AZUL | SERVICIOS DIGITALES POPULAR

GUÍA
REQUISITOS SITIO WEB O APLICACIÓN MÓVIL E-COMMERCE

ÍNDICE

Checklist 3
Requisitos del sitio web 4
- Nombre del comercio claro 4
- Descripción completa y clara de los bienes y servicios 4
- Despliegue de las marcas de tarjetas aceptadas 5
- Políticas claras de devoluciones, reembolsos y cancelaciones 6
- Información para contacto de servicio al cliente 7
- Política clara de entrega 7
- Dirección permanente del negocio 8
- Moneda de compra 9
- Política de privacidad 9
- Políticas de seguridad para la transmisión de datos de tarjetas 10
- Check Out en un checkbox para aceptar los términos y condiciones del sitio web 11
- Recibo claro y completo 12
- Agregar logos del servicio de Autenticación del Tarjetahabiente 13

Recomendaciones para prevención de ataques de robots 14
- Herramientas técnicas 14
- Creación de cuentas 14
- Detección de comportamientos anormales 15
- Seguridad en el almacenamiento y procesamiento de datos 15

Checklist

Utiliza este checklist para asegurarte de que tengas todos los requisitos para empezar a utilizar tu E-Commerce:

REQUISITOS DE AFILIACIÓN

- ☐ Formulario Gestión de Prospecto
- ☐ Autorización de buró
- ☐ Contrato de afiliación
- ☐ Registro mercantil
- ☐ Estados financieros al último cierre fiscal o plan de negocios (si es empresa nueva)
- ☐ Fotos del establecimiento e inventario
- ☐ Copia de documentos de identidad de los socios
- ☐ Link de la página web y usuario de prueba
- ☐ Contacto de su programador o desarrollador de su página web

REQUISITOS DEL SITIO WEB

- ☐ Nombre comercial claro
- ☐ Descripción completa y clara de los productos y servicios
- ☐ Desplegar los logos de las marcas Visa y Mastercard
- ☐ Políticas claras de devoluciones, reembolsos y cancelaciones. Estas políticas deben de estar visibles para el tarjetahabiente a fin de informarles de sus derechos y responsabilidades. Si el comercio no tiene políticas de reembolso, debe de estar claro para el tarjetahabiente antes de realizar la compra.
- ☐ Información para contactar a servicio al cliente (correo electrónico y número telefónico)
- ☐ Política clara de entrega
- ☐ La dirección permanente del comercio, incluyendo el país
- ☐ Moneda(s) de compra. Debe de estar representada en símbolo monetario local (Ejemplo: US$, RD$) o ISO 4217 (Ejemplo: USD, DOP)
- ☐ Políticas de privacidad
- ☐ Políticas de seguridad para la transmisión de datos de tarjetas (En el documento adjunto hay un ejemplo de estas políticas)
- ☐ Desplegar en el **Check Out** un **CheckBox** donde el cliente indique que acepte los términos y condiciones del sitio web. Ejemplos:
  - Estoy de acuerdo con los Términos y Condiciones. *
  - Acepto los Términos y Condiciones de nombredetiendaecomm. *
  - He leído y estoy de acuerdo con los términos y condiciones de esta página. *
  - Otra opción sin utilizar un checkbox o slider, es antes de continuar al dar clic al botón de completar o finalizar compra/pedido aceptar las políticas
- ☐ Enviar modelo del recibo o comprobante de pago que le enviarán al cliente luego del pago
- ☐ Para el servicio 3D Secure, es necesario también agregar los logos de Verified by Visa, Mastercard ID Check y AMEX SafeKey en:
  - La página principal
  - La página de las Políticas de seguridad para la transmisión de datos de tarjetas
  - La página del Check Out

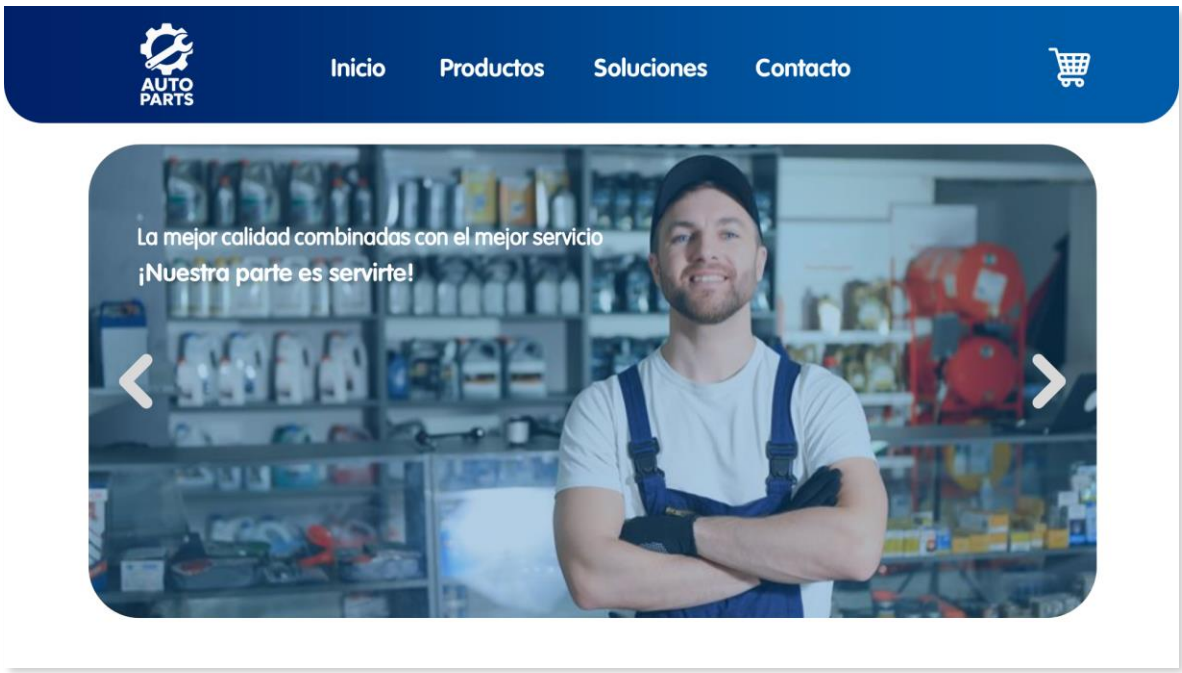
Requisitos del sitio web

Mientras más tu cliente sepa de tu tienda virtual, ¡mejor! Es por esto que las marcar requieren que tu sitio web o aplicación móvil incluya ciertos requisitos de contenido que eviten malos entendidos con tus clientes que puedan resultar en disputas innecesarias.

Aquí te incluimos los requisitos y recomendaciones de las marcas para tu tienda virtual.

Nombre del comercio claro

Tu tienda virtual debe contener el nombre comercial de tu negocio para que tu cliente pueda identificar exactamente a quién le está comprando y reconozca posteriormente el cargo en su estado de cuenta. Es importante que dicho nombre se encuentre en un lugar visible, preferiblemente, en la parte superior de la página.



Descripción completa y clara de los bienes y servicios

Asegúrate de que tus bienes y servicios estén claramente descritos en tu tienda virtual.

- Crea descripciones claras y completas de los productos y servicios que ofreces para que, al comprar, los clientes sepan exactamente lo que están adquiriendo y no tengan insatisfacciones entre lo recibido y lo descrito en tu página.
- Incluye imágenes de tus productos, muy similares a lo que el cliente recibirá al realizar su compra.
- Incluye la información sobre el tamaño, color, peso, talla, modelo, precio, etc.

Punto clave: Si estás operando en un mercado global, esto aumenta las oportunidades para mal entendidos de los clientes. Por ejemplo, si vendes bienes eléctricos, asegúrate de incluir los requerimientos de voltaje, lo cual varía alrededor del mundo.



Despliegue de las marcas de tarjetas aceptadas

Es importante que coloques los nombres y/o logos de las marcas de tarjetas que aceptas en tu tienda. Así evitas declinaciones en las órdenes de tus clientes debido al uso de una marca de tarjeta no aceptada en tu tienda. Esto también tiene impacto en la experiencia de compra de tu cliente. A continuación, te colocamos los enlaces en los que puedes descargar los logos de las marcas que aceptas.

IMPORTANTE: Para el caso de American Express, debes estar afiliado con el Scotiabank, quienes son los representantes de esta marca en el país.

Logos de marcas	
Visa	https://www.merchantsignage.visa.com/brandguidelines
Mastercard	https://www.mastercard.com/brandcenter/us/en/download-artwork.html#tabs-4aac18340b-item-6f39c2ce9a-tab
American Express	https://www.amexpop.com/Asset/Index/5
Logos 3D Secure	
Visa Secure	https://www.merchantsignage.visa.com/brandguidelines
Mastercard ID Check	https://www.mastercard.com/brandcenter/us/en/download-artwork.html#tabs-4aac18340b-item-11f8546d08-tab



Políticas claras de devoluciones, reembolsos y cancelaciones

Establece una política clara y concisa para las devoluciones, reembolsos y cancelaciones de tus clientes.

- Coloca esta política a disposición de los clientes a través de un enlace en tu página de inicio. En caso de que no aceptes devoluciones, de igual manera, debes incluirlo dentro de tus políticas.
- Coloca una opción para aceptación vía clic de puntos importantes de la política. Por ejemplo, al comprar boletos para un evento deportivo, los clientes deberían hacer clic en un botón:
    - "**Aceptar**" o "**Acepto**", para reconocer que entiendes que los boletos no son reembolsables a menos que el evento sea pospuesto o cancelado

Punto clave: Tu política de devoluciones, reembolsos y cancelaciones debe ser consistente con los objetivos de tu negocio y los productos que provees. Para mejores resultados, trata de lograr un balance entre un buen servicio al cliente y un buen manejo de riesgo.

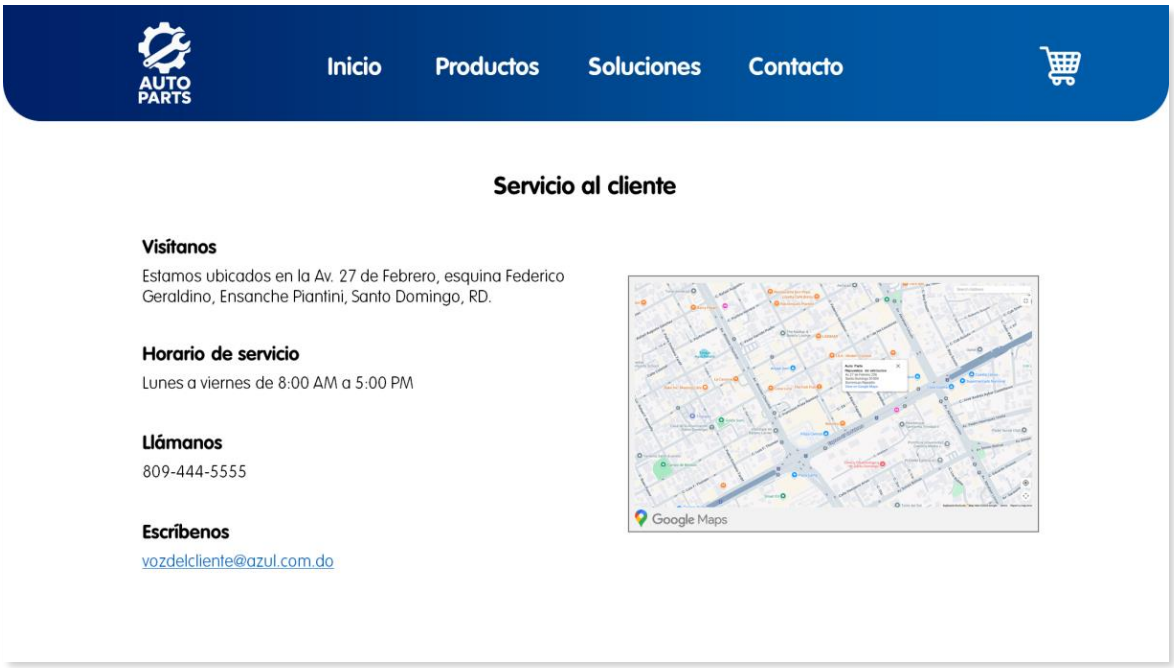


Información para contacto de servicio al cliente

Incluye de forma visible en tu página web o app el correo electrónico y número telefónico en el que los clientes podrán recibir asistencia de parte de tu comercio concerniente a su compra en línea. Al ofrecer un canal de fácil contacto y pronta respuesta para tus clientes, podrás reducir el riesgo de reclamaciones que pudieran convertirse en contracargos.

Para colocar las vías de contacto, puedes crear una opción de fácil acceso "**Contáctanos**" en un lugar visible de tu página web o app.

Para facilitar el procesamiento interno de las solicitudes de los clientes, provee distintos correos electrónicos según el tipo de solicitud: información de productos y servicios, servicio al cliente, información sobre órdenes, etc.



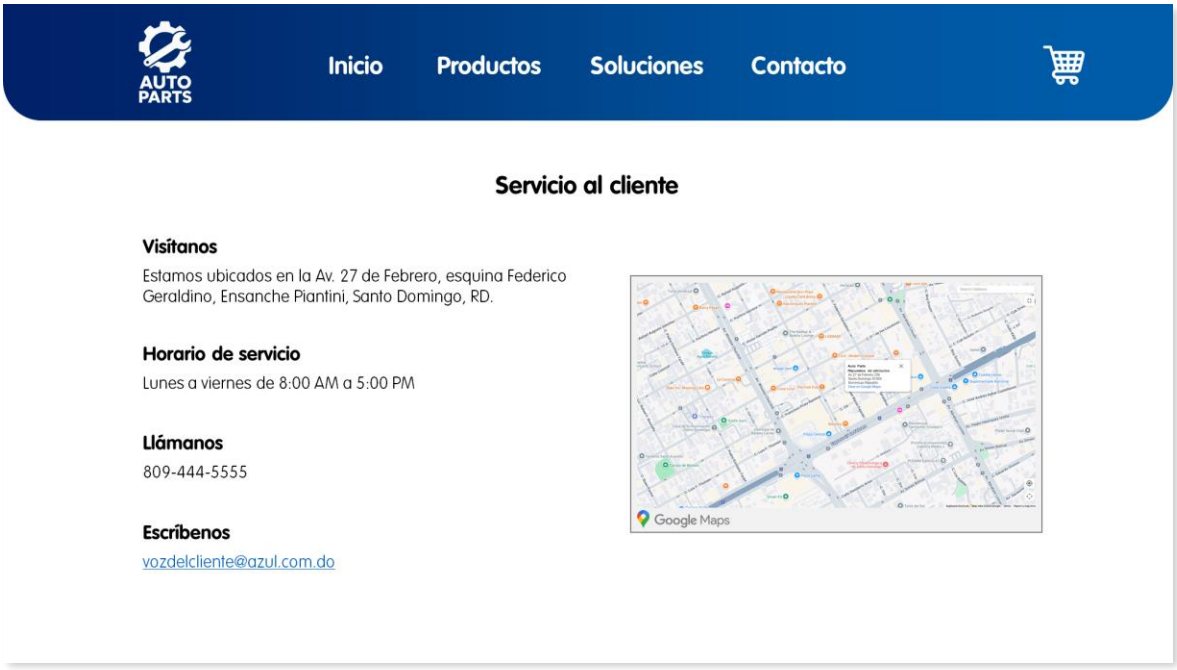
Política clara de entrega

- Establece una política de envió clara y completa. Colócala a disposición de los clientes a través de un enlace en tu página de inicio y en el momento de la compra en línea.
    - Explica las opciones de envío y el tiempo estimado de entrega.
    - Coloca de forma clara y completa los gastos de envío y manejo de mercancía.
- Crea una notificación por correo electrónico para informar a los clientes de cualquier retraso en la entrega de los productos o servicios.



Dirección permanente del negocio

Incluye en un lugar visible de tu sitio web o app la dirección permanente del comercio, incluyendo el país.



Moneda de compra

La moneda debe estar claramente indicada en la página del sitio web o app y en la descripción de los productos y servicios, especialmente si la unidad de moneda no es única (por ejemplo, un peso podría ser peso dominicano, peso mexicano o peso argentino).



Política de privacidad

- Establece una política de privacidad clara y completa. Colócala a disposición de los clientes a través de un enlace en tu página de inicio para que tus clientes sientan confianza al suministrar sus datos personales en tu página web. Tu política de privacidad debe definir:
  - Qué datos del cliente se recolectan y se almacenan,
  - Con quién esta información será compartida, y
  - Cómo los clientes pueden eliminar su registro
- Regístrate de una organización de privacidad y publica un "sello de aprobación" en tu sitio web.



Políticas de seguridad para la transmisión de datos de tarjetas

- Crea una sección que oriente a los clientes sobre las prácticas y controles de seguridad de la información de tu sitio.
- Explica cómo la información de pago de la tarjeta es protegida:
  - Durante la transmisión
  - Mientras está en tu servicio, y
  - En tu lugar físico de trabajo
- Coloca esta sección a disposición de los clientes a través de un enlace en tu página de inicio.
- Crea una sección de Preguntas Frecuentes que incluya preguntas y respuestas de cómo los clientes pueden protegerse al realizar compras en línea.
- Desmotiva el uso del correo electrónico para envío del número de tarjeta para el pago de órdenes. Para proteger a tus clientes y fomentar su lealtad, destaca las prácticas de seguridad en tu sitio web y en cualquier correo electrónico de respuesta. Enfatiza que el correo electrónico no es un método de comunicación seguro y nunca debe utilizarse para envío de números de tarjetas ni otras informaciones sensibles.
- La capacidad de cifrado de transacciones de tu sitio web ofrece una protección fiable contra el acceso no autorizado y proporciona a los tarjetahabientes la forma más segura de efectuar compras a través de internet.
- Crea una sección en la que orientes a los clientes sobre el funcionamiento de los programas "Verified by Visa" y "Mastercard ID Check" (aplica para los clientes afiliados al servicio de autenticación del tarjetahabiente).
- Incluye los logos de los programas correspondientes.
- Incluye un párrafo con la descripción y funcionamiento de los programas. Recomendación:
  - **Descripción**: "Verified by Visa" y "Mastercard ID Check" son programas de las marcas Visa y Mastercard respectivamente, que proporcionan un método de autenticación del

tarjetahabiente para asegurar que la compra la está efectuando el propietario de la tarjeta.

- **Funcionamiento**: Cuando un tarjetahabiente procesa su pago, si su tarjeta está enrolada al programa, será dirigido a la página de Visa o Mastercard (según corresponda), en la que deberá autenticarse según el método definido por su banco emisor. Una vez el cliente es autenticado, se completa la transacción de forma habitual.



Check Out en un checkbox para aceptar los términos y condiciones del sitio web

Despliega en el Check Out un checkbox donde el cliente indique que acepte los términos y condiciones de tu sitio web. Crea una sección donde el cliente pueda indicar:

- Estoy de acuerdo con los Términos y Condiciones. *
- Acepto los Términos y Condiciones de nombredetiendaecomm. *
- He leído y estoy de acuerdo con los términos y condiciones de esta página. *
- Otra opción sin utilizar un checkbox o slider, es antes de continuar al dar clic al botón de completar o finalizar compra/pedido aceptar las políticas.



Recibo claro y completo

Envía una confirmación de la orden del cliente a su correo electrónico que incluya las siguientes informaciones:

- Nombre y dirección del comercio
- Fecha de transacción
- Descripción de bienes o servicios comprados, incluyendo precio
- Detalle de descuentos aplicados
- Detalle de impuestos aplicados
- Detalle del costo de envío
- Monto total de la transacción
- Método de pago utilizado



Auto Parts

Av. 27 de Febrero #256
Ensanche Piantini, Santo Domingo, RD.
Fecha de la orden: 27 de octubre 2025
www.autoparts.com.do

 # Orden: 45698152

Dirección de envío:
Juan Pérez
Calle César Canó #209
Apto. 504, Santo Domingo,
República Dominicana

Envío:
Gran Santo Domingo

Artículos ordenados

1 **Bujía para motor** Caja de 4 unidades RD$ 2,150.00

Subtotal artículo(s):	RD$ 2,150.00
Envío y manejo de mercancía:	RD$ 0.00
Descuentos:	RD$ 500.00
Total del envío:	**RD$ 1,650.00**

Información de pago Versión imprimible

Método de pago:
Marca de la tarjeta ***0123
Código de aprobación: XXXXXX
Tipo de transacción: Compra

Dirección de la facturación:
Juan Pérez
Calle César Canó #209
Apto. 504, Santo Domingo,
República Dominicana

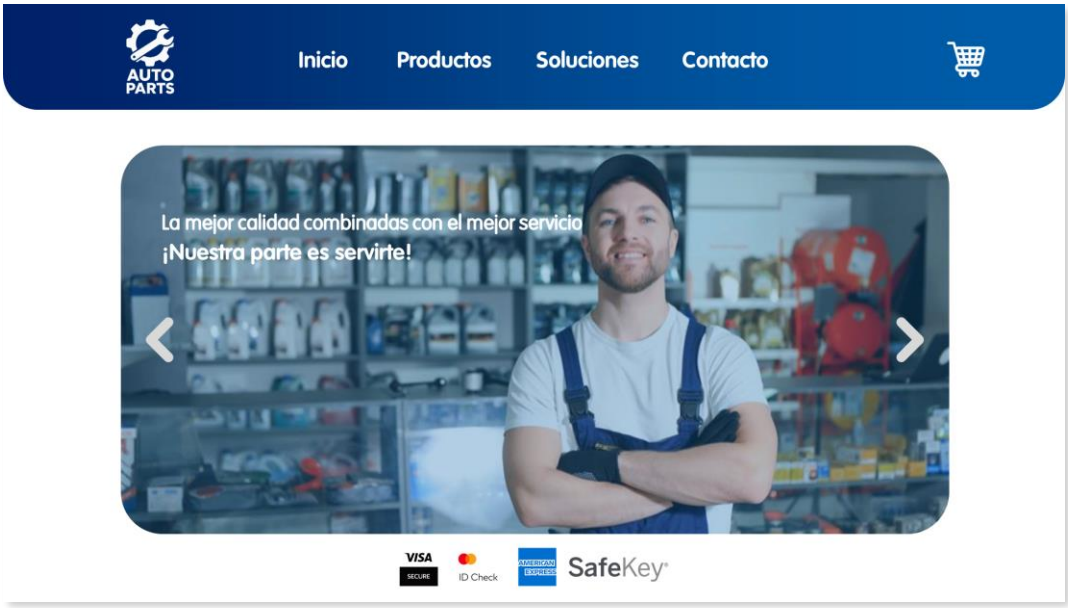
Subtotal artículo(s):	RD$ 2,150.00
Envío y manejo de mercancía:	RD$ 0.00
Descuentos:	RD$ 500.00
Total antes de ITBIS:	RD$ 1,650.00
ITBIS (18%):	RD$ 297.00
Total:	**RD$ 1,947.00**

No se aceptan reembolsos después de 30 días. Consulte nuestras políticas de devolución.
¿Dudas? Contáctenos al 809-444-5555

Agregar logos del servicio de Autenticación del Tarjetahabiente

Para el servicio de Autenticación del Tarjetahabiente es necesario agregar los logos de Verified by Visa y Mastercard ID Check en:

- La página principal,
- La página de las políticas de seguridad para la transmisión de datos de tarjetas, y
- La página de Check Out





Recomendaciones para prevención de ataques de robots

Los ataques de enumeración o fuerza bruta son intentos fraudulentos en el que un delincuente envía sistemáticamente transacciones con valores enumerados, para validar información sensible, como:

- Número de tarjeta (PAN)
- CVV2
- Fecha de expiración

Los estafadores apuntan a **páginas web sin controles robustos**. Para los fines, desarrollan y utilizan bots (ejecución de tareas programadas) que automatizan el envío de múltiples combinaciones de datos de tarjetas en poco tiempo.

Herramientas técnicas

1. Implementar un firewall de aplicaciones web (WAF) para:
   - Detección, prevención y eliminación de botnets.
   - Limitar el envío de formularios y acciones repetidas en los sitios web.
   - Prohibir automáticamente a visitantes y usuarios de orígenes maliciosos conocidos.
   - Determinar de dónde proviene la dirección IP en las transacciones y bloquear direcciones IP maliciosas.

2. Implementar CAPTCHA en los formularios web y asegurarse que:
   - Requiera validación en todas las solicitudes que habiliten el pago con tarjeta.
   - Permitan tomar acciones basadas en análisis, sin necesidad de interrumpir la experiencia de los usuarios. (Eje.: tecnología de Google reCAPTCHA v3).

3. Implementar otros Sistemas de Detección de Intrusiones de Red (NIDS), paquetes de detección de rootkits, analizadores de red y programas anti-bot especializados.

Creación de cuentas

1. Limitar el número de cuentas que se pueden crear por dirección IP dentro de un límite de tiempo establecido.
2. Limitar el número de tarjetas que se pueden agregar por "Cuenta" y sesión según el comportamiento promedio de tus clientes.
3. Monitorear la frecuencia de cambios en los métodos de pago en las cuentas.
4. Utilizar reCAPTCHA para los registros de usuarios.
5. Terminar las sesiones pendientes de usuarios después de un cierto período de tiempo.

Como medidas adicionales, también es importante que:

1. **Inyectar pausas aleatorias** (limitación de velocidad) al verificar una cuenta, para ralentizar los ataques de fuerza bruta que dependen del tiempo, especialmente para los BIN, con una alta tasa de fraude.
2. Incluir velocidades de sesión HTTP, que **limiten el número de operaciones por sesión** de usuario y configuren la sesión para que expire después de períodos de inactividad.

3. **Bloquear una cuenta** si un usuario introduce incorrectamente el nombre de usuario/contraseña y cualquier dato de autenticación de la cuenta un número "x" de intentos de inicio de sesión.
4. **Establecer umbrales** en el número de transacciones dentro de un periodo de tiempo especificado.
5. **Monitorear la velocidad** en varios elementos de datos, como dirección IP, dispositivo y correo electrónico.
6. Incluir direcciones IP u otros elementos con múltiples datos de pagos con tarjeta fallidos en una **base de datos de detección de fraude** para revisión manual.

Detección de comportamientos anormales

1. **Incrementos repentinos** en los promedios diarios de transacciones aprobadas y también las declinadas.
2. **Patrones de solicitudes** repetitivas de autorización en un corto periodo de tiempo.
3. **Inconsistencias entre los datos del dispositivo** versus los datos del navegador con la dirección IP. Por ejemplo, diferencia entre la zona horaria del dispositivo y la zona horaria correspondiente a la dirección IP del navegador.
4. **Uso excesivo** y consumo de ancho de banda de un solo usuario.
5. **Múltiples compras vinculadas al mismo dispositivo:** Por ejemplo, múltiples transacciones con diferentes cuentas de pago (PAN) utilizando la misma dirección de correo electrónico y el mismo ID de dispositivo.
6. Inicios de sesión para una sola cuenta de pago provenientes de distintas direcciones IP.

Seguridad en el almacenamiento y procesamiento de datos

- **Seguridad**: Asegurarse de que el almacenamiento y procesamiento de datos cumplan con los Estándares de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS).
- **Actualizaciones**: Implementar las últimas actualizaciones de parches de seguridad disponibles en tus sistemas.
- **Evaluaciones**: Realizar evaluaciones/auditorías de riesgos y vulnerabilidades periódicamente.