¿Qué es PCI DSS? y los principales retos al cumplimiento

B I E N V E N I D O S

Ivonne Bazán

- Ingeniera en Informática con más de 8 años de experiencia en proyectos de TI y gestión de equipos de alto desempeño.

- Especialista en los medios de pago como lo es tarjeta presente, e-commerce, CODI, así como también en las regulaciones que emite el banco de México y la CNBV para la figura Agregador.

Certificaciones:

- Certificación en scrum master
- Certificación en Product Owner
- Certificación en management 3.0

- Actualmente se desempeña como Gerente de especialidad de Productos Financieros y CoDi.

Erik Alba

- Ingeniero en Computación con estudios de posgrado en Seguridad de la Información y especialista en Medios de Pago con mas de 15 de años de experiencia.
- Actualmente se desempeña como Oficial de Cumplimiento dentro de la especialidad de Productos Financieros, así como responsable de la integración de diferentes canales de pago.

Los datos de las tarjetas de pago son un objetivo muy deseable para los delincuentes...

PRAXIS

Mayores robos de tarjetas

2005
40 millones
de tarjetas perdidas

Procesador de tarjetas de pago

- Acceden a base de datos con conectividad directa a Internet.
- Empresa ya no está en el negocio.

2007
45,7 millones
de tarjetas perdidas

Importante minorista Retail

- Malware no detectado por 18 meses.
- Informes sugieren costos directos del orden de 256 millones de dólares.

2009
160 millones
de tarjetas perdidas

Procesador de pagos

- Malware se utilizó para capturar datos de los tarjetahabientes, ya procesados.
- Informes sugieren costos directos cercanos 171 millones de dólares.

2013
1,8 millones
de tarjetas perdidas

Minorista de alimentos

- Malware instalado en POS robo datos cuando estos eran capturados.
- Costos estimados podrían superar los 80 millones de dólares.

PRAXIS

Los métodos más utilizados explotan debilidades de seguridad presentes en el medio ambiente

PRAXIS

Métodos más usados para el robo de datos de tarjetas

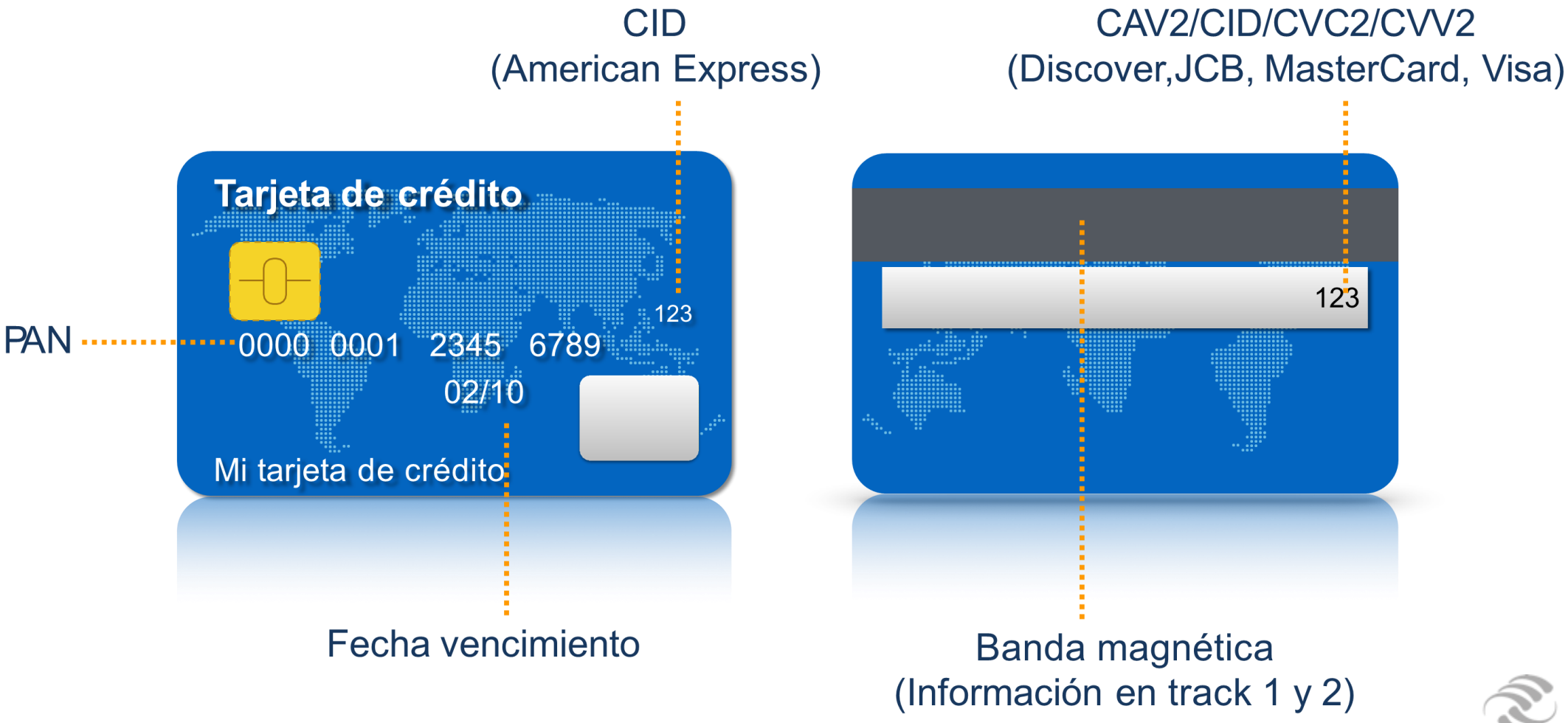
Payment Card Industry Data Security Standard (PCI DSS)

PRAXIS

La Norma de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrolló para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar las medidas de seguridad consistentes a nivel mundial

PRAXIS

Tipos de Datos de Tarjetas de Pago



PRAXIS

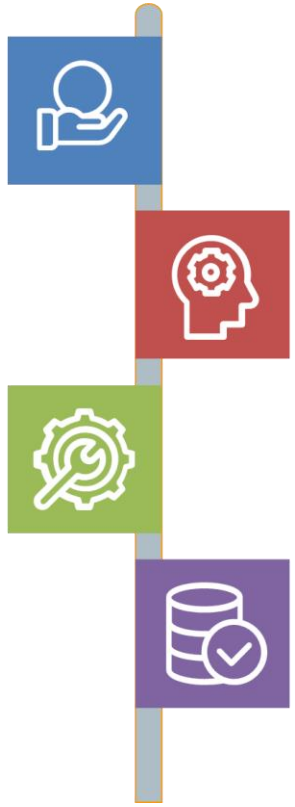
Empresas Fundadoras

PRAXIS

Payment Card Industry Data Security Standard (PCI DSS)

Ofrece una línea de base de requisitos técnicos y operativos diseñados para proteger los datos de titulares de tarjetas.

Se aplica a todas las entidades involucradas en el procesamiento de tarjetas de pago - incluyendo comerciantes, procesadores, adquirentes, emisores y proveedores de servicios.



Comprende conjunto mínimo de requisitos para la protección de datos de tarjeta, puede ser reforzada por controles y prácticas para mitigar aún más riesgos adicionales.

Se aplica donde se almacenan los datos de cuenta, procesan o transmiten.

PRAXIS

Estándares de la Industria PCI

Ecosistema de dispositivos de pago, aplicaciones, infraestructura y usuarios

PRAXIS

A quienes aplica…

Entidades que ofrecen servicios a dichos entornos que pueden verse afectadas por el cumplimiento de PCI DSS si sus servicios se encuentran involucrados dentro del entorno de cumplimiento de PCI DSS de alguno de sus clientes. Algunos ejemplos son:

PROVEEDORES		SERVICIOS	
Servicios gestionados (Managed Service Providers- MSP)	Servicios de centro de datos (data centers y colocation/hosting)	Alojamiento Web (Web hosting)	Seguridad física
Infraestructura tecnológica	Proveedores de Desarrollo de Software	Externalización de personal (outsorcing)	Servicios de destrucción segura de documentación y/o medios del almacenamiento electrónicos
Servicios en la nube (cloud)			

En estos casos, estas entidades optan por someterse a evaluaciones a solicitud de sus clientes y/o participar en cada una de las revisiones de la PCI DSS de sus clientes o realizar una o varias evaluaciones anuales de PCI DSS por cuenta propia y proporcionar evidencia a sus clientes a fin de demostrar el cumplimiento

PRAXIS

Datos de la cuenta

	Elementos de datos	Almacenamiento permitido	Hace que los datos de la cuenta almacenados no se puedan leer según requisito 3.4
Datos del titular de la tarjeta	Número de cuenta principal (PAN)	✓	✓
	Nombre del titular de tarjeta	✓	✗
	Código de servicio	✓	✗
	Fecha de vencimiento	✓	✗
Datos confidenciales de autenticación	Datos completos de la banda magnética	✗	No se pueden almacenar (req3.2)
	CAV2/CVC2/CVV2/CID	✗	No se pueden almacenar (req3.2)
	PIN/Bloqueo de PIN	✗	No se pueden almacenar (req3.2)

Los requisitos 3.3 y 3.4 sólo se aplican al PAN. Si el PAN se almacena con otros elementos de los datos del titular de la tarjeta, únicamente el PAN debe ser ilegible (Req3.4).

PRAXIS

Almacenamiento de tracks NO está permitido

No está permitido almacenar Tracks u otros datos sensibles después de la autorización.

PRAXIS

Almacenamiento de tracks ~~NO~~ está permitido

A excepción de emisores y procesadores están autorizados a conservar datos sensibles, si son necesarios para efectos de correcciones

PRAXIS

6 Objetivos

12 Requerimientos

PRAXIS

Tabla de requisitos PCI DSS

Desarrollar y mantener redes y sistemas seguros	Proteger los datos del titular de la tarjeta	Mantener un programa de administración de vulnerabilidad	Implementar medidas sólidas de control de acceso	Supervisar y evaluar las redes con regularidad	Mantener una política de seguridad de información
1. Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta. 2. No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.	3. Proteja los datos del titular de la tarjeta que fueron almacenados 4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.	5. Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente 6. Desarrollar y mantener sistemas y aplicaciones seguros	7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. 8. Identificar y autenticar el acceso a los componentes del sistema. 9. Restringir el acceso físico a los datos del titular de la tarjeta.	10. Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta 11. Probar periódicamente los sistemas y procesos de seguridad.	12. Mantener una política que aborde la seguridad de la información para todo el personal

PRAXIS

Principales retos al cumplimiento

“La forma más segura de reducir el alcance de PCI DSS es NO almacenar los datos de los tarjetahabientes”

PRAXIS

Principales retos al cumplimiento

PRAXIS

Formato PCI DSS v3.2.1

Requerimiento PCI DSS: Define los requisitos de la norma de seguridad de datos; El cumplimiento de PCI DSS se valida con estos requisitos.

Procedimiento de prueba: Muestra los procesos a seguir por el evaluador para validar que se han cumplido los requisitos de PCI DSS y están "en su lugar".

Guía: Describe la intención o la seguridad objetiva detrás de cada uno de los requisitos de PCI DSS. Esta columna contiene orientativo, y está destinado a facilitar la comprensión del propósito de cada requisito. la guía en esta columna no pretende sustituir o ampliar los requisitos de PCI DSS y procedimientos de prueba.

Requerimiento PCI DSS	Procedimiento de prueba	Guía
1.1 Establezca e implemente normas de configuración para para firewalls y routers que incluyan lo siguiente:	1.1Inspeccione las normas de configuración de firewalls y routers routers y otros documentos especificados a continuación para verificar el cumplimiento e implementación de las normas.	Los firewalls y los routers son componentes clave de la arquitectura que controla la entrada a y la salida de la red. stos dispositivos son unidades de software o hardware que bloquean

PRAXIS

Reporte de Cumplimiento

El cumplimiento con PCI DSS se puede demostrar mediante dos formas:

1.- Empleando un cuestionario de autoevaluación (o Self-assessment Questionnaire – SAQ)

2.- Realizando una evaluación formal de cumplimiento

El criterio para identificar cuál de los dos métodos se debe emplear por lo general se basa en la cantidad de transacciones mensuales con tarjetas de pago realizadas por la entidad. A continuación se analizan las diferencias entre el SAQ y la evaluación formal de cumplimiento:

Reporte de cumplimiento de PCI DSS	Cuestionario de autoevaluación *Self-Assessment Questionnaire* (SAQ)	Evaluación formal de cumplimiento
¿Quién debe usarlo?	Comercios y proveedores de servicio con base en las categorizaciones de cada marca y en función de la cantidad de transacciones anuales procesadas (nivel 2, nivel 3 y nivel 4)	Comercios, proveedores de servicio, adquirientes, emisores y otras entidades financieras catalogadas como nivel 1 por cada programa de las marcas.
Tipos de plantillas	Existen 9 tipos de plantilla de SAQ dependiendo del canal de pago empleado: *SAQ A, SAQ A-EP, SAQ B, SAQ B-IP, SAQ C, SAQ C-VT, SAQ P2PE, SAQ D para comerciantes y SAQ D para proveedores de servicios*	Se debe emplear la plantilla del documento de Reporte de Cumplimiento (*Report on Compliance* – RoC) por parte del asesor QSA
Documentación a presentar	• Cuestionario de autoevaluación (SAQ) aplicable • Declaración de Cumplimiento (*Attestation on Compliance* - AoC)	• Reporte de Cumplimiento (*Report on Compliance* – RoC) • Declaración de Cumplimiento (*Attestation on Compliance* - AoC)
¿Requiere de un Asesor Cualificado de PCI DSS (*Qualified Security Assessor - QSA*)?	No es obligatorio. No obstante, tanto las marcas de pago como los adquirientes pueden exigirlo de forma discrecional.	Si. Las evaluaciones formales de cumplimiento de PCI DSS deben ser ejecutadas obligatoriamente por un QSA.
¿Requiere de escaneos de vulnerabilidades ejecutados por un Proveedor Aprobado de Escaneo (*Approved Scanning Vendor* - ASV)	Depende del tipo de SAQ empleado. No obstante, tanto las marcas de pago como los adquirientes pueden exigirlo de forma discrecional.	Si
Periodo de validez del reporte	Anual	Anual

PRAXIS

Que ocurre si No se cumple con PCI DSS…?

El cumplimiento del estándar PCI DSS es obligatorio, aunque la aplicabilidad de sus requerimientos y los tipos de evaluación o reporte de cumplimiento varíen en función del tipo de entidad.

Este estándar establece las bases mínimas en términos de seguridad para proteger las transacciones con datos de tarjetas de pago, por lo que su incumplimiento implica:

Limitación por parte de las marcas de tarjetas de pago, bancos adquirientes o pasarelas de pago para procesar transacciones provenientes desde la entidad que no cumple con el estándar.

En el caso de la ocurrencia de un **incidente de seguridad** que afecte datos de tarjetas, la entidad que no cumple con el estándar debe asumir la totalidad de los Costos derivados, incluyendo:

PRAXIS

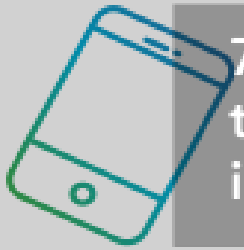
Que ocurre si No se cumple con PCI DSS…?

Costos de demandas e indemnizaciones a los afectados	Costos de los fraudes con transacciones realizadas con las tarjetas afectadas	Multas por parte de las marcas de pago, en función de la cantidad de datos de tarjetas de pago involucrados	Multas legales por afectación de datos de carácter –personal (en casos específicos como GDPR/RGPD)
Costos de renovación de las tarjetas de pago afectadas	Costos de la implementación de los controles de PCI DSS post-incidente	Costos derivados de la pérdida de imagen de cara al público	Costos de la investigación forense, a cargo de un profesional PCI Forensic Investigator (PFI)

PRAXIS


TUCOIN
Tu cobro inteligente

Antecedentes:

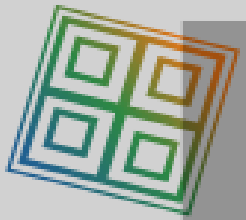


75% de los mexicanos tienen un teléfono inteligente.

47% de los adultos en México, tienen una cuenta en un banco o institución financiera.

54 millones más de personas con acceso financiero en México.

En los últimos años, se ha incrementado la población con más de un producto financiero , aumentando a 2.6 millones.



Está estipulado que para 2022, 37 millones de mexicanos utilicen CoDi.

¿Qué es CoDi?

- Nueva plataforma de cobro digital, que opera a partir del 29 de Septiembre 2019.
- Iniciativa impulsada por Banco de México, junto con el Sistema Financiero Mexicano.
- Utiliza las tecnologías de códigos QR y NFC.
- Uso del **Sistema de Pagos Electrónicos Interbancarios (SPEI).**
- Facilita que tanto comercios como usuarios, puedan realizar transacciones sin dinero en efectivo.

¿Por qué sumarme al **nuevo sistema de pagos CoDi?**

1. **No necesitas de una tarjeta o efectivo.** Solamente se requiere el uso de un dispositivo móvil y contar con acceso a internet.

2. **Fácil de usar,** únicamente debes generar un código QR y ¡listo!

3. **Elimina comisiones** por pagos con tarjeta, o a proveedores de medios de pago.

4. **Transacciones efectuadas en segundos,** con disponibilidad 24X7.

5. **Obtienes tu dinero de forma inmediata,** sin importar día y hora.

6. **¡Completamente seguro!** Sin riesgo por clonaciones de tarjeta o uso de billetes falsos.

7. **No se requiere certificación PCI.**

Componentes de **CoDi**

SPEI (Sistema de pago electrónico interbancario) operado por el Banco de México (Banxico), que permite enviar y recibir dinero a través de cuentas bancarias a través de Internet.

Servidor de Banco de México, Servicios de Cobro Digital desarrollados y operados por Banxico, que permiten enviar notificaciones a los participantes, sobre el resultado de los mensajes de Cobro.

Mensaje de cobro

Una cadena cifrada (QR o NFC) presentada a un comprador por un vendedor, que solicita una orden de pago.

Banco Emisor

Un participante habilitado para **realizar transferencias** de dinero a través de SPEI., Banco de donde s cargan los recursos

Componentes de **CoDi**

Banco Beneficiario

Un participante, habilitado para **recibir transferencias** de dinero a través de **SPEI**, Banco de donde se abonan los recursos.

App del comprador

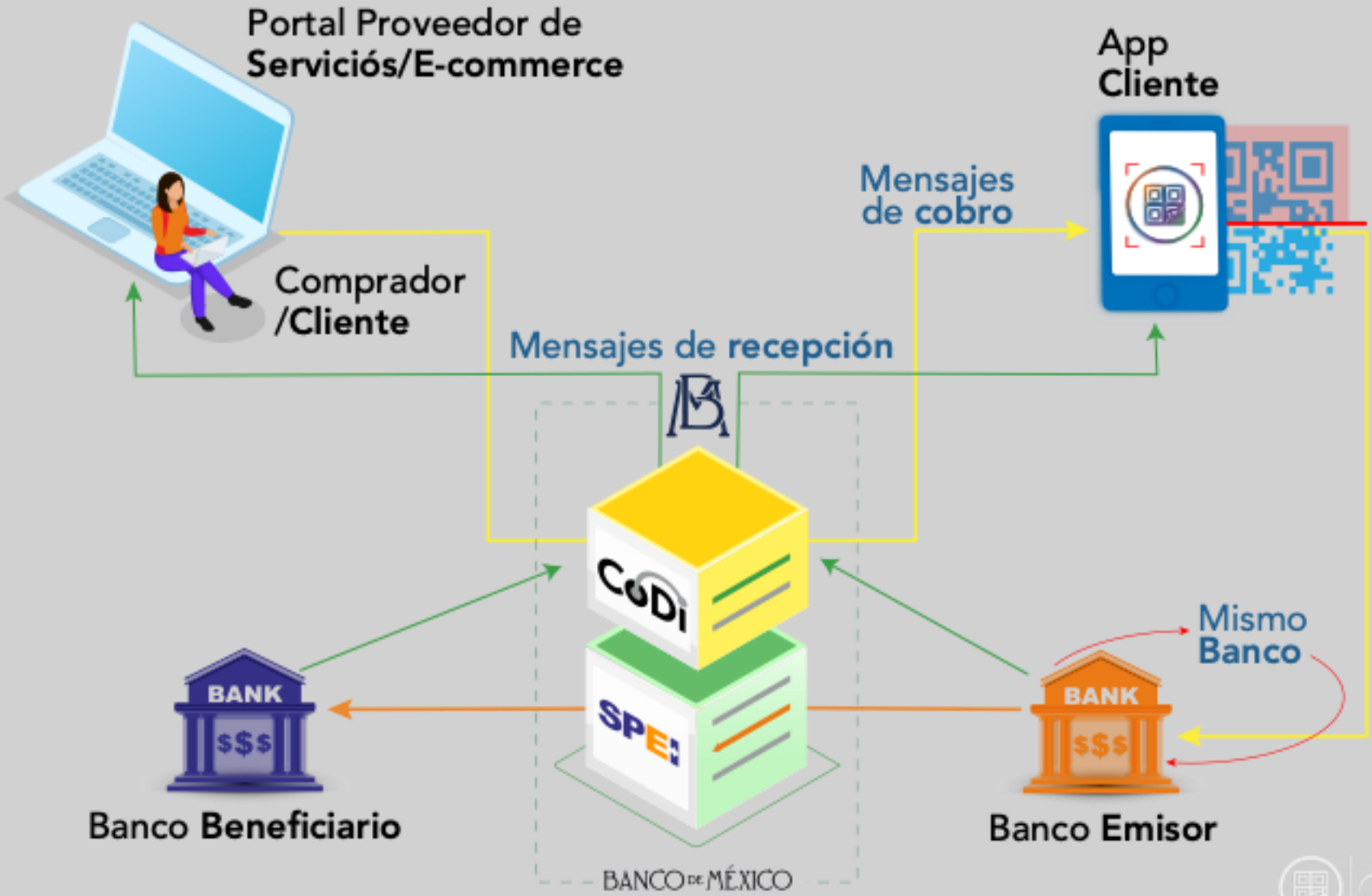
La aplicación, que el comprador usa para leer el mensaje de cobro para ejecutar una transferencia como pago a un vendedor.

App del vendedor o portal Web proveedor de servicios

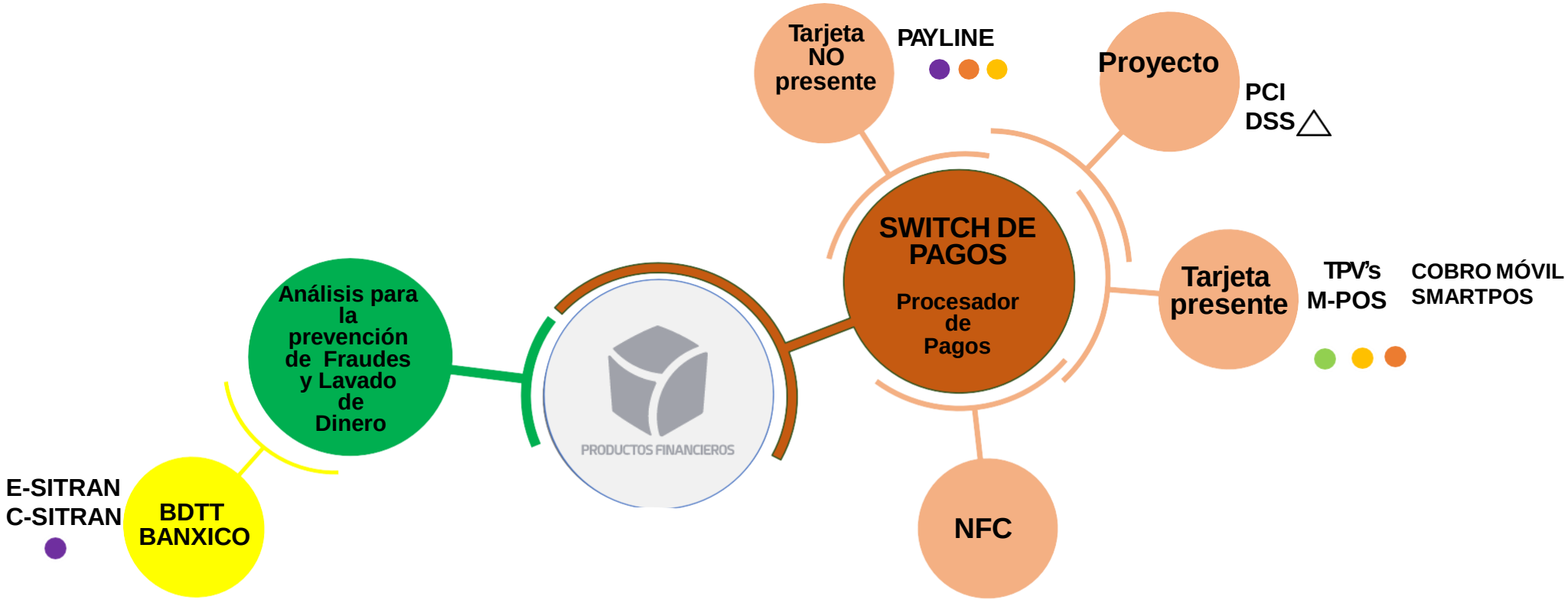
La aplicación que el vendedor utiliza para generar el **mensaje de cobro**, para solicitar un pago a un comprador o Potal Web proveedor de servicios con funcionalidad de generar el **mensaje de cobro** para solicitar un pago a un comprador.

Funcionamiento **cobro presencial CoDi**

Funcionamiento **cobro no presencial CoDi**



Productos y Servicios



Modalidades
Simbología

- Capacitación y procesos
- Esquema de venta transaccional (cobro)
- Esquema de venta SaaS
- Esquema de venta AMS
- Esquema de venta Producto (licencia + mtto y spte)
- Esquema de venta de equipo (venta/renta)

PRAXIS

¿PREGUNTAS?

CONTACTO

Ivonne E. Bazán Estrada
Productos Financieros
Gerente de Especialidad
correo: baei@praxis.com.mx

Erik Alba
Oficial de Cumplimiento
Correo: alme@praxis.com.mx