPAL	Pago con PayPal	PAYPAL	✗
PAYPAL_SB	Pago con PayPal - Modo sandbox	PAYPAL_SB	✗
PIM	Pim	PIM	✗
PRISMA	Cabal	CABAL	✓
PRISMA	Cabal Débito	CABAL_DEBIT	✓
PRISMA	CMR	CMR	✓
PRISMA	Maestro	MAESTRO	✗
PRISMA	Mastercard	MASTERCARD	✗
PRISMA	Mastercard Débito	MASTERCARD_DEBIT	✗
PRISMA	Mastercard BBVA	MC_BBVA	✗
PRISMA	Mastercard Cencosud	MC_CENCOSUD	✗
PRISMA	Mastercard CityBank	MC_CITYBANK	✗
PRISMA	Mastercard Columbia	MC_COLOMBIA	✗
PRISMA	Mastercard Comafi	MC_COMAFI	✗
PRISMA	Mastercard Cordobesa	MC_CORDOBESA	✗
PRISMA	Mastercard Falabella	MC_FALABELLA	✗
PRISMA	Mastercard Galicia	MC_GALICIA	✗
PRISMA	Mastercard ICBC	MC_ICBC	✗
PRISMA	Mastercard Itau	MC_ITAU	✗

Código Red	Medio de pago	Tipo de tarjetas (vads_payment_cards)	Acepta el pago por token
PRISMA	Mastercard Macro	MC_MACRO	✖
PRISMA	Mastercard Nación	MC_NACION	✖
PRISMA	Mastercard Patagonia	MC_PATAGONIA	✖
PRISMA	Mastercard Santander	MC_SANTANDER	✖
PRISMA	Naranja	NARANJA	✔
PRISMA	Visa	VISA	✔
PRISMA	Visa BBVA	VISA_BBVA	✔
PRISMA	Visa Chaco	VISA_CHACO	✔
PRISMA	Visa Ciudad	VISA_CIUDAD	✔
PRISMA	Visa Columbia	VISA_COLUMBIA	✔
PRISMA	Visa Comafi	VISA_COMAFI	✔
PRISMA	Visa Cordobesa	VISA_CORDOBESA	✔
PRISMA	Visa Corrientes	VISA_CORRIENTES	✔
PRISMA	Visa Credicoop	VISA_CREDICOOP	✔
PRISMA	Visa Credicoop	VISA_CREDICOOP	✔
PRISMA	Visa Débito	VISA_DEBIT	✔
PRISMA	Visa Electron	VISA_ELECTRON	✔
PRISMA	Visa Formosa	VISA_FORMOSA	✔
PRISMA	Visa Galicia	VISA_GALICIA	✔
PRISMA	Visa Hipotecario	VISA_HIPOTECARIO	✔
PRISMA	Visa HSBC	VISA_HSBC	✔
PRISMA	Visa ICBC	VISA_ICBC	✔
PRISMA	Visa Industrial	VISA_INDUSTRIAL	✔
PRISMA	Visa Itau	VISA_ITAU	✔
PRISMA	Visa Macro	VISA_MACRO	✔
PRISMA	Visa Nación	VISA_NACION	✔
PRISMA	Visa Neuquen	VISA_NEUQUEN	✔
PRISMA	Visa Patagonia	VISA_PATAGONIA	✔
PRISMA	Visa Provincia	VISA_PROVINCIA	✔
PRISMA	Visa Santander	VISA_SANTANDER	✔

4. COMPARTIR EL TOKEN

Es posible compartir el token entre varias entidades jurídicas.

Los tokens compartidos entre varias entidades jurídicas deben ser únicos y deben ser generados obligatoriamente por la plataforma de pago.

Sin embargo, esta funcionalidad está sujeta a condiciones particulares. Por favor, contacte al interlocutor de su plataforma de pago para conocerlas.

5. CASOS DE USO

El formulario de pago permite realizar las siguientes operaciones clasificadas por caso.

Cada uno de estos casos corresponde a una valorización diferente del campo **vads_page_action**.

Casos de uso	Valorización del campo vads_page_action
Creación del token sin pago	REGISTER
Actualización de la información asociada al token.	REGISTER_UPDATE
Creación del token durante un pago	REGISTER_PAY
Creación del token al suscribirse a una recurrencia	REGISTER_SUBSCRIBE
Creación del token al suscribir a una recurrencia acompañada de un pago	REGISTER_ PAY_SUBSCRIBE
Pago por Token	PAYMENT
Uso de un token para suscribirse a una recurrencia	SUBSCRIBE

Según el tipo de uso (valorización del campo **vads_page_action**), las interacciones entre el comprador y la página de pago diferirán.

5.1. Creación del token sin pago

Este caso corresponde a la simple creación de un token.

1. El sitio web vendedor una *solicitud de creación de token*.

   El comprador elige el método de pago que se debe registrar, entrega los datos de este y luego valida.
2. La plataforma de pago inicia el proceso de autenticación del portador con el emisor.
3. Una vez que la autentificación ha terminado, la plataforma realiza la solicitud de información con los datos de autentificación del titular.
4. La plataforma de pago notifica al sitio web vendedor el *resultado*.

Esta operación, se da lugar a la creación de una transacción de tipo VERIFICATION, que aparece en el Back Office Vendedor y posee las siguientes características:

- su monto es de 1.00 USD,
- su estado es, o bien "Aceptado" o bien "Rechazado",
- nunca se envía al banco y permanece en la pestaña "Transacciones en curso".

El token no se creará si la solicitud de autorización es rechazada.

La plataforma muestra el ticket al comprador. En particular, contiene:

- ell token creado recientemente,
- Los datos del comprador.

Si ha configurado las reglas de notificación correspondientes, el comprador recibirá un correo electrónico:

- la confirmación del registro de sus datos bancarios en la plataforma de pago de la tienda,
- su token que podrá utilizar posteriormente para efectuar otra operación bancaria.

5.2. Cambio de información asociada al token

Por iniciativa del comprador, este caso corresponde a la actualización de los datos relacionados con su medio de pago y/o sus datos personales.

1. El sitio web vendedor una *solicitud de actualización de un token*.

   El comprador elige el método de pago que se debe registrar, entrega los datos de este y luego valida.

2. La plataforma de pago inicia el proceso de autenticación del portador con el emisor.
3. Una vez que la autentificación ha terminado, la plataforma realiza la solicitud de información con los datos de autentificación del titular.
4. La plataforma de pago notifica al sitio web vendedor el *resultado*.

> Esta operación, se da lugar a la creación de una transacción de tipo VERIFICATION, que aparece en el Back Office Vendedor y posee las siguientes características:
>
> - su monto es de 1.00 USD,
> - su estado es, o bien "Aceptado" o bien "Rechazado",
> - nunca se envía al banco y permanece en la pestaña "Transacciones en curso".

> El token no se actualizará si la solicitud de autorización es rechazada.

La plataforma muestra el ticket al comprador. En particular, contiene:

- el token,
- Los datos del comprador.

Si ha configurado las reglas de notificación correspondientes, el comprador recibirá un correo electrónico:

- la confirmación del registro de sus datos bancarios en la plataforma de pago de la tienda,
- su token que podrá utilizar posteriormente para efectuar otra operación bancaria.

5.3. Creación del token durante un pago

En este caso, los parámetros necesarios para la inscripción se completan con los parámetros que se requieren para una solicitud de pago.

1. El sitio web vendedor emite una *solicitud de pago con creación de token*.

   El comprador elige el método de pago que se debe registrar, entrega los datos de este y luego valida.

2. La plataforma de pago inicia el proceso de autenticación del portador con el emisor.

   > En este caso, la reglamentación exige una autentificación fuerte.
   >
   > La Autenticación se realiza en el monto del pago.

3. Una vez que la autentificación ha terminado, la plataforma realiza la solicitud de autorización con los datos de autentificación del titular.

4. La plataforma de pago notifica al sitio web vendedor el *resultado*.

   > El token no se creará si la solicitud de autorización es rechazada.

   La plataforma muestra el ticket al comprador. En particular, contiene:

   - el resultado del pago,
   - el token creado recientemente.

   Si ha configurado las reglas de notificación correspondientes, el comprador recibirá un correo electrónico:

   - el ticket de pago
   - la confirmación del registro de sus datos bancarios en la plataforma de pago de la tienda,
   - su token que podrá utilizar posteriormente para efectuar otra operación bancaria.

5.4. Creación del token al suscribirse a una recurrencia

Además de la información utilizada en el caso de la **Creación del token sin pago**, este caso de uso también debe mostrar la información relacionada con la recurrencia, tal como:

- el monto inicial de la recurrencia (monto utilizado durante el/los primer/os vencimientos) si este es diferente (opcional),
- el monto de la recurrencia (monto de los vencimientos, o bien el utilizado en los siguientes vencimientos cuando el primer es diferente).

> **No se realizará ningún pago al momento de la recurrencia. Solamente se realizará una solicitud de información para confirmar los datos del medio de pago.**
>
> El primer pago se realizará en la fecha efectiva, entre las 00:00 y las 05:00 h.

El día del pedido:

1. El sitio web vendedor una *solicitud de creación de token y inscripción a una suscripción.*

   El comprador elige el método de pago que desea registrar, entrega los datos de este y luego valida.
2. La plataforma de pago inicia el proceso de autenticación del portador con el emisor.
3. Una vez que la autentificación ha terminado, la plataforma realiza la solicitud de información con los datos de autentificación del titular.
4. La plataforma de pago notifica al sitio web vendedor el *resultado*.

> Esta operación, se da lugar a la creación de una transacción de tipo VERIFICATION, que aparece en el Back Office Vendedor y posee las siguientes características:
>
> - su monto es de 1.00 USD,
> - su estado es, o bien "Aceptado" o bien "Rechazado",
> - nunca se envía al banco y permanece en la pestaña "Transacciones en curso".

> El token no se creará si la solicitud de autorización es rechazada.

La plataforma muestra el ticket al comprador. En particular, contiene:

- ell token creado recientemente,
- Los montos de la recurrencia.

Si ha configurado las reglas de notificación correspondientes, el comprador recibirá un correo electrónico:

- la confirmación del registro de sus datos bancarios en la plataforma de pago de la tienda,
- la confirmación del registro de la recurrencia.

A cada cuotas :

1. La plataforma de pago realiza una solicitud de autorización por el monto de la cuota.
2. El emisor procede a la solicitud de autorización.

3. Si el comercio ha activado la regla de notificación **URL de notificación al crear una recurrencia**, la plataforma de pago notifica al sitio web vendedor el *resultado del pago*.

5.5. Creación del token al suscribir a una recurrencia acompañada de un pago

Este caso de uso debe mostrar información tal como:

- la información sobre el comprador,
- el identificador de la transacción,
- la información sobre la recurrencia (montos).

Ejemplo de uso: una recurrencia de un monto de X USD/ N meses con gastos de puesta en servicio para pagar al tomar el pedido.

El día del pedido:

1. El sitio web vendedor emite una *solicitud de creación de token y de suscripción con pago inmediato*.

   El comprador elige el método de pago que se debe registrar, entrega los datos de este y luego valida.
2. La plataforma de pago inicia el proceso de autenticación del portador con el emisor.
3. Una vez que la autentificación ha terminado, la plataforma realiza la solicitud de autorización con los datos de autentificación del titular.
4. La plataforma de pago notifica al sitio web vendedor el *resultado*.

   En particular, la respuesta contiene:

   - el resultado del pago,
   - el detalle de la recurrencia,
   - el token creado recientemente.

   > El token y la suscripción no se crearán si la solicitud de autorización es rechazada.

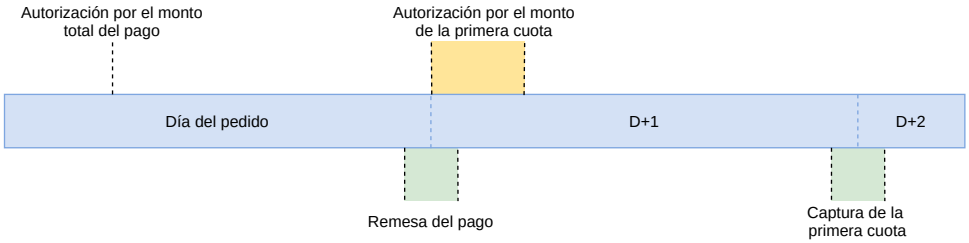
   La plataforma muestra el ticket al comprador. En particular, contiene:

   - el resultado del pago,
   - Los montos de la recurrencia,
   - ell token creado recientemente.

   Si ha configurado las reglas de notificación correspondientes, el comprador recibirá un correo electrónico:

   - el ticket de pago,
   - la confirmación del registro de sus datos bancarios en la plataforma de pago de la tienda,
   - la confirmación del registro de la recurrencia,
   - su token que podrá utilizar posteriormente para efectuar otra operación bancaria.

> El monto del pago se cobrará al comprador el día del pedido (o al día siguiente del pedido según el adquirente).
>
> El cobro de la primera cuota de la suscripción se realizará en la fecha efectiva, entre las 00:00 y las 05:00 de la mañana.
>
> Si la fecha efectiva se fija al día del pedido, se cobrará al comprador dos días seguidos (el día del pago y al día siguiente, la primera cuota)



Si desea que el pago realizado el día del pedido corresponda a la primera cuota de la suscripción, debe adaptar la fecha efectiva. Por ejemplo, para una suscripción mensual, la fecha efectiva debe fijarse a +30 días al hacer la solicitud de creación de la suscripción.

A cada cuotas :

1. La plataforma de pago realiza una solicitud de autorización por el monto de la cuota.
2. El emisor procede a la solicitud de autorización.
3. Si el comercio ha activado la regla de notificación **URL de notificación al crear una recurrencia**, la plataforma de pago notifica al sitio web vendedor el *resultado del pago*.

5.6. Pago por Token

El pago por token permite, si ya se ha registrado un token previamente, realizar pagos unitarios o múltiples sin tener que seleccionar un medio de pago ni ingresar datos bancarios.

En dicho caso, se presenta una simple etapa de confirmación con un resumen de la transacción (número y monto).

1. El sitio web vendedor emite una *solicitud de pago con reutilización de un token*.

   El comprador verifica la información que muestra la página de pago, introduce el CVV de su tarjeta y la valida.

   > Si el token está asociado a un medio de pago expirado, la plataforma de pago propondrá automáticamente al comprador ingresar nuevos datos bancarios a fin de realizar el pago y actualizar el token asociado a este.

2. La plataforma de pago inicia el proceso de autenticación del portador con el emisor.
3. Una vez que la autentificación (challenge o frictionless) ha terminado, la plataforma realiza la solicitud de autorización con los datos de autentificación del titular.
4. La plataforma de pago notifica al sitio web vendedor el *resultado*.

   La plataforma muestra el ticket al comprador.

   Si ha configurado las reglas de notificación correspondientes, el comprador recibirá la confirmación del pago por correo electrónico.

5.7. Uso de un token para suscribirse a una recurrencia

Una vez creado el token, es posible agregar una o varias recurrencia/s adicional/es que utilizará/n este token.

Al suscribirse a una nueva recurrencia, no se solicitará ingresar ningún dato bancario. Solo se requerirá una confirmación por parte del comprador.

No se realizará ningún pago al momento de la recurrencia. Solamente se realiza una solicitud de información para confirmar los datos del medio de pago.

El primer pago se realizará en la fecha efectiva, entre las 00:00 y las 05:00 h.

El día del pedido:

1. El sitio web vendedor emite una *solicitud de suscripción a partir de un token existente*.

   El comprador verifica los datos de la suscripción y valida.

2. La plataforma de pago notifica al sitio web vendedor el *resultado*.

   La plataforma muestra el ticket al comprador. Contiene los montos de la suscripción.

   Si ha configurado las reglas de notificación correspondientes, el comprador recibirá un correo electrónico de confirmación del registro de la recurrencia.

A cada cuotas :

1. La plataforma de pago realiza una solicitud de autorización por el monto de la cuota.
2. El emisor procede a la solicitud de autorización.
3. Si el comercio ha activado la regla de notificación **URL de notificación al crear una recurrencia**, la plataforma de pago notifica al sitio web vendedor el *resultado del pago*.

6. CICLO DE VIDA DE UN PAGO RECURRENTE

La recurrencia se inicia en su fecha efectiva.

La plataforma de pago creará entonces los pagos conforme al registro de vencimientos definido por la regla de recurrencia enviada en el formulario de creación de la recurrencia (campo vads_sub_desc).

Por cada vencimiento de una recurrencia, si la regla **URL de notificación al crear una recurrencia** se activa y configura correctamente, el sitio del vendedor recibirá el resultado del pago en su URL de notificación (IPN).

En particular, la notificación contiene:

- el campo **vads_subscription**, que indica la referencia de la recurrencia,
- el campo **vads_recurrence number**, que indica el número del vencimiento,
- el campo **vads_occurrence_type**, que indica de qué vencimiento se trata (primero, enésimo o último vencimiento),
- el campo **vads_trans_status**, que indica el estado del pago (aceptado o rechazado).

En caso de pago denegado:

- el vendedor no será notificado por correo electrónico,
- el pago no volverá a solicitarse automáticamente.

Si el medio de pago alcanza su fecha de vencimiento, se crea una transacción rechazada sin llamada al banco emisor. El detalle del error (vads_payment_error) se establece en 8 - La fecha de vencimiento de la tarjeta no permite esta acción.

Si los datos del medio de pago fueron purgados tras un periodo de inactividad de 15 meses, se crea una transacción rechazada sin llamada al banco emisor. El detalle del error (vads_payment_error) se establece en 107 - El medio de pago asociado al token ya no es válido.

Caso particular de las recurrencias con frecuencia diaria

Si solicita la creación de una recurrencia para debitar el portador a diario (RRULE:FREQ=DAILY;INTERVAL=1) y que la fecha de efecto solicitada (vads_sub_effect_date) corresponde a la fecha de creación de la recurrencia, entonces la plataforma de pago tratará esta recurrencia al día siguiente (entre medianoche y las 5:00), se crearán 2 pagos:

- el de la víspera (que corresponde a la fecha de efecto),
- y el del día.

Para evitarlo, se aconseja transmitir una fecha de efecto al día siguiente del día en que se creó la recurrencia.

7. OFRECER INTENTOS DE PAGO ADICIONALES

Cuando se rechaza un pago, puede ofrecer al comprador la posibilidad de intentar con otro medio de pago.

La cantidad de intentos suplementarios se puede parametrizar desde el Back Office Vendedor:

1. Abra el menú **Configuración** > **Tienda** y haga clic en el nombre de la tienda cuya configuración desea modificar.
2. Seleccione la pestaña **Configuración**.
3. Indique el número de intentos adicionales autorizados en caso de rechazo de un pago.

   Si usted configura 2 intentos suplementarios, entonces el comprador podrá realizar en total 3 intentos de pago.
4. Si lo desea, puede activar el envío de una notificación al final del pago (IPN) para cada intento rechazado marcando la casilla **URL de notificación sobre tentativa rechazada**.
5. Haga clic en el botón **Guardar**.

No se podrán ofrecer intentos adicionales:

- si el vendedor solicitó un retorno automático a la tienda en el campo **vads_redirect_error_timeout**,
- si se trata de un pago en varios vencimientos.

Intentos de pago suplementarios y pago por alias (1 clic).

Si el pago en 1 clic es rechazado, el comprador deberá elegir otro método de pago e ingresar los datos de su tarjeta.

Si el pago es aceptado:

- la transacción no se asociará al token transmitido en la solicitud,
- el token no será actualizado.

8. ESTABLECER DIÁLOGO CON LA PLATAFORMA DE PAGO

El diálogo entre el sitio web vendedor y la plataforma de pago se realiza mediante un intercambio de datos.

Para crear un pago, estos datos se envían a través de un formulario HTML por el navegador del comprador.

Al final del pago, el resultado se transmite al sitio web vendedor de dos maneras:

- automáticamente mediante notificaciones denominadas URL de notificación instantánea (también conocidas como IPN, del inglés Instant Payment Notification), consulte el capítulo **Configurar notificaciones**.
- en el navegador cuando el comprador hace clic en el botón para volver al sitio web vendedor, consulte el capítulo **Gestionar el diálogo al sitio web vendedor**.

Para garantizar la seguridad de los intercambios, los datos se firmarán mediante una clave conocida solamente por el comerciante y la plataforma de pago.

8.1. Similitudes con el pago unitario

Todas las funcionalidades disponibles para el pago unitario lo están también para los pagos por token y por recurrencias.

Para más información, consulte el *Guía de implementación Formulario API*

A continuación, encontrará una lista no exhaustiva:

- Pago unitario: se realiza en una vez o en forma fraccionada.
- Gestión de varias monedas.
- Gestión de varios medios de pago y de afiliaciones de vendedores asociados.
- Personalización de las páginas de pago.
- Visualización en un iframe.

9. CONFIGURAR NOTIFICACIONES

Varios tipos de notificaciones están a disposición en el Back Office Vendedor.

- Llamada URL de notificación
- E-mail enviado al vendedor
- E-mail enviado al comprador

Permiten gestionar los eventos (pago aceptado, abandono por parte del comprador, cancelación por parte del vendedor...) que generarán el envío de una notificación al sitio web vendedor, al vendedor o al comprador.

Las notificaciones de tipo Llamada URL de notificación son las más importantes, pues representan el único medio confiable para que el sitio del comerciante pueda obtener el resultado de un pago.

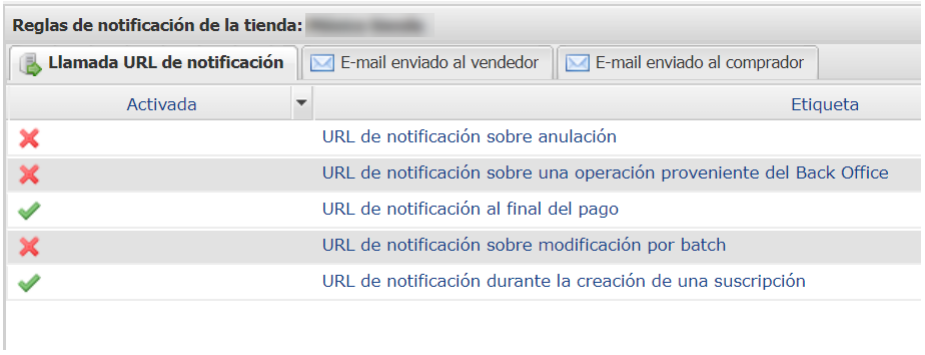
Si la plataforma no logra conectarse a la URL de su página, se enviará un correo electrónico a la dirección especificada.

Este contiene:

- El código HTTP del error encontrado
- Elementos de análisis en función del error
- Sus consecuencias
- El procedimiento a seguir desde el Back Office Vendedor para enviar la solicitud a la URL definida.

Para acceder a la gestión de las reglas de notificación:

Vaya al menú **Configuración** > **Reglas de notificaciones**.



9.1. Configurar la notificación al final del pago

Esta regla permite notificar al sitio del comerciante en los siguientes casos:

- Pago aceptado
- Pago rechazado
- Creación o actualización de un token
- Registro de una recurrencia

Esta notificación es indispensable para comunicar el resultado de una solicitud de pago, de una creación de token o de una creación de suscripción.

Esta informará el resultado al sitio del vendedor si el cliente no ha hecho clic en el botón Volver a la tienda.

1. Haga clic derecho en la línea **URL de notificación al final del pago**.
2. Seleccione **Gestionar la Regla**.
3. En la sección **Configuración general**, ingrese el campo **Dirección(es) e-mail(s) a notificar en caso de falla**.

   Para especificar varias direcciones de e-mail, sepárelas con un punto y coma.
4. Marque la casilla **Reenvío automático en caso de falla** si desea autorizar a la plataforma a reenviar automáticamente la notificación hasta 4 veces en caso de falla.

   Para más información, consulte el capítulo *Reejecutar automáticamente en caso de fallo* en la página 32.
5. En la sección **URL de notificación de la API formulario V1, V2**, ingrese la URL de su página en los campos **URL a llamar en modo PRUEBA** y **URL a llamar en modo PRODUCCIÓN** si desea recibir las notificaciones en el formato Formulario API.
6. Guarde sus cambios.

9.2. Configurar la notificación en caso de abandono/cancelación

Esta regla permite notificar al sitio del comerciante en los siguientes casos:

- En caso de abandono o cancelación por parte del comprador, a través del botón **Cancelar y regresar a la tienda**.
- Cuando el comprador no ha terminado su pago antes de la expiración de su sesión de pago.

  La duración máxima de una sesión de pago es de 10 minutos.

Esta regla está **desactivada por defecto**.

1. Haga clic derecho en la línea **URL de notificación al abandonar (comprador)**.
2. Seleccione **Gestionar la Regla**.
3. En la sección **Configuración general**, ingrese el campo **Dirección(es) e-mail(s) a notificar en caso de falla**.

   Para especificar varias direcciones de e-mail, sepárelas con un punto y coma.
4. Marque la casilla **Reenvío automático en caso de falla** si desea autorizar a la plataforma a reenviar automáticamente la notificación hasta 4 veces en caso de falla.

   Para más información, consulte el capítulo *Reejecutar automáticamente en caso de fallo* en la página 32.
5. En la sección **URL de notificación de la API formulario V1, V2**, ingrese la URL de su página en los campos **URL a llamar en modo PRUEBA** y **URL a llamar en modo PRODUCCIÓN** si desea recibir las notificaciones en el formato Formulario API.
6. En la sección **URL de notificación de la API REST**, ingrese la URL de su página en los campos **URL de la IPN a llamar en modo prueba** y **URL de la IPN a llamar en modo producción** si utiliza el cliente JavaScript.
7. Guarde sus cambios.
8. Active la regla con un clic derecho en **URL de notificación al abandonar (comprador)** y seleccione **Activar la regla**.

9.3. Configurar la notificación de una operación proveniente del Back Office

Esta regla permite notificar al sitio del comerciante cada vez que se realiza una operación en el Back Office Vendedor:

- Creación de un pago manual (aceptado o rechazado)
- Modificación de una transacción
- Duplicación de una transacción
- Reembolso de una transacción
- Cancelación de una transacción
- Validación de una transacción
- Creación de un token
- Actualización de un token

1. Haga clic derecho en la línea **URL de notificación al modificar una transacción en el Back Office (vendedor)**.
2. Seleccione **Gestionar la Regla**.
3. En la sección **Configuración general**, ingrese el campo **Dirección(es) e-mail(s) a notificar en caso de falla**.

   Para especificar varias direcciones de e-mail, sepárelas con un punto y coma.
4. Marque la casilla **Reenvío automático en caso de falla** si desea autorizar a la plataforma a reenviar automáticamente la notificación hasta 4 veces en caso de falla.

   Para más información, consulte el capítulo *Reejecutar automáticamente en caso de fallo* en la página 32.
5. En la sección **URL de notificación de la API formulario V1, V2**, ingrese la URL de su página en los campos **URL a llamar en modo PRUEBA** y **URL a llamar en modo PRODUCCIÓN** si desea recibir las notificaciones en el formato Formulario API.
6. En la sección **URL de notificación de la API REST**, ingrese la URL de su página en los campos **URL de la IPN a llamar en modo prueba** y **URL de la IPN a llamar en modo producción** si utiliza el cliente JavaScript.
7. Guarde sus cambios.
8. Active la regla con un clic derecho en **URL de notificación al modificar una transacción en el Back Office (vendedor)** y seleccione **Activar la regla**.

9.4. Configurar la notificación al crear una recurrencia

Esta regla permite notificar al sitio del comerciante en los siguientes casos:

- Cuando la plataforma de pago crea un nuevo vencimiento de un pago recurrente.
- En cada nuevo intento de pago, después de que un vencimiento de un pago recurrente fue rechazado.

  Necesita la activación de la opción de autorización anticipada.

Esta regla está **desactivada por defecto**.

1. Haga clic derecho en la línea **URL de notificación al crear una recurrencia**.
2. Seleccione **Gestionar la Regla**.
3. En la sección **Configuración general**, ingrese el campo **Dirección(es) e-mail(s) a notificar en caso de falla**.

   Para especificar varias direcciones de e-mail, sepárelas con un punto y coma.
4. Marque la casilla **Reenvío automático en caso de falla** si desea autorizar a la plataforma a reenviar automáticamente la notificación hasta 4 veces en caso de falla.

   Para más información, consulte el capítulo *Reejecutar automáticamente en caso de fallo* en la página 32.
5. En la sección **URL de notificación de la API formulario V1, V2**, ingrese la URL de su página en los campos **URL a llamar en modo PRUEBA** y **URL a llamar en modo PRODUCCIÓN** si desea recibir las notificaciones en el formato Formulario API.
6. En la sección **URL de notificación de la API REST**, ingrese la URL de su página en los campos **URL de la IPN a llamar en modo prueba** y **URL de la IPN a llamar en modo producción** si utiliza el cliente JavaScript.
7. Guarde sus cambios.
8. Active la regla con un clic derecho en **URL de notificación al crear una recurrencia** y seleccione **Activar la regla**.

9.5. Reejecutar automáticamente en caso de fallo

El reenvío automático no se aplica a las notificaciones activadas manualmente desde el Back Office Vendedor.

El vendedor puede activar un mecanismo que permita a la plataforma de pago reenviar automáticamente las notificaciones cuando el sitio del comerciante es realmente inalcanzable **hasta 4 veces**.

Una notificación se considerará infructuosa si el código de retorno HTTP devuelto por el sitio del comerciante no se encuentra en la siguiente lista: **200**, **201**, **202**, **203**, **204**, **205**, **206**, **301**, **302**, **303**, **307**, **308**.

Los intentos de llamada se programan a horas fijas cada 15 minutos (00, 15, 30, 45).

Tras cada tentativa infructuosa, se enviará un e-mail de alerta a la dirección especificada en la configuración de la regla de notificación correspondiente.

El asunto del e-mail de alerta contiene el número del intento de enviar la notificación. Se presenta en la forma attempt # seguida del número de intento.

- Ejemplo de asunto de un correo electrónico de alerta recibido después de la primera notificación fallida al final de un pago:

```
[MODE TEST] Mi Tienda - Tr. Ref. 067925 / FALLO al invocar a su URL de notificación
 [unsuccessful attempt #1]
```

- Ejemplo de asunto de e-mail recibido en el segundo error:

```
[MODE TEST] Mi Tienda - Tr. Ref. 067925 / FALLO al invocar a su URL de notificación
 [unsuccessful attempt #2]
```

- Ejemplo de asunto de e-mail recibido en el tercer error:

```
[MODE TEST] Mi Tienda - Tr. Ref. 067925 / FALLO al invocar a su URL de notificación
 [unsuccessful attempt #3]
```

- Ejemplo de asunto de e-mail recibido en el último intento:

```
[MODE TEST] Mi Tienda - Tr. Ref. 067925 / FALLO al invocar a su URL de notificación
 [unsuccessful attempt #last]
```

  Para notificar al sitio del comerciante el fallo del último intento de notificación, el asunto del e-mail incluirá attempt #last.

Cuando hay reenvío automático, parte de la información no se guarda en la base de datos o se modifica.

Ejemplos de campos no disponibles / no registrados en la base de datos:

Nombre del campo	Descripción
vads_page_action	Operación realizada
vads_payment_config	Tipo de pago (al contado o en vencimientos)
vads_action_mode	Modo de adquisición de la información del medio de pago

Ejemplos de campos enviados con diferentes valores:

Nombre del campo	Nuevo valor
vads_url_check_src	Se asignará el valor **RETRY** en el caso de un reenvío automático.
vads_trans_status	El estado de la transacción puede variar entre la llamada inicial y el reenvío automático (cancelación del vendedor, remesa al banco de la transacción, etc.).
vads_hash	El valor de este campo se regenera en cada llamada.
firma	El valor de la firma depende de los diferentes estados que pueden variar entre la llamada inicial y el reenvío automático.

Estos e-mails detallan:

- el problema encontrado
- los elementos de análisis en función del error
- sus consecuencias
- el procedimiento a seguir desde el Back Office Vendedor para activar la notificación de forma manual.

Después del cuarto intento, todavía es posible reenviar la URL de notificación **manualmente** desde su Back Office Vendedor.

Atención, durante el período de reenvío automático, cualquier llamada manual a la URL de notificación afectará el número de reintentos automáticos:

- una llamada manual exitosa detendrá el reenvío automático
- una llamada manual fallida no tendrá ningún impacto en el reenvío automático actual.

9.6. Configurar correos electrónicos enviados al comprador

En la pestaña **E-mail enviado al comprador**:

1. Haga clic derecho en la regla por modificar y seleccione **Activar la regla**.
2. Haga otro clic derecho en la regla y seleccione **Gestionar la Regla**.
   Aparece el asistente de gestión de una regla de notificación.
3. En la sección Configuración general, puede personalizar la descripción de la regla.
4. Para personalizar el contenido del correo electrónico:
   a. Haga clic en **Configuración e-mail comprador**.
   b. Seleccione el modelo de e-mail que aplicará.
   c. Seleccione el idioma en el cual desea realizar modificaciones.
   d. Haga clic en el enlace **Personalizar valores de texto predeterminados** si desea modificar el asunto y el contenido del e-mail "por defecto".
   e. Haga clic en **Campos a incluir** para mostrar la lista de campos disponibles para personalizar el correo electrónico.
   f. Seleccione los campos que desea incluir. Se agregará un resumen detallado del procesamiento de la solicitud al contenido del correo electrónico.

   > Para obtener una vista previa de los cambios realizados, haga clic en **Vista previa del correo electrónico** en la parte inferior del cuadro de diálogo.

5. Para modificar los eventos que activan la notificación:
   a. Haga clic en la pestaña **Condiciones de la regla**
      Una condición consiste en una variable, un operador de comparación y un valor de referencia.
      Ejemplo: "mode = TEST", "monto superior a 1000". Al ejecutar una regla, el valor de la variable se recupera y se compara con el valor de referencia.
   b. Haga doble clic en una condición existente para modificarla.
   c. Haga clic en **Agregar** para crear una nueva condición.
      Todas las condiciones deben ser validadas para que se ejecute la regla.
6. Haga clic en **Guardar**.

10. GENERAR UN FORMULARIO DE PAGO

Para generar una solicitud de pago, debe crear un formulario HTML de la siguiente forma:

```
<form method="POST" action="https://secure.cobroinmediato.tech/vads-payment/">
 <input type="hidden" name="parametre1" value="valeur1" />
 <input type="hidden" name="parametre2" value="valeur2" />
 <input type="hidden" name="parametre3" value="valeur3" />
 <input type="hidden" name="signature" value="signature"/>
 <input type="submit" name="pagar" value="Pagar"/>
</form>
```

Este contiene:

- Los siguientes elementos técnicos:
  - Las etiquetas <form> y </form> que permiten crear un formulario HTML.
  - El atributo method="POST" que especifica el método utilizado para enviar los datos.
  - El atributo action="*https://secure.cobroinmediato.tech/vads-payment/*" que especifica a dónde enviar los datos del formulario.
- Los datos del formulario:
  - El identificador de la tienda.
  - Las características del pago en función del caso de utilización.
  - Información adicional según sus necesidades.
  - La fecha que asegura la integridad del formulario.

  Estos datos son agregados al formulario utilizando la etiqueta <input>:

  <input type="hidden" name="parametre1" value="valeur1" />

  Para asignar un valor a los atributos name y value, consulte el **Diccionario de datos** disponible también en el sitio de documentación.

  Todos los datos del formulario deben estar codificados en **UTF-8.**

  De esta forma, los caracteres especiales (acentos, puntuación, etc.) serán interpretados correctamente por la plataforma de pago. En el caso contrario, el cálculo de la firma será erróneo y el formulario será rechazado.

- El botón **Pagar** para enviar los datos:

  <input type="submit" name="pagar" value="Pagar"/>

En los capítulos siguientes se presentan casos de utilización. Estos le permitirán construir su formulario de pago en función de sus necesidades.

La siguiente tabla proporciona indicaciones sobre los diferentes formatos que puede encontrar durante la construcción de su formulario.

Notación	Descripción
a	Caracteres alfabéticos (de 'A' a 'Z' y de 'a' a 'z')
n	Caracteres numéricos
s	Caracteres especiales
an	Caracteres alfanuméricos
ans	Caracteres alfanuméricos y especiales (excepto "<" y ">")
3	Longitud fija de 3 caracteres
..12	Longitud variable hasta 12 caracteres
json	JavaScript Object Notation. Un objeto que contiene pares clave/valor separados por comas. Comienza con un refuerzo izquierdo " { " y termina con un refuerzo derecho " } ". Cada par de clave/valor contiene el nombre de la clave entre comillas dobles seguidas de " : ", seguido de un valor. El nombre de la clave debe ser alfanumérico. El valor puede ser: • una cadena de caracteres (en este caso debe estar encuadrada entre comillas dobles) • un número • un objeto • un tablero • un booleano • vacío Ejemplo: {"name1":45,"name2":"value2", "name3":false}
bool	Booleano. Puede tomar el valor **true** o **false**.
enum	Caracteriza un campo con un número finito de valores. La lista de valores posibles se da en la definición del campo.
lista de enum	Lista de valores separados por un " ; ". La lista de valores posibles se da en la definición del campo. Ejemplo: vads_available_languages=fr;en
map	Lista de pares clave/valores separados por un " ; ". Cada par de clave / valor contiene el nombre de la clave seguido de " = ". El valor puede ser: • una cadena de caracteres • un booleano • un objeto json • un objeto xml La lista de valores posibles para cada par de clave / valor se proporciona en la definición del campo. Ejemplo: vads_theme_config=SIMPLIFIED_DISPLAY=true;RESPONSIVE_MODEL=Model_1

10.1. Crear un formulario 'Creación del token sin pago'

Caso de uso: creación de un token para efectuar rápidamente pagos posteriores.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
vads_page_action	Acción a realizar	enum	**REGISTER**
vads_action_mode	Modo de adquisición de la información del medio de pago	enum	**INTERACTIVE**
vads_currency	Código numérico de la moneda que se utilizará para el pago, según la norma ISO 4217 (código numérico)	n3	Ejemplo: 840 para el dólar norteamericano (USD)
vads_ctx_mode	Adquisición de los datos en la plataforma de pago	enum	**TEST** o **PRODUCTION**
vads_cust_email	Dirección de correo electrónico del comprador	ans..150	Ej.: abc@example.com
vads_site_id	Identificador de la tienda	n8	Ejemplo: 12345678
vads_trans_date	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
vads_version	Versión del protocolo de intercambio con la plataforma de pago	enum	**V2**
signature	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo **signature** utilizando todos los campos de su formulario, cuyo nombre comienza con **vads_** (véase capítulo ***Calcular la firma***).

2. Utilice el campo **vads_identifier** si desea generar el identificador del token asociado al medio de pago.

   El formato del token no debe ser an..32. Este formato está reservado para los tokens generados por la plataforma de pago.

   Si ha activado la detección de la unidad de los tokens, el valor del campo **vads_identifier** transmitido en el formulario puede ser diferente al presente en la notificación si el medio de pago ya está asociado a otro token.

3. Agregue los campos opcionales en función de sus necesidades (véase capítulo ***Utilizar funciones complementarias***).

La lista de los campos devueltos en la notificación se describen en el capítulo *Creación de un token sin pago* en la página 62.

10.2. Crear un formulario 'Cambio de información asociada al token'

Caso de uso: actualización de los datos bancarios asociados a un token.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
vads_page_action	Acción a realizar.	enum	**REGISTER_UPDATE**
vads_ctx_mode	Adquisición de los datos en la plataforma de pago	enum	**TEST** o **PRODUCTION**

Nombre del campo	Descripción	Formato	Valor
vads_cust_email	Dirección de correo electrónico del comprador	ans..150	Ej.: abc@example.com
vads_action_mode	Modo de adquisición de la información del medio de pago	enum	**INTERACTIVE**
vads_identifier	Token (único) asociado a un medio de pago.	ans..50	Ejemplo: MiToken **Nota**: dos formatos posibles: • **an32**: cuando el identificador es generado por la plataforma • **ans..50**: cuando el identificador es generado por el vendedor
vads_site_id	Identificador de la tienda	n8	Ejemplo: 12345678
vads_trans_date	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
vads_version	Versión del protocolo de intercambio con la plataforma de pago	enum	**V2**
signature	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo **signature** utilizando todos los campos de su formulario, cuyo nombre comienza con **vads_** (véase capítulo ***Calcular la firma***).

2. Agregue los campos opcionales en función de sus necesidades (véase capítulo ***Utilizar funciones complementarias***).

La lista de los campos devueltos en la notificación se describen en el capítulo *Cambio de información asociada al token* en la página 66.

10.3. Crear un formulario 'Creación del token durante un pago'

Caso de uso: pago con creación de un token.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
vads_page_action	Acción a realizar	enum	**REGISTER_PAY**
vads_amount	Monto del pago en su unidad monetaria más pequeña (el centavo para el dólar estadunidense)	n..12	Ejemplo: 4525 para 45,25 USD
vads_ctx_mode	Adquisición de los datos en la plataforma de pago	enum	**TEST** o **PRODUCTION**
vads_currency	Código numérico de la moneda que se utilizará para el pago, según la norma ISO 4217 (código numérico)	n3	Ejemplo: 840 para el dólar norteamericano (USD)
vads_cust_email	Dirección de correo electrónico del comprador	ans..150	Ej.: abc@example.com
vads_action_mode	Modo de adquisición de la información del medio de pago	enum	**INTERACTIVE**
vads_payment_config	Tipo de pago	enum	**SINGLE**
vads_site_id	Identificador de la tienda	n8	Ejemplo: 12345678
vads_trans_date	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
vads_trans_id	Número de la transacción. Debe ser único en un mismo día (de 00:00:00 a 23:59:59 UTC). **Atención: Este campo no distingue entre mayúsculas y minúsculas.**	an6	Ejemplo: xrT15p
vads_version	Versión del protocolo de intercambio con la plataforma de pago	enum	**V2**
signature	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo **signature** utilizando todos los campos de su formulario, cuyo nombre comienza con **vads_** (véase capítulo ***Calcular la firma***).

2. Utilice el campo **vads_identifier** si desea generar el identificador del token asociado al medio de pago.

   El formato del token no debe ser an..32. Este formato está reservado para los tokens generados por la plataforma de pago.

   Si ha activado la detección de la unidad de los tokens, el valor del campo **vads_identifier** transmitido en el formulario puede ser diferente al presente en la notificación si el medio de pago ya está asociado a otro token.

3. Agregue los campos opcionales en función de sus necesidades (véase capítulo ***Utilizar funciones complementarias***).

La lista de los campos devueltos en la notificación se describen en el capítulo *Creación del token durante un pago* en la página 69.

10.4. Crear un formulario Creación del token al suscribirse a una recurrencia'

Caso de uso: recurrencia de una recurrencia con creación de un token.

No se realizará ningún pago al momento de la recurrencia. Solamente se realizará una solicitud de verificación para confirmar los datos del medio de pago.

El primer pago se realizará en la fecha efectiva, entre las 00:00 y las 05:00 h.

Si desea que el comprador pague el primer vencimiento al momento de la recurrencia, consulte el capítulo: ***Crear un formulario 'Creación del token al suscribir a una recurrencia acompañada de un pago'* en la página 42**.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
vads_page_action	Acción a realizar	enum	**REGISTER_SUBSCRIBE**
vads_ctx_mode	Adquisición de los datos en la plataforma de pago	enum	**TEST** o **PRODUCTION**
vads_cust_email	Dirección de correo electrónico del comprador	ans..150	Ej.: abc@example.com
vads_action_mode	Modo de adquisición de la información del medio de pago	enum	**INTERACTIVE**
vads_site_id	Identificador de la tienda	n8	Ejemplo: 12345678
vads_sub_amount	Monto de los vencimientos de la recurrencia (en su unidad monetaria más pequeña). **El monto de los vencimientos no se puede valorar en 0.**	n..12	Ejemplo: 4525 para 45,25 USD
vads_sub_effect_date	Fecha de inicio de la recurrencia (o fecha efectiva) el en huso UTC, en formato AAAAMMDD.	n8	Ejemplo: 20210601
vads_sub_currency	Código de la moneda utilizada para la recurrencia.	n3	Ejemplo: 840 para el dólar norteamericano (USD)

vads_sub_desc	Regla de recurrencia para aplicar de acuerdo con la especificación iCalendar RFC5545.
	Si solicita la creación de una recurrencia para debitar el portador a diario (RRULE:FREQ=DAILY;INTERVAL y que la fecha de efecto solicitada (vads_sub_effect_date) corresponde a la fecha de creación de la recurrencia, entonces la plataforma de pago tratará esta recurrencia al día siguiente (entre medianoche y las 5:00), se crearán 2 pagos:
	• el de la víspera (que corresponde a la fecha de efecto),
	• y el del día.
		string	La frecuencia de la recurrencia puede ser diaria, semanal o mensual.
			Puede especificar el número del día o del mes (por ejemplo “el día 10 del mes” o “cada 3 meses”).
			Nota: la cadena no debe tener espacios.
			Ejemplos:
			• Para definir una recurrencia semanal:
			`RRULE:FREQ=WEEKLY`
			• Para definir una recurrencia cada dos semanas, hoy y cada 7 días.
			`RRULE:FREQ=WEEKLY;INTERVAL=2`
			• Para definir los vencimientos de pago que tienen lugar el último día de cada mes, durante 12 meses:
			`RRULE:FREQ=MONTHLY;`
			`BYMONTHDAY=28,29,30,31;`
			`BYSETPOS=-1;COUNT=12`

Nombre del campo	Descripción	Formato	Valor

	Para evitarlo, se aconseja transmitir una fecha de efecto al día siguiente del día en que se creó la recurrencia.		• Para definir los vencimientos de pago que tienen lugar el día 10 de cada mes, durante 12 meses:
			`RRULE:FREQ=MONTHLY;`
			`COUNT=12;BYMONTHDAY=10`

vads_trans_date	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
vads_version	Versión del protocolo de intercambio con la plataforma de pago	enum	**V2**
signature	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo **signature** utilizando todos los campos de su formulario, cuyo nombre comienza con **vads_** (véase capítulo ***Calcular la firma***).

El valor de **vads_sub_effect_date** no debe estar en el pasado.

2. Utilice el campo **vads_identifier** si desea generar el identificador del token asociado al medio de pago.

   El formato del token no debe ser an..32. Este formato está reservado para los tokens generados por la plataforma de pago.

   Si ha activado la detección de la unidad de los tokens, el valor del campo **vads_identifier** transmitido en el formulario puede ser diferente al presente en la notificación si el medio de pago ya está asociado a otro token.

3. Agregue los campos opcionales en función de sus necesidades (véase capítulo ***Utilizar funciones complementarias***).

La lista de los campos devueltos en la notificación se describen en el capítulo *Creación del token al suscribirse a una recurrencia* en la página 73.

10.5. Crear un formulario 'Creación del token al suscribir a una recurrencia acompañada de un pago'

Caso de uso: pago y una recurrencia de una recurrencia con creación de un token.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
vads_page_action	Acción a realizar	enum	**REGISTER_PAY_SUBSCRIBE**
vads_amount	Monto del pago en su unidad monetaria más pequeña (el centavo para el dólar estadunidense)	n..12	Ejemplo: 4525 para 45,25 USD
vads_ctx_mode	Adquisición de los datos en la plataforma de pago	enum	**TEST** o **PRODUCTION**
vads_currency	Código numérico de la moneda que se utilizará para el pago, según la norma ISO 4217 (código numérico)	n3	Ejemplo: 840 para el dólar norteamericano (USD)
vads_cust_email	Dirección de correo electrónico del comprador	ans..150	Ej.: abc@example.com
vads_action_mode	Modo de adquisición de la información del medio de pago	enum	**INTERACTIVE**
vads_payment_config	Tipo de pago	enum	**SINGLE**
vads_site_id	Identificador de la tienda	n8	Ejemplo: 12345678
vads_sub_amount	Monto de los vencimientos de la recurrencia (en su unidad monetaria más pequeña). **El monto de los vencimientos no se puede valorar en 0.**	n..12	Ejemplo: 4525 para 45,25 USD
vads_sub_currency	Código de la moneda utilizada para la recurrencia.	n3	Ejemplo: 840 para el dólar norteamericano (USD)

vads_sub_desc	Regla de recurrencia para aplicar de acuerdo con la especificación iCalendar RFC5545.
	Si solicita la creación de una recurrencia para debitar el portador a diario (RRULE:FREQ=DAILY;INTERVAL y que la fecha de efecto solicitada (vads_sub_effect_date) corresponde a la fecha de creación de la recurrencia, entonces la plataforma de pago tratará esta recurrencia al día siguiente (entre medianoche y las 5:00), se crearán 2 pagos:
	• el de la víspera (que corresponde a la fecha de efecto),
	• y el del día.
	Para evitarlo, se aconseja transmitir una fecha de efecto al día siguiente
		string	La frecuencia de la recurrencia puede ser diaria, semanal o mensual.
			Puede especificar el número del día o del mes (por ejemplo “el día 10 del mes” o “cada 3 meses”).
			Nota: la cadena no debe tener espacios.
			Ejemplos:
			• Para definir una recurrencia semanal:
			`RRULE:FREQ=WEEKLY`
			• Para definir una recurrencia cada dos semanas, hoy y cada 7 días.
			`RRULE:FREQ=WEEKLY;INTERVAL=2`
			• Para definir los vencimientos de pago que tienen lugar el último día de cada mes, durante 12 meses:
			`RRULE:FREQ=MONTHLY;`
			`BYMONTHDAY=28,29,30,31;`
			`BYSETPOS=-1;COUNT=12`

Nombre del campo	Descripción	Formato	Valor

	del día en que se creó la recurrencia.		• Para definir los vencimientos de pago que tienen lugar el día 10 de cada mes, durante 12 meses:
			`RRULE:FREQ=MONTHLY;`
			`COUNT=12;BYMONTHDAY=10`

vads_sub_effect_date	Fecha de inicio de la recurrencia (o fecha efectiva) el en huso UTC, en formato AAAAMMDD.	n8	Ejemplo: 20210601
vads_trans_date	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
vads_trans_id	Número de la transacción. Debe ser único en un mismo día (de 00:00:00 a 23:59:59 UTC). **Atención: Este campo no distingue entre mayúsculas y minúsculas.**	an6	Ejemplo: xrT15p
vads_version	Versión del protocolo de intercambio con la plataforma de pago	enum	**V2**
signature	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo **signature** utilizando todos los campos de su formulario, cuyo nombre comienza con **vads_** (véase capítulo ***Calcular la firma***).

El valor de **vads_sub_effect_date** no debe estar en el pasado.

2. Utilice el campo **vads_identifier** si desea generar el identificador del token asociado al medio de pago.

   El formato del token no debe ser an..32. Este formato está reservado para los tokens generados por la plataforma de pago.

   Si ha activado la detección de la unidad de los tokens, el valor del campo **vads_identifier** transmitido en el formulario puede ser diferente al presente en la notificación si el medio de pago ya está asociado a otro token.

3. Agregue los campos opcionales en función de sus necesidades (véase capítulo ***Utilizar funciones complementarias***).

La lista de los campos devueltos en la notificación se describen en el capítulo *Creación del token al suscribir a una recurrencia acompañada de un pago* en la página 77.

10.6. Crear un formulario 'Pago por token'

Caso de uso: pago con un clic (uso de un token existente y válido).

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
vads_page_action	Acción a realizar	enum	**PAYMENT**
vads_amount	Monto del pago en su unidad monetaria más pequeña (el centavo para el dólar estadunidense)	n..12	Ejemplo: 4525 para 45,25 USD
vads_ctx_mode	Adquisición de los datos en la plataforma de pago	enum	**TEST** o **PRODUCTION**
vads_currency	Código numérico de la moneda que se utilizará para el pago, según la norma ISO 4217 (código numérico)	n3	Ejemplo: 840 para el dólar norteamericano (USD)
vads_action_mode	Modo de adquisición de la información del medio de pago	enum	**INTERACTIVE**
vads_identifier	Token (único) asociado a un medio de pago.	ans..50	Ejemplo: MiToken **Nota**: dos formatos posibles: • **an32**: cuando el identificador es generado por la plataforma • **ans..50**: cuando el identificador es generado por el vendedor
vads_payment_config	Tipo de pago	enum	**SINGLE**
vads_site_id	Identificador de la tienda	n8	Ejemplo: 12345678
vads_trans_date	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
vads_trans_id	Número de la transacción. Debe ser único en un mismo día (de 00:00:00 a 23:59:59 UTC). **Atención: Este campo no distingue entre mayúsculas y minúsculas.**	an6	Ejemplo: xrT15p
vads_version	Versión del protocolo de intercambio con la plataforma de pago	enum	**V2**
signature	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo **signature** utilizando todos los campos de su formulario, cuyo nombre comienza con **vads_** (véase capítulo ***Calcular la firma***).

2. Agregue los campos opcionales en función de sus necesidades (véase capítulo ***Utilizar funciones complementarias***).

La lista de los campos devueltos en la notificación se describen en el capítulo *Pago por Token* en la página 81.

10.7. Crear un formulario 'Usar un token para suscribirse a una recurrencia'

Caso de uso: uso de un token existente y válido para suscribirse a una recurrencia.

No se realizará ningún pago al momento de la recurrencia.

El primer pago se realizará en la fecha efectiva, entre las 00:00 y las 05:00 h.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
vads_page_action	Acción a realizar.	enum	**SUBSCRIBE**
vads_ctx_mode	Adquisición de los datos en la plataforma de pago	enum	**TEST** o **PRODUCTION**
vads_action_mode	Modo de adquisición de la información del medio de pago	enum	**INTERACTIVE**
vads_identifier	Token (único) asociado a un medio de pago.	ans..50	Ejemplo: MiToken **Nota**: dos formatos posibles: • **an32**: cuando el identificador es generado por la plataforma • **ans..50**: cuando el identificador es generado por el vendedor
vads_site_id	Identificador de la tienda	n8	Ejemplo: 12345678
vads_sub_amount	Monto de los vencimientos de la recurrencia (en su unidad monetaria más pequeña). **El monto de los vencimientos no se puede valorar en 0.**	n..12	Ejemplo: 4525 para 45,25 USD
vads_sub_effect_date	Fecha de inicio de la recurrencia (o fecha efectiva) el en huso UTC, en formato AAAAMMDD.	n8	Ejemplo: 20210601
vads_sub_currency	Código de la moneda utilizada para la recurrencia.	n3	Ejemplo: 840 para el dólar norteamericano (USD)

vads_sub_desc	Regla de recurrencia para aplicar de acuerdo con la especificación iCalendar RFC5545.
	Si solicita la creación de una recurrencia para debitar el portador a diario (RRULE:FREQ=DAILY;INTERVAL y que la fecha de efecto solicitada (vads_sub_effect_date) corresponde a la fecha de creación de la recurrencia, entonces la plataforma de pago tratará esta recurrencia al día siguiente (entre medianoche y las 5:00), se crearán 2 pagos:
	• el de la víspera (que corresponde a la fecha de efecto),
	• y el del día.
		string	La frecuencia de la recurrencia puede ser diaria, semanal o mensual.
			Puede especificar el número del día o del mes (por ejemplo “el día 10 del mes” o “cada 3 meses”).
			Nota: la cadena no debe tener espacios.
			Ejemplos:
			• Para definir una recurrencia semanal:
			`RRULE:FREQ=WEEKLY`
			• Para definir una recurrencia cada dos semanas, hoy y cada 7 días.
			`RRULE:FREQ=WEEKLY;INTERVAL=2`
			• Para definir los vencimientos de pago que tienen lugar el último día de cada mes, durante 12 meses:
			`RRULE:FREQ=MONTHLY;`
			`BYMONTHDAY=28,29,30,31;`

Nombre del campo	Descripción	Formato	Valor

	Para evitarlo, se aconseja transmitir una fecha de efecto al día siguiente del día en que se creó la recurrencia.		`BYSETPOS=-1;COUNT=12`
			• Para definir los vencimientos de pago que tienen lugar el día 10 de cada mes, durante 12 meses:
			`RRULE:FREQ=MONTHLY;`
			`COUNT=12;BYMONTHDAY=10`

vads_trans_date	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
vads_version	Versión del protocolo de intercambio con la plataforma de pago	enum	**V2**
signature	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo **signature** utilizando todos los campos de su formulario, cuyo nombre comienza con **vads_** (véase capítulo ***Calcular la firma***).

El valor de **vads_sub_effect_date** no debe estar en el pasado.

2. Agregue los campos opcionales en función de sus necesidades (véase capítulo ***Utilizar funciones complementarias***).

La lista de los campos devueltos en la notificación se describen en el capítulo *Suscripción a una recurrencia* en la página 83.

11. USAR FUNCIONES ADICIONALES

11.1. Definir un monto diferente para las primeras n cuotas

Desea definir una recurrencia a cuyo/s primer/os vencimiento/s se le asigna/n un valor diferente al/a los asignado/s por el campo **vads_sub_amount**.

Ejemplo: definir una recurrencia cuyos 3 primeros vencimientos son a 45,25 USD, y las demás a 75,90 USD.

Para ello:

1. Utilice todos los campos necesarios para su caso de uso para crear su formulario de pago.

2. Utilice los siguientes campos:

Nombre del campo	Descripción	Valor
vads_sub_init_amount_number	Número de vencimientos a los que aplicar el monto definido por **vads_sub_init_amount**	3
vads_sub_init_amount	Monto de los primeros vencimientos. El número de los primeros vencimientos lo define **vads_sub_init_amount_number**.	2500
vads_sub_amount	Monto de los vencimientos de la recurrencia, excepto las posiblemente definidas por **vads_sub_init_amount_number**.	3000
vads_sub_currency	Moneda utilizada en todos los vencimientos de la recurrencia	Ejemplo: 840 para el dólar norteamericano (USD)

Los campos **vads_sub_init_amount** y **vads_sub_amount** no pueden tener asignado el valor 0.

Para definir una recurrencia cuyos 3 primeros meses son gratuitos, basta con escalonan la fecha efectiva (**vads_sub_effect_date**) hasta 3 meses.

Ejemplo de formulario :

```
<form method="POST" action="https://secure.cobroinmediato.tech/vads-payment/">
<input type="hidden" name="vads_action_mode" value="INTERACTIVE" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="TEST" />
<input type="hidden" name="vads_currency" value="978" />
<input type="hidden" name="vads_cust_country" value="FR" />
<input type="hidden" name="vads_cust_email" value="exemple@gmail.com" />
<input type="hidden" name="vads_cust_first_name" value="Paul" />
<input type="hidden" name="vads_cust_last_name" value="Juve" />
<input type="hidden" name="vads_cust_title" value="M." />
<input type="hidden" name="vads_page_action" value="REGISTER_SUBSCRIBE" />
<input type="hidden" name="vads_payment_config" value="SINGLE" />
<input type="hidden" name="vads_site_id" value="91335531" />
<input type="hidden" name="vads_trans_date" value="20190716080441" />
<input type="hidden" name="vads_trans_id" value="362812" />
<input type="hidden" name="vads_validation_mode" value="0" />
<input type="hidden" name="vads_sub_currency" value="840" />
<input type="hidden" name="vads_sub_init_amount_number" value="3" />
<input type="hidden" name="vads_sub_init_amount" value="2500" />
<input type="hidden" name="vads_sub_amount" value="3000" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="G6oZchxNT+ySm7YQ/zvQvfgxmOmubvZ0lPwFKKVUSyI="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

11.2. Definir la moneda para crear o actualizar un token

En caso de que:

- posea una afiliación que acepta varias monedas,
- posea varias tiendas,
- sus tiendas estén asociadas a la misma afiliación,
- cada tienda genere pagos en una moneda diferente,

  (Ejemplo: US dólar para la primera tienda, Euro para la segunda tienda)

es posible que la moneda utilizada al crear o actualizar un token no sea compatible con la tienda.

Efectivamente, la plataforma de pago seleccionará por defecto la primera moneda que encuentre en orden alfabético para efectuar las verificaciones necesarias con el emisor del medio de pago.

Para evitar errores de procesamiento de IPN, tiene la posibilidad de enviar la moneda que utilizará en el formulario.

Para efectuar pagos con cualquier moneda aceptada por la afiliación, siempre podrá utilizar el token.

Nombre del campo	Descripción	Formato	Valor
vads_currency	Código numérico de la moneda que se utilizará para el pago, según la norma ISO 4217 (código numérico)	n3	Ejemplo: 840 para el dólar norteamericano (USD)

12. CALCULAR LA FIRMA

Para poder calcular la firma debe disponer:

- de los campos cuyos nombres comienzan con**vads_**
- del tipo de algoritmo elegido en la configuración de la tienda;
- de la **clave**.

El valor de la clave está disponible en el Back Office Vendedor en el menú **Configuración** > **Tienda** > pestaña **Claves**.

El tipo de algoritmo se define en su Back Office Vendedor en el menú **Configuración** > **Tienda** > pestaña **Configuración**.

Para calcular la firma:

1. Ordena los campos cuyos nombres comienzan con**vads_**por orden alfabético.
2. Asegúrese de que todos los campos estén codificados en UTF-8.
3. Concatene los valores de estos campos separándolos con el carácter “**+**".
4. Concatene el resultado con la clave de prueba o de producción separándolos con el carácter "**+**".
5. Calcule y codifique en formato Base64 la firma usando el algoritmo **HMAC-SHA-256** con los siguientes parámetros:
   - la función hash SHA-256,
   - la clave de prueba o de producción (según el valor del campo**vads_ctx_mode**) como clave compartida,
   - el resultado del paso anterior como mensaje a autenticar.
6. Guarde el resultado del paso anterior en el campo**signature**.

Ejemplo de parámetros enviados a la plataforma de pago:

```
<form method="POST" action="https://secure.cobroinmediato.tech/vads-payment/">
<input type="hidden" name="vads_action_mode" value="INTERACTIVE" />
<input type="hidden" name="vads_amount" value="5124" />
<input type="hidden" name="vads_ctx_mode" value="TEST" />
<input type="hidden" name="vads_currency" value="840" />
<input type="hidden" name="vads_page_action" value="PAYMENT" />
<input type="hidden" name="vads_payment_config" value="SINGLE" />
<input type="hidden" name="vads_site_id" value="12345678" />
<input type="hidden" name="vads_trans_date" value="20170129130025" />
<input type="hidden" name="vads_trans_id" value="123456" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="92dec271594ddef9842a33340ffc8532ac5a3a44"/>
<input type="submit" name="pagar" value="Pagar"/>
</form>
```

Este ejemplo de formulario se desglosa de la siguiente manera:

1. Se organizan en orden **alfabética** los campos cuyo nombre comienza**vads_** :
   - vads_action_mode
   - vads_amount
   - vads_ctx_mode
   - vads_currency
   - vads_page_action
   - vads_payment_config
   - vads_site_id
   - vads_trans_date
   - vads_trans_id
   - vads_version
2. Se concatena el valor de estos campos con el carácter "**+**" :

   ```
   INTERACTIVE+5124+TEST+840+PAYMENT+SINGLE+12345678+20170129130025+123456+V2
   ```

3. Se agrega el valor de la clave de prueba al final del string, separado por el carácter "**+**". En este ejemplo, la clave de prueba es**1122334455667788**

   ```
   INTERACTIVE+5124+TEST+840+PAYMENT+SINGLE+12345678+20170129130025+123456+V2+1122334455667788
   ```

4. Calcule y codifique en formato Base64 la firma del mensaje usando el algoritmo **HMAC-SHA-256** con los siguientes parámetros:
   - la función hash SHA-256,
   - la clave de prueba o de producción (según el valor del campo**vads_ctx_mode**) como clave compartida,
   - el resultado del paso anterior como mensaje a autenticar.

   El resultado a transmitir en el campo firma es:

   EKrcj4e8N38LGCP/xkJMaHUajUfvsRG50mDwYLNBsMU=

13. ENVÍO DE LA SOLICITUD DE PAGO

En cada transacción, se debe redirigir al comprador a la página de pago para finalizar su compra.

Su navegador debe transmitir los datos del formulario de pago.

13.1. Redirección del comprador hacia la página de pago

La URL de la plataforma de pago es la siguiente:

https://secure.cobroinmediato.tech/vads-payment/

Ejemplo de parámetros enviados a la plataforma de pago:

```
<form method="POST" action="https://secure.cobroinmediato.tech/vads-payment/">
<input type="hidden" name="vads_action_mode" value="INTERACTIVE" />
<input type="hidden" name="vads_amount" value="2990" />
<input type="hidden" name="vads_ctx_mode" value="TEST" />
<input type="hidden" name="vads_currency" value="840" />
<input type="hidden" name="vads_cust_country" value="CL" />
<input type="hidden" name="vads_cust_email" value="me@example.com" />
<input type="hidden" name="vads_order_id" value="CMD012859" />
<input type="hidden" name="vads_page_action" value="REGISTER_PAY" />
<input type="hidden" name="vads_payment_config" value="SINGLE" />
<input type="hidden" name="vads_site_id" value="12345678" />
<input type="hidden" name="vads_trans_date" value="20200426101407" />
<input type="hidden" name="vads_trans_id" value="x6Z41p" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="NM25DPLKEbtGEHCDHn8MBT4ki6aJI/ODaWhCzCnAfvY="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

13.2. Gestión de errores

Si la plataforma detecta una anomalía durante la recepción del formulario, se mostrará un mensaje de error y el comprador no podrá proceder con el pago.

En modo TEST

El mensaje indica el origen del error y muestra un vínculo hacia la descripción del código del error para ayudarle a identificar las posibles causas.

En modo PRODUCTION

El mensaje simplemente indica al comprador que ocurrió un problema técnico.

En los dos casos, el vendedor recibe un e-mail de advertencia.

Este contiene:

- el origen del error,
- un vínculo hacia las posibles causas para este código de error para facilitar el diagnóstico,
- todos los campos contenidos en el formulario.

El e-mail se envía al contacto administrador de la marca.

Si desea modificar esta dirección o añadir una dirección adicional, póngase en contacto con el servicio de atención al cliente.

También tiene la posibilidad de crear una regla de notificación personalizada para recibir ese e-mail en otra dirección.

Para esto:

1. Conéctese a su Back Office Vendedor.

   https://secure.cobroinmediato.tech/vads-merchant/

2. Abra el menú **Configuración** > **Reglas de notificaciones**.
3. Seleccione **Notificación avanzada**.
4. Seleccione el tipo de notificación **E-mail enviado al vendedor**.
5. Haga clic en **Siguiente**.
6. Seleccione el evento desencadenante **Formulario de pago inválido**.
7. En la sección **Configuración general**, ingrese los campos:
   - **Etiqueta de la regla**
   - **Dirección e-mail a notificar**
8. Haga clic en el botón **Crear**.

Una descripción de los códigos de error con sus posibles causas está disponible en nuestro sitio de Internet.

https://secure.cobroinmediato.tech/doc/es-AR/error-code/error-00.html

Otros mensajes pueden surgir durante el pago.

A continuación hay una lista de los mensajes más comunes:

Mensaje	Descripción
Su solicitud de pago ha sido denegada por su banco.	• El banco del comprador rechazó la solicitud de autorización o de información. • Las reglas de gestión de riesgos provocaron el rechazo de la transacción.
Su solicitud de inscripción fue rechazada por su establecimiento financiero.	• El banco del comprador rechazó la solicitud de autorización o de información. • Las reglas de gestión de riesgos provocaron el rechazo de la transacción.
Esta solicitud de pago expiró. Establezca contacto con su tienda.	El comprador hizo clic en el enlace de pago después de la fecha final de validez de la solicitud.
Esta solicitud de pago ya ha sido pagada	El comprador hizo clic de nuevo en el enlace de pago después de haber realizado el pago previamente.
Ocurrió una fallo durante la solicitud de pago; el sitio del comerciante fue informado sobre la posibilidad de finalizar la transacción.	El formulario de pago fue rechazado. El responsable de la tienda recibió un e-mail que detalla el origen del error.
La transacción ya fue realizada.	El sitio web vendedor envía un identificador de transacción ya utilizado para otra transacción (aceptada o rechazada). El identificador de transacción debe ser único en un día (00:00:00 a 23:59:59 UTC).
Lo sentimos, se ha superado el tiempo máximo de inactividad, ha sido desconectado por motivos de seguridad.	• El comprador trata de validar su número de tarjeta cuando su sesión de pago expiró. La duración de la sesión es de 10 minutos. • El sitio del comerciante envía un identificador de transacción ya utilizado pero que no dio lugar a una transacción (por ejemplo, pago abandonado). El

Mensaje	Descripción
	identificador de transacción debe ser único en un día (00:00:00 a 23:59:59 UTC).
Su navegador bloqueó las cookies. Autorícelas antes de reiniciar la operación.	El comprador desactivó el uso de cookies en su navegador. Las cookies son indispensables para el correcto desarrollo del pago.

13.3. Administrar tiempos de espera

Concepto de sesión de pago

Una "sesión de pago" es el tiempo que pasa un comprador en la página de pago.

La sesión de pago comienza al recibir el formulario por la plataforma de pago.

La duración de la sesión es de 10 minutos (a excepción de ciertos medios de pago).

Dicha duración es:

- **suficiente** para permitir a cada comprador hacer su pago
- **fijo**: no se restablece a todas las acciones del usuario.
- **no modificable**: es fijado por la plataforma de pago para cumplir con las limitaciones técnicas.

Después de este tiempo, la sesión se agota y los datos de la sesión se borran.

Caducidad de la sesión de pago.

Es posible que en algunos casos la sesión de pago caduque mientras el comprador no haya completado el pago.

Casos más frecuentes:

1. Una vez redirigido a la página de pago, el comprador se da cuenta de que es hora de ir a almorzar, por ejemplo.

   Una hora más tarde, decide continuar con su pago y hace clic en el logotipo correspondiente a sus medios de pago.

   Su sesión de pago ha caducado, la plataforma de pago muestra un mensaje de error que indica que se desconectó debido a una inactividad demasiado larga.

   Luego, el comprador tiene la oportunidad de hacer clic en un botón para volver al sitio web vendedor.

   El retorno a la tienda es a la URL especificada por el vendedor:

   - en el campo *vads_url_return* enviado en el formulario de pago,
   - en el campo "URL de la tienda" Back Office Vendedor, si la URL no se especifica en el campo *vads_url_return* del formulario de pago.
2. Una vez redirigido a la página de pago, el comprador cierra su navegador (por error o porque ya no quiere hacer el pago).

Notificación en caso de expiración de la sesión

El sitio web vendedor tiene la posibilidad de ser notificado en caso de expiración de la sesión.

Para ello, el vendedor debe configurar y activar la regla ***URL de notificación al abandonar (comprador)*** (consultar capítulo *Configurar la notificación en caso de abandono/cancelación* en la página 29).

14. IMPLEMENTAR LA IPN

El script debe incluir al menos los siguientes pasos:

- Recuperar la lista de campos presentes en la respuesta enviada en POST
- Calcular la firma tomando en cuenta los datos recibidos
- Comparar la firma calculada con la recibida.
- Analizar la naturaleza de la notificación
- Recuperar el resultado del pago

El script puede, por ejemplo, probar el estado del pedido (o la información de su elección) para verificar que no se haya actualizado.

Una vez que se han completado estos pasos, el script puede actualizar la base de datos (nuevo estado del pedido, actualización del stock, registro de la información de pago, etc.).

A fin de facilitar el soporte y el diagnóstico por el vendedor en caso de error durante una notificación, se recomienda escribir mensajes que permitan conocer en qué etapa del procesamiento se produjo el error.

La plataforma lee y guarda los primeros 256 bytes del cuerpo de la respuesta HTTP.

Usted puede escribir mensajes durante todo el procesamiento. Aquí tiene un ejemplo de mensaje que puede utilizar:

Mensaje	Casos de uso
Data received	Mensaje que se mostrará durante la recuperación de los datos. Permite confirmar que el sitio del comerciante ha recibido correctamente la notificación.
POST is empty	Mensaje que se mostrará durante la recuperación de los datos. Permite indicar una eventual redirección que ha perdido los parámetros publicados por la plataforma de pago.
An error occurred while computing the signature.	Mensaje que se mostrará cuando haya fracasado la verificación de la firma.
Order successfully updated.	Mensaje que se mostrará al final del archivo una vez que sus procesamientos se hayan terminado con éxito.
An error occurred while updating the order.	Mensaje que se mostrará al final del archivo si se produjo un error durante sus procesamientos.

14.1. Preparar su entorno

Las notificaciones de tipo Llamada URL de notificación son las más importantes, pues representan el único medio confiable para que el sitio del comerciante pueda obtener el resultado de un pago.

Por lo tanto, es fundamental controlar que las notificaciones funcionen correctamente.

A continuación le presentamos algunas recomendaciones:

- Para que el diálogo entre la plataforma de pago y su sitio comerciante funcione, usted debe comprobar con sus equipos técnicos que el rango de la dirección IP **194.50.38.0/24** esté autorizada en los diferentes dispositivos de su arquitectura (firewalls, servidor apache, servidor proxy, etc.)

  Las notificaciones se envían desde una dirección IP dentro del rango 194.50.38.0/24 **en modo TEST y en modo PRODUCTION**.

- Los redireccionamientos dan como resultado la pérdida de datos en POST.

  Este caso se da si existe una configuración en sus dispositivos o en su proveedor que redirige las URL de tipo "http://**www.**example.com" vers "http://example.com" o "**http**://example.com" hacia "**https**://example.com".

- La página no debe tener una vista HTML. El acceso a recursos como imágenes o hojas de estilo ralentizan los intercambios entre la plataforma de pago y el sitio web vendedor.

- Evite las tareas que consumen tanto tiempo como generar facturas PDF o enviar e-mails en su script.

  El tiempo de procesamiento tiene un efecto directo en el plazo de la visualizacion de la página de resumen de pago.

  Cuanto mayor sea el procesamiento de la notificación, más se demora la visualización. Si el tiempo de procesamiento supera los 35 segundos, la plataforma considera que la llamada ha fallado (timeout).

- Si a su página solo se puede acceder por https, pruebe su URL en el sitio deQualys SSL Labs (*https://www.ssllabs.com/ssltest/* y modifique su configuración, si fuera necesario, a fin de obtener un grado A.

  Su certificado SSL debe firmarlo una autoridad de certificación conocida y reconocida en el mercado.

- Asegúrese de utilizar las últimas versiones del protocolo TLS a fin de mantener un alto nivel de seguridad.

14.2. Recuperar los datos devueltos en la respuesta

Los datos devueltos en la respuesta dependen de los parámetros enviados en la solicitud de pago, el tipo de pago realizado y las opciones de su tienda y del formato de la notificación.

Los datos siempre son enviados en **POST** por la plataforma de pago.

Por lo tanto, el primer paso es recuperar el contenido recibido en el modo POST.

Ejemplos:

- En PHP, los datos se almacenarán en la variable superglobal **$_POST**.
- En ASP.NET (C #), debe usar la propiedad **Form** de la clase **HttpRequest**.
- En java, debe usar el método **getParameter** de la clase **HttpServletRequest**.

La respuesta constituye una lista de campos. Cada campo contiene un valor de respuesta. La lista de campos puede cambiar.

El script tendrá que hacer un bucle para recuperar todos los campos transmitidos.

Se recomienda probar la presencia del campo **vads_hash**, presente solo durante una notificación.

```
if (empty ($_POST)){
 echo 'POST is empty';

}else{
 echo 'Data Received ';
 if (isset($_POST['vads_hash'])){

  echo 'Form API notification detected';
  //Signature computation
  //Signature verification
  //Order Update
 }
}
```

14.3. Calcular la firma de la IPN

La firma se calcula de acuerdo con la misma lógica utilizada al solicitar el pago.

Los datos transmitidos por la plataforma de pago están codificados en UTF-8. Cualquier alteración de los datos recibidos dará lugar a un cálculo de firma errónea.

Debe calcular la firma con los campos recibidos en la notificación y no con los que transmitió en la solicitud de pago.

1. Considere todos los campos cuyos nombres comienzan con **vads_**.
2. Ordene estos campos alfabéticamente.
3. Concatene los valores de estos campos separándolos con el carácter “**+**".
4. Concatene el resultado con la clave de prueba o de producción separándolos con el carácter "**+**".
5. Calcule y codifique en formato Base64 la firma usando el algoritmo **HMAC-SHA-256** con los siguientes parámetros:
   - la función hash SHA-256,
   - la clave de prueba o de producción (según el valor del campo**vads_ctx_mode**) como clave compartida,
   - el resultado del paso anterior como mensaje a autenticar.

Ejemplos en PHP:

```
función getSignature ($params,$key)
{
    /**
     * Función que calcula la firma.
     * $ params: matriz que contiene los campos que se enviarán en la IPN.
     * $key : clave de TEST o PRODUCTION
     */
    //Inicialización de la variable que contendrá el string a cifrar
    $contenu_signature = "";

    //Ordenar los campos alfabéticamente
    ksort($params);
    foreach($params as $nom=>$valeur){

        //Recuperación de los campos vads_
        if (substr($nom,0,5)=='vads_'){

            //Concatenación con el separador  "+"
            $contenu_signature .= $valeur."+";
         }
    }
    //Añadir la clave al final del string
    $contenu_signature .= $key;

    //Codificación base64 del string cifrada con el algoritmo HMAC-SHA-256
    $sign = base64_encode(hash_hmac('sha256',$contenu_signature, $key, true));
    return $sign;
 }
```

14.4. Comparar firmas

Para garantizar la integridad de la respuesta, debe comparar el valor de la firma contenida en la IPN con el valor calculado en el paso anterior.

No se debe comparar la firma de la IPN con la firma que transmitió en su solicitud de pago.

Si las firmas coinciden,

- luego puede considerar la respuesta como segura y proceder como resultado del análisis.
- de lo contrario, el script lanzará una excepción y advertirá al vendedor de la anomalía.

Ejemplo PHP:

```
if ($_POST['signature'] == $sign){

    //Processing data

}else{
    throw new Exception('An error occurred while computing the signature');
}
```

Las firmas no coinciden en el caso:

- error de implementación (error en su cálculo, problema de codificación UTF-8, etc.),
- un error en el valor de la clave utilizada o en el campo **vads_ctx_mode** (un problema frecuente al entrar en producción),
- intento de corromper los datos.

14.5. Analizar la naturaleza de la notificación

El campo **vads_url_check_src** permite diferenciar las notificaciones según su evento desencadenante:

- creación de un token (con o sin recurrencia a una recurrencia).
- pago de un vencimiento de una recurrencia.
- Referencia de la notificación en el Back Office Vendedor por el vendedor.

Especifica la regla de notificación aplicada:

Valor	Regla aplicada
PAY	El valor PAY se envía en los siguientes casos: • solicitud de creación de una orden o de un token (REGISTER) • solicitud de creación de una orden o de un token al registrar una suscripción (REGISTER_SUBSCRIBE) • pago inmediato (pago al contado o primer vencimiento de un pago en vencimientos) • pago abandonado o cancelado por el comprador. solo si el vendedor ha configurado la regla **URL de notificación al abandonar (comprador)**.
BO	Ejecución de la notificación desde el Back Office Vendedor (haga clic con el botón derecho en una transacción > **Ejecutar la URL de notificación**). Compruebe la presencia del campo vads_recurrence_number: • si está presente, la notificación corresponde al resultado de un pago recurrente (repetición de una notificación de tipo **REC**), • si está ausente, la notificación corresponde a una notificación de fin de pago.
BATCH	El valor BATCH se envía al actualizar el estado de una transacción tras la sincronización con el adquirente. Este es el caso de los pagos redirigidos al adquirente. Solo si el vendedor ha configurado la regla **URL de notificación al modificar por batch**.
BATCH_AUTO	El valor BATCH_AUTO se envía en los siguientes casos: • pago diferido a más de 7 días • vencimientos para un pago en vencimientos (excepto el primero). solo si el vendedor ha configurado la regla **URL de notificación al autorizar por batch**. La notificación se enviará cuando se solicite autorización para un pago con el estado "autorización pendiente".
REC	El valor REC solo se enviará para los pagos por suscripción si el vendedor ha establecido la regla **URL de notificación para crear un pago recurrente**. Consulte el capítulo *Pago de un vencimiento de una recurrencia en la página 85* para el detalle de las informaciones enviadas.
MERCH_BO	El valor MERCH_BO se enviará: • durante una operación realizada desde el Back Office Vendedor (cancelación, reembolso, modificación, validación, duplicación, creación o actualización de token), si el vendedor ha configurado la regla de notificación: **URL de notificación al modificar una transacción en el Back Office (vendedor)**
RETRY	Repetición automática de la URL de notificación. Compruebe la presencia del campo vads_recurrence_number: • si está presente, la notificación corresponde al resultado de un pago recurrente (repetición de una notificación de tipo **REC**), • si está ausente, la notificación corresponde a una notificación de fin de pago.

Tabla 1: Valores asociados al campo vads_url_check_src

Al probar su valor, el script puede realizar un procesamiento diferente según la naturaleza de la notificación.

Por ejemplo:

Si **vads_url_check_src** tiene asignado el valor **PAY** o **BATCH_AUTO** entonces el script actualizará el estado del pedido, ...

Si **vads_url_check_src** tiene asignado el valor **REC** entonces el script recuperará la referencia de recurrencia e incrementará el número de vencimientos vencidas en caso de pago aceptado...

En el marco de un débito recurrente (procedente de un REGISTER_SUBSCRIBE), la plataforma de pago notifica al acreedor (vendedor) cada vez que se crea una transacción.

14.6. Tratamiento de los datos de la respuesta

14.6.1. Creación de un token sin pago

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es **REGISTER**.
vads_identifier_status	Estado de la creación de token. Los valores posibles son: • **CREATED**: la solicitud de autorización es aceptada. El token se crea correctamente y se ve en el Back Office Vendedor. • **NOT_CREATED**: la solicitud de autorización es rechazada. El token no se crea. • **ABANDONED**: acción abandonada por el comprador. El token no se crea.
vads_identifier	Identificador del token. El valor devuelto es: • igual al valor enviado en la solicitud, cualquiera sea el resultado de la creación del token, incluso en caso de abandono, • o el valor generado por la plataforma, si el campo no es enviado en la solicitud y si el token se crea correctamente (vads_identifier_status=CREATED). Nota Si ha activado la verificación de la unicidad de los token y que el medio de pago ya está registrado con otro token, entonces es otro token el que se devolverá. El campo **vads_identifier** no se devolverá: • si no es enviado en la solicitud y si el comprador abandona (vads_identifier_status=ABANDONED), • si no es enviado en la solicitud y si el token no se crea (vads_identifier_status=NOT_CREATED).
vads_identifier_previously_registered	únicamente presente si las dos condiciones son verdaderas: • usted ha activado la verificación de la unidad de los token,

Nombre del campo	Descripción
	• el medio de pago utilizado ya está registrado con otro token.
vads_cust_email	Dirección de correo electrónico del comprador enviada en la solicitud.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.
vads_ctx_mode	Modo de funcionamiento. El valor devuelto (**TEST** o **PRODUCTION**) es igual al enviado en la solicitud.

Una solicitud de "creación de token sin pago" permite crear una transacción de tipo VERIFICATION, que se ve en el Back Office Vendedor.

La función de esta transacción es ayudar al vendedor a entender, desde su Back-Office, las razones de rechazo de la creación del token.

A continuación, encontrará sus características:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es **VERIFICATION**.
vads_trans_status	Estado de la transacción. Los valores posibles son: • **ACCEPTED** La solicitud de autorización o de información ha sido aceptada. El token se crea y aparece en el Back Office Vendedor. • **REFUSED** La solicitud de autorización o de información ha sido denegada. El token no se crea.
vads_occurrence_type	Tipo de ocurrencia de la transacción. Su valor es **UNITAIRE**.
vads_amount	**100**
vads_trans_id	Identificador de la transacción. La plataforma de pago genera el valor.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización. Su valor es **MARK**.
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Vacío si aparece un error antes de la autorización.

vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada.
	Las reglas relativas al monto o cuya acción es "Validar manualmente" no se aplican en el caso de una transacción de tipo VERIFICATION.
	Los valores posibles son:
	• **ENABLE_3DS**: 3D Secure activado.
	• **DISABLE_3DS**: 3D Secure desactivado.
	• **CHALLENGE_REQUESTED**:
	  • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.
	  • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge).
	• **CHALLENGE_MANDATE**:
	  • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.

Nombre del campo	Descripción
	• Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge por razones reglamentarias) por motivos normativos. • **REFUSE**: El token es rechazado. • **RUN_RISK_ANALYSIS**: Resultado del analizador de riesgos externo. Consulte la descripción del campo **vads_risk_analysis_result** para más detalles. • **INFORM**: Se levanta una alerta. El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo **Medios de pago compatibles** para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto..
vads_expiry_month	Mes de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

Detalles de la autenticación del portador:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Es obligatoria una autenticación fuerte del portador al registrar una tarjeta. Por lo tanto, el campo siempre se valorizará en **CHALLENGE**.
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: • **Y**: Autenticación disponible. • **N**: Autenticación no disponible • **U**: Estado de la inscripción al programa 3DS desconocido • vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	Resultado de la autenticación 3D Secure. Los valores posibles son: • **Y**: Portador autenticado correctamente. • **N**: Error de autenticación del portador. • **U**: Autenticación imposible • **A**: Tentativa de autenticación, pero no se realizó la autenticación.

Nombre del campo	Nota
	• vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

14.6.2. Cambio de información asociada al token

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es **REGISTER_UPDATE**.
vads_identifier_status	Estado de la actualización del token. Los valores posibles son: • **UPDATED**: el token se actualizó correctamente. • **NOT_UPDATED**: el token no se ha actualizado. • **ABANDONED**: acción abandonada por el comprador. El token no se crea, por lo tanto, no se ve en el Back Office Vendedor.
vads_identifier	Identificador del token para actualizar. El valor devuelto es igual al enviado en la solicitud.
vads_cust_email	Dirección de correo electrónico del comprador enviada en la solicitud.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.
vads_ctx_mode	Modo de funcionamiento. El valor devuelto (**TEST** o **PRODUCTION**) es igual al enviado en la solicitud.

Una solicitud de "actualización de token" permite crear una transacción de tipo VERIFICATION, que se ve en el Back Office Vendedor.

La función de esta transacción es ayudar al vendedor a entender, desde su Back-Office, las razones de rechazo de la creación del token.

A continuación, encontrará sus características:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es **VERIFICATION**.
vads_trans_status	Estado de la transacción. Los valores posibles son: • **ACCEPTED** La solicitud de autorización o de información ha sido aceptada. El token se crea y aparece en el Back Office Vendedor. • **REFUSED** La solicitud de autorización o de información ha sido denegada. El token no se crea.
vads_occurrence_type	Tipo de ocurrencia de la transacción. Su valor es **UNITAIRE**.
vads_amount	**100**
vads_trans_id	Identificador de la transacción. La plataforma de pago genera el valor.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización. Su valor es **MARK**.
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Vacío si aparece un error antes de la autorización.
vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada.

Nombre del campo	Descripción

	Las reglas relativas al monto o cuya acción es "Validar manualmente" no se aplican en el caso de una transacción de tipo VERIFICATION.
	Los valores posibles son:
	• **ENABLE_3DS**: 3D Secure activado.
	• **DISABLE_3DS**: 3D Secure desactivado.
	• **CHALLENGE_REQUESTED**:
	  • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.
	  • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge).
	• **CHALLENGE_MANDATE**:
	  • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.
	  • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge por razones reglamentarias) por motivos normativos.
	• **REFUSE**: El token es rechazado.
	• **RUN_RISK_ANALYSIS**: Resultado del analizador de riesgos externo. Consulte la descripción del campo **vads_risk_analysis_result** para más detalles.
	• **INFORM**: Se levanta una alerta.
	El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo **Medios de pago compatibles** para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto..
vads_expiry_month	Mes de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

Detalles de la autenticación del portador:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Es obligatoria una autenticación fuerte del portador al registrar una tarjeta. Por lo tanto, el campo siempre se valorizará en **CHALLENGE**.
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son:

Nombre del campo	Nota
	• **Y**: Autenticación disponible. • **N**: Autenticación no disponible • **U**: Estado de la inscripción al programa 3DS desconocido • vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	Resultado de la autenticación 3D Secure. Los valores posibles son: • **Y**: Portador autenticado correctamente. • **N**: Error de autenticación del portador. • **U**: Autenticación imposible • **A**: Tentativa de autenticación, pero no se realizó la autenticación. • vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

14.6.3. Creación del token durante un pago

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es **REGISTER_PAY**.
vads_identifier_status	Estado de la creación de token. Los valores posibles son: • **CREATED**: la solicitud de autorización es aceptada. El token se crea con éxito. • **NOT_CREATED**: la solicitud de autorización es rechazada. El token no se crea, por lo tanto, no se ve en el Back Office Vendedor. • **ABANDONED**: acción abandonada por el comprador. El token no se crea, por lo tanto, no se ve en el Back Office Vendedor.
vads_trans_status	Estado de la transacción. Los valores posibles son: • **AUTHORISED** La solicitud de autorización o de información ha sido aceptada. El token se crea y aparece en el Back Office Vendedor. • **AUTHORISED_TO_VALIDATE** La solicitud de autorización o de información ha sido aceptada. El vendedor debe validar la transacción de forma manual. El token se crea y aparece en el Back Office Vendedor. • **CAPTURED** La solicitud de autorización o de información ha sido aceptada. El pago aparece en la pestaña “Transacciones capturadas” del Back-Office. El token se crea y aparece en el Back Office Vendedor. • **WAITING_AUTHORISATION** El plazo de captura al banco es superior a la duración de validez de la autorización. La solicitud de autorización por el monto total aún no se ha creado. El token se crea y aparece en el Back Office Vendedor. • **WAITING_AUTHORISATION_TO_VALIDATE** **Para validar y autorizar** El plazo de captura al banco es superior a la duración de validez de la autorización. Se aceptó una autorización 1 USD. El vendedor debe validar manualmente la transacción para que se realice la solicitud de autorización y la captura. • **REFUSED** La solicitud de autorización o de información ha sido denegada. El token no se crea. • **ABANDONED** Operación abandonada por el comprador. La transacción no aparece en el Back Office Vendedor. El token no se crea.
vads_identifier	Identificador del token. El valor devuelto es: • igual al valor enviado en la solicitud, cualquiera sea el resultado de la creación del token, incluso en caso de abandono, • o el valor generado por la plataforma, si el campo no es enviado en la solicitud y si el token se crea correctamente (vads_identifier_status=CREATED). Nota Si ha activado la verificación de la unicidad de los token y que el medio de pago ya está registrado con otro token, entonces es otro token el que se devolverá.

Nombre del campo	Descripción
	El campo **vads_identifier** no se devolverá: • si no es enviado en la solicitud y si el comprador abandona (vads_identifier_status=ABANDONED), • si no es enviado en la solicitud y si el token no se crea (vads_identifier_status=NOT_CREATED).
vads_identifier_previously_registered	únicamente presente si las dos condiciones son verdaderas: • usted ha activado la verificación de la unidad de los token, • el medio de pago utilizado ya está registrado con otro token.
vads_cust_email	Dirección de correo electrónico del comprador enviada en la solicitud.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.
vads_ctx_mode	Modo de funcionamiento. El valor devuelto (**TEST** o **PRODUCTION**) es igual al enviado en la solicitud.

Para conocer el detalle del pago, consulte los siguientes parámetros:

Información sobre la transacción:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es **DEBIT**.
vads_occurrence_type	Tipo de ocurrencia de la transacción. Su valor es **UNITAIRE**.
vads_amount	Monto de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_currency	Código de la moneda utilizada para el pago.
vads_trans_id	Identificador de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_contract_used	Número de la afiliación asociada a la transacción.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización: • **MARK**: corresponde a una autorización de 1 USD. Valor utilizado también si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente posterior al período de validez de la autorización. • **FULL**: corresponde a una autorización del monto total de la transacción. Valor utilizado si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente anterior al período de validez de la autorización.
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Vacío si aparece un error antes de la autorización.
vads_risk_control	Resultado de los controles de riesgo. Cuando, al menos, un control devuelve el valor **ERROR**, la transacción es rechazada. Consulte la descripción del campo **vads_risk_analysis_result** para más detalles.
vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada. Los valores posibles son: • **ENABLE_3DS**: 3D Secure activado. • **DISABLE_3DS**: 3D Secure desactivado. • **CHALLENGE_REQUESTED**: • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.

Nombre del campo	Descripción

	• Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge).
	• **CHALLENGE_MANDATE**:
	  • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.
	  • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge por razones reglamentarias) por motivos normativos.
	• **MANUAL_VALIDATION**: La transacción se crea con validación manual.
	La remesa del pago se bloquea temporalmente para permitir que el vendedor realice todas las verificaciones deseadas.
	• **REFUSE**: La transacción se ha rechazado.
	• **RUN_RISK_ANALYSIS**: Resultado del analizador de riesgos externo.
	Consulte la descripción del campo **vads_risk_analysis_result** para más detalles.
	• **INFORM**: Se levanta una alerta.
	El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo **Medios de pago compatibles** para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto..
vads_expiry_month	Mes de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

Detalles de la autenticación del portador:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Es obligatoria una autenticación fuerte del portador al registrar una tarjeta. Por lo tanto, el campo siempre se valorizará en **CHALLENGE**.
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: • **Y**: Autenticación disponible. • **N**: Autenticación no disponible • **U**: Estado de la inscripción al programa 3DS desconocido • vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	Resultado de la autenticación 3D Secure.

Nombre del campo	Nota
	Los valores posibles son: • **Y**: Portador autenticado correctamente. • **N**: Error de autenticación del portador. • **U**: Autenticación imposible • **A**: Tentativa de autenticación, pero no se realizó la autenticación. • vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

14.6.4. Creación del token al suscribirse a una recurrencia

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es **REGISTER_SUBSCRIBE**.
vads_identifier_status	Estado de la creación de token. Los valores posibles son: • **CREATED**: la solicitud de autorización es aceptada. El token se crea con éxito. Consulte el valor del campo vads_recurrence_status para determinar si se ha creado la recurrencia. • **NOT_CREATED**: la solicitud de autorización es rechazada. El token no se crea, por lo tanto, no se ve en el Back Office Vendedor. La recurrencia no se crea. • **ABANDONED**: acción abandonada por el comprador. El token no se crea, por lo tanto, no aparece en el Back Office Vendedor. La recurrencia no se crea.
vads_recurrence_status	Estado de la creación de la recurrencia. Los valores posibles son: • **CREATED**: La afiliación fue creada con éxito. • **NOT_CREATED**: La recurrencia no se crea. • **ABANDONED**: acción abandonada por el comprador. La recurrencia no se crea.
vads_identifier	Identificador del token. El valor devuelto es: • igual al valor enviado en la solicitud, cualquiera sea el resultado de la creación del token, incluso en caso de abandono, • o el valor generado por la plataforma, si el campo no es enviado en la solicitud y si el token se crea correctamente (vads_identifier_status=CREATED). Nota Si ha activado la verificación de la unicidad de los token y que el medio de pago ya está registrado con otro token, entonces es otro token el que se devolverá. El campo **vads_identifier** no se devolverá: • si no es enviado en la solicitud y si el comprador abandona (vads_identifier_status=ABANDONED), • si no es enviado en la solicitud y si el token no se crea (vads_identifier_status=NOT_CREATED).
vads_identifier_previously_registered	únicamente presente si las dos condiciones son verdaderas: • usted ha activado la verificación de la unidad de los token, • el medio de pago utilizado ya está registrado con otro token.
vads_cust_email	Dirección de correo electrónico del comprador enviada en la solicitud.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.
vads_ctx_mode	Modo de funcionamiento. El valor devuelto (**TEST** o **PRODUCTION**) es igual al enviado en la solicitud.

Para conocer el detalle de la recurrencia consulte los siguientes parámetros:

Nombre del campo	Nota
vads_subscription	Identificador de la recurrencia. El valor devuelto es:

Nombre del campo	Nota
	• el valor enviado en la solicitud, cualquiera sea el resultado de la creación de la recurrencia; • o el valor generado por la plataforma de pago, si el campo no es enviado en la solicitud y si la recurrencia se crea correctamente (vads_recurrence_status=CREATED). El campo vads_subscription no se devolverá: • si no es enviado en la solicitud y si el comprador abandona (vads_recurrence_status=ABANDONED), • si no es enviado en la solicitud y si la recurrencia no se crea (vads_recurrence_status=NOT_CREATED).
vads_sub_amount	Monto de los vencimientos de la recurrencia (en su unidad monetaria más pequeña).
vads_sub_currency	Código de la moneda utilizada para la recurrencia. Ejemplo: 840 para el dólar norteamericano (USD)
vads_sub_desc	Regla de recurrencia para aplicar de acuerdo con la especificación iCalendar RFC5545. Ejemplo: RRULE:FREQ=MONTHLY
vads_sub_effect_date	Fecha de inicio de la recurrencia (o fecha efectiva) el en huso UTC, en formato AAAAMMDD. Ejemplo: 20210601
vads_sub_init_amount	Monto de los primeros vencimientos. El número de los primeros vencimientos lo define **vads_sub_init_amount_number**. Ejemplo: 1000
vads_sub_init_amount_number	Número de vencimientos a los que aplicar el monto definido por. **vads_sub_init_amount**. Ejemplo: 3

Una solicitud de "creación de token al suscribir una recurrencia" permite crear una transacción de tipo VERIFICATION, que se ve en el Back Office Vendedor.

La función de esta transacción es ayudar al vendedor a entender, desde su Back-Office, las razones de rechazo de la creación del token.

A continuación, encontrará sus características:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es **VERIFICATION**.
vads_trans_status	Estado de la transacción. Los valores posibles son: • **ACCEPTED** La solicitud de autorización o de información ha sido aceptada. El token se crea y aparece en el Back Office Vendedor. • **REFUSED** La solicitud de autorización o de información ha sido denegada. El token no se crea.
vads_occurrence_type	Tipo de ocurrencia de la transacción. Su valor es **UNITAIRE**.
vads_amount	**100**
vads_trans_id	Identificador de la transacción. La plataforma de pago genera el valor.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización. Su valor es **MARK**.
vads_auth_number	Número de autorización devuelto por el servidor bancario.

Nombre del campo	Descripción
	Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Vacío si aparece un error antes de la autorización.

vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada.
	Las reglas relativas al monto o cuya acción es "Validar manualmente" no se aplican en el caso de una transacción de tipo VERIFICATION.
	Los valores posibles son:
	• **ENABLE_3DS**: 3D Secure activado.
	• **DISABLE_3DS**: 3D Secure desactivado.
	• **CHALLENGE_REQUESTED**:
	  ◦ Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.
	  ◦ Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge).
	• **CHALLENGE_MANDATE**:
	  ◦ Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.
	  ◦ Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge por razones reglamentarias) por motivos normativos.
	• **REFUSE**: El token es rechazado.
	• **RUN_RISK_ANALYSIS**: Resultado del analizador de riesgos externo. Consulte la descripción del campo **vads_risk_analysis_result** para más detalles.
	• **INFORM**: Se levanta una alerta.
	El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo **Medios de pago compatibles** para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto..
vads_expiry_month	Mes de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

Detalles de la autenticación del portador:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Es obligatoria una autenticación fuerte del portador al registrar una tarjeta. Por lo tanto, el campo siempre se valorizará en **CHALLENGE**.
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: • **Y**: Autenticación disponible. • **N**: Autenticación no disponible • **U**: Estado de la inscripción al programa 3DS desconocido • vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	Resultado de la autenticación 3D Secure. Los valores posibles son: • **Y**: Portador autenticado correctamente. • **N**: Error de autenticación del portador. • **U**: Autenticación imposible • **A**: Tentativa de autenticación, pero no se realizó la autenticación. • vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

14.6.5. Creación del token al suscribir a una recurrencia acompañada de un pago

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es **REGISTER_PAY_SUBSCRIBE**.
vads_identifier_status	Estado de la creación de token. Los valores posibles son: • **CREATED**: la solicitud de autorización es aceptada. El token se crea con éxito. Consulte el valor del campo vads_recurrence_status para determinar si se ha creado la recurrencia. • **NOT_CREATED**: la solicitud de autorización es rechazada. El token no se crea, por lo tanto, no se ve en el Back Office Vendedor. La recurrencia no se crea. • **ABANDONED**: acción abandonada por el comprador. El token no se crea, por lo tanto, no aparece en el Back Office Vendedor. La recurrencia no se crea.
vads_trans_status	Estado de la transacción. Los valores posibles son: • **AUTHORISED** La solicitud de autorización o de información ha sido aceptada. El token se crea y aparece en el Back Office Vendedor. • **AUTHORISED_TO_VALIDATE** La solicitud de autorización o de información ha sido aceptada. El vendedor debe validar la transacción de forma manual. El token se crea y aparece en el Back Office Vendedor. • **CAPTURED** La solicitud de autorización o de información ha sido aceptada. El pago aparece en la pestaña “Transacciones capturadas” del Back-Office. El token se crea y aparece en el Back Office Vendedor. • **WAITING_AUTHORISATION** El plazo de captura al banco es superior a la duración de validez de la autorización. La solicitud de autorización por el monto total aún no se ha creado. El token se crea y aparece en el Back Office Vendedor. • **WAITING_AUTHORISATION_TO_VALIDATE** **Para validar y autorizar** El plazo de captura al banco es superior a la duración de validez de la autorización. Se aceptó una autorización 1 USD. El vendedor debe validar manualmente la transacción para que se realice la solicitud de autorización y la captura. • **REFUSED** La solicitud de autorización o de información ha sido denegada. El token no se crea. • **ABANDONED** Operación abandonada por el comprador. La transacción no aparece en el Back Office Vendedor. El token no se crea.
vads_recurrence_status	Estado de la creación de la recurrencia. Los valores posibles son: • **CREATED**: La afiliación fue creada con éxito. • **NOT_CREATED**: La recurrencia no se crea.

Nombre del campo	Descripción
	• **ABANDONED**: acción abandonada por el comprador. La recurrencia no se crea.
vads_identifier	Identificador del token. El valor devuelto es: • igual al valor enviado en la solicitud, cualquiera sea el resultado de la creación del token, incluso en caso de abandono, • o el valor generado por la plataforma, si el campo no es enviado en la solicitud y si el token se crea correctamente (vads_identifier_status=CREATED). Nota Si ha activado la verificación de la unicidad de los token y que el medio de pago ya está registrado con otro token, entonces es otro token el que se devolverá. El campo **vads_identifier** no se devolverá: • si no es enviado en la solicitud y si el comprador abandona (vads_identifier_status=ABANDONED), • si no es enviado en la solicitud y si el token no se crea (vads_identifier_status=NOT_CREATED).
vads_identifier_previously_registered	únicamente presente si las dos condiciones son verdaderas: • usted ha activado la verificación de la unidad de los token, • el medio de pago utilizado ya está registrado con otro token.
vads_cust_email	Dirección de correo electrónico del comprador enviada en la solicitud.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.
vads_ctx_mode	Modo de funcionamiento. El valor devuelto (**TEST** o **PRODUCTION**) es igual al enviado en la solicitud.

Para conocer el detalle de la recurrencia consulte los siguientes parámetros:

Nombre del campo	Nota
vads_subscription	Identificador de la recurrencia. El valor devuelto es: • el valor enviado en la solicitud, cualquiera sea el resultado de la creación de la recurrencia; • o el valor generado por la plataforma de pago, si el campo no es enviado en la solicitud y si la recurrencia se crea correctamente (vads_recurrence_status=CREATED). El campo vads_subscription no se devolverá: • si no es enviado en la solicitud y si el comprador abandona (vads_recurrence_status=ABANDONED), • si no es enviado en la solicitud y si la recurrencia no se crea (vads_recurrence_status=NOT_CREATED).
vads_sub_amount	Monto de los vencimientos de la recurrencia (en su unidad monetaria más pequeña).
vads_sub_currency	Código de la moneda utilizada para la recurrencia. Ejemplo: 840 para el dólar norteamericano (USD)
vads_sub_desc	Regla de recurrencia para aplicar de acuerdo con la especificación iCalendar RFC5545. Ejemplo: RRULE:FREQ=MONTHLY
vads_sub_effect_date	Fecha de inicio de la recurrencia (o fecha efectiva) el en huso UTC, en formato AAAAMMDD. Ejemplo: 20210601
vads_sub_init_amount	Monto de los primeros vencimientos. El número de los primeros vencimientos lo define **vads_sub_init_amount_number**. Ejemplo: 1000

Nombre del campo	Nota
vads_sub_init_amount_number	Número de vencimientos a los que aplicar el monto definido por. **vads_sub_init_amount**. Ejemplo: 3

Para conocer el detalle del pago, consulte los siguientes parámetros:

Información sobre la transacción:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es **DEBIT**.
vads_occurrence_type	Tipo de ocurrencia de la transacción. Su valor es **UNITAIRE**.
vads_amount	Monto de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_currency	Código de la moneda utilizada para el pago.
vads_trans_id	Identificador de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_contract_used	Número de la afiliación asociada a la transacción.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización: • **MARK**: corresponde a una autorización de 1 USD. Valor utilizado también si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente posterior al período de validez de la autorización. • **FULL**: corresponde a una autorización del monto total de la transacción. Valor utilizado si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente anterior al período de validez de la autorización.
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Vacío si aparece un error antes de la autorización.
vads_risk_control	Resultado de los controles de riesgo. Cuando, al menos, un control devuelve el valor **ERROR**, la transacción es rechazada. Consulte la descripción del campo **vads_risk_analysis_result** para más detalles.

vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada.
	Los valores posibles son:
	• **ENABLE_3DS**: 3D Secure activado.
	• **DISABLE_3DS**: 3D Secure desactivado.
	• **CHALLENGE_REQUESTED**:
	  ◦ Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.
	  ◦ Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge).
	• **CHALLENGE_MANDATE**:
	  ◦ Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.
	  ◦ Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge por razones reglamentarias) por motivos normativos.
	• **MANUAL_VALIDATION**: La transacción se crea con validación manual.
	La remesa del pago se bloquea temporalmente para permitir que el vendedor realice todas las verificaciones deseadas.

Nombre del campo	Descripción
	• **REFUSE**: La transacción se ha rechazado. • **RUN_RISK_ANALYSIS**: Resultado del analizador de riesgos externo. Consulte la descripción del campo **vads_risk_analysis_result** para más detalles. • **INFORM**: Se levanta una alerta. El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo **Medios de pago compatibles** para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto..
vads_expiry_month	Mes de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

Detalles de la autenticación del portador:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Es obligatoria una autenticación fuerte del portador al registrar una tarjeta. Por lo tanto, el campo siempre se valorizará en **CHALLENGE**.
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: • **Y**: Autenticación disponible. • **N**: Autenticación no disponible • **U**: Estado de la inscripción al programa 3DS desconocido • vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	Resultado de la autenticación 3D Secure. Los valores posibles son: • **Y**: Portador autenticado correctamente. • **N**: Error de autenticación del portador. • **U**: Autenticación imposible • **A**: Tentativa de autenticación, pero no se realizó la autenticación. • vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

14.6.6. Pago por Token

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es **PAYMENT**.
vads_trans_status	Estado de la transacción. Los valores posibles son: • **AUTHORISED** La solicitud de autorización fue aceptada. • **AUTHORISED_TO_VALIDATE** La solicitud de autorización fue aceptada. El vendedor debe validar la transacción de forma manual. • **CAPTURED** La solicitud de autorización fue aceptada. El pago aparece en la pestaña “Transacciones capturadas” del Back-Office. • **WAITING_AUTHORISATION** El plazo de captura al banco es superior a la duración de validez de la autorización. La solicitud de autorización por el monto total aún no se ha creado. • **WAITING_AUTHORISATION_TO_VALIDATE** **Para validar y autorizar** El plazo de captura al banco es superior a la duración de validez de la autorización. Se aceptó una autorización 1 USD. El vendedor debe validar manualmente la transacción para que se realice la solicitud de autorización y la captura. • **REFUSED** La solicitud de autorización fue denegada. • **ABANDONED** Operación abandonada por el comprador. La transacción no aparece en el Back Office Vendedor.
vads_identifier	Identificador del token para debitar. El valor devuelto es igual al enviado en la solicitud.
vads_cust_email	Dirección de correo electrónico del comprador asociado al token.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.
vads_ctx_mode	Modo de funcionamiento. El valor devuelto (**TEST** o **PRODUCTION**) es igual al enviado en la solicitud.

Para conocer el detalle del pago, consulte los siguientes parámetros:

Información sobre la transacción:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es **DEBIT**.
vads_occurrence_type	Tipo de ocurrencia de la transacción. Su valor es **RECURRENT_INTERMEDIAIRE**.
vads_amount	Monto de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_currency	Código de la moneda utilizada para el pago.
vads_trans_id	Identificador de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_trans_uuid	Identificador único de la transacción.

Nombre del campo	Descripción
	La plataforma de pago genera el valor.
vads_contract_used	Número de la afiliación asociada a la transacción.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización: • **MARK**: corresponde a una autorización de 1 USD. Valor utilizado también si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente posterior al período de validez de la autorización. • **FULL**: corresponde a una autorización del monto total de la transacción. Valor utilizado si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente anterior al período de validez de la autorización.
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Vacío si aparece un error antes de la autorización.
vads_risk_control	Resultado de los controles de riesgo. Cuando, al menos, un control devuelve el valor **ERROR**, la transacción es rechazada. Consulte la descripción del campo **vads_risk_analysis_result** para más detalles.

vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada.
	Los valores posibles son:
	• **ENABLE_3DS**: 3D Secure activado.
	• **DISABLE_3DS**: 3D Secure desactivado.
	• **CHALLENGE_REQUESTED**:
	  • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.
	  • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge).
	• **CHALLENGE_MANDATE**:
	  • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.
	  • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge por razones reglamentarias) por motivos normativos.
	• **MANUAL_VALIDATION**: La transacción se crea con validación manual.
	La remesa del pago se bloquea temporalmente para permitir que el vendedor realice todas las verificaciones deseadas.
	• **REFUSE**: La transacción se ha rechazado.
	• **RUN_RISK_ANALYSIS**: Resultado del analizador de riesgos externo.
	Consulte la descripción del campo **vads_risk_analysis_result** para más detalles.
	• **INFORM**: Se levanta una alerta.
	El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo **Medios de pago compatibles** para obtener la lista de valores posibles.

Nombre del campo	Nota
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto..
vads_expiry_month	Mes de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

Detalles de la autenticación fuerte:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Los valores posibles son: • "Vacío" si el comprador no se autenticó correctamente, • **FRICTIONLESS**: autenticación del titular sin interacción con el servidor de autenticación. Valor devuelto únicamente con 3DS v2, • **CHALLENGE**: autenticación interactiva del titular (ingreso de una contraseña de uso único o respuesta a una serie de preguntas). Valor devuelto con 3DS v1 y 3DS v2.
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: • **Y**: Autenticación disponible. • **N**: Autenticación no disponible • **U**: Estado de la inscripción al programa 3DS desconocido • vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	Resultado de la autenticación 3D Secure. Los valores posibles son: • **Y**: Portador autenticado correctamente. • **N**: Error de autenticación del portador. • **U**: Autenticación imposible • **A**: Tentativa de autenticación, pero no se realizó la autenticación. • vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

14.6.7. Suscripción a una recurrencia

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es **SUBSCRIBE**.
vads_recurrence_status	Estado de la creación de la recurrencia. Los valores posibles son:

Nombre del campo	Descripción
	• **CREATED**: La afiliación fue creada con éxito. • **NOT_CREATED**: La recurrencia no se crea. • **ABANDONED**: acción abandonada por el comprador. La recurrencia no se crea.
vads_identifier	Identificador del token para debitar. El valor devuelto es igual al enviado en la solicitud.
vads_cust_email	Dirección de e-mail del comprador asociada al token.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.
vads_ctx_mode	Modo de funcionamiento. El valor devuelto (**TEST** o **PRODUCTION**) es igual al enviado en la solicitud.

Para conocer el detalle de la recurrencia consulte los siguientes parámetros:

Nombre del campo	Nota
vads_subscription	Identificador de la recurrencia. El valor devuelto es: • el valor enviado en la solicitud, cualquiera sea el resultado de la creación de la recurrencia; • o el valor generado por la plataforma de pago, si el campo no es enviado en la solicitud y si la recurrencia se crea correctamente (vads_recurrence_status=CREATED). El campo vads_subscription no se devolverá: • si no es enviado en la solicitud y si el comprador abandona (vads_recurrence_status=ABANDONED), • si no es enviado en la solicitud y si la recurrencia no se crea (vads_recurrence_status=NOT_CREATED).
vads_sub_amount	Monto de los vencimientos de la recurrencia (en su unidad monetaria más pequeña).
vads_sub_currency	Código de la moneda utilizada para la recurrencia. Ejemplo: 840 para el dólar norteamericano (USD)
vads_sub_desc	Regla de recurrencia para aplicar de acuerdo con la especificación iCalendar RFC5545. Ejemplo: RRULE:FREQ=MONTHLY
vads_sub_effect_date	Fecha de inicio de la recurrencia (o fecha efectiva) el en huso UTC, en formato AAAAMMDD. Ejemplo: 20210601
vads_sub_init_amount	Monto de los primeros vencimientos. El número de los primeros vencimientos lo define **vads_sub_init_amount_number**. Ejemplo: 1000
vads_sub_init_amount_number	Número de vencimientos a los que aplicar el monto definido por. **vads_sub_init_amount**. Ejemplo: 3

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo **Medios de pago compatibles** para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.

Nombre del campo	Nota
vads_card_number	Número de tarjeta truncado/oculto..
vads_expiry_month	Mes de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

Detalles de la autenticación fuerte realizada al crear el token:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Es obligatoria una autenticación fuerte del portador al registrar una tarjeta. Por lo tanto, el campo siempre se valorizará en **CHALLENGE**.
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: • **Y**: Autenticación disponible. • **N**: Autenticación no disponible • **U**: Estado de la inscripción al programa 3DS desconocido • vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	Resultado de la autenticación 3D Secure. Los valores posibles son: • **Y**: Portador autenticado correctamente. • **N**: Error de autenticación del portador. • **U**: Autenticación imposible • **A**: Tentativa de autenticación, pero no se realizó la autenticación. • vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

14.6.8. Pago de un vencimiento de una recurrencia

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es **PAYMENT**.
vads_trans_status	Estado de la transacción. Los valores posibles son: • **AUTHORISED** La solicitud de autorización fue aceptada. • **AUTHORISED_TO_VALIDATE** La solicitud de autorización fue aceptada. El vendedor debe validar la transacción de forma manual. • **CAPTURED** La solicitud de autorización fue aceptada. El pago aparece en la pestaña “Transacciones capturadas” del Back-Office.

Nombre del campo	Descripción
	• **REFUSED** La solicitud de autorización fue denegada.
vads_identifier	Identificador del token.
vads_cust_email	Correo electrónico del comprador.
vads_site_id	Identificación de la tienda.
vads_ctx_mode	Modo de funcionamiento.

Para conocer el detalle de la recurrencia consulte los siguientes parámetros:

Nombre del campo	Nota
vads_subscription	Identificador de la recurrencia.
vads_recurrence_number	Número de vencimiento de la recurrencia.

Para conocer el detalle del pago, consulte los siguientes parámetros:

Información sobre la transacción:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es **DEBIT**.
vads_occurrence_type	Tipo de ocurrencia de la transacción. Valores posibles: • **RECURRENT_INITIAL**: Primer vencimiento. • **RECURRENT_INTERMEDIAIRE**: Enésimo vencimiento. Consulte el campo **vads_recurrence_number** para conocer el número del vencimiento. • **RECURRENT_FINAL**: último vencimiento.
vads_amount	Monto de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_currency	Código de la moneda utilizada para el pago.
vads_trans_id	Identificador de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_contract_used	Número de la afiliación asociada a la transacción.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización: • **MARK**: corresponde a una autorización de 1 USD. Valor utilizado también si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente posterior al período de validez de la autorización. • **FULL**: corresponde a una autorización del monto total de la transacción. Valor utilizado si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente anterior al período de validez de la autorización.
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Vacío si aparece un error antes de la autorización.
vads_risk_control	Resultado de los controles de riesgo. Cuando, al menos, un control devuelve el valor **ERROR**, la transacción es rechazada. Consulte la descripción del campo **vads_risk_analysis_result** para más detalles.
vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada. Los valores posibles son: • **ENABLE_3DS**: 3D Secure activado.

Nombre del campo	Descripción

	• **DISABLE_3DS**: 3D Secure desactivado.
	• **CHALLENGE_REQUESTED**:
	  • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.
	  • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge).
	• **CHALLENGE_MANDATE**:
	  • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autentificación 3DS.
	  • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autentificación con interacción del portador (challenge por razones reglamentarias) por motivos normativos.
	• **MANUAL_VALIDATION**: La transacción se crea con validación manual. La remesa del pago se bloquea temporalmente para permitir que el vendedor realice todas las verificaciones deseadas.
	• **REFUSE**: La transacción se ha rechazado.
	• **RUN_RISK_ANALYSIS**: Resultado del analizador de riesgos externo. Consulte la descripción del campo **vads_risk_analysis_result** para más detalles.
	• **INFORM**: Se levanta una alerta. El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

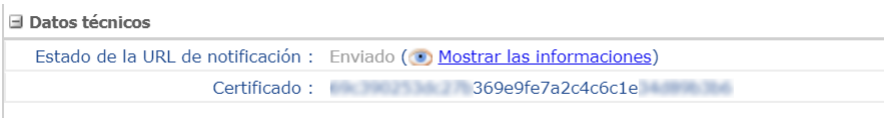
Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo **Medios de pago compatibles** para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto..
vads_expiry_month	Mes de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada. Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

14.7. Test y troubleshooting

Para probar las notificaciones, siga las siguientes etapas:

1. Realice un pago (en modo TEST o en modo PRODUCTION).
2. Una vez finalizado el pago, busque la transacción en su Back Office (Menú **Gestión** > **Transacciones** o **Transacciones de TEST** si realizó el pago en modo TEST).
3. Haga doble clic en la transacción para ver el **detalle de la transacción**.
4. En el detalle de la transacción, busque la sección **Datos técnicos**.
5. Compruebe el estado de la URL de notificación:



La lista de los estados posibles se presenta a continuación:

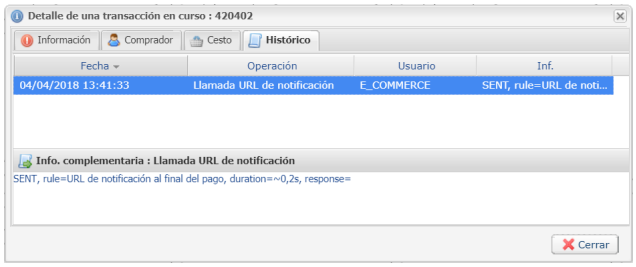
Estado	Descripción
N/A	La transacción no dio lugar a una notificación o no se activó ninguna regla de notificación.
URL no definido	Un evento activó la regla de notificación de fin de pago, pero la URL no está configurada.
Llamada en curso	La notificación está en curso Este estado es temporal.
Enviado	La notificación se ha enviado correctamente y un equipo distante respondió con un código HTTP 200, 201, 202, 203, 204, 205 ou 206.
Enviado (redirección permanente)	El sitio del comerciante ha devuelto un código HTTP 301 o 308 con una nueva URL para contactar. Una nueva llamada en modo POST se realiza hacia la nueva URL.
Enviado (redirección temporal)	El sitio del comerciante ha devuelto un código HTTP 302 o 307 con una nueva URL para contactar. Una nueva llamada en modo POST se realiza hacia la nueva URL.
Enviado (redirección a otra página)	El sitio del comerciante ha devuelto un código HTTP 301 con una nueva URL para contactar. Una nueva llamada en modo GET se realiza hacia la nueva URL.
Fallido	Error genérico diferente de los códigos descritos a continuación.
Servidor inalcanzable	La notificación duró más de 35 s.
Error con SSL handshake	La configuración de su servidor no es correcta. Realice un diagnóstico en el sitio de Qualys (*https://www.ssllabs.com/ssltest/*) y corrija los errores.
Conexión interrumpida	Error de comunicación.
Conexión rechazada	Error de comunicación.
Error servidor 300	Caso de redirección no aceptado por la plataforma.
Error servidor 304	Caso de redirección no aceptado por la plataforma.
Error servidor 305	Caso de redirección no aceptado por la plataforma.
Error servidor 400	El sitio del vendedor ha devuelto un código HTTP 400 Bad Request.
Error servidor 401	El sitio del vendedor ha devuelto un código HTTP 401 Unauthorized. Asegúrese de que el recurso no esté protegido por un archivo .htaccess.
Error servidor 402	El sitio del vendedor ha devuelto un código HTTP 402 Payment Required.
Error servidor 403	El sitio del vendedor ha devuelto un código HTTP 403 Forbidden. Asegúrese de que el recurso no esté protegido por un archivo .htaccess.
Error servidor 404	El sitio del vendedor ha devuelto un código HTTP 404 Not Found. Verifique que el ingreso de la URL esté correcto en la configuración de la regla. También verifique que el archivo esté presente en su servidor.
Error servidor 405	El sitio del vendedor ha devuelto un código HTTP 405 Method Not allowed.
Error servidor 406	El sitio del vendedor ha devuelto un código HTTP 406 Not Acceptable.
Error servidor 407	El sitio del vendedor ha devuelto un código HTTP 407 Proxy Authentication Required.
Error servidor 408	El sitio del vendedor ha devuelto un código HTTP 408 Request Time-out.

Estado	Descripción
Error servidor 409	El sitio del vendedor ha devuelto un código HTTP 409 Conflict.
Error servidor 410	El sitio del vendedor ha devuelto un código HTTP 410 Gone.
Error servidor 411	El sitio del vendedor ha devuelto un código HTTP 411 Length Required.
Error servidor 412	El sitio del vendedor ha devuelto un código HTTP 412 Precondition Failed.
Error servidor 413	El sitio del vendedor ha devuelto un código HTTP 413 Request Entity Too Large.
Error servidor 414	El sitio del vendedor ha devuelto un código HTTP 414 Request-URI Too long.
Error servidor 415	El sitio del vendedor ha devuelto un código HTTP 415 Unsupported Media Type.
Error servidor 416	El sitio del vendedor ha devuelto un código HTTP 416 Requested range unsatisfiable.
Error servidor 417	El sitio del vendedor ha devuelto un código HTTP 417 Expectation failed.
Error servidor 419	El sitio del vendedor ha devuelto un código HTTP 419 Authentication Timeout.
Error servidor 421	El sitio del vendedor ha devuelto un código HTTP 421 Misdirected Request.
Error servidor 422	El sitio del vendedor ha devuelto un código HTTP 422 Unprocessable Entity.
Error servidor 423	El sitio del vendedor ha devuelto un código HTTP 423 Locked.
Error servidor 424	El sitio del vendedor ha devuelto un código HTTP 424 Failed Dependency.
Error servidor 425	El sitio del vendedor ha devuelto un código HTTP 425 Too Early.
Error servidor 426	El sitio del vendedor ha devuelto un código HTTP 426 Upgrade Required.
Error servidor 429	El sitio del vendedor ha devuelto un código HTTP 431 Request Header Fields Too Large.
Error servidor 431	El sitio del vendedor ha devuelto un código HTTP 415 Unsupported Media Type.
Error servidor 451	El sitio del vendedor ha devuelto un código HTTP 451 Unavailable For Legal Reasons.
Error servidor 500	El sitio del vendedor ha devuelto un código HTTP 500 Internal Server Error. Se ha producido un error aplicativo en el servidor de su tienda. Consulte los registros de su servidor HTTP (generalmente apache). El problema solo puede corregirse al intervenir en su servidor.
Error servidor 501	El sitio del vendedor ha devuelto un código HTTP 501 Not Implemented.
Error servidor 502	El sitio del vendedor ha devuelto un código HTTP 502 Bad Gateway / Proxy Error.
Error servidor 503	El sitio del vendedor ha devuelto un código HTTP 503 Service Unavailable.
Error servidor 504	El sitio del vendedor ha devuelto un código HTTP 504 Gateway Time-out. El servidor del vendedor no ha aceptado la llamada dentro del tiempo de espera establecido de 10 s.
Error servidor 505	El sitio del vendedor ha devuelto un código HTTP 505 HTTP Version not supported.

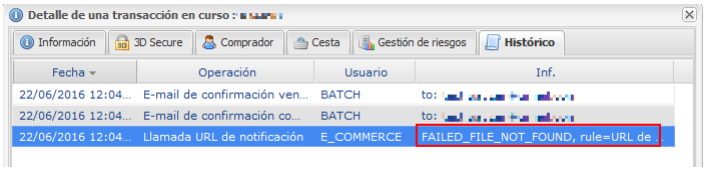
Para obtener más información sobre una notificación, haga clic en el enlace **Mostrar la información** o haga clic en la pestaña **Historial** y busque la línea **Llamada URL de notificación**.

Para ayudar al vendedor a identificar el origen del error, la plataforma analiza sistemáticamente los primeros 512 caracteres que devuelve el sitio del comerciante y los muestra en la columna **Información**.

- Ejemplo de notificación procesada con éxito:



- Ejemplo de notificación incorrecta



Si la plataforma no logra conectarse a la URL de su página, se enviará un e-mail de alerta a la dirección especificada.

Este contiene:

- El código HTTP del error encontrado
- Elementos de análisis en función del error
- Sus consecuencias
- El procedimiento a seguir desde el Back Office Vendedor para reenviar la solicitud a la URL definida en la configuración de la regla.

15. OBTENER AYUDA

¿Necesita ayuda? Consulte las preguntas frecuentes en nuestro sitio web

https://secure.cobroinmediato.tech/doc/es-AR/faq/sitemap.html

Para cualquier pregunta técnica o solicitud de asistencia, contacte *el soporte técnico*.

Para facilitar el procesamiento de sus solicitudes, se le pedirá que informe su ID de tienda (número de 8 dígitos).

Esta información está disponible en el correo electrónico de registro de su tienda o en el Back Office Vendedor (menú **Configuración** > **Tienda** > **Configuración**).

16. APÉNDICES

16.1. Crear automáticamente una recurrencia por Web Services

Utilice el método **Charge/CreateSubscription** para realizar pagos recurrentes (recurrencias) con un token existente y válido.

Para más informaciones, consultar la descripción del método *Charge/CreateSubscription*.

16.2. Dar de baja automáticamente una recurrencia por Web Services

Utilice el método **Subscription/Cancel** para dar de baja una recurrencia.

Para más informaciones, consultar la descripción del método *Subscription/Cancel*.

16.3. Tarjetas de test

Las tarjetas de test están disponibles en la página de pago.

En función del escenario de test asociado a la tarjeta, permiten:

- crear un token y / o un pago recurrente únicamente si el resultado del test es "Pago aceptado".
- no crear token si el resultado de test es "Pago rechazado".

Para probar el comportamiento cuando se rechaza un vencimiento, debe utilizar la siguiente tarjeta de test:

Número de tarjeta	Caso de prueba verificado
4970101000001002	Creación de token OK - Pago rechazado debido al límite excedido si el monto del vencimiento es superior a 0.

Nota

Esta tarjeta no se propone en la página de pago al crear un token.

