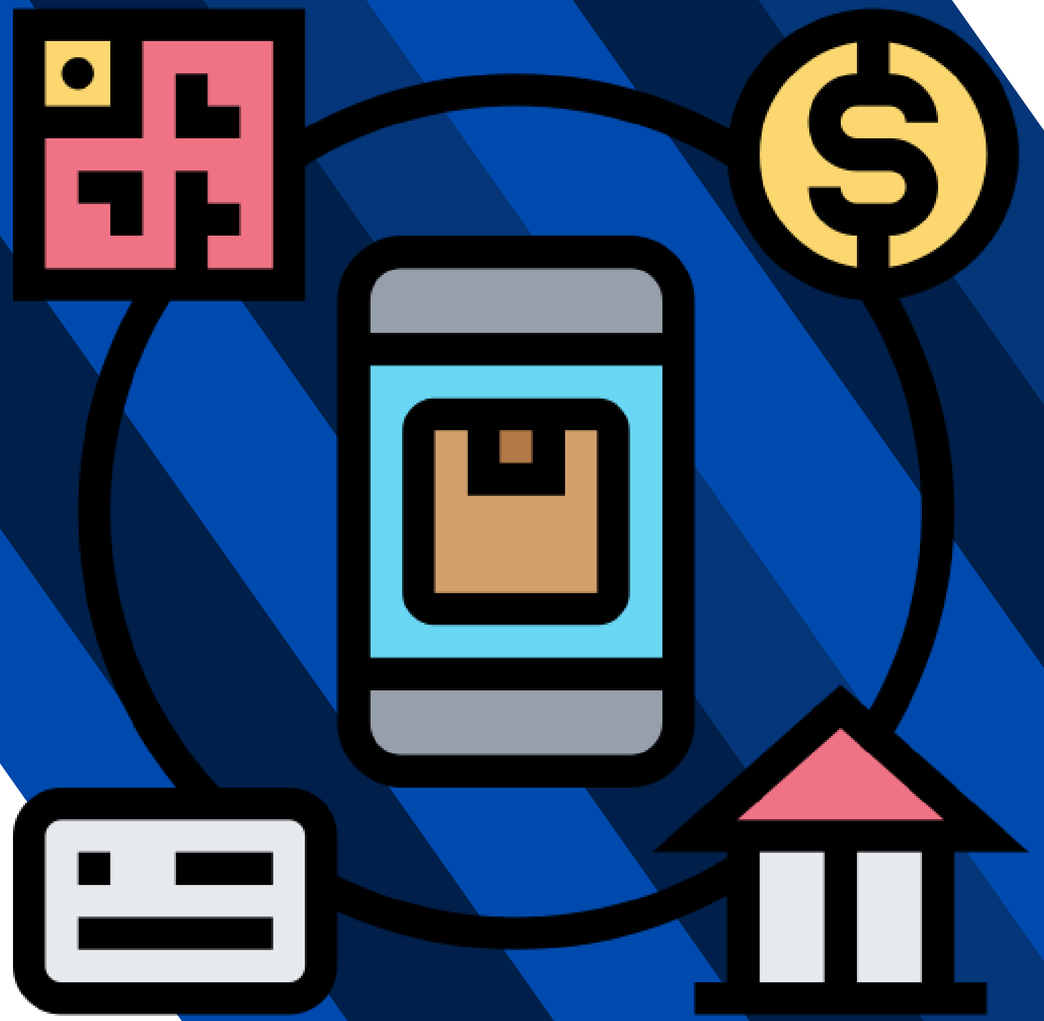
SISTEMAS DE SEGURIDAD PARA LAS PASARELAS DE PAGOS



TRANSPORT LAYER SECURITY (TLS)/ SSL/ OV:

TLS/SSL

TLS (Transport Layer Security) y SSL (Secure Sockets Layer) Son protocolos de seguridad diseñados para garantizar la privacidad y la seguridad de los datos en las comunicaciones por Internet.

TLS cifra las comunicaciones entre aplicaciones web y servidores, asegurando la confiabilidad e integridad de los datos.

OV (Validación de la organización) es un tipo de certificación que verifica la autenticidad de la organización detrás de un sitio web.

EMPRESAS QUE UTILIZAN TSL:

Stripe:

- TLS cifra los datos transmitidos, protegiendo la información confidencial como los detalles de pago.
- Proporciona características como procesamiento de pagos, gestión de suscripciones y prevención de fraudes.

PayPal:

- Emplea TLS para proteger la información confidencial de los usuarios durante las transacciones en línea.
- Ha actualizado su seguridad del protocolo TLS 1.1 al TLS 1.2 para aumentar la protección de los datos.
- Ofrece características como pagos seguros, protección del vendedor y aplicación móvil.

Amazon:

- Utiliza TLS para garantizar la seguridad de las comunicaciones y proteger la privacidad de los datos en su plataforma.
- Cifra los datos transmitidos y asegura la integridad de los mismos.

ENCRIPTACIÓN PARA LAS PASARELAS DE PAGO

HMAC (Hash-based Message Authentication Code):

Se utiliza para verificar la autenticidad e integridad de los mensajes mediante la combinación de una función hash y una clave secreta.

Es un código de autenticación de mensajes basado en hash (MAC) que asegura la integridad y autenticidad del mensaje.

HMAC (Hash-based Message Authentication Code):

- La pasarela de pagos que utiliza el sistema de encriptación HMAC es Redsys.
- Redsys emplea la firma HMAC SHA256 para la conexión por Web Service y la redirección del navegador del titular.
- Este sistema de encriptación garantiza la seguridad y privacidad de los datos de pago durante el proceso de transacción.

Funcionamiento de la encriptación HMAC:

- La encriptación HMAC combina una función hash criptográfica con una clave secreta para generar un valor MAC único que garantiza la integridad y autenticidad del mensaje.
- Las claves HMAC también pueden utilizarse para autenticar solicitudes en la API de XML de Google Cloud Storage y pueden ser generadas y verificadas en AWS KMS.

PCI DSS (ESTÁNDAR DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO)

El cumplimiento con los estándares de PCI DSS es esencial para garantizar la protección de los datos de tarjetas de crédito durante las transacciones.

PCI DSS comprende 12 requisitos clave, divididos en 78 requisitos básicos y 400 procedimientos de prueba.

TOKENIZACIÓN:

- La tokenización es una técnica de seguridad que reemplaza la información confidencial de los clientes con un conjunto de números aleatorios llamados "tokens".

- Promovida por PCI DSS, la tokenización añade una capa adicional de protección a los datos de pago, ya que incluso si se produce una violación, los datos no tienen sentido y no son útiles para los ciberdelincuentes.

- La tokenización ayuda a mitigar los riesgos asociados con el manejo de datos sensibles durante las transacciones, mejorando la seguridad y la confianza del cliente en las pasarelas de pago.

2FA

Implementa métodos efectivos de autenticación de usuario. Esto puede incluir la verificación de contraseña, preguntas de seguridad, o incluso la implementación de autenticación de dos factores (2FA) si la pasarela lo permite.

Autenticación de Dos Factores (2FA):

- La autenticación de dos factores es un método de seguridad que requiere dos formas de identificación para acceder a recursos y datos, proporcionando una capa adicional de protección.

Implementación de 2FA:

- En Go4Mobility, se ofrece una API robusta para implementar la autenticación de dos factores, donde los usuarios reciben un código único por SMS (OTP) después de ingresar sus credenciales de acceso.

DDOS

Mitigación de Ataques DDoS:

- Los ataques de denegación de servicio (DDoS) son ataques cibernéticos que sobrecargan un sitio web, servidor o recurso de red con tráfico malicioso, causando la indisponibilidad del servicio.
- Un ataque de denegación de servicio distribuido (DDoS) utiliza múltiples computadoras o máquinas para inundar un recurso específico con tráfico malicioso, lo que dificulta la mitigación del ataque.

Prácticas de Seguridad:

Es crucial mantener todos los componentes del sistema actualizados, incluyendo software, firmware y sistemas operativos, para remediar vulnerabilidades conocidas y reducir la superficie de ataque.

EMV

El estándar EMV (Europay, Mastercard y Visa) es una tecnología global utilizada en tarjetas de pago que ofrece características avanzadas de seguridad.

Características de EMV:

- **Tarjetas con Chip: Las tarjetas EMV tienen un chip incorporado que almacena y procesa información de manera segura.**
- **Autenticación Dinámica: EMV utiliza métodos de autenticación dinámica que generan códigos únicos para cada transacción, lo que hace más difícil la duplicación de tarjetas.**
- **Transacciones más Seguras: El uso de tarjetas EMV contribuye a transacciones más seguras al reducir el riesgo de fraude relacionado con tarjetas físicas.**

Componentes del Sistema EMV:

- Tarjeta EMV: La tarjeta de crédito o débito que contiene el chip EMV.
- Terminal de Punto de Venta (POS): El dispositivo utilizado por los comerciantes para aceptar pagos con tarjetas.
- Sistema de Procesamiento del Emisor: El sistema utilizado por el banco emisor de la tarjeta para autorizar y procesar transacciones.

Proceso de Transacción EMV:

Autenticación del Chip: El chip EMV interactúa con el terminal POS para autenticar la tarjeta y la transacción.

Código Criptográfico: Se genera un código criptográfico único para cada transacción, lo que dificulta la falsificación de la tarjeta.

Verificación del PIN: En algunos casos, se requiere que el titular de la tarjeta ingrese un PIN para completar la transacción, lo que agrega una capa adicional de seguridad.

CVV

El código de seguridad CVV (Card Verification Value) es una medida de seguridad importante en las tarjetas de crédito y débito.

- Código de Seguridad: El CVV es un código de seguridad de tres dígitos (a veces cuatro en algunas tarjetas) que se encuentra en la parte posterior de la tarjeta de crédito o débito.
- Verificación de Usuario: Se utiliza para verificar que el usuario que realiza la transacción físicamente posee la tarjeta, añadiendo una capa adicional de seguridad en las transacciones.

Función de Seguridad:

El CVV de tipo 2, al ser solicitado en cada transacción en línea, ayuda a reducir el riesgo de fraude en compras por Internet, ya que solo el poseedor físico de la tarjeta debería tener acceso a este código.

TIPOS DE CVV:

ACVV de Tipo 1: Este código está encriptado en la banda magnética de la tarjeta y no es visible a simple vista. Los TPV (Terminal de Punto de Venta) lo leen automáticamente al realizar una transacción en un establecimiento físico.

CVV de Tipo 2: Es un código de tres dígitos (o cuatro en algunas tarjetas) impreso en el reverso de la tarjeta. Se utiliza especialmente en transacciones en línea como una medida de seguridad adicional. Este código no se almacena en la pasarela de pago y se solicita en cada transacción en línea.

PA–DSS (PAYMENT APPLICATION DATA SECURITY STANDARD)

Desarrollado por el PCI SSC, el PA-DSS es un estándar de seguridad destinado a garantizar la seguridad de las aplicaciones de software que procesan datos de tarjetas de crédito.

Su objetivo es proteger la información de tarjetas de crédito y débito y prevenir el acceso no autorizado a estos datos sensibles.

Es esencial para las aplicaciones de pago cumplir con el PA-DSS para garantizar la seguridad en el procesamiento de transacciones con tarjetas.

DV (CERTIFICADOS CON VALIDACIÓN DE DOMINIO)

Los certificados DV se utilizan para autenticar la identidad de un sitio web y asegurar la información transmitida entre el usuario y el servidor.

Proceso de Validación Rápido y Automático: Los propietarios de sitios web pueden obtener un certificado DV en minutos o incluso segundos al demostrar la propiedad o el control del dominio

Costo Generalmente Más Bajo: La accesibilidad hace que los certificados DV sean populares para sitios web más pequeños o con presupuestos limitados.

Indicador Básico de Seguridad en Navegadores: Muestran indicadores básicos como un candado y la conexión "https://" en la barra de direcciones, indicando una conexión segura.

PSE

PSE, Pagos Seguros en Línea, es un sistema de pago electrónico operativo en Colombia que permite a las empresas ofrecer a sus clientes la opción de realizar pagos y compras por Internet

Propiedad y Operación: El sistema PSE es propiedad de ACH Colombia, una empresa fundada en 1997 por cinco redes de cajeros automáticos del país. Actualmente, ACH Colombia pertenece a quince bancos.