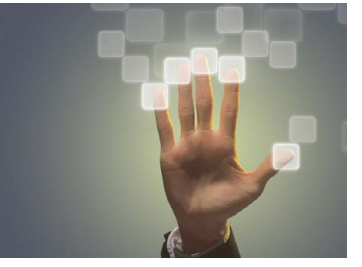
Capítulo 8

MEDIOS DE PAGO

Verificación de un tarjetahabiente

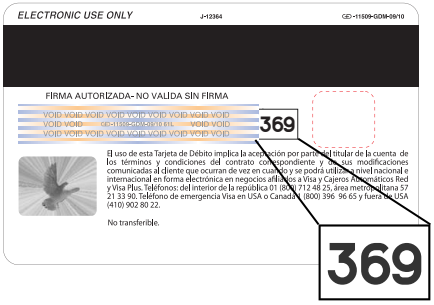


Verificación de un tarjetahabiente

Garantizar que los clientes que realizan una transacción en el negocio sean legítimos también es fundamental en el e-commerce y para ello existen herramientas para la **verificación de la legitimidad de los tarjetahabientes.**

Verificación de plástico (CVV2)[1]

- Número de tres dígitos impreso en la parte posterior del plástico.
- CVV2 es requerido en todas las tarjetas.



3DSecure

- Permite a las instituciones financieras autenticar la identidad de los tarjetahabientes durante el proceso de pago mediante una contraseña personal adicional.

Autenticación selectiva

- Herramienta de gestión de riesgos que en tiempo real provee calificaciones de riesgo dadas las características de la transacción.

Sistema de verificación de dirección (AVS)

- Permite al comercio verificar la dirección de una tarjeta con el emisor.
- El AVS provee al comercio un indicador clave para verificar si la transacción es válida.

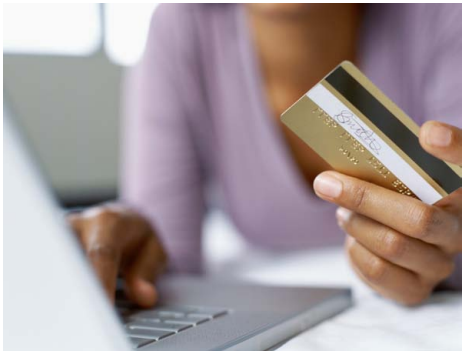
- Únicamente aplica en países como Estados Unidos y Reino Unido.

1. CVV2 (Card Verification Value) o Valor de verificación de tarjeta 2 es un número de seguridad de 3 ó 4 dígitos impreso sin relieve en el dorso de tarjeta que se usa para reducir los riesgos en transacciones.

Descripción de la tecnología de autenticación **3DSecure:**

¿Cómo funciona 3DSecure?	1	El cliente se inscribe en el programa a través del banco emisor de la tarjeta.
	2	El cliente entra a realizar una compra al sitio que se encuentre afiliado al programa (el comercio cuenta con un sello visible).
	3	Durante el proceso de pago el cliente debe ingresar la contraseña correspondiente al programa.
¿Qué beneficios tiene?	1	El cliente tiene mayor confianza y seguridad al prevenir transacciones fraudulentas.
	2	El comercio minimiza el riesgo de contracargos (chargebacks) y fortalece la marca a partir del sello 3DSecure en el sitio.
	3	El banco aumenta el volumen de facturación y representa un valor agregado para los tarjetahabientes.
¿Qué tecnología usa?	1	Tecnología de autenticación que usa encriptamiento Secure Sockets Layer (SSL) y una conexión al servidor del comercio de fácil instalación.
	2	El tarjetahabiente no requiere ningún software o hardware especial en su dispositivo de acceso.

Adicionalmente, existen **herramientas de administración y prevención de fraude** que permiten determinar el nivel de riesgo de las transacciones[1]:



El usuario lleva a cabo una transacción y los datos de la misma son enviados a un proveedor de servicios de autenticación.

a. Transacción rechazada
b. Solicitar autenticación vía electrónica o vía telefónica.
c. Transacción aceptada

La herramienta define el **nivel de riesgo** para determinar si la **transacción debe ser aceptada o rechazada.**

- Representa un paso adicional en el proceso de análisis y acreditación de los tarjetahabientes para las compras en Internet.
- Son herramientas particularmente útiles para los comercios pero deben ser implementadas buscando no afectar la experiencia de compra de los clientes.

1. Ver Anexo **Utilización de herramientas de detección de fraude.**