

MANUAL OPERATIVO DEL AFILIADO

Getnet México Servicios de Adquirencia, S.A. de C.V.
Última actualización: Agosto 2026



Nota de alcance

Este Manual tiene finalidad operativa y debe leerse como una guía práctica para procesar Transacciones, documentar ventas, atender aclaraciones, prevenir fraude, conservar evidencia y operar canales autorizados.

Las obligaciones, responsabilidades, restricciones, aspectos económicos, causas de terminación y demás condiciones jurídicas de la relación entre Getnet y el Afiliado se rigen por el Contrato de Afiliación y sus anexos vigentes.

La descripción de un canal, servicio o funcionalidad en este Manual no implica autorización automática para operarlo; **el Afiliado solo podrá utilizar aquello que haya sido autorizado conforme al Contrato, la Solicitud, carátula, anexos, apéndices o habilitaciones operativas aplicables.**



Contenido

1. Objeto y alcance operativo	3
1.1 Entornos de operación	3
1.2 Transacciones prohibidas y restricciones operativas	3
2. Lineamientos generales de operación	4
2.1 Aceptación operativa de Medios de Pago	4
2.2 Conciliación diaria	4
2.3 Manejo interno de documentación	4
3. Seguridad, datos y credenciales	5
3.1 Protección de datos del Tarjetahabiente	5
3.2 Contraseñas y accesos	5
3.3 Equipos, terminales y plataformas	5
3.4 Incidentes de información	5
4. Procesamiento de Transacciones	6
4.1 Flujo general de Autorización	6
4.2 Respuestas operativas posibles	6
4.3 Buenas prácticas de autorización	6
5. Operación con Tarjeta Presente	7
5.1 Validaciones previas	7
5.2 Comprobante de operación presencial	7
5.3 Errores frecuentes	7
6. Comercio electrónico y Tarjeta No Presente	8
6.1 Requisitos operativos de la Tienda Virtual	8
6.2 Datos de captura en comercio electrónico	8
6.3 Orden de pedido y acuse de recibo	9
6.4 3D Secure y herramientas de riesgo	9
7. Devoluciones y documentación soporte	9
7.1 Buenas prácticas para devoluciones en operaciones con tarjeta no presente	9
7.2 Evidencia recomendada	10
8. Peticiones de comprobantes, aclaraciones y Contracargos	10
8.1 Atención de una Petición de comprobante	10
8.2 Atención de Contracargos	10
8.3 Causas frecuentes de reclamación	10
9. Prevención de fraudes	11
9.1 Señales de alerta en comercio electrónico	11
9.2 Validaciones recomendadas antes de entregar	11
9.3 Prevención de fraude interno	12
10. Prevención operativa de lavado de dinero	12
10.1 Señales de alerta operativa	12
10.2 Acción recomendadas ante la sospecha	13
11. Servicios y módulos especiales	13
12. Información adicional	14
Apéndice A. Glosario operativo	15
Apéndice B. Verificación de coherencia	16



1.Objeto y alcance operativo

El presente Manual Operativo del Afiliado establece reglas, procedimientos y controles operativos aplicables al procesamiento de Transacciones, documentación de ventas, atención de aclaraciones, prevención de fraude, conservación de evidencia y operación de canales autorizados. Su propósito es servir como herramienta de consulta para el personal del Afiliado y para los equipos que dan seguimiento a la operación diaria.

Este Manual no reproduce ni sustituye disposiciones jurídicas, económicas o contractuales del Contrato de Afiliación. Los términos definidos, la integración contractual, el orden de prelación, las consecuencias por incumplimiento, la vigencia, terminación, comisiones, cargos, compensaciones, Fondo de Reserva y demás condiciones jurídicas o comerciales se regirán por el Contrato de Afiliación y los documentos que lo integran.

Regla de uso

Use este Manual para saber cómo operar. Use el Contrato para conocer derechos, obligaciones, responsabilidades, efectos económicos y consecuencias jurídicas.

La descripción de canales, servicios o funcionalidades en este Manual no debe interpretarse como autorización para utilizarlos. Cada canal operativo debe estar previamente habilitado y autorizado para el Afiliado conforme al Contrato de Afiliación, la Solicitud, carátula, anexos, apéndices o instrucciones operativas aplicables.

1.1 Entornos de operación

Entorno	Descripción operativa
Tarjeta presente	La Tarjeta o Medio de Pago se presenta físicamente o se utiliza presencialmente en el Dispositivo TPV o solución equivalente.
Tarjeta No Presente	La Transacción se procesa sin presencia física de la Tarjeta, incluyendo comercio electrónico, ventas telefónicas, cargos recurrentes o links de pago cuando estén habilitados.
Comercio electrónico	El Tarjetahabiente ingresa datos en una Tienda Virtual, página de pago o flujo digital autorizado.
Módulos especiales	Servicios como DCC, cargos recurrentes, MSI, Cashback, Get Commerce, Get Link & Pay u otros módulos, según estén habilitados y contratados.

1.2 Transacciones prohibidas y restricciones operativas

El Afiliado no deberá procesar operaciones que no correspondan a una venta legítima, documentada y realizada dentro de su giro autorizado. Esta regla protege la integridad de la operación, reduce riesgos de fraude, evita el uso indebido del número de afiliación y permite que las Transacciones puedan ser defendidas con evidencia suficiente ante aclaraciones o Contracargos. En ese sentido, el Afiliado deberá:

- No procesar Transacciones ilegales, fraudulentas, simuladas o no autorizadas.
- No utilizar el número de afiliación, Dispositivo TPV, Tienda Virtual o canal autorizado para operaciones de terceros.
- No procesar operaciones relacionadas con bienes o servicios no prestados por el Afiliado.
- No dividir artificialmente una venta para modificar controles de autorización o revisión.
- No reprocesar operaciones rechazadas de forma indebida o repetitiva.
- No utilizar Transacciones para obtener efectivo, refinanciar deudas o mover fondos sin una venta real.



2. Lineamientos generales de operación

Los lineamientos de esta sección describen controles de uso cotidiano para aceptar Medios de Pago, conciliar operaciones y conservar documentación de forma ordenada. Su finalidad es reducir errores de captura, cargos duplicados, reclamaciones, Contracargos, pérdida de evidencia y riesgos de fraude. Las obligaciones jurídicas relacionadas se encuentran en el Contrato de Afiliación y en las Reglas de Tarjeta aplicables.

2.1 Aceptación operativa de Medios de Pago

La aceptación de Medios de Pago debe realizarse de forma clara, uniforme y conforme al canal autorizado. El Afiliado debe evitar prácticas que confundan al Tarjetahabiente sobre el importe, la moneda, el comercio que realiza el cargo o las condiciones de la compra. Debido a lo anterior, el Afiliado debe:

- Confirmar que la Tarjeta o Medio de Pago se encuentre habilitado para el canal utilizado.
- Usar únicamente el canal, dispositivo o plataforma correspondiente a la operación que se pretende procesar.
- Evitar prácticas que generen confusión al Tarjetahabiente respecto del importe, moneda, comercio o descripción de la operación.
- No dividir una venta en múltiples Transacciones con el objetivo de modificar indebidamente la autorización o el control operativo.
- No reprocesar una Transacción rechazada sin revisar la causa del rechazo y el procedimiento aplicable.

2.2 Conciliación diaria

La conciliación diaria permite detectar diferencias antes de que se conviertan en reclamaciones, duplicidades o errores de liquidación. Por ello, debe realizarse como cierre operativo ordinario y no únicamente cuando exista una aclaración. Se recomienda:

- Conciliar ventas, devoluciones y reportes del Dispositivo TPV o plataforma al cierre de cada jornada operativa.
- Comparar importes contra reportes individuales y totales del lote.
- Identificar cargos duplicados, operaciones rechazadas, operaciones incompletas y diferencias de importe.
- Documentar internamente cualquier inconsistencia detectada para facilitar su seguimiento.
- Conservar evidencia operativa conforme a las reglas del Contrato y del procedimiento aplicable.

2.3 Manejo interno de documentación

La documentación soporte debe conservarse de forma segura, legible, ordenada y accesible. Su valor operativo no depende solo de que exista, sino de que pueda localizarse oportunamente y vincularse con la Transacción correcta cuando sea requerida. Para una mejor operación, se recomienda:

- Mantener ordenados comprobantes, pagarés, órdenes de pedido, acuses de recibo, notas de devolución y evidencia digital.
- Clasificar los documentos por fecha, número de afiliación, canal, folio de pedido o referencia de Transacción.
- Asegurar que la información sea legible, completa y recuperable cuando se requiera atender una aclaración.
- Evitar alteraciones, tachaduras o deterioro que dificulten la lectura o validación de la evidencia.
- No conservar datos sensibles que no deban mantenerse después de la autorización, como CVV2/CVC2.

3. Seguridad, datos y credenciales

Esta sección conserva controles operativos para proteger datos del Tarjetahabiente, credenciales, Dispositivos TPV, plataformas, Tiendas Virtuales, sistemas y documentación relacionada con Transacciones. Las obligaciones legales y contractuales de confidencialidad, protección de datos, incidentes y cumplimiento de programas de seguridad se encuentran en el Contrato de Afiliación y en los estándares aplicables.

3.1 Protección de datos del Tarjetahabiente

El Afiliado deberá:

- Solicitar únicamente la información necesaria para completar, autenticar, documentar o entregar la Transacción.
- No registrar ni almacenar CVV2/CVC2 después de solicitar la Autorización.
- No imprimir CVV2/CVC2 en comprobantes, pagarés, documentos de entrega, correos o documentos entregados al Tarjetahabiente.
- Usar truncamiento del número de Tarjeta cuando sea necesario incluirlo en documentos soporte.
- Restringir el acceso a la información de Tarjetahabientes al personal que lo requiera para operar o atender aclaraciones.

Lo anterior en el entendido de que la minimización de datos reduce exposición operativa y facilita el cumplimiento de controles de seguridad.

3.2 Contraseñas y accesos

Las credenciales deben tratarse como un control de acceso personal e intransferible. Compartir usuarios o contraseñas dificulta la trazabilidad de operaciones, impide identificar responsabilidades operativas y aumenta el riesgo de uso indebido de sistemas o plataformas, por lo que se recomien-

- Asignar credenciales únicamente a usuarios autorizados.
- Evitar compartir contraseñas entre usuarios, sucursales o áreas.
- Cambiar o revocar accesos cuando exista sospecha de compromiso.
- No guardar contraseñas en documentos visibles o dispositivos compartidos.
- Capacitar al personal para reconocer solicitudes inusuales o intentos de obtención de credenciales.

3.3 Equipos, terminales y plataformas

Se recomienda al Afiliado:

- Usar los dispositivos y plataformas conforme al flujo operativo previsto para cada canal.
- Proteger físicamente terminales, equipos, servidores y dispositivos móviles utilizados para cobrar.
- Evitar operar equipos que presenten fallas o mensajes de error sin revisar el procedimiento aplicable.
- Mantener los equipos en condiciones que permitan imprimir o generar comprobantes legibles.
- Conservar respaldos o reportes que permitan reconstruir la operación si ocurre una falla técnica.

3.4 Incidentes de información

Ante cualquier sospecha de acceso, uso, divulgación, transmisión o compromiso no autorizado de información, sistemas, documentos o credenciales, la prioridad operativa es preservar evidencia y escalar el incidente por los canales definidos. La manipulación o eliminación de registros puede impedir la reconstrucción de hechos.



Se recomienda al Afiliado:

- Ante sospecha de acceso no autorizado, preservar registros, reportes, logs, correos y evidencia electrónica.
- Evitar borrar, alterar o manipular evidencia relacionada con el incidente.
- Escalar internamente el incidente conforme a los canales definidos por Getnet y el Contrato.
- Cooperar en la reconstrucción de hechos y en la identificación de datos involucrados.
- Aplicar medidas correctivas para reducir el riesgo de repetición.

4. Procesamiento de Transacciones

El procesamiento de una Transacción comprende, de forma general, la captura de datos de la operación, la solicitud de Autorización, la respuesta del Emisor, la documentación de la operación y la liquidación operativa del lote o registro correspondiente. La Autorización permite continuar con el flujo de venta, pero no garantiza pago definitivo ni elimina el riesgo de Contracargo, reclamación, reverso, rechazo posterior o solicitud documental.

4.1 Flujo general de Autorización

1. El Cliente o Tarjetahabiente solicita adquirir bienes o servicios usando un Medio de Pago.
2. El Afiliado captura o recibe los datos de la operación mediante el canal autorizado: Dispositivo TPV, Tienda Virtual, software, liga de pago o plataforma correspondiente.
3. La solicitud se envía de forma electrónica al Adquirente o al sistema que corresponda para su enrutamiento.
4. El Emisor determina si aprueba, rechaza o refiere la Transacción.
5. El Afiliado recibe la respuesta y actúa conforme al resultado obtenido.
6. La operación se documenta con el comprobante, referencia, orden, acuse o evidencia aplicable al canal utilizado.

4.2 Respuestas operativas posibles

Respuesta	Acción operativa sugerida
Autorizada	Completar la venta y conservar evidencia de la Transacción, entrega o prestación del servicio.
Rechazada	Solicitar otra forma de pago y evitar reintentos indebidos o repetitivos.
Referida / verificación adicional	Seguir el procedimiento de verificación aplicable antes de completar la operación.
Error técnico	No asumir que la venta fue aprobada; revisar reportes, duplicidad y estado de la operación antes de reprocesar.

4.3 Buenas prácticas de autorización

Las buenas prácticas de autorización buscan asegurar que el monto, canal, fecha y evidencia correspondan a la operación real. El Código de Autorización debe conservarse junto con la documentación aplicable, pero no debe interpretarse como defensa suficiente por sí solo.

Adicionalmente como buena práctica el Afiliado deberá:



- Solicitar Autorización por el monto exacto de la Transacción.
- Procesar la operación en la fecha en que se realiza la venta o prestación del servicio, salvo que el procedimiento del canal indique otra cosa.
- No completar la entrega de bienes o servicios si no existe confirmación operativa suficiente de la autorización o pago aplicable.
- No asumir que un Código de Autorización elimina la posibilidad de reclamaciones posteriores.
- Conservar el Código de Autorización o la referencia generada por el sistema.

5. Operación con Tarjeta Presente

La operación presencial requiere validar que el Medio de Pago sea procesado mediante el dispositivo correspondiente y que el comprobante o registro refleje correctamente los datos mínimos de la Transacción.

5.1 Validaciones previas

Antes de procesar la operación, el Afiliado deberá realizar las siguientes validaciones en operaciones con tarjeta presente:

- Confirmar que la Tarjeta no esté vencida cuando la validación física sea aplicable.
- Utilizar Chip, NIP, contactless, banda magnética o captura autorizada según el flujo disponible.
- Cuando el flujo solicite firma, obtenerla y revisar consistencia con la Tarjeta si aplica.
- No solicitar al Tarjetahabiente que revele verbalmente su NIP.
- No procesar la operación si el dispositivo indica rechazo o si no se obtiene autorización.

5.2 Comprobante de operación presencial

Después de procesar la operación, el Afiliado deberá realizar las siguientes validaciones en operaciones con tarjeta presente:

- Verificar que el comprobante muestre importe, fecha, comercio, referencia y autorización cuando corresponda.
- Mantener la copia o registro del Afiliado en buen estado y legible.
- Entregar al Tarjetahabiente la copia o comprobante aplicable.
- Evitar alterar, perforar, engrapar o dañar el comprobante si ello afecta su lectura.
- Registrar internamente cualquier anomalía operativa detectada durante la venta.

5.3 Errores frecuentes

Para reducir errores de procesamiento, reclamaciones y Contracargos, el Afiliado deberá evitar las siguientes prácticas:

- Procesar dos veces la misma venta.
- Capturar un importe distinto al informado al Cliente.
- Cerrar el lote sin revisar diferencias.
- Operar con comprobantes ilegibles.
- Reprocesar operaciones rechazadas sin justificación operativa.
- Usar una terminal o canal no correspondiente al establecimiento o flujo operativo.



6. Comercio electrónico y Tarjeta No Presente

Las Transacciones de Tarjeta No Presente presentan un nivel de riesgo operativo mayor porque la Tarjeta no se presenta físicamente al Afiliado y la identidad del Tarjetahabiente puede depender de controles digitales, documentales o de autenticación. Por ello, este apartado conserva controles de validación, información visible al Cliente, seguridad y evidencia documental para reducir reclamaciones, fraude y disputas por falta de entrega o prestación del servicio.

6.1 Requisitos operativos de la Tienda Virtual

La Tienda Virtual deberá proporcionar al Tarjetahabiente información clara, completa y visible antes de que concluya la compra. Esto permite que el Cliente identifique al Afiliado o comercio, conozca las condiciones relevantes de la operación y pueda reconocer el cargo en sus estados de cuenta. Para tal efecto, la Tienda Virtual deberá incluir, cuando resulte aplicable, la siguiente información:

- Nombre del Afiliado o comercio, visible para el Tarjetahabiente.
- Descripción completa de los bienes o servicios ofrecidos.
- Precio, importe total y moneda de la Transacción.
- Política de entrega, incluyendo tiempos, costos y condiciones aplicables.
- Política de devolución, reembolso y cancelación, cuando corresponda.
- Datos de contacto para atención a clientes, como correo electrónico, teléfono o domicilio.
- Domicilio del establecimiento permanente o información de localización requerida por el canal.
- Restricciones legales, de exportación, geográficas o de entrega, cuando existan.
- Política de privacidad o tratamiento de datos del Cliente.
- Medidas de seguridad aplicables al flujo de pago, como SSL, 3D Secure u otras herramientas habilitadas.

6.2 Datos de captura en comercio electrónico

Finalidad	Datos contemplados por los documentos fuente
Pago	Número de Tarjeta, fecha de expiración, CVV2/CVC2, marca de Tarjeta y, cuando el flujo lo requiera, nombre del Emisor.
Identificación	Nombre completo del Tarjetahabiente y teléfono de contacto cuando sea necesario.
Facturación	Domicilio completo de facturación cuando sea requerido por el flujo o por validaciones.
Entrega	Domicilio de entrega y nombre de la persona autorizada para recibir bienes o servicios.
Evidencia	Orden de pedido, folio, acuse de recibo, fecha de entrega, nombre y firma de quien recibe, según aplique.

Minimización de datos

La lista anterior no implica que deban solicitarse todos los datos en todos los casos. Deben solicitarse únicamente los necesarios para operar, autenticar, documentar, entregar o atender la transicción



6.3 Orden de pedido y acuse de recibo

La orden de pedido y el acuse de recibo son piezas clave para acreditar qué se vendió, cuándo se autorizó la operación, a quién se entregó y en qué condiciones. En operaciones disputadas, estos documentos ayudan a conectar la Transacción con la entrega o prestación correspondiente.

Cuando la operación implique entrega de bienes o prestación de servicios, el Afiliado deberá:

- Generar una orden o referencia de pedido por cada venta que implique entrega de producto o prestación de servicio.
- Incluir folio, nombre comercial, fecha, nombre del Tarjetahabiente, importe, autorización y descripción del bien o servicio.
- Incluir domicilio de entrega y persona autorizada a recibir cuando aplique.
- Obtener acuse de recibo con fecha, domicilio de entrega, nombre y firma de quien recibe cuando la naturaleza de la entrega lo permita.
- Conservar orden y acuse como evidencia operativa para aclaraciones o reclamaciones.

6.4 3D Secure y herramientas de riesgo

Las herramientas de autenticación y gestión de riesgo, como 3D Secure, módulos de riesgo, validaciones adicionales o tokenización, pueden fortalecer el control operativo de las Transacciones de Tarjeta No Presente. Sin embargo, su uso no sustituye la documentación de la venta ni elimina por completo el riesgo de fraude, reclamación o Contracargo. Su efectividad dependerá del canal utilizado, del motivo de la disputa, de las Reglas de Tarjeta aplicables, de la configuración habilitada y de la evidencia disponible.

Cuando estas herramientas se encuentren habilitadas para el producto, canal o flujo correspondiente, el Afiliado deberá:

- Utilizar 3D Secure u otros mecanismos de autenticación cuando resulten aplicables.
- Conservar evidencia del resultado de autenticación, cuando esté disponible.
- Aplicar reglas de riesgo, validaciones de correo, revisión manual, tokenización u otros controles únicamente cuando estén habilitados para el servicio correspondiente.
- Evitar asumir que una herramienta de seguridad elimina por completo el riesgo de fraude, reclamaciones o Contracargos.
- Revisar las operaciones atípicas antes de liberar la entrega o prestación del servicio, cuando las señales de riesgo lo ameriten.

7. Devoluciones y documentación soporte

Las devoluciones deben documentarse con claridad para evitar duplicidades, diferencias contables o reclamaciones. Esta sección describe controles operativos sin regular consecuencias económicas o contractuales.

7.1 Buenas prácticas para devoluciones en operaciones con tarjeta no presente

En operaciones con Tarjeta No Presente, las devoluciones deben procesarse de forma trazable y vinculada con la Transacción original. Esto permite evitar duplicidades, acreditar la devolución frente al Cliente y conservar evidencia suficiente en caso de aclaraciones, reclamaciones o Contracargos. Para estos efectos, el Afiliado deberá:

- Procesar la devolución por el canal correspondiente a la Transacción original cuando sea aplicable.
- Identificar la Transacción original, fecha, importe, autorización o referencia.
- Generar comprobante o nota de devolución cuando el sistema lo permita.
- Entregar copia o confirmación al Cliente según el canal utilizado.
- Registrar internamente la causa de la devolución y conservar evidencia soporte.



7.2 Evidencia recomendada

Tipo de operación	Evidencia operativa
Venta presencial	Comprobante, pagaré o registro electrónico, autorización, lote y reporte del dispositivo.
Venta ecommerce	Orden de pedido, confirmación de pago, resultado 3DS, evidencia de entrega o prestación del servicio.
Devolución	Nota de devolución, referencia original, comprobante procesado y confirmación al cliente.
Contracargo o aclaración	Documentación solicitada en el requerimiento: comprobante, orden, acuse, evidencia de servicio o comunicación relacionada.

8. Peticiones de comprobantes, aclaraciones y Contracargos

Una Petición de comprobante o de Pagaré de Venta tiene como finalidad obtener evidencia de una Transacción. Un Contracargo es una Transacción disputada por el Tarjetahabiente o el Emisor. En ambos casos, la capacidad de respuesta del Afiliado depende de que la documentación exista, sea legible, esté completa y pueda relacionarse claramente con la operación requerida.

8.1 Atención de una Petición de comprobante

La respuesta a una petición de comprobante debe ser rápida y ordenada. El objetivo es localizar la evidencia correcta, verificar que corresponda a la Transacción solicitada y remitirla por el canal indicado sin alterar su contenido. Para efectos el Afiliado deberá:

- Identificar de inmediato la Transacción solicitada usando fecha, importe, número de afiliación, autorización y referencia.
- Localizar el comprobante o evidencia equivalente.
- Confirmar legibilidad y correspondencia entre comprobante, importe y fecha.
- Remitir la documentación por el medio operativo indicado por Getnet.
- Guardar constancia de envío y de la documentación remitida.

8.2 Atención de Contracargos

La atención de Contracargos requiere analizar el motivo de disputa y preparar una respuesta documental coherente. No basta acumular documentos; la evidencia debe explicar de forma consistente la venta, autorización, entrega, devolución o prestación del servicio, según corresponda.

Para atender un Contracargo, el Afiliado deberá:

- Leer la notificación o requerimiento para identificar causa, plazo operativo y evidencia solicitada.
- Reunir documentos soporte de la venta, entrega, servicio, devolución o comunicación con el Cliente.
- Revisar que la evidencia sea consistente y legible.
- Enviar la documentación por el canal indicado.
- Registrar internamente el caso para seguimiento y aprendizaje operativo.

8.3 Causas frecuentes de reclamación

Las reclamaciones pueden originarse por diferencias entre lo que el Cliente reconoce, lo que el Afiliado documentó y lo que efectivamente ocurrió durante la operación. Identificar las causas más frecuentes permite reforzar controles, conservar mejor evidencia y reducir el riesgo de Contracargos. Entre las causas más comunes se encuentran:



- El Cliente no reconoce la Transacción.
- El Cliente reclama falta de entrega de bienes o prestación de servicios.
- El Cliente cuestiona la calidad o características del bien o servicio.
- Existe cargo duplicado.
- La operación fue procesada después de un rechazo o sin evidencia suficiente.
- La documentación solicitada no fue localizada o resulta ilegible.

9. Prevención de fraudes

La prevención de fraude requiere combinar validaciones de sistema, revisión del personal, evidencia documental y monitoreo de patrones inusuales. El objetivo es identificar operaciones que puedan ser fraudulentas antes de entregar bienes o prestar servicios.

9.1 Señales de alerta en comercio electrónico

En operaciones de comercio electrónico, el Afiliado deberá prestar especial atención a patrones de compra, datos de contacto, domicilios de entrega y comportamiento transaccional que se aparten del perfil ordinario del comercio. La presencia de una señal de alerta no implica necesariamente que la operación sea fraudulenta; sin embargo, debe motivar una revisión adicional antes de liberar la entrega del producto o la prestación del servicio.

Entre las señales de alerta más relevantes se encuentran:

- Órdenes inusualmente grandes en cantidad o importe frente al patrón del comercio.
- Pedidos múltiples con distintas Tarjetas y mismo usuario, correo, domicilio o IP.
- Pedidos con Tarjetas que muestran números en secuencia o patrones anómalos.
- Entregas solicitadas a apartados postales o direcciones atípicas.
- Solicitudes de entrega a transportistas o terceros sin justificación clara.
- Compras de productos de fácil reventa en volúmenes inusuales.
- Múltiples Transacciones en corto tiempo o en horarios inusuales.
- Diferencias relevantes entre datos de facturación, entrega, usuario y método de contacto.

Cuando se identifique una o más señales de alerta, el Afiliado deberá aplicar validaciones adicionales, conservar evidencia de la revisión realizada y evitar liberar la entrega o prestación del servicio si no cuenta con elementos suficientes para confirmar la legitimidad de la operación.

9.2 Validaciones recomendadas antes de entregar

Antes de liberar la entrega de bienes o la prestación del servicio en operaciones de comercio electrónico, el Afiliado deberá verificar que la información de la operación sea consistente y razonable conforme al patrón habitual del comercio. Estas validaciones permiten identificar posibles inconsistencias antes de completar la entrega y conservar evidencia suficiente en caso de reclamaciones o Contracargos.



Para estos efectos, el Afiliado deberá:

- Revisar que el nombre, teléfono, correo electrónico, domicilio de entrega, domicilio de facturación y patrón de compra sean consistentes entre sí.
- Aplicar validaciones adicionales cuando la operación resulte inusual por su monto, frecuencia, horario, origen, destino o características del pedido.
- Revisar el resultado de autenticación 3D Secure o de las herramientas de riesgo disponibles, cuando se encuentren habilitadas para el canal correspondiente.
- Conservar evidencia de la comunicación con el Cliente cuando sea necesario confirmar la operación.
- Documentar la entrega mediante acuse de recibo, guía, comprobante de entrega o evidencia equivalente, cuando sea posible.
- Si la revisión muestra inconsistencias relevantes, el Afiliado deberá analizar la operación con mayor detalle antes de liberar la entrega del producto o iniciar la prestación del servicio.

9.3 Prevención de fraude interno

El Afiliado deberá implementar controles internos para reducir el riesgo de uso indebido de información, accesos, sistemas o funciones operativas sensibles. Estos controles deben permitir identificar quién realiza cada operación, limitar el acceso conforme a las funciones del personal y detectar movimientos inusuales o fuera del patrón ordinario del comercio.

Para estos efectos, el Afiliado deberá:

- Limitar el acceso a información de Tarjetahabientes únicamente al personal que lo requiera para cumplir sus funciones.
- Restringir operaciones sensibles, como devoluciones, ajustes, cancelaciones o modificaciones, al personal expresamente autorizado.
- Monitorear accesos, cambios, devoluciones, ajustes y operaciones que se aparten del patrón habitual del comercio.
- Evitar almacenar datos sensibles de Tarjetas en archivos, hojas de cálculo, correos electrónicos, notas internas o cualquier otro medio no autorizado.
- Capacitar al personal sobre el manejo adecuado de información, uso de credenciales, señales de fraude y procedimientos de escalamiento.

10. Prevención operativa de lavado de dinero

El Manual conserva una visión operativa de prevención, limitada a señales de alerta y conductas que deben escalarse internamente. Las obligaciones legales y contractuales específicas se encuentran en el Contrato de Afiliación.

10.1 Señales de alerta operativa

El Afiliado deberá prestar atención a operaciones que no correspondan con su actividad ordinaria, que involucren a terceros no autorizados o que aparenten no tener una venta real de bienes o servicios. Estas situaciones pueden representar un uso indebido de la afiliación y deben ser revisadas antes de procesar o continuar con la operación.



Entre las principales señales de alerta se encuentran:

- Procesar Transacciones por cuenta de un tercero o de un negocio distinto al informado.
- Permitir que otro comercio utilice la afiliación para cobrar sus propias ventas.
- Procesar operaciones que no correspondan al giro, actividad o perfil operativo del Afiliado.
- Recibir operaciones con montos, frecuencia, volumen o naturaleza que no correspondan al comportamiento ordinario del comercio.
- Recibir propuestas de terceros para procesar pagos a cambio de una cuota, comisión o beneficio.
- Procesar operaciones que aparenten estar destinadas a refinanciar deudas, obtener efectivo, mover fondos o simular ventas sin una operación real de bienes o servicios.

Cuando se identifique alguna de estas señales, el Afiliado deberá abstenerse de procesar la operación hasta confirmar que corresponde a una venta legítima, documentada y realizada dentro de su giro autorizado.

10.2 Acción recomendada ante la sospecha

Cuando el Afiliado identifique una operación inusual, una propuesta de procesamiento por cuenta de terceros o cualquier situación que no corresponda a una venta legítima y documentada, deberá actuar con cautela y escalar el caso por los canales correspondientes. El objetivo es evitar el uso indebido de la afiliación, preservar la evidencia disponible y reducir riesgos operativos.

Para estos efectos, el Afiliado deberá:

- Abstenerse de procesar operaciones sospechosas cuando no exista una venta legítima, real y documentada.
- Escalar internamente la situación al área o canal definido por Getnet.
- Conservar la evidencia disponible sin alterarla, eliminarla o modificarla.
- Rechazar instrucciones de terceros que busquen simular ventas, procesar operaciones ajenas o modificar el origen real de los fondos.
- Capacitar al personal para identificar y escalar propuestas de procesamiento por cuenta de terceros o de uso indebido de la afiliación.

Si la operación no puede justificarse como una venta real, documentada y dentro del giro autorizado del Afiliado, se recomienda no procesarse.

11. Servicios y módulos especiales

Los servicios y módulos especiales deben tratarse en el Manual únicamente desde su uso operativo. Sus condiciones comerciales, configuraciones específicas, costos, cancelaciones, anexos y efectos contractuales se rigen por el Contrato y los documentos aplicables. La inclusión de un servicio en este apartado no implica que todos los Afiliados estén autorizados para utilizarlo.



Servicio / módulo	Tratamiento en este Manual
DCC	Conservar instrucciones operativas para obtener consentimiento del Tarjetahabiente cuando el flujo lo requiera. No incluir costos ni condiciones contractuales.
MOTO / venta telefónica	Mantener controles de captura, evidencia y validación de datos de Tarjeta No Presente.
Cargos recurrentes	Mantener controles documentales de autorización, soporte y cancelación operativa si se encuentran en los documentos fuente.
Cashback	Incluir únicamente flujo operativo, identificación de importe de compra y retiro cuando esté habilitado. No incluir comisiones.
Meses sin intereses	Incluir instrucciones de selección del plazo y validación de promoción cuando esté habilitado. No incluir tasas ni montos mínimos contractuales.
Get Link & Pay	Conservar descripción operativa de generación y envío de ligas de pago cuando el producto esté habilitado.
Get Commerce	Conservar descripción operativa de integración de gateway y módulos de seguridad. No incluir garantía de Contracargos ni comisiones.
CoDi	Incluir únicamente referencia operativa de habilitación y conciliación si el servicio está contratado.

12. Información adicional

El Afiliado deberá consultar las fuentes vigentes aplicables para conocer reglas de operación, estándares de seguridad, lineamientos de las Redes de Pago y condiciones específicas de productos o canales. Este apartado funciona únicamente como remisión general y no sustituye las versiones vigentes de dichas fuentes, ni modifica lo previsto en el Contrato de Afiliación, sus anexos o comunicaciones aplicables.

Entre las fuentes de consulta relevantes se encuentran:

- Redes de Pago: Visa, MasterCard, American Express y las demás que resulten aplicables según el Medio de Pago habilitado.
- Estándares de seguridad: PCI DSS y demás programas de seguridad asociados a las Redes de Pago.
- Guías operativas de marca: incluyendo la Guía Operativa del Comerciante American Express, cuando resulte aplicable.
- Contrato de Afiliación y anexos vigentes: para condiciones jurídicas, comerciales, económicas, operativas o de responsabilidad.
- Canales de soporte de Getnet: aquellos indicados contractualmente o comunicados al Afiliado para atención, soporte o aclaraciones.



Apéndice A. Glosario operativo

Término	Definición operativa
Adquirente	Getnet México Servicios de Adquirencia, S.A. de C.V., en su carácter de adquirente.
Afiliado	Persona física o moral que acepta pagos mediante Medios de Pago dentro del Programa de Afiliación.
Autorización	Respuesta del Emisor que aprueba, rechaza o refiere una Transacción.
Código de Autorización	Código generado cuando el Emisor autoriza una Transacción.
Contracargo	Transacción disputada por el Tarjetahabiente o el Emisor.
CVV2/CVC2	Código de seguridad usado en operaciones de Tarjeta No Presente; no debe conservarse después de la autorización.
Dispositivo TPV	Terminal, software o dispositivo de punto de venta utilizado para procesar Transacciones.
Emisor	Institución o entidad que emite la Tarjeta al Tarjetahabiente.
Medio de Pago	Tarjeta, dispositivo o mecanismo utilizado para procesar una Transacción.
Pagaré de Venta / Comprobante	Registro físico o electrónico que documenta una Transacción.
Tarjeta No Presente	Operación sin presencia física de la Tarjeta, como ecommerce, MOTO, link de pago o cargos recurrentes.
Tarjeta Presente	Operación en la que la Tarjeta o Medio de Pago está físicamente presente o se usa presencialmente.
Tienda Virtual	Sitio, página o flujo digital mediante el cual el Tarjetahabiente realiza una compra por Internet.
3D Secure	Servicio de autenticación del Emisor para Transacciones de Tarjeta No Presente.



Apéndice B. Verificación de coherencia

Antes de entregar esta versión del Manual, se verificó que el documento mantuviera utilidad práctica, claridad editorial y subordinación al Contrato de Afiliación. La revisión buscó evitar que el Manual se convierta en una simple lista de bullets, preservando explicaciones introductorias, criterios de uso, tablas de consulta y controles operativos.

Punto de revisión	Resultado
No inventar datos	Cumple. El texto se construyó sólo con materias identificadas en los documentos disponibles.
No agregar información ajena	Cumple. Se evitó incorporar procedimientos, plazos o costos no contenidos en las fuentes.
No alterar hechos	Cumple. Las materias contractuales se depuraron sin modificar su contenido; se remitieron al Contrato.
Eliminar duplicidades	Cumple. Se eliminaron comisiones, cuotas, fondo de reserva, terminación, indemnizaciones, responsabilidad económica y demás materias contractuales.
Mantener finalidad operativa	Cumple. El Manual conserva procesos, flujos, controles, evidencias y recomendaciones prácticas.
Extensión máxima	Cumple. El documento se diseñó para mantenerse por debajo de 40 hojas.
Información faltante	NO ENCONTRADO: no se incorporaron imágenes o diagramas no recuperados como texto.
Coherencia terminológica	Cumple. Se usaron términos consistentes: Afiliado, Adquirente, Tarjetahabiente, Emisor, Medio de Pago, Transacción, Contracargo y Tienda Virtual.

Conclusión de revisión

El Manual resultante conserva la utilidad operativa de los manuales fuente y evita duplicar materias reguladas en el Contrato de Afiliación. Su lectura debe mantenerse subordinada al Contrato y anexos vigentes para cualquier cuestión jurídica, económica o de responsabilidad.

